UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escuela Técnica Superior de Ingeniería Informática

Universitat Politècnica de València

Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad.

Proyecto Final de Carrera

Ingeniería Técnica en Informática de Sistemas

Autor: Julián Ignacio Alfonso Beltrán

Director: Juan Vicente Oltra Gutiérrez

Septiembre de 2015

Resumen

Estudio y recopilación de casos y análisis de técnicas empleados por los estados en la lucha contra otros estados o particulares, o viceversa. Ataques DDOS, phishing, etc., al servicio de causas políticas o en conflictos bélicos o prebélicos. Del terrorismo al espionaje.

Palabras clave: ciberactivismo, ciberdefensa, ciberespionaje, ciberguerra, ciberseguridad, ciberterrorismo, cibervigilancia, ENS, Esquema Nacional de Seguridad.

Tabla de contenidos

1. Objeto y objetivos.

El objeto del presente Proyecto de Fin de Carrera es la obtención del título de Ingeniería Técnica en Informática de Sistemas expedido por la Universidad Politécnica de Valencia.

El objetivo es recopilar casos de ataques y analizar las técnicas empleadas por los estados en la lucha contra otros estados o particulares (guerra electrónica y ciberguerra, y ciberespionaje), y viceversa (hacktivismo y ciberterrorismo), utilizando las comunicaciones de Internet.

Se mostrará cómo, en los últimos años, son ya muchos los estados que han construido una estrategia que centra sus actividades de inteligencia y militares en el dominio del ciberespacio, tanto en lo que atañe a la obtención de información, como al apoyo a misiones de ataque convencionales, inhabilitando los sistemas de información y defensa, perturbando las redes de mando del oponente, o infiltrando y afectando alguno de sus recursos o servicios críticos, y que han supuesto una considerable ventaja en algunos de los últimos conflictos.

Estas tecnologías han emergido, en parte, a partir de las técnicas utilizadas por hackers, cibercriminales y ciberactivistas, pero en otros casos son resultado de un conocimiento profundo de las redes y sus usuarios, las tecnologías usadas en la construcción de estas redes, y los sistemas empleados en el tratamiento de la información.

Como consecuencia de estas capacidades y de las vulnerabilidades que se han ido evidenciando en los sistemas de información, y conforme ha ido creciendo en los gobiernos la concienciación sobre los efectos de los ciberataques, se han elaborado estrategias de defensa para hacer frente a intrusiones inhabilitantes o incluso potencialmente devastadoras, o ante cualquier tipo de vulnerabilidad de los sistemas de mando y control, no sólo de las redes militares de defensa, inteligencia o logística de las que se han dotado los estados, sino también de las redes de infraestructuras críticas: energía, servicios básicos, banca, etc., de las cuales los estados son absolutamente dependientes.

En este contexto se analizarán las estrategias de ciberseguridad que han implementado los estados. En particular y en el caso de España, se analizará el Esquema Nacional de Seguridad, como marco legal de la estrategia, las metodologías empleadas, así como el conjunto de medidas previstas para afrontar las vulnerabilidades de los sistemas informáticos de las administraciones públicas y su información, y el conjunto de herramientas que se han ido implementando para determinar los riesgos y vulnerabilidades, favorecer la comunicación y

concienciación, implantar el propio Esquema Nacional de Seguridad, gestionar los incidentes de seguridad, detectar APTs y código dañino, y finalmente ofrecer una estrategia de ciberresiliencia efectiva.

En el caso de España la exposición a internet de las AA.PP. es especialmente intensa dado que una de las prioridades políticas desde hace varias legislaturas ha sido el desarrollo de la sociedad de la información y de la administración electrónica, lo que lo convierte en uno de los estados más vulnerables.

Para la recopilación de casos se ha consultado mucha información esencialmente de Internet, en su mayoría de prensa nacional e internacional, y blogs especializados, pero la información obtenida es redundante y carente de profundidad, por lo que también se ha recurrido a bibliografía. En todos los casos se ha tratado de buscar las fuentes originales, y se han referenciado directamente siempre que han estado disponibles. Los documentos de Wikileaks resultaron bastante decepcionantes para el objetivo del proyecto, aunque las informaciones consultadas en los Spy Files permitieron comprobar que algunas de las capacidades atribuidas a PRISM eran ofrecidas comercialmente por algunos de los contratistas de defensa de EE.UU. Se ha consultado mucha información también de las webs oficiales de empresas del sector de la seguridad informática. En particular las webs de Kaspersky, Symantec, McAffee y TrendMicro han sido muy útiles en el apartado dedicado al cibercrimen. En este apartado se reseña también que se ha aportado información de un caso real de spear phishing a usuarios de la Administración General del Estado. Se ha consultado también mucha documentación disponible en las webs oficiales de organismos españoles e internacionales, que ha sido muy útil para concretar las estrategias de ciberdefensa adoptadas por los estados. En particular han sido de gran utilidad la web del Parlamento Europeo, y la web del CERT del Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (CNI), en la que se han consultado las guías STIC, y a través de la que se ha accedido a las herramientas que se ofrecen para la implantación del Esquema Nacional de Seguridad. Se han consultado también los manuales de los cursos referentes a la metodología MAGERIT y a la herramienta PILAR ofrecidos por el Instituto Nacional de Administración Pública (INAP). Por último, se han consultado varios proyectos de fin de carrera relacionados con el tema, en particular han resultado de gran utilidad en el apartado dedicado al hacking y las herramientas de intrusión y ataque empleadas.

"Si obtienes la ventaja del terreno, puedes vencer a los adversarios."

Sun Tzu. El Arte de la Guerra[1].

2. Ciberamenazas.

2.1. Espionaje, espionaje electrónico y ciberespionaje.

Las actividades llevadas a cabo para la obtención de información que aporte una ventaja potencial en una confrontación, pero también para verificar las intenciones reales de un oponente y evitar un conflicto declarado, son tan antiguas como la humanidad, y forman parte de los cometidos de los servicios exteriores de los estados. En un porcentaje elevado esa información fundamental para la toma de decisiones se nutre de fuentes de acceso público, pero en otros casos se trata de información confidencial y mantenida en secreto por los gobiernos. Puede afectar a información de carácter militar, decisiones en política exterior, política monetaria, informaciones económicas, industriales, nuevas tecnologías, negocios o inversiones en el exterior, información sobre tensiones internas, etc.

Los estados han buscado siempre la manera de acceder a informaciones de carácter secreto, interviniendo las comunicaciones realizadas a través de mensajeros y, más modernamente, los sistemas basados en tecnologías de la información y las comunicaciones. Del mismo modo, y conscientes de esa actividad, y las ventajas que puede aportar conocer las intenciones, estrategias, y organización internas, los estados han tratado también de proteger esas comunicaciones, securizándolas ante una intrusión o encriptándolas de modo que sean ilegibles e inútiles en caso de que resulten interceptadas.

El espionaje no es más que el robo organizado de información.

Al margen del empleo de personas infiltradas o captadas como agentes, desde la aparición de las telecomunicaciones, se ha desarrollado una carrera en paralelo, por un lado de procedimientos y tecnologías accesorias para proteger medios y tecnologías de comunicación, y por otro lado para romper esas protecciones y acceder a la información.

[1] Sun Tzu. "El Arte de la Guerra (Versión de Thomas Cleary)". Ed. EDAF. 31ª edición, enero 2007.

Si la mayoría de estados interceptan las comunicaciones militares y diplomáticas de otros estados, no hacen menos con las comunicaciones interiores entre sus propios ciudadanos, con objeto de detectar actividad subversiva y terrorista que pueda suponer un riesgo para la seguridad de los ciudadanos o de los recursos del estado. Estas capacidades, como veremos, han servido para localizar y detener grupos peligrosos con capacidad y determinación para llevar a cabo atentados y actividades delictivas, pero en otros casos han servido para afianzar un control totalitario sobre la sociedad, persiguiendo de forma sistemática cualquier actividad disidente o anulando las posibilidades de una libre circulación de la información pública.

Durante la 2ª Guerra Mundial se desarrollaron las primeras computadoras, y con ellas los primeros sistemas que automatizaban los procesos de encriptado y desencriptado de las comunicaciones. Los alemanes disponían de ENIGMA, diseñada en 1919 por el holandés Hugo Alexander Koch, quien cedió sus derechos al ingeniero alemán Arthur Scherbius. Se produjeron aproximadamente unas 100.000 máquinas durante la guerra.

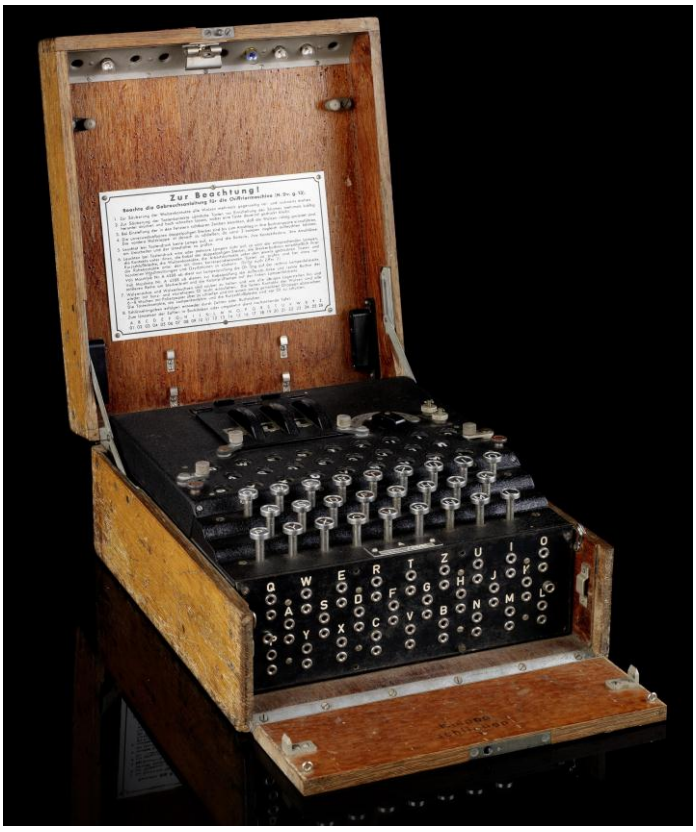

Figura 1: *Máquina ENIGMA original de 1941. Fuente: The History Blog, vía Google Images. http://www.thehistoryblog.com/archives/21186 (Último acceso: 17/09/2015)*

El ejército polaco consiguió hacerse con una de estas máquinas en 1929, robándola de una oficina de correos, y en 1937 disponían de seis máquinas electrónicas, a las que denominaban BOMBAS capaces de descifrar una gran parte de los mensajes alemanes. Sin embargo una modificación de ENIGMA llevó a los polacos a compartir sus conocimientos con los servicios secretos británicos. En febrero de 1940, con la captura del submarino alemán U-33, los británicos consiguieron una nueva máquina ENIGMA, lo que les permitió estudiar las nuevas modificaciones, y crearon un grupo especial, denominado ULTRA, en el que llegaron a trabajar más de siete mil personas, y construyeron en Blechley Park un sistema que fue capaz de descifrar el 83% de los mensajes alemanes.[2]

La Guerra Fría, al término de la 2ª Guerra Mundial, dividió el planeta en dos bloques enfrentados en torno a las dos grandes superpotencias de la época, los EE.UU. y la U.R.S.S., lo que derivó en una escalada armamentista, cuya vertiente nuclear constituyó la máxima amenaza y factor disuasorio, enunciado en el concepto MAD (Mutual Assured Destruction)[3], en inglés literalmente "locura". Esta disuasión habría sido imposible sin el conocimiento de las capacidades reales del oponente y de sus planes estratégicos en caso de ataque, lo que favoreció de forma exponencial las actividades de espionaje y contraespionaje en todos los campos. Como consecuencia de ello fue posible establecer una política de entendimiento mínimo, que cristalizó a partir de 1969 en los acuerdos SALT[4] (Strategic Arms Limitation Talks).

La invasión soviética de Afganistán (1978-1989) y las crisis de los "euromisiles"[5], supusieron un cambio de contexto, y el Senado norteamericano se negó a ratificar los acuerdos SALT II para la limitación de los misiles balísticos intercontinentales (ICBM), alcanzados en 1979 en Viena entre Breznev y Carter. El nuevo rearme promovido por Reagan (la Iniciativa de Defensa Estratégica[6], basada en sistemas antimisiles, conocida popularmente como "Guerra de las Galaxias") llevó al fin de los acuerdos SALT, y en 1986, los EE.UU. se desvincularon oficialmente de esos tratados.

Se generó no obstante en ambas potencias durante esas casi tres décadas la mentalidad de que el espionaje podía resultar beneficioso para la distensión y la consecución de acuerdos de paz efectivos. Se desarrollaron entonces las técnicas de intercepción e interpretación de señales electromagnéticas de todos los tipos, lo que se denomina inteligencia de señales o actividad

[2] Jesús de Marcelo Rodao. "Piratas cibernéticos. Cyberwars, seguridad informática e Internet". Ed. RAMA, 2003.
[3] MAD. http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-mutual-assured-destruction.htm (Ú.a.: 14/08/2015)
[4] Acuerdos SALT. http://www.historiasiglo20.org/GLOS/SALT.htm (Ú.a.: 14/08/2015)
[5] Crisis de los Euromisiles. http://www.historiasiglo20.org/GLOS/euromisiles.htm (Ú.a.: 14/08/2015)
[6] Gustavo Alonso. "La Iniciativa de Defensa Estratégica (SDI)". GSI de la UPM, 1990. http://www.gsi.dit.upm.es/~fsaez/intl/libro_complejidad/16-iniciativa-de-defensa-estrategica.pdf (Ú.a.: 14/08/2015)

SIGINT[7]. Cuando la información no se obtiene directamente de las señales, sino de su organización, por ejemplo la información de valor militar que puede aportar la detección de señales de radar, para establecer como se ha estructurado un sistema de defensa antiaéreo, entonces se habla de inteligencia electrónica o ELINT.

Estas señales pueden capturarse por estaciones terrestres fijas, buques o aviones especialmente diseñados para la captura de señales electromagnéticas (AWACS), satélites en órbita baja, o satélites semi-geoestacionarios SIGINT.

Conforme emergían las tecnologías de la información y las comunicaciones, en algunos casos fruto de desarrollos visionarios en el ámbito docente e investigador, pero en otros casos como consecuencia de necesidades de carácter militar y de inteligencia, el espionaje continuó siendo una prioridad para ambas potencias. Y aunque se han producido posteriormente cambios políticos que han significado un cambio en las relaciones de poder entre los estados, adquiriendo relevancia nuevos actores en el teatro internacional, las actividades de inteligencia, y los medios de apoyo para realizar estas actividades no han dejado de desarrollarse. Esa mentalidad sobre la pertinencia del espionaje ha pervivido en la política norteamericana.

Entre 1991 y 2004, el Parlamento Europeo (PE), de conformidad con el apartado 2 del artículo 150 del Reglamento, decidió crear una comisión temporal para el estudio de posibles redes de interceptación de las comunicaciones cuya actividad presuntamente alcanzase a todos o parte de los estados miembros de la Unión Europea, a través de STOA[8] (Scientific and Technological Options Assessment), servicio de la Dirección General de Estudios del PE. Fruto de las investigaciones llevadas a cabo por esta comisión, se presentaron varios informes determinantes.

El primer informe STOA de 1997, sobre el tema "Evaluación de las tecnologías de control político", dedicó un capítulo a la existencia de redes nacionales e internacionales de vigilancia de las comunicaciones, y afirmaba que, dentro de Europa, la Agencia Nacional de Seguridad (NSA) de EE.UU. interceptaba de forma habitual todas las comunicaciones de correo electrónico, teléfono y fax.

[7] SIGINT. https://www.nsa.gov/sigint/ (Ú.a.: 14/08/2015)
[8] STOA. http://www.europarl.europa.eu/stoa/ (Ú.a.: 14/08/2015)

Figura 2: *GCHQ Bude. Composite Signals Organisation (CSO) Station en Morwenstow (Cornwall, Inglaterra), operada por el GCHQ. Fuente: Imagen tomada de la web de Duncan Campbell dedicada a sus investigaciones sobre la red ECHELON.* http://www.duncancampbell.org/content/echelon *(Último acceso: 28/08/2015)*

El informe STOA de 1999, conocido como Informe Campbell, sobre "Desarrollo de la Tecnología de vigilancia y riesgos de uso indebido de la información económica", estaba dividido en cinco partes. El volumen 2/5, redactado por Duncan Campbell, estudiaba las capacidades de interceptación e información y el modo de funcionamiento de ECHELON, y presentó la tesis de que la red de vigilancia, de carácter global, no se utilizaba exclusivamente en cometidos de seguridad, sino que se empleaba para el espionaje industrial.

En julio de 2001 STOA hizo público su informe definitivo sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON) (2001/2098(INI))[9], que es el primer informe público en el que se identifican las capacidades y se describen los sistemas empleados para la intercepción global e interpretación de todo tipo de comunicaciones, y, fundamentalmente, se establecen propuestas de iniciativas políticas y legislativas para evitar o reducir los riesgos derivados de las actividades de los servicios secretos para los ciudadanos y empresas de la UE.

En el mismo informe se señaló la existencia de amplios indicios de que tanto Rusia como Francia podían disponer de sistemas similares.

[9] Informe STOA (2001/2098(INI)), de 11 de julio de 2001. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//ES (Ú.a.: 30/05/2015)

Como se indica en el informe, esta red de escuchas, que inicialmente debía operar como sistema SIGINT para la intercepción de comunicaciones al servicio de la seguridad exterior e interior de los países del acuerdo UKUSA (del que participaron EE.UU., Reino Unido, Canadá, Australia y Nueva Zelanda), hubiera sido compatible con el Derecho de la UE, ya que el Tratado de la UE no abordaba las cuestiones relacionadas con las actividades en el ámbito de la seguridad nacional, sino que recaían en el ámbito de aplicación del Título V del Tratado, que no incluían ningún tipo de disposiciones en la materia. Se indica también que el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que garantiza el respeto a la vida privada, permite este tipo de intervenciones cuando se trata de garantizar la seguridad nacional, siempre que no contravenga las normas del derecho nacional de cada estado, y se precise en qué circunstancias y bajo qué condiciones pueden ser realizadas por las autoridades competentes.

Sin embargo la red ECHELON no limitó sus actividades a un propósito de defensa, sino que se utilizó de forma indiscriminada para las escuchas de todos los ciudadanos de la UE, violando cualquier principio de proporcionalidad; y para el espionaje industrial, favoreciendo los intereses comerciales de las empresas de los países miembros del acuerdo UKUSA en su competencia con las empresas de otros países miembros de la UE. Si bien en ese momento este tipo de actividad no fue considerado como una agresión entre estados, sino una violación del derecho comunitario, los cambios durante las décadas siguientes sí permitirían considerar esta actividad como una forma de agresión, y podría ser considerada como una forma de guerra económica entre los estados, tendente a erosionar de forma activa los recursos y capacidades de los oponentes.

En particular se consideró probado que las empresas Airbus y Thompson habían resultado perjudicadas en la concesión de contratos con terceros, frente a empresas norteamericanas (Boeing y McDonnell Douglas, y Raytheon respectivamente)[10].

Al sistema ECHELON se le atribuía la capacidad de ejercer una vigilancia simultánea de la totalidad de las comunicaciones, por redes de telefonía o por internet, de forma global, conociendo su contenido, y mediante estaciones de interceptación de comunicaciones transoceánicas y por satélite. Todo ello la distinguía de los sistemas nacionales y significaba un salto cualitativo tanto en las capacidades de interceptación como en las de interpretación de la información.

[10] Jerome Thorel. "Pourquoi l'affaire Echelon embarrasse Thomson-CSF". ZDNet. 14/07/2000. http://www.zdnet.fr/actualites/pourquoi-l-affaire-echelon-embarrasse-thomson-csf-2060838.htm (Ú.a.:22/08/2015)

Más allá, ECHELON planteaba un problema importante, al operar en un ámbito carente de regulación jurídica, dejaba a la persona observada, por ser extranjera para el país observador, indefensa y sin ningún tipo de protección jurídica internacional. Tampoco cabía esperar ningún interés ni control parlamentario en los estados que operaban el sistema, dado que se utilizaba sobre personas que vivían en el extranjero y cuidando los intereses de sus electores. De hecho la reunión acordada en 2001, a consecuencia de la publicación del informe STOA, entre el Director de la NSA y una delegación de parlamentarios del PE, nunca llegó a celebrarse.

Si bien las capacidades técnicas de la red ECHELON eran portentosas y permitían la intercepción de la práctica totalidad de las comunicaciones electromagnéticas, su actividad se basaba en las escuchas de transmisiones de radio, satélite, microondas, y los 300 enlaces transoceánicos de fibra óptica, que en su mayor parte son infraestructuras tendidas entre los estados miembros del acuerdo UKUSA.

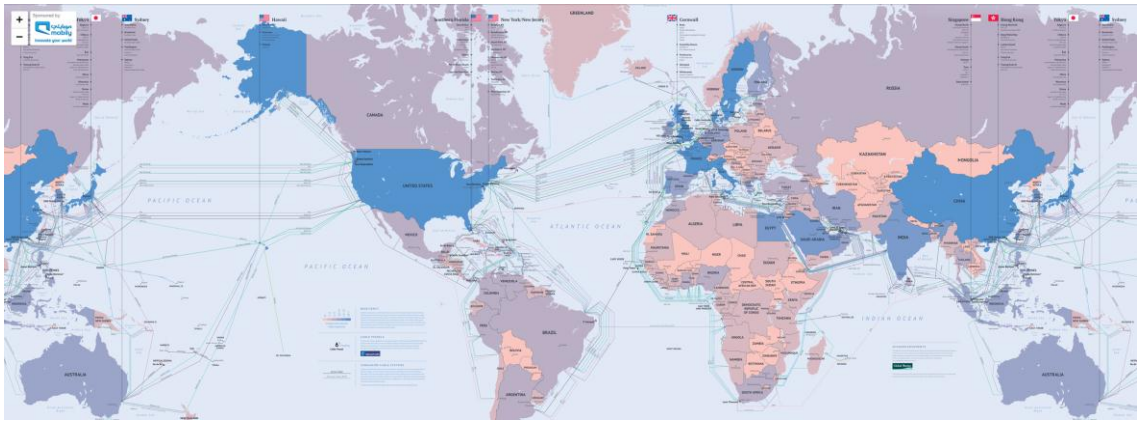

Figura 3: *Mapa de la red de Cables Submarinos de fibra óptica en 2014. Fuente: Web de ExtremeTech a través de Google Images (reproducida también en otras fuentes). Infografía interactiva de alta resolución originalmente publicada por TeleGeografy: http://submarine-cable-map-2014.telegeography.com/ (Último acceso: 17/09/2015)*

Sin embargo, el tráfico de Internet se produce protocolizado y fraccionado en paquetes y siguiendo rutas (teóricamente) impredecibles. Se calcula que un 20% de paquetes de los correos electrónicos intranacionales, discurren en realidad por rutas internacionales y cruzan varias veces los routers de los nodos de primer nivel y puntos de conmutación entre estados, accediendo a cables transoceánicos, lo que permitiría a ECHELON acceder a su contenido, interviniendo estas comunicaciones o accediendo a los routers y puntos de conmutación ubicados en los estados UKUSA.

Sin embargo una gran parte del tráfico de Internet sería inaccesible. En un momento en que las redes 2,5G -GPRS- y 3G -UMTS- aún no estaban implantadas (empezaron su uso comercial en 2001), provocó que las consecuencias esperadas de la publicación de los informes STOA resultaran muy limitadas (se aceleró el acuerdo respecto al puesto, papel y poderes del futuro representante de la UE para Asuntos Exteriores y Política de Seguridad -PESC-, que quedó definitivamente incluido en el Tratado de Lisboa[11], y una vaga resolución del Consejo de Europa sobre necesidades operativas que se pretendían encauzar a través de ENFOPOL[12]), ya que la totalidad de los estados consideraron que las ventajas de la existencia de un sistema como ECHELON en el marco de un acuerdo bilateral para la seguridad eran muy superiores. En lo que afecta a España, durante varios años de espectaculares éxitos en la lucha antiterrorista, aparecieron varias publicaciones en prensa escrita o en Internet que especulaban con la posibilidad de la existencia de una colaboración entre el gobierno español, los servicios de inteligencia británicos y la NSA, para controlar la actividad de ETA[13].

Las revelaciones sobre la existencia del sistema, así como la descripción de sus capacidades y forma de operar, supusieron en cambio un terremoto entre las personas vinculadas con la seguridad informática, y especialmente entre los hackers[14] de Internet. Tras la aparición del Informe STOA de 1999 (popularizado como Informe Campbell) varias organizaciones de hacktivistas realizaron un llamamiento internacional para provocar un bloqueo del sistema, el denominado "Día del Atasco de Echelon" (JED - Jam Echelon Day[15]), el 21 de octubre de 1999. La propuesta consistía en añadir una extensa lista de palabras clave, supuestamente etiquetadas y controladas por ECHELON, a listas de noticias que se publicaran ese día y a todos los correos electrónicos que se enviaran, de forma que se produjeran más alertas de las que el sistema pudiera procesar. Se trataba por tanto de orquestar un incipiente ataque de privación de servicio. Según algunas fuentes alternativas (incluida Wikipedia), la NSA habría informado del bloqueo de varios de los servidores. Estas informaciones sin embargo no han podido ser comprobadas y son inciertas. La mayoría de expertos y publicaciones, tanto en el JED de 1999, como en el

[11] Tratado de Lisboa. Innovaciones en materia de Política Exterior y de Seguridad Común (PESC). Eurogersinformation (2010). http://www.eurogersinfo.com/espagne/actes2209.htm (Ú.a.: 22/08/2015)
[12] ENFOPOL 55. Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services. 20/06/2001. http://www.statewatch.org/news/2001/sep/9194.pdf (Ú.a.: 22/08/2015)
[13] Gilles Tremlet. "US offers to spy on Eta for Spain". The Guardian. 15/06/2001. http://www.theguardian.com/world/2001/jun/15/spain.usa (Ú.a.: 14/08/2015)
[14] En su acepción más extendida, con el término "hacker" se denomina en los ambientes de seguridad informática a las personas que realizan entradas no autorizadas a los sistemas utilizando redes de comunicaciones. Esta acepción es la recogida por la RAE, aunque muy cuestionada desde la cultura hacker, que reivindica una acepción más ética, y distingue al *cracker*, que sería el cibercriminal, del *hacker*, que identifica a personas con talento y conocimiento en el mundo de los sistemas y su programación, las comunicaciones y su seguridad, y que promueven la idea de que toda información debe ser libre. Aquí se consideran ambas acepciones.
[15] JED (Jam Echelon Day). https://www.thing.net/~rdom/ecd/jam.html (Ú.a.: 19/08/2015)

nuevo intento en el JEDII de 2001, señalaban que ECHELON es mucho más sofisticado que un simple sistema con una gran capacidad de adquisición de entradas, análisis en tiempo real, categorización y almacenamiento, utilizando potentes procedimientos de inteligencia artificial para contextualizar la información, juzgar las relaciones entre palabras y analizar cadenas de texto[16].

En cualquier caso, las convocatorias JED tenían también mucho de "agitprop" (término de origen ruso, agitación y propaganda), había una clara componente antisistema junto al propósito de llamar la atención internacional sobre la red ECHELON, concienciar a gobiernos y particulares sobre la violación del derecho a la privacidad que implica su actividad, el coste económico de perder propiedad intelectual, información comercial o industrial, y el riesgo que puede suponer para las personas vivir bajo vigilancia si la información se usa de forma inadecuada, sin que exista mandato judicial, o si cae en manos de gobiernos que no respeten los derechos fundamentales de sus ciudadanos.

Cualquier simpatía de la que este tipo de movimientos hacktivista y antisistema pudiera gozar en ese momento, se volatilizó en septiembre de 2001, tras los ataques de Al Qaeda en suelo de EE.UU., conocidos como 11S.

Como consecuencia de estos ataques, se pusieron en cuestión muchos de los protocolos de seguridad y el alcance de los sistemas de vigilancia. La revelación de que el contacto entre los terroristas se había realizado utilizando cuentas de correo electrónico en las que se habían guardado borradores, pero nunca habían sido enviados correos electrónicos, evidenció que sistemas como ECHELON podían ser burlados, y los servicios de inteligencia y de lucha antiterrorista requerían nuevas capacidades de los sistemas de cibervigilancia.

Hasta 2013 no se hicieron públicas informaciones que confirmaban la existencia de sistemas mucho más sofisticados y con más alcance que los descritos para ECHELON en los informes STOA, entre ellos PRISM, XKeyscore y MUSCULAR. Estas informaciones fueron reveladas por Edward Snowden, exempleado de Booz Allen Hamilton, una de las principales empresas contratistas militares y de inteligencia del gobierno de EE.UU., y se han ido filtrando desde entonces a la prensa mundial usando los servidores de Wikileaks[17] .

Además de la descripción de los sistemas empleados por la NSA para tareas de cibervigilancia y ciberespionaje, los informes aportados por Snowden evidenciaban que esas actividades habían sido también realizadas para el espionaje de las comunicaciones de numerosos líderes

[16] Wendy McAuliffe. "'Jam Echelon Day' doomed to failure, say Experts". ZDNet, 26/07/2001. http://www.zdnet.com/article/jam-echelon-day-doomed-to-failure-say-experts/ (Ú.a.: 19/08/2015)
[17] Wikileaks. The Spy Files. https://wikileaks.org/the-spyfiles.htm (Ú.a.: 28/07/2015)

mundiales, que mostraron públicamente una gran afectación[18], pero sus gobiernos aparecían citados como partícipes de la red de vigilancia global, y, en cualquier caso, todos ellos eran conocedores de los informes STOA del Parlamento Europeo.

Posiblemente lo más irritante para los gobiernos europeos fueran las revelaciones sobre el espionaje a cuentas bancarias de los ciudadanos europeos, y se llegó a plantear la suspensión del acuerdo SWIFT (Society for Worldwide Interbank Financial Telecommunication)[19], bajo el que funciona la red de comunicaciones interbancarias que permite las transacciones internacionales. Der Spiegel se hacía eco de esta posibilidad, dando veracidad a las revelaciones de Snowden[20].

Estos sistemas habrían estado operativos desde 2007, pero las actividades de cibervigilancia y ciberespionaje habrían sido realizadas igualmente en el periodo 2001-2007, sin ninguna cobertura ni garantía legal y únicamente apoyadas en el Programa Presidencial de Vigilancia (President's Surveillance Program, PSP por sus siglas en inglés), aprobado por el Presidente George W. Bush a raíz del 11S, y se habría renovado periódicamente la autorización presidencial para mantener las actividades hasta la aprobación en 2007 de la Ley PAA (Protect America Act), que habilita la vigilancia sobre objetivos extranjeros con valor para los servicios de inteligencia, y protege los derechos de los ciudadanos americanos sólo si ello no significa un impedimento para la obtención de información por parte de dichos servicios de inteligencia[21]; y en 2008 de la Enmienda a la Ley FISA (Foreign Intelligence Surveillance Act), que habilitaría permanentemente a los servicios de inteligencia norteamericanos, y, en particular a la NSA, a realizar actividades de vigilancia masiva y a la recopilación ilimitada de datos personales, garantizando inmunidad ante presuntos abusos, y permitiendo el seguimiento y vigilancia de cualquier persona durante un máximo de una semana (168 horas) sin autorización judicial, especialmente de ciudadanos norteamericanos que hayan podido estar en el extranjero y ser susceptibles de ser agentes de una potencia extranjera.

Ambas leyes han generado una enorme controversia en EE.UU., y en el resto del mundo, porque implican de hecho una total desprotección jurídica para las personas vigiladas[22]. Pero, a todos los efectos, las actividades de cibervigilancia y ciberespionaje por parte de los servicios de

[18] Alejandro López de Miguel. "La reacción de sorpresa de los estados de la UE ante el espionaje es hipócrita, puro teatro". Público. 30/10/2013. http://www.publico.es/internacional/reaccion-sorpresa-estados-ue-espionaje.html (Ú.a.: 15/08/2015)
[19] SWIFT http://www.swift.com/index.page?lang=es (Ú.a.: 15/08/2015)
[20] Gregor Peter Schmitz. "SWIFT Suspension? EU Parliament Furious about NSA Bank Spying.". Der Spiegel. 18/09/2013. http://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920.html (Ú.a.: 15/08/2015)
[21] Objetivos de Protect America Act. Departamento de Justicia de EE.UU. http://www.justice.gov/archive/ll/ (Ú.a.: 16/08/2015)
[22] Una copia desclasificada del informe sobre el PCP, preceptivo antes de la aprobación de la Enmienda a la Ley FISA, y elaborado por ponentes de las agencias de inteligencia de EE.UU. (Departamento de Justicia, Departamento de Defensa, CIA y NSA, que se hace eco de esta controversia, se encuentra en esta dirección: https://oig.justice.gov/special/s0907.pdf (Ú.a.: 15/08/2015)

inteligencia norteamericanos, gozan en EE.UU. de absoluta protección operativa e inmunidad legal.

Quedaría así establecida la base legal para la existencia de sistemas como PRISM[23] que complementarían las capacidades SIGINT y permitirían acceder a los ordenadores y bases de datos de las principales empresas de Internet que ofrecen soporte a los usuarios de correo electrónico, mensajería, publicación de contenidos y el establecimiento de redes de contactos, las denominadas "redes sociales". En particular entre las informaciones aportadas por Snowden se menciona a Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL y Apple. Pero cabe suponer que en algún momento se habrían accedido otras redes sociales de interés como Twitter, Linkedin, Instagram, Pinterest, Amazon, etc. Este acceso podría haberse realizado con la anuencia de las empresas, o incluso sin su consentimiento, accediendo mediante el uso de puertas traseras existentes en el software utilizado en los sistemas de soporte de estas redes sociales. TechCrunch recopiló declaraciones de algunas de estas empresas, negando categóricamente su colaboración con la NSA[24]. Aunque en el caso concreto de Facebook se aportó algún subterfugio que evidenció la existencia de una colaboración consentida.

PRISM sería la herramienta preferida por la NSA, pero podría estar siendo también operada, puntualmente o en parte, por los servicios secretos de Dinamarca, Francia, Paises Bajos y Noruega (Nine Eyes), además de Bélgica, España, Italia y Suecia, y de forma destacada por el Servicio Federal de Inteligencia alemán, conocido como la BND por sus siglas en alemán (Bundesnachrichtendienst)[25], y por el Cuartel General de Comunicaciones del Gobierno británico, más conocido por sus siglas en inglés GCHQ (Government Communications Headquarters)[26], perteneciente como el MI6 al Foreign Office británico, y cuya sede central está ubicada en Blechley Park.

El grupo de europeos involucrados, conocido como Fourteen Eyes, oficialmente se denominaría SIGINT Seniors Europe, o SSEUR.

Conjuntamente con PRISM se utilizaría MUSCULAR que recopilaría información interceptando las acometidas de comunicaciones privadas que unen los centros de datos de estas empresas para acceder a los correos electrónicos. Estas acometidas soportarían tráfico desencriptado entre los diferentes servidores de los centros de datos. Este tipo de intervenciones

[23] Electrospaces. "What is known about NSA's PRISM program". 23/04/14 (Updated 06/06/15). http://electrospaces.blogspot.com.es/2014/04/what-is-known-about-nsas-prism-program.html (Ú.a.:14/08/2015)
[24] Frederic Lardinois. "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program". TechCrunch. 06/06/2013. http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/ (Ú.a.: 16/08/2015)
[25] BND. http://www.bnd.bund.de/EN/Scope_of_Work/Mission/Mission_node.html (Ú.a.: 16/08/2015)
[26] GCHQ. http://www.gchq.gov.uk/what_we_do/Pages/index.aspx (Ú.a.: 16/08/2015)

contarían con la colaboración de los operadores de telecomunicaciones (o, al menos, éstos habrían recibido los correspondientes requerimientos gubernamentales). Por último XKeyscore sería una herramienta capaz de detectar la nacionalidad de los extranjeros mediante el análisis del lenguaje utilizado en los correos electrónicos interceptados.

Las tres herramientas actuarían coordinadamente como parte de una evolucionada ECHELON, más centrada en Internet, en los perfiles y datos de usuario, y con capacidad de realizar un seguimiento on-line de la actividad en Internet a través de las redes tradicionales, y también a través de las redes móviles.

El principal problema técnico al que se enfrenta una red de estas características, con una capacidad supuesta de hacer un seguimiento a más de tres mil millones de comunicaciones diarias, es el filtrado y la discriminación de la información.

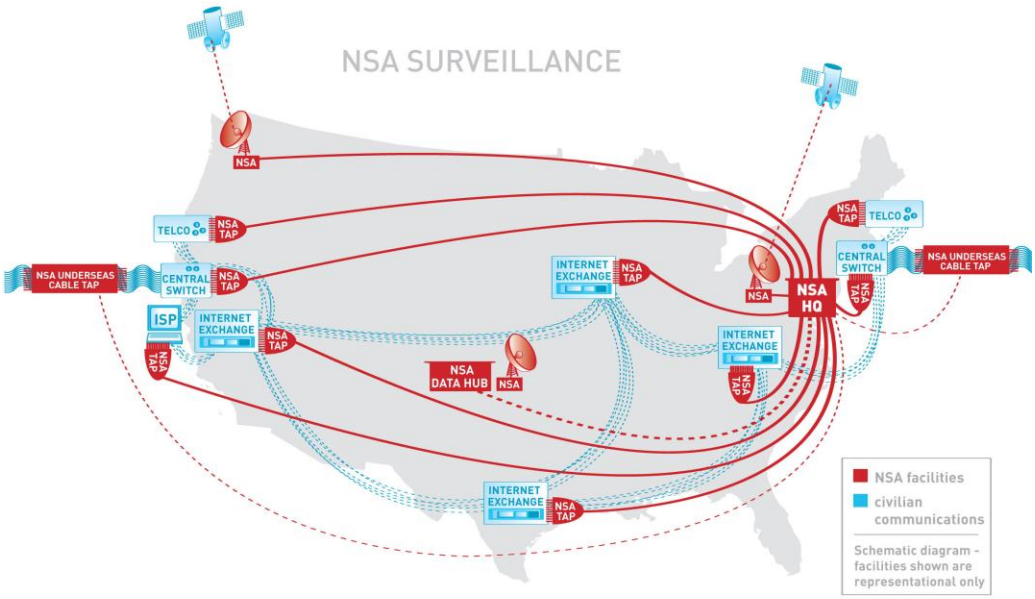

Figura 4: *Sistema de intercepción de comunicaciones de la NSA. Fuente: Web oficial de la NSA (https://nsa.gov1.info/surveillance/index.html). Originalmente publicada por la American Civil Liberties Union*[27]*. Más información sobre este mapa en la dirección: https://www.aclu.org/files/pdfs/eavesdropping101.pdf (Último acceso: 04/09/2015)*

A nivel legal, Alemania ha sido el primer país europeo en aprobar una regulación que habilita a los jueces alemanes para que autoricen a la policía la intervención de los ordenadores de los

[27] American Civil Liberties Union. "What can the NSA do?". 2006. https://www.aclu.org/files/pdfs/eavesdropping101.pdf (Ú.a.: 16/08/2015)

ciudadanos investigados, infectándolos con un troyano, para obtener la información que contienen o a la que se puede acceder a través de ellos, permitiendo el acceso remoto de equipos informáticos y dispositivos móviles, en el caso de que se estén investigando delitos con penas máximas superiores a tres años, para investigar el cibercrimen y para el terrorismo y el crimen organizado, y siempre que el juez justifique la proporcionalidad de la intervención. Según diversas fuentes la BND alemana y la NSA colaboran estrechamente, y se calcula que entre ambos servicios se cruzan unos 97.000 millones de datos de inteligencia mensuales, contenidos en unos 500 millones de registros. Según Der Spiegel, la NSA ofreció a la BND acceso a XKeyscore a cambio de sus sistemas Mira4 y Veras[28].

Según informaciones publicadas en El País, este mismo debilitamiento de la legislación de protección de la privacidad, habría sido propuesto por la Comisión Gallardón en el borrador de anteproyecto de Código Penal elaborado por el Ministerio de Justicia en España. En principio, el borrador solo prevé estas técnicas para los delitos cometidos intencionadamente (con dolo) cuya pena máxima supere los tres años de cárcel. También para los perpetrados por un grupo u organización criminal, es decir, los relacionados con el crimen organizado y el terrorismo, y para todos aquellos que se consumen a través de instrumentos informáticos: estafas por internet, pornografía infantil, grooming (acoso sexual a menores por internet), ciberbullying (acoso en la red), etc. El ordenador a investigar, además, se tiene que encontrar en España. Este sería el primer paso para una coordinación más estrecha con la NSA en un modelo de colaboración similar al alemán, y que, como hemos visto ya se produjo con anterioridad. En el artículo referido se aportan las declaraciones de Juan Carlos Ortíz Pradillo, profesor de Derecho Procesal de la UCLM, y experto en delitos telemáticos, quien indica que con estos troyanos puede accederse al correo electrónico, a todas las redes sociales, y conocer los movimientos del investigado, con quién se relaciona o cuáles son sus hábitos; o a programas de comunicaciones como Skype. Incluso a todo lo que el investigado almacene en servidores extranjeros, como pueda ser Gmail, Dropbox, etc. Las claves para al desencriptado de la información, si está protegida, o los movimientos de las cuentas bancarias, si se gestionan online. El troyano podría además proporcionar a los investigadores de los Cuerpos y Fuerzas de Seguridad del Estado, las IP de los ordenadores o dispositivos con los que se haya compartido información o dar acceso a las búsquedas de Internet del supuesto criminal, llegando a conocer la personalidad del delincuente y, en algunos casos, predecir lo que va a hacer.[29] Este "profiling" (perfilación

[28] Hubert Gude, Laura Poitras and Marcel Rosenbach. "Transfers from Germany Aid US Surveillance". Der Spiegel. 05/08/2013. http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html (Ú.a.: 21/08/2015)

[29] Manuel Altozano. "La policía podrá usar troyanos para investigar ordenadores y tabletas". El País. 03/06/2013. http://sociedad.elpais.com/sociedad/2013/06/03/actualidad/1370289646_865495.html (Ú.a.:21/08/2015)

criminal inductiva)[30], sin embargo, no sería indiscriminado, como sí estarían efectuándolo las redes de vigilancia globales.

Si bien las revelaciones de Snowden hacen referencia a los sistemas y actividades de vigilancia de los servicios de inteligencia de EE.UU., otros estados, entre los que podemos contar a algunos de los que protestaron con más energía ante el Departamento de Estado norteamericano, disponen de sistemas de capacidades similares.

Francia, a través de la Direction Générale de la Sécurité Extérieure (DGSE), y gracias a sus territorios de ultramar que les permite el despliegue de estaciones de escucha con capacidad para cubrir la totalidad del globo, operaría desde 2009 con un sistema de características muy parecidas[31].

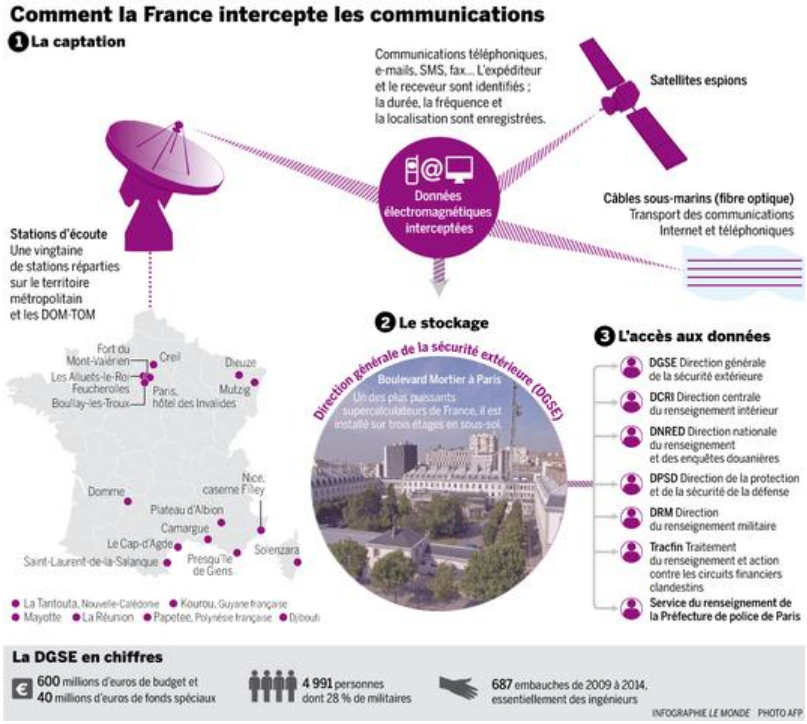

Figura 5: *Sistema de intercepción de comunicaciones francés. Fuente: Jacques Follorou et Franck Johannès. "Révélations sur le Big Brother français". Le Monde. 04/07/2013. http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (Último acceso: 28/08/2015)*

[30] En oposición a la perfilación criminal deductiva, obtenida a partir de los indicios físicos y psicológicos encontrados en la escena del crimen.

[31] Jacques Follorou et Franck Johannès. "Révélations sur le Big Brother français". Le Monde. 04/07/2013. http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (Ú.a.: 28/08/2015)

De hecho son públicos proyectos que involucran a varios países europeos y que describen sistemas que evidenciarían una extendida capacidad de interceptación de las comunicaciones globales, y la subsiguiente necesidad de procesar esa información. Entre ellos se cuenta por ejemplo el proyecto OSEMINTI, que están desarrollando los ministerios de defensa de España, Francia e Italia desde 2006, denominado "Infraestructura de inteligencia semántica operacional", desarrollado por la Agencia Europea de Defensa, CapTech IAP04 (acrónimo de "Information Acquisition & Processing" en el ámbito "CIS & Networks"). Su objetivo es conseguir diseñar y desplegar sistemas inteligentes, que tengan conocimiento y capacidad de aprender, para la gestión de situaciones complejas en tiempo real.[32]

OSEMINTI no es específicamente un sistema de ciberespionaje, es una herramienta capaz de interpretar el significado de un discurso. Lo interesante es su capacidad para trabajar con cualquier tipo de información, y construir una representación semántica, que puede aplicarse a textos, a un conjunto heterogéneo de informaciones sacadas del exterior con medios de captación como radares, sensores o cualquier sistema de espionaje, o a datos y metadatos resultado de actividades de data mining[33] sobre informaciones diversas almacenadas a lo largo del tiempo.

Su uso se apoya en la directiva de retención de datos[34], que regula en Europa tanto la guarda de datos de las comunicaciones telefónicas y por Internet durante el plazo de dos años, como las órdenes judiciales para interceptar el contenido de llamadas o comunicación por Internet y la obligación de identificar a los compradores de las tarjetas prepago para teléfonos móviles.

Es un sistema inteligente programado para aprender a medida que interactúa con las personas, de modo que no serán necesarios medios humanos para cotejar esa información que se genera. Francia es la encargada de liderar este proyecto, en el que España aporta 2.784.000 €, el 3% de su Presupuesto de Defensa entre el 2007 y el 2009, según autorización del Consejo de Ministros: acuerdo técnico B-0034-IAP04 ERG.

En 2014, el Tribunal de Justicia de la Unión Europea (TJUE) declaró ilegal la directiva sobre retención de datos aprobada en diciembre de 2005 por el Consejo de Ministros de Justicia e Interior europeos, después de que el Tribunal de Justicia de Irlanda y el Tribunal Constitucional de Austria presentaran ante la Justicia europea sus dudas sobre la legalidad de esta norma.

---

[32] Miguel A. Gallardo. OSEMINTI. 2006. http://www.miguelgallardo.es/oseminti/ (Ú.a.: 10/07/2015)
[33] Jean-Michel Franco y EDS-Institut Promèthéus. "El Data Warehouse. El Data Mining". Ed. Gestión 2000. Barcelona, 1997. (p. 163-174)
[34] Navegante. "El Parlamento Europeo aprueba la retención de datos contra el terrorismo". El Mundo. 14/12/2005. http://www.elmundo.es/navegante/2005/12/14/esociedad/1134560239.html (Ú.a.:05/09/2015)

Según el TJUE, la directiva "se inmiscuye de manera especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal". Argumenta que la norma abarca de manera generalizada a todas las personas, medios de comunicación electrónica y no establece por tanto ninguna limitación, sobrepasando los límites que exige el respeto del principio de proporcionalidad.

No existen informaciones que permitan acreditar si el proyecto OSEMINTI está paralizado o continúa su desarrollo en una vertiente puramente científica. En cualquier caso, su existencia hace pensar que la NSA puede disponer en uso de tecnología semántica similar, posiblemente derivada del analizador semántico de tráfico, para inspección profunda de paquetes, creado por la empresa Narus[35], y del software de data mining creado para el programa Total Information Awareness (TIA), posteriormente renombrado como Terrorism Information Awareness Program, y suspendido por el Congreso norteamericano para su uso en actividades domésticas en 2003, fecha en que, según informaciones publicadas por el New York Times[36], el software pasó a ser explotado por la NSA, y operaría integrado en PRISM desde el Data Center de Bluffdale, en Utah.[37] [38]

[35] PrivacySOS. "NARUS, deep packet inspection and the NSA". 09/04/2015. https://www.privacysos.org/technologies_of_control/naurus (Ú.a.: 29/08/2015)
[36] Shane Harris. "Giving In to the Surveillance". The New York Times. 22/08/2012. http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html?_r=0 (Ú.a.:29/08/2015)
[37] James Bamford. "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". Wired. 15/03/2012. http://www.wired.com/2012/03/ff_nsadatacenter/all/ (Ú.a.: 29/08/2015)
[38] NSA Utah Data Center. https://nsa.gov1.info/utah-data-center/ (Ú.a.: 29/08/2015)

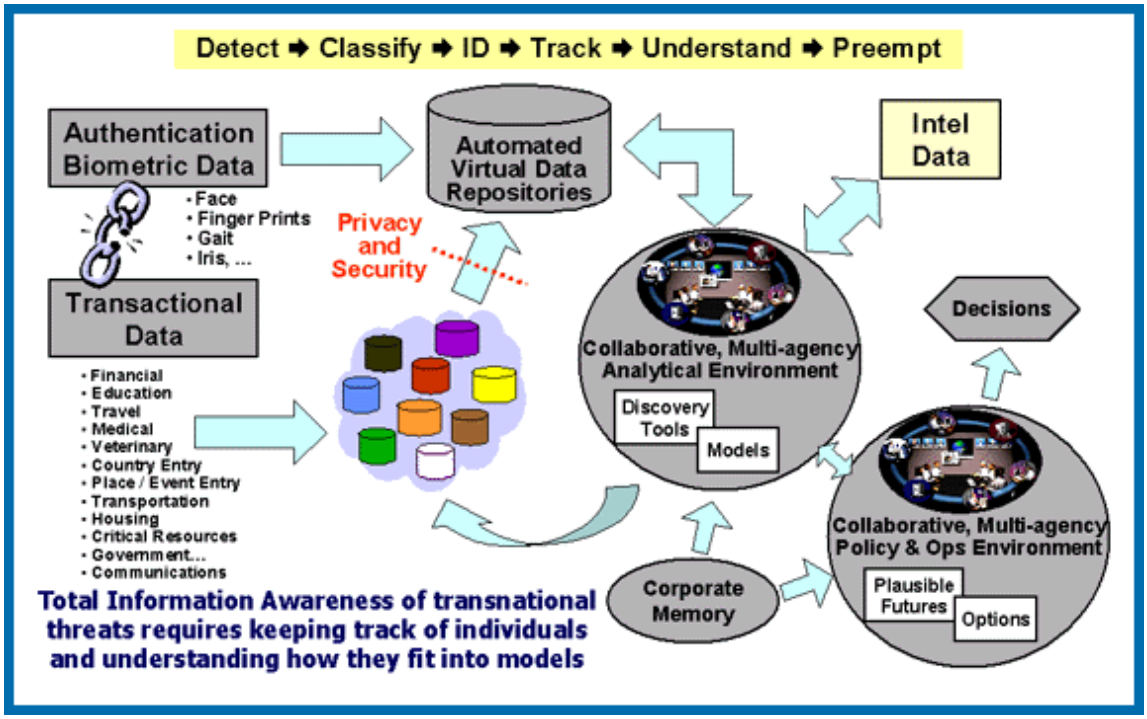

Figura 6: *Infografía sobre el programa TIA. Fuente: Wikimedia, https://en.wikipedia.org/wiki/Information_Awareness_Office (Último acceso: 31/08/2015)*

Omitiendo el dominio global, y en lo que se refiere a España, el uso conjunto de OSEMINTI y el sistema SITEL, Sistema Integral de Intercepción de las Comunicaciones Electrónicas del Mº del Interior, ofrecería capacidades de intercepción y vigilancia similares a las descritas para los sistemas de vigilancia global, pero no es descartable un futuro despliegue vía satélite.

SITEL está operado conjuntamente por la Policía Nacional, la Guardia Civil y el Servicio de Vigilancia Aduanera, compartiendo equipos electrónicos con el Centro Nacional de Inteligencia (CNI). Se dio a conocer en 2001, durante la Presidencia Europea de España, momento en que se destinaron partidas presupuestarias a este sistema. Posteriormente en 2007 se publicó una "Resolución de la División de Coordinación Económica y Técnica de la Dirección General de la Policía y de la Guardia Civil, por la que se hace público el anuncio de adjudicación del contrato para la ejecución del servicio de mantenimiento plurianual del entorno de alta disponibilidad y plataforma de almacenamiento/archivado/back up del Sistema de Interceptación Legal de las Telecomunicaciones (SITEL), del Cuerpo Nacional de Policía, ubicado en el Complejo Policial de Canillas." (BOE-B-2007-256021)[39].

[39] BOE-B-2007-256021. http://www.boe.es/buscar/doc.php?id=BOE-B-2007-256021 (Ú.a.: 30/08/2015)

Según la Asociación de Internautas[40], basándose en una noticia publicada por La Gaceta (las referencias a esta noticia no están ya disponibles, pero se hace eco también Libertad Digital[41]), el Gobierno de José María Aznar pagó 36 millones de euros a Ericsson por el software. Un año y medio después, la compañía entregó el programa al Ministerio del Interior, que se convirtió en propietario. Sin embargo, el ejecutivo del PP no lo puso en marcha por no encontrar una cobertura legal adecuada. Los informes de los ministerios de Justicia y Defensa y del Consejo General del Poder Judicial en 2001 y 2002 ponían demasiados reparos.

Cuando el ejecutivo socialista llegó al poder, por el vuelco electoral que se produjo tras los atentados terroristas del 11M en Madrid, no dudó en trabajar con el innovador software, que proporcionaba descomunales ventajas respecto a los procedimientos de intervención de comunicaciones anteriores.

Conocedor de los informes judiciales negativos, el PSOE decidió enfocar la cuestión como un asunto meramente técnico, por lo que encargó el desarrollo legal al Ministerio de Industria, ignorando los nuevos problemas sobre privacidad y conservación de datos personales. Utilizó el mismo texto abandonado por el Gobierno Aznar y lo incluyó en el capítulo segundo del título V del Reglamento de la Ley General de Telecomunicaciones, del 15 de abril de 2005 (RD 424/2005).

Para entonces, SITEL ya llevaba un año funcionando en pruebas sin marco legal. Así lo denunció el teniente fiscal de Madrid, Pedro Martínez, en un informe que elevó ante el Fiscal General del Estado, Cándido Conde Pumpido, en junio de 2006. Martínez advertía que SITEL había sido utilizado sin cobertura jurídica y que el Reglamento aprobado en 2005 no tenía rango normativo suficiente, ya que la Constitución exige que estos asuntos sean regulados por ley orgánica. Los mismos argumentos fueron utilizados por la Asociación de Internautas en el recurso que interpuso el 29 de junio de 2005 ante el Tribunal Supremo contra el citado Reglamento. El alto tribunal sentenció el 5 de octubre de 2008 que un reglamento no es suficiente para regular el secreto de las comunicaciones, aunque no aclaró si es necesario alcanzar el rango de ley orgánica. Sí deja la puerta abierta a todo el que se sienta perjudicado por una interceptación a que pueda recurrir.

La polémica recuerda en gran medida a la planteada con motivo de la aprobación del Programa Presidencial de Vigilancia (PSP) tras los atentados del 11S, para dar cobertura a las actividades de vigilancia desarrolladas por la NSA, y sus sucesivas prórrogas.

[40] "Sitel Requiere un control". Asociación de Internautas. 09/09/2009. http://www.internautas.org/html/5711.html (Ú.a.: 31/08/2015)
[41] "Así funciona Sitel, el "Gran Hermano" de Zapatero". Libertad Digital. 15/10/2009. http://www.libertaddigital.com/nacional/asi-funciona-sitel-el-gran-hermano-de-zapatero-1276373188/ (Ú.a.: 31/08/2015)

El proceso legal de interceptación se lleva a cabo a partir de la solicitud que un agente de Policía Judicial, en el curso de la investigación de un delito grave, realiza al Juzgado de Instrucción de Guardia, la solicitud debe estar motivada y explicar las razones de la solicitud de interceptación. El Juez de Instrucción examina la solicitud y si la encuentra ajustada a derecho procede a la apertura de diligencias previas, y, dentro de estas, acuerda por Auto motivado la interceptación solicitada. Este Auto es escaneado por el Agente solicitante y, en el caso de la Guardia Civil, a través de la intranet corporativa accede al sistema 'GAITA' por el que transmite la solicitud y la copia escaneada del Auto a la central donde se encuentra el agente facultado. Éste, revisa la base de datos 'GAITA' y reenvía a la compañía operadora, a través de un canal seguro administrativo los datos de la interceptación adjuntando la copia del Auto. La persona legalmente autorizada de la compañía operadora examina la petición y procede a efectuar físicamente la interceptación y a comunicar, por el canal administrativo, al agente facultado que la interceptación está realizada. La grabación se realiza a través del software de SITEL, que además aporta datos sobre la identidad, localización u operadora. El agente realiza las escuchas a partir del material almacenado en SITEL. La Policía muestra al juez la grabación en CD, y éste decide qué parte incorpora al Sumario y qué parte destruye. Siempre se destruye el CD, pero el archivo original continúa almacenado en SITEL.

En enero de 2010, la Agencia Española de Protección de Datos[42], elaboró un informe sobre SITEL que remitió al Ministerio de Interior, tras las actuaciones inspectoras efectuadas tanto a operadoras de telecomunicaciones como a Fuerzas y Cuerpos de Seguridad del Estado[43]. Sin embargo no se pronunció sobre el hecho de que la información quede almacenada indefinidamente, tan solo con la legalidad del estricto cumplimiento de los procedimientos de interceptación y la cadena de custodia de los datos.

A continuación se detallan las conclusiones derivadas de las actuaciones de inspección realizadas por la AEPD:

1. La incorporación de los datos a SITEL sólo es posible cuando la operadora que presta el servicio a la línea objeto de interceptación, una vez recibida y analizada la autorización judicial, activa dicha inclusión. Las Fuerzas y Cuerpos de Seguridad no pueden por sí mismas, introducir información en SITEL.

[42] Agencia Española de Protección de Datos. http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (Ú.a.: 01/09/2015)
[43] Conclusiones de la Inspección de la AEPD sobre SITEL. http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/enero/190110_np_conclusiones_sitel.pdf (Ú.a.: 01/09/2015)

2. La actividad de las Fuerzas y Cuerpos de Seguridad en relación con SITEL queda enmarcada en el ejercicio de las funciones de policía judicial previstas en la LOPJ[44] y en la LECrim[45]. En consecuencia, dicho acceso se efectúa exclusivamente en los términos previstos por la autoridad judicial y para la investigación concreta a la que se refiera dicha autorización de interceptación, pudiendo acceder al sistema los agentes facultados por ella designados. Por tanto, el tratamiento de datos en SITEL se produce siempre bajo el control de la autoridad judicial que ordena la interceptación.

3. La finalidad de SITEL es la de poner la información obtenida como consecuencia de la interceptación a disposición de la autoridad judicial que hubiera ordenado aquélla. Por tanto, los agentes facultados encuentran limitada su capacidad de acceso y uso a la información en los términos derivados de la autorización judicial de interceptación, quedando la información contenida en SITEL bajo el control de la autoridad judicial.

4. SITEL almacena la información relacionada con el contenido de la comunicación y la información relativa a la interceptación con el alcance que se deriva de la orden dictada por la autoridad judicial que controla la interceptación, cumpliendo así el principio de proporcionalidad previsto en el artículo 4.1 de la LOPD[46].

5. Los datos contenidos en SITEL son objeto de bloqueo una vez concluida la investigación que motivó la interceptación y ordenada judicialmente la restricción de los accesos al sistema, no pudiendo producirse el acceso a los mismos salvo que sea requerido por dicha autoridad. El borrado físico se producirá también a instancia de la autoridad judicial a la que corresponde el control de la información contenida en SITEL. De este modo, se da cumplimiento al principio de conservación previsto por el artículo 4.5, en relación con el artículo 16.3 de la LOPD.

6. El tratamiento de datos efectuado por SITEL se encuentra amparado en el artículo 579 de la Ley de Enjuiciamiento Criminal y en el artículo 33 de la Ley General de Telecomunicaciones[47], habiendo considerado el Tribunal Supremo en STS de 5 de febrero de 2008 (Sala de lo Contencioso-Administrativo) y 5 de noviembre de 2009 (Sala de lo Penal), entre otras que ésta cita, adecuado el rango normativo de ambas disposiciones.

[44] LOPJ. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (Vigente hasta el 01 de Octubre de 2015). http://noticias.juridicas.com/base_datos/Admin/lo6-1985.l1t1.html (Ú.a.: 01/09/2015)
[45] LECrim. Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal (Vigente hasta el 28 de Octubre de 2015).. http://noticias.juridicas.com/base_datos/Penal/lecr.html (Ú.a.: 01/09/2015)
[46] LOPD. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html (Ú.a.: 01/09/2015)
[47] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. http://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950 (Ú.a.: 11/09/2015)

7. De conformidad con las previsiones de la LOPD, así como de las necesarias garantías de integridad, exactitud y control judicial de la información contenida en SITEL, las Fuerzas y Cuerpos de Seguridad no han de cumplir con el deber de información al afectado acerca del tratamiento de sus datos ni pueden atender las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

8. Se considera que los procedimientos de firma electrónica implantados en el momento en que la información se incorpora al sistema, su grabación en otros soportes y su transmisión a la autoridad judicial, garantizan los principios de exactitud e integridad previstos en la LOPD.

9. SITEL garantiza el cumplimiento de las medidas de seguridad de nivel alto previstas en el RLOPD, debiéndose hacer especial referencia a aquellas relacionadas con el acceso al sistema por los distintos usuarios del mismo y la seguridad del trasporte de los soportes que contengan la información hasta su entrega a la autoridad judicial.

SITEL se ha empleado para la vigilancia de la actividad terrorista, tanto de ETA como del yihadismo. Sin embargo la actuación con más eco mediático fue la identificación de los líderes del movimiento hacktivista Anonymous en España, que llevó a su detención en junio de 2011[48].

Figura 7: *Imagen de la rueda de prensa ofrecida tras el desmantelamiento de la red Anonymous en España. Fuente: obtenida en el blog de Anonymous Iberoamérica*[49]*. Originalmente de la web de RTVE, y disponible en http://img.rtve.es/imagenes/policia-da-desmatelada-cupula-espana-anonymous/1307713707178.jpg (Último acceso: 31/08/2015)*

[48] Pablo Romero. "Así actuó la Policía para identificar a los supuestos 'líderes' de Anonymous". El Mundo. 27/06/2011. http://www.elmundo.es/elmundo/2011/06/24/navegante/1308937468.html (Ú.a.:31/08/2015)
[49] Blog oficial de Anonymous Iberoamérica. http://anonopsibero.blogspot.com/2014/12/operacion-elaborada-por-la-policia-en.html (Ú.a.: 31/08/2015)

Según las pruebas presentadas por el Grupo de Seguridad Lógica de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, ampliamente reflejadas en el sumario, Anonymous sería responsable de varias actuaciones y campañas que habrían supuesto ataques desde un número indeterminado de ordenadores a varios sitios web:

1. Operación contra la Ley Sinde. Realizada el 21 de diciembre de 2010, tras la votación en el Congreso de la llamada Ley Sinde que "daría pleno poder para cerrar sitios web de enlaces de contenidos sin necesidad de contar con autorización de un juez" (sic), se realiza un ataque DDoS contra los sitios web del PSOE; la SGAE, el congreso y el Ministerio de Cultura. Este último presentó hasta dos denuncias, asegura el informe policial.

2. Ataque contra el sitio web del Senado. Anonymous trata de 'tumbar' el 16 de enero de 2011 el sitio web de la Cámara Alta y la del Partido Popular, como protesta a la 'renovada' Ley Sinde.

3. Operación Goya. El 13 de febrero de 2011, el sitio web de la Academia de Cine quedó colapsado a las 16.00 horas. Durante la celebración de la gala de los Premios Goya se dieron "una serie de protestas y abucheos por parte de varios centenares de Anonymous que acudieron usando la tradicional careta de V de Vendetta", afirma literalmente el informe.

4. Operación hipoteca. Se trata de ataques a los sitios web de las principales entidades financieras españolas, como BBVA, Santander, La Caixa y Bankia, justificados en los "fuertes abusos financieros" y la aplicación de la Ley Hipotecaria. La Policía asegura que este ataque fue coordinado desde www.anonymous-spain.es, cuya titularidad atribuye a uno de los detenidos, R.T.S., alias 'Devnuller'.

5. Operación contra el Ministerio de Trabajo. Se iba a efectuar el 9 de mayo de 2011, aunque quedó frustrada por un ataque interno dentro de la red de servidores Anonops por parte de un operador cuyo nick es 'Ryan' (Este atacante llegó a hacerse con el control de toda la red IRC de Anonops, formada por 12 servidores, e hizo públicas las contraseñas y las direcciones IP de sus usuarios, afirma el informe). En ese momento, los miembros se dispersaron en dos redes: Anonworld.net y Anonnet.org, "las cuales comparten los mismos objetivos".

6. Operación V de votaciones. La Policía afirma que "se convoca para el 20 de mayo, dos días antes de las elecciones municipales en España, contra las páginas web de PP, PSOE y CiU.

7. Operación Posterdeface. Paralela a la anterior, "consiste en imprimir la máscara de 'V de Vendetta' y ponerlas en las caras de los carteles electorales de los candidatos". Esta operación también se atribuye a R. T. S., al aparecer como contacto un correo con su alias.

8. Operación Spanish Revolution. Paralela a la manifestación del 15M bajo el lema 'Democracia Real Ya', "se centró en un ataque a la página de la Junta Electoral Central desde el día 18 de mayo. Existieron otros ataques entoces contra los sitios web del Congreso y del sindicato UGT, según la Policía. También durante los días 27 al 29 de mayo se realizaron ataques DDoS contra los sitios de los Mossos D'Esquadra y CiU, con motivo del desalojo de la acampada en la Plaza de Catalunya de Barcelona.

9. Ataque a Telefónica y MoviStar. El colectivo de ciberactivistas logró tumbar, el domingo 26 de junio, la página de Movistar en España como había anunciado previamente en un vídeo colgado en el portal YouTube. El grupo anunció por la mañana que además atacaría el web telefonica.com, aunque finalmente no se registró ningún incidente.

2.2 Hacking, hacktivismo y ciberactivismo.

Las actuaciones realizadas por grupos organizados, como el caso de Anonymous, son muy comunes en todo el mundo, se ha convertido en una de las formas de protesta con más eco mediático desde los 90. El “hacktivismo”, acrónimo de hacker y activismo, también conocido como desobediencia civil electrónica, utiliza las técnicas del hacking y la tecnología para conseguir un objetivo político o social mediante la acción directa.

Ya se ha hecho mención a las diferencias entre un cracker y un hacker, aunque muchas veces ambos conceptos se confunden y el término hacker se usa para describir a un cibercriminal. El hacker es esencialmente un entusiasta de la informática, con grandes conocimientos e interés en aprender sobre los sistemas informáticos, las comunicaciones y cómo utilizarlas de forma innovadora. Dentro de la ética del hacker está justificada la intrusión a través de Internet en los sistemas informáticos buscando información y experiencia. La búsqueda de conocimiento es la motivación fundamental del hacker. Los crackers, que provocan daños a los sistemas que

invaden, los “script kiddies”, gente que accede a sistemas utilizando scripts, programas o técnicas de otros hackers, son en general despreciados por los auténticos hackers. Algo similar ocurre con los piratas de software. En la ética del hacker está justificado el pirateo y uso de programas para obtener conocimientos con los que construir programas propios. A ésto se añade que el hacker es un acérrimo defensor del software libre. Sin embargo un hacker difícilmente violará las licencias vendiendo software pirateado, aunque es obvio que el pirateo de software está en auge.

El hacker centra su actividad en campañas de alcance social y político, es muy reivindicativo y puede llegar a ser muy agresivo, aunque la frontera entre hacktivismo y ciberterrorismo siempre ha estado muy definida. El primero busca apoyo social y mediático para obtener un cambio de mentalidad en la sociedad. El segundo, llevando al extremo la teoría sobre el derecho de rebelión y el tiranicidio, hace un uso sistemático del terror para implantar respuestas en la sociedad que provoquen la claudicación del estado de derecho, y tratar de alcanzar así un fin político.

Según varias fuentes[50] [51] [52], el escritor Jason Sack usó por primera vez el término hacktivismo en un artículo sobre la artista multimedia Shu Lea Chang publicado en 'InfoNation' en 1995. En 1996 el término aparece en la web en un artículo escrito por ‘Omega’, un miembro del grupo de hackers americanos Cult of the Dead Cow (cDc), para referirse a las acciones de protesta on-line. En 2000, Oxblood Ruffin, otro miembro del grupo cDc, se apropió del término, defendiendo que los hacktivistas emplean la tecnología para defender los derechos humanos, recurriendo a la literalidad del artículo 19 de la Declaración Universal de los DD.HH.[53]. Con referencias puntuales a ideales libertarios (apoyo a la libre empresa, las libertades individuales, la libertad de expresión y la libertad de difusión de información), muchos hacktivistas consideran también que Internet debería ser independiente.

El primer caso conocido de hacktivismo, documentado por Suelette Dreyfus y Julian Assange en su libro Underground[54] (Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier), se remite a octubre de 1989, cuando un gusano informático, posiblemente desarrollado por un hacker australiano, penetró en las redes del Departamente de Energía del gobierno norteamericano, en la Red de Física de Alta Energía HEPNET y en el programa SPAN

[50] Wikipedia. https://es.wikipedia.org/wiki/Hacktivismo (Ú.a.: 28/08/2015)
[51] François Paget. “Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas”. McAfee Labs, 2012. http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf?view=legacy (Ú.a.:17/09/2015)
[52] Mercé Molist. “¿Cómo nació el 'Hacktivismo'?”. El Mundo. 16/04/2015. http://www.elmundo.es/tecnologia/2015/04/16/552fc9a2ca4741be608b4578.html (Ú.a.: 28/08/2015)
[53] Declaración Universal de los DD.HH. http://www.un.org/es/documents/udhr/ (Ú.a.: 16/09/2015)
[54] Suelette Dreyfus, Julian Assange, "Underground". Ed. Seix Barral. 2011. Existe una versión electrónica libre del libro en www.underground-book.net (Ú.a.: 12/09/2015)

de la NASA. El gusano, llamado WANK, cambió el mensaje de entrada a estos sistemas: "Your System Has Been Officially WANKed[55]. You talk of times of peace for all, and then prepare for war".

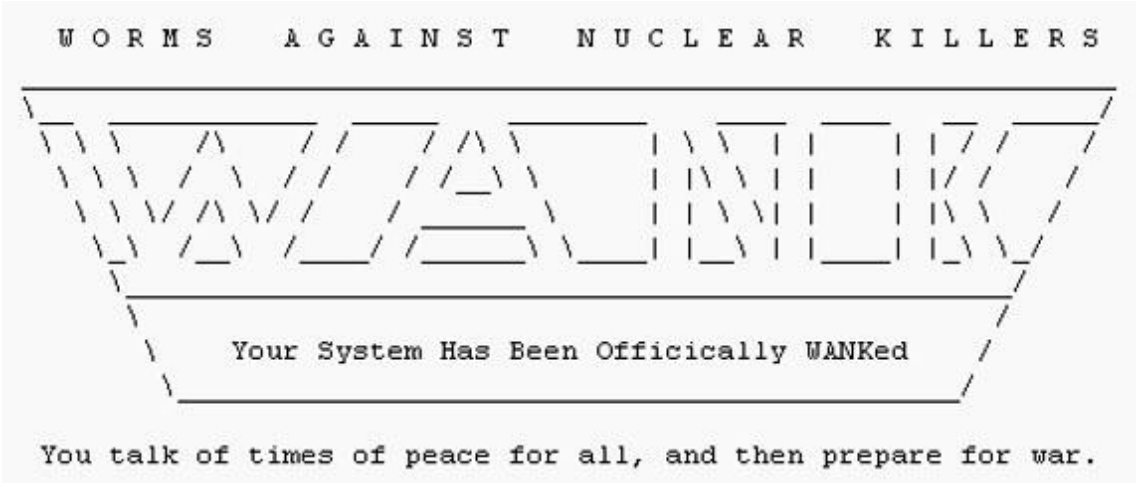

Figura 8: *Mensaje de entrada a los sistemas infectados por el gusano WANK. Fuente: Imagen obtenida del artículo de Eline van Audenaerde "YOU GOT WANKed: Hactions of Political Hacktivism" publicado en Youth-LeadeR.org, a través de Google Images.* *http://www.global1.youth-leader.org/2011/05/you-got-wanked-hactions-of-political-hacktivism/* *(Último acceso: 17/09/2015). Originalmente publicada en el libro Underground de Julian Assange, y reproducida en otras numerosas fuentes, incluida la Wikipedia.)*

Algunos de los primeros ejemplos de hacktivismo fueron las sentadas y manifestaciones virtuales, o netstrikes. Las manifestaciones se fijaban con un objetivo concreto, y mediante la instalación de un pequeño programa, compartido por el hacker con el manifestante virtual, se realizaban continuas solicitudes de servicio al objetivo marcado, intentando colapsarlo, como haría una manifestación frente a un servicio real. Aunque aparentemente legal, se trata de provocar en el sistema objetivo la denegación de servicio (Denial of Service, DoS por sus siglas en inglés).

En noviembre de 1994 un grupo de San Francisco, Los Zippies, realizaron una protesta contra servidores del gobierno británico para protestar contra una ley que prohibía los conciertos de música con un ritmo repetitivo al aire libre. Un año después, Strano Network lanzó un ataque contra sitios web del gobierno francés en protesta por las pruebas nucleares en los atolones de Mururoa. Utilizando la misma técnica se organizaron los eventos JED y JEDII, en 1999 y 2001 respectivamente para tratar de bloquear ECHELON, como ya se ha comentado.

[55] En jerga inglesa, literalmente "masturbado".

En junio de 1997 un grupo de hackers portugués UrBan Ka0s atacó cerca de 30 sitios web del gobierno indonesio para llamar la atención sobre la opresión que sufren los habitantes de Timor Oriental, en la camaña que denominaron Free East Timor. Este ataque, liderado por el portugués T0XyN, contó con el soporte técnico del hacktivista catalán Savage, del grupo Apòstols.

El software utilizado en este ataque sirvió posteriormente para desarrollar varias herramientas que permitían localizar servicios en las máquinas atacadas. Entre ellos Savage desarrolló QueSO, una utilidad que averiguaba el SO operativo de la máquina remota (OS fingerprint).

En 1998, QueSO provocó una gran alarma en Israel. El desencadenante fue el "Internet Operating System Counter"[56], una estadística mensual sobre los ordenadores europeos conectados a Internet, para conocer qué sistema operativo era el más popular, usando QueSO. Su promotor, Hans Zoebelein, afincado en Alemania, realizaba la estadística desde una máquina sita en Estados Unidos y mantenida por Alex Khalil, de origen libanés, llamada beirut.leb.net.

El estudio mensual comprendía también a Israel, ya que este país está dentro del Réseaux IP Européens (RIPE), organismo que gestiona la asignación de IPs. Dos empresas de seguridad israelíes, Comsec y Publicom, acusaron a Zoebelein de estar atacando centenares de máquinas de Israel, incluídos bancos, sitios militares y compañías tecnológicas. Los ataques, según estas empresas, eran escaneos de puerto intensos y de alto nivel, para posteriormente asaltarlas. Aseguraban que QueSO había traspasado incluso un firewall Checkpoint. La prensa israelí se hizo eco, con titulares sensacionalistas en los que denunciaban un presunto ataque terrorista alemán o libanes.

Mercé Molist, en su artículo "Pequeña guía histórica de los primeros hackers españoles" [57], publicado en El Mundo, en abril de 2014, ofrece un resumen muy interesante de las actividades de los hackers españoles, recopilada en su libro de licencia libre "Hackstory.es. La historia nunca contada del underground hacker en la Península Ibérica" [58], parte del impresionante proyecto Hackstory.es[59].

Muchos de los primeros hackers eran fanáticos del warez, el pirateo de juegos, una auténtica epidemia en España en los 80, y fueron posteriormente los creadores de algunas BBS de referencia, como Public NME, God's House, Encomix, MSX-ACC, Jurassic Park o Paradise BBS. El primer grupo de hackers españoles, de los que existe referencia, fue Glaucoma, activo

[56] The Internet Operating System Counter. http://www.leb.net/hzo/ioscount/ (Ú.a.: 02/09/2015)
[57] Mercé Molist. "Pequeña guía histórica de los primeros hackers españoles". El Mundo. 21/04/2014. http://www.elmundo.es/tecnologia/2014/04/20/53523c03ca474132388b456c.html (Ú.a.: 02/09/2015)
[58] Mercé Molist. "Hackstory.es. La historia nunca contada del underground hacker en la Península Ibérica". 2012. http://hackstory.es/ebook/Hackstory%20-%20Merce%20Molist%20Ferrer.pdf (Ú.a.: 30/08/2015)
[59] Hackstory.es http://hackstory.net/Hackstory.es_Index (Ú.a.: 02/09/2015)

desde 1987 a 1989 en Zaragoza. Fueron los primeros en acceder a RedIRIS para poder conectarse a las redes internacionales de X.25, por donde accedían a Minitel en Francia y al chat QSD, centro de reunión del hacktivismo europeo de la época. Les siguieron el grupo catalán Apòstols, autores de diversos programas de comunicaciones usados mundialmente. Su dominio del phreaking (acrónimo de phone break hacking), el hacking del sistema telefónico, les hizo famosos al difundir por qué en España no funcionaban las "blueboxes" para llamar gratis, que se describían en las webs americanas (la frecuencia que señalizaba a las centralitas la espera de marcación en España no era 2600 Hz, como en EE.UU., sino 2500 Hz).

Todas estas BBS disponían de un rincón H/P/A/V/C (Hacking / Phreaking / Anarchy / Virii / Cracking), en donde los usuarios compartían herramientas y experiencias, o incluso algunas BBS se dedicaban integramente al tema, con lo que se convirtieron en un auténtico semillero.

Cuando las redes IRC comenzaron a sustituir a las BBS, en Undernet surgieron los canales #warezspain, #esphack o #!hispahack, que en 1993 daría lugar al grupo del mismo nombre. Algunos de los hackers más destacados en los 90 fueron miembros de !Hispahack, y gozaron de prestigio hasta que en 1998, la Guardia Civil detuvo a algunos de sus miembros por revelación de secretos y daños. Sólo uno de ellos fue juzgado, Jfs, y absuelto por inconsistencia de las pruebas. Este juicio fue el primero contra hackers en España, por lo que la sentencia sentó precedentes. Otros grupos de los 90 fueron Big Bro Killerz, Sindicato de Hackers Españoles, Legión Oscura o Konspiradores Hacker Klub (KHK). Mave, un joven madrileño de 19 años integrante de este grupo, se convirtió en el primer detenido por hacking en España[60], aunque su caso no llegó a juicio, quedó en un acuerdo para indemnizar a la Universidad Carlos III. Debido a estos casos sonados trascendió al público español la imagen del hacker asociada a una "internet oscura" y "underground".

Entre todos estos grupos destacaron 29A, el grupo más internacional de la escena española, y también el más prolífico en la creación de virus, para diferentes sistemas operativos, pero también los primeros en crear virus para PDAs (Dust) y móviles (Cabir). La colaboración internacional siempre ha estado presente, especialmente con otros grupos latinoamericanos. De esta colaboración surgió una gran base de datos de información denominada Página de Karpoff, la lista de correo CracksLatinos y los grupos Whiskey kon Tekila!, TNT!Crack!Team, MaGuNa teAM, Kr@cKerZ United Team o Askatasuna Krackers Society.

[60] Mercé Molist. "El primer detenido por 'hacking' en España fue un madrileño de 19 años". El Mundo. 01/02/2014. http://www.elmundo.es/tecnologia/2014/02/01/52eca305ca474133388b456d.html (Ú.a.: 02/09/2015)

Respecto al hacking puro, destacan varios hackers murcianos que dieron cuerpo a Iberhack[61], un sitio web que compiló multitud de enlaces en castellano, y promovió la primera UnderCon, inicialmente denominada SETCon en octubre de 1997. Además de hacking, en esta reunión con ánimo de convención americana, que reunió a un buen número de hackers españoles, se compartió mucha información muy interesante en aquel momento, como los 900 de acceso a internet de algunas grandes compañías como IBM, Samsung, Telefónica o Microsoft, y que todo el mundo quería poder usar[62].

***Figura 9**: Logo de la convención UnderCon. Fuente: Imagen obtenida de la web del proyecto libre Hackstory.net, via Google Images. http://hackstory.net/Hackstory.es_La_comunidad. (Último acceso: 02/09/2015).*

La segunda UnderCon, en 1998, resultó más exitosa, con la participación de 29A, The Den of the Demons (TDD), formado por un grupo de expertos en phreaking de cabinas telefónicas, y Com30, un grupo que trascendería poco después porque su detención propició la Operación Millenium, la mayor redada por phreaking en España, a cargo del entonces Grupo de Delitos Telemáticos de la Guardia Civil. Esta redada significó la detención de 55 personas en 16 provincias españolas, en enero del 2000, por presunta utilización fraudulenta de los números de teléfono gratuitos 900. Cuatro años después sin embargo, la mayoría de las sentencias fueron absolutorias[63], no se pudo probar que existiera una organización ni vinculación de los detenidos para producir el proceso de fraude, ya que la información se demostró que circulaba en numerosos foros, y otras muchas denuncias no prosperaron por defectos de forma.

[61] Iberhack. http://web.archive.org/web/19980201050415/http://iberhack.islatortuga.com/index.html (Ú.a.: 02/09/2015)
[62] JeCk's Page. Lineas 900. 09/11/1999. http://jeck.8m.com/900.htm (Ú.a.: 03/09/2015)
[63] Almeida Asociados. "Caso Millenium: no concurre prueba concreta del proceso de defraudación". 14/02/2005. http://www.bufetalmeida.com/54/caso-millenium-1-no-concurre-prueba-concreta-del-proceso-de-defraudacion.html (Ú.a.: 04/09/2015)

El caso resultó muy mediático y se explotó políticamente, al coincidir las detenciones con la organización en Madrid de las Primeras Jornadas sobre Delitos Cibernéticos de la Guardia Civil y la campaña electoral en marzo de 2000. Esta operación tuvo también un enorme impacto en la comunidad hacker, que profundizó en su carácter "underground". Los grupos se hicieron más cerrados y desconfiados, y algunos abandonaron su actividad.

Otro sitio muy conocido entre la comunidad hacker hispana fue Isla Tortuga, un portal que ofrecía alojamiento web a varios grupos de hackers, además de pornografía y "cracks" para juegos y programas. La Policía Nacional detuvo en 1997 a varios de los mantenedores del sitio, entre ellos Fer13, Angeloso y Maki. Se trató de la primera vez que se actuó en España contra un sitio web, y se hizo además con carácter de redada.

Pero el sitio de referencia de la comunidad hacker hispana fue IRC-Hispano. Los grupos y hackers vinculados al sitio fueron los promotores de muchas iniciativas en pro del software libre, entre ellas el proyecto LuCAS o la asociación Hispalinux. También fueron promotores de los primeros hackmeetings, inspirándose en las reuniones anuales organizadas por hackers italianos, que se convertirían en los actuales hackLabs. Entre la enorme actividad desarrollada surgieron también las primeras iniciativas de hacktivismo puro. En aquellas fechas, y con espíritu reivindicativo, tuvimos el virus Anti-Tel del grupo catalán Los Dalton, que en 1991 se quejaba de las elevadas tarifas de Telefónica. O el Anti-ETA creado por GriYo del grupo 29A en 1998, como protesta por el asesinato del concejal del PP Miguel Ángel Blanco, y que como payload (la parte maliciosa del malware) mostraba una mano blanca.

En este momento, el hacktivismo, tanto a nivel nacional como internacional, combina tres grupos principales:

1. Anonymous, componen el colectivo más conocido por el público. Sus miembros promueven la independencia de Internet y se oponen a todo aquel que impida la libre circulación de la información. Sus acciones se basan habitualmente en el uso del hacking, como ataques DDoS o el robo y distribución de información personal y/o confidencial. Ocasionalmente se centran más en actos llamativos que en los actos meramente políticos.

2. Ciberocupas (o ciberpunks), los verdaderos activistas. Utilizan Internet y las redes sociales de forma muy pragmática y en un sentido verdaderamente anarquista, fomentando las relaciones para la distribución de información y la construcción de una democracia más participativa. En este grupo cabe incluir a los ciberdisidentes que, al igual que sus homólogos en la vida real, han dejado de reconocer la legitimidad del poder político e incluso del estado de derecho, aún así, les motiva la pretensión de estar

reforzando la democracia y la lucha contra la corrupción en sus países, mediante acciones ideadas para tener una gran repercusión social.

3. Ciberguerreros, en este colectivo se encuadran los “patriotas” que forman "ciberejércitos", muy habituales en muchos países con tendencia totalitaria. Ocasionalmente podrían actuar siguiendo las directrices de los servicios secretos de sus gobiernos, o, en cualquier caso, actúan en función de intereses de carácter nacionalista, expansionista y extremista. Sus acciones se centran en deformar sitios web. Y, mediante el uso de ataques DDoS, tratan de bloquear y silenciar a los oponentes de las políticas de sus gobiernos. De las acciones de estos grupos se habla con más detalle más adelante.

El fenómeno Anonymous tiene sus orígenes en los foros de la web 4chan, creada en 2003 por Christopher Pool, conocido como ‘moot’. La web se organizaba como un imageboard ,o tablero, para la publicación de imágenes sobre manga, anime y hentai, y un segundo tablero denominado “/b/”, para cualquier otro tema. Este segundo foro se hizo muy popular porque permitía la publicación de imágenes y la discusión de forma anónima, al carecer de un sistema de registro. Tampoco los moderadores ni el sysop publicaban con su nombre, de hecho identificarse como moderador significaba la expulsión inmediata, porque podía resultar coactivo e impactar negativamente la participación y colaboración de otros usuarios. En inglés todas estas publicaciones anónimas están atribuidas al usuario genérico Anonymous, entendido no como un usuario particular sino como una comunidad de usuarios.

En 2006 se produjo el llamado ataque Habbo, que consistió en el bloqueo de usuarios a la piscina del mundo virtual Habbo-Hotel, únicamente se permitió el acceso de usuarios con avatares negros. La coordinación de los autores se realizó a través de los foros de 4chan.

Otro de los primeros objetivos fue en contra de la actividad de los pedófilos en Internet, destruyendo información e identificando a este tipo de usuarios. En 2007 Anonymous se atribuyó la identificación de Chris Forcand, un pedófilo canadiense que fue denunciado anónimamente y que más tarde sería arrestado por la policía de Toronto[64].

Anonymous ganó notoriedad a partir de 2008 cuando puso en marcha la operación Chanology[65], contracción de Chan (4chan) y Scientology, en contra de la secta Iglesia de la Cienciología, que en EE.UU. goza de gran presencia mediática dado que algunos de sus miembros son muy

[64] Jonathan Jenkins. “Man trolled the web for girls: cops”. Sun Media. 7/12/2007. http://cnews.canoe.com/CNEWS/Crime/2007/12/07/4712680-sun.html (Ú.a.: 04/09/2015)
[65] Howard Dahdah. “'Anonymous' group declares online war on Scientology”. Computerwold. 08/02/2008. http://www.computerworld.com.au/article/206359/_anonymous_group_declares_online_war_scientology_/ (Ú.a.: 03/09/2015)

conocidos. Las acciones de Anonymous se han centrado en desenmascarar el oscurantismo y los riesgos que sufren sus miembros al ser captados por la secta, de carácter muy destructivo. En una de estas acciones se convocó a una manifestación en Los Ángeles en la que los participantes utilizaron máscaras de Guy Fawkes, para evitar ser identificados por los miembros de la secta, que tienen la costumbre de grabar o fotografiar a la gente que se manifiesta en su contra.

Guy Fawkes fué un católico inglés, de carácter integrista, que apoyaba al Restauracionismo Católico en Inglaterra. Sirvió como mercenario en el Ejército Español en Flandes, y en 1605 participó en la conspiración para destruir con explosivos el Palacio de Westminster y asesinar al rey Jacobo I, junto a los Lores ingleses. Fawkes fue detenido, pero se negó a delatar a sus cómplices, declarando que su intención era acabar con las persecuciones religiosas, y finalmente se le ejecutó en la hoguera. A raíz del complot se ejerció una represión más fuerte contra los católicos, a los que se les negó el derecho de voto al Parlamento inglés hasta 1829. Aunque Fawkes nunca fue un lider de los conspiradores, su figura se recuerda en la Noche de las Hogueras (Bonfire Night en inglés), en la que es típico llevar una "careta" con su rostro.

En la película "V de Vendetta", de James McTeigue (2005), basada en la serie de comics del mismo nombre, escritos por Alan Moore e ilustrados por David Lloyd, y cuyo argumento es una distopía en la que en Inglaterra hay implantado un estado totalitario, el personaje principal ejecuta el plan original de Fawkes y oculta su identidad detrás de una de estas máscaras.

Anonymous utiliza copias de estas máscaras para mantener el anonimato de las personas que participan en las manifestaciones que convoca, y, aunque no es su logo oficial, sin embargo es el icono por el que son reconocidos mundialmente. Es necesario señalar, que esta máscara utilizada por los manifestantes que responden a las convocatorias de Anonymous, es el elemento de mayor venta en Amazon, que vende cientos de miles de unidades al año, y Time Warner, que posee los derechos de imagen como distribuidora de la película, recibe un porcentaje de cada máscara que se vende, lo que puede dar pie a cualquier conjetura. [66]

[66] Nick Carbone. "How Time Warner Profits from the 'Anonymous' Hackers". Time. 29/08/2011. http://newsfeed.time.com/2011/08/29/how-time-warner-profits-from-the-anonymous-hackers/ (Ú.a.: 02/09/2015)

Figuras 10 y 11: *El logo de Anonymous (Fuente: Wikipedia, https://es.wikipedia.org/wiki/Anonymous, accedida el 03/08/2015), y la máscara de Guy Fawkes, popularizada en la película "V de Vendetta" (Fuente: WhyWeProtest, https://whyweprotest.net/threads/simple-poster.100865/ , vía Google Images, accedida el 17/09/2015), los dos iconos de referencia del movimiento.*

Al margen de estas convocatorias en el mundo real, el campo de batalla de Anonymous se centra en Internet, y sus acciones se desarrollan en contra de cualquier intento de regular la Web. Sus objetivos no son muy complejos, generalmente se centran en dejar uno o varios sitios web inaccesibles, utilizando software diverso, como LOIC (Low Orbit Ion Cannon, algo así como Cañon de iones de órbita baja), una herramienta de código abierto para pruebas de red, capaz de sobrecargar de consultas el sitio web elegido hasta saturarlo, provocando que deniegue el servicio (ataque distribuido de denegación de servicio, o DDoS). La atribución de las operaciones se realiza publicando videos reivindicativos, generalmente con una gran calidad de imagen y utilizando voz sintética. Estos videos siempre concluyen con la misma frase: "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us." (Somos Anonymous. Somos legión. No perdonamos. No olvidamos. Espéranos).

En noviembre de 2010 Wikileaks comenzó a publicar información sobre las comunicaciones del Departamento de Estado de EE.UU. con otros gobiernos, y comunicaciones internas durante las guerras de Iraq y Afganistán, en lo que se conoció como Cablegate[67]. La respuesta del gobierno norteamericano fue intentar silenciar a Wikileaks, suspender su cuenta de PayPal, y perseguir y tratar de procesar de algún modo a su responsable, Julian Assange.

[67] Press Release. "Wikileaks empieza a publicar cables diplomáticos de la embajada de EE.UU.". Wikileaks. 28/11/2010. https://wikileaks.org/Wikileaks-empieza-a-publicar.html (Ú.a.: 15/09/2015)

Un ciberguerrero, conocido como The Jester (th3j35t3r), se atribuyó el cierre temporal de Wikileaks, que se reprodujo a continuación en una veintena de sitios diferentes (mirrors). Uno de estos sitios se estableció en Rusia por mediación de un proveedor de dudosa reputación, Heihachi Ltd., relacionado con el cibercrimen ruso, y, a partir de diciembre, el tráfico de Wikileaks comenzó a ser redirigido con preferencia desde su dominio oficial a este sitio. Spamhaus[68], una organización internacional que se dedica a realizar un seguimiento de la actividad de spam y determinar su origen, y es responsable de las listas anti-spam de mayor difusión en Internet, avisó de los riesgos de acceder al sitio ruso, y recibió inmediatamente un severo ataque DDoS.

En los días siguientes todas las compañías que pusieron alguna traba a Wikileaks, inmediatamente fueron víctimas de ataques DDoS. Estas actuaciones fueron posteriormente reivindicadas por Anonymous, y enmarcadas dentro de la Operación Payback. A los hacktivistas se les pedía que descargaran LOIC y usaran su función "hive mind" para convertir su máquina en un bot voluntario, y realizar ataques coordinados.

La operación se amplió mucho más tras los primeros análisis de la información publicada en Wikileaks. Varios países fueron acusados de violar la libertad de expresión en Internet y sus organismos oficiales comenzaron a recibir ataques. Varios ciberguerreros, entre ellos Jester, se mantuvieron muy activos tratando de desenmascarar a otros hacktivistas que estuvieran colaborando con Anonymous. Cuando se produjeron varios arrestos en EE.UU., Reino Unido y Paises Bajos, la policía se convirtió también en objetivo.

Aaron Barr, CEO de HBGary Federal, una empresa del sector de la seguridad informática, quiso sumarse a las acciones de los ciberguerreros y anunció que proporcionaría al FBI toda la información que había recopilado sobre Anonymous. Inmediatamente los servidores de la empresa comenzaron a ser atacados utilizando técnicas de inyección SQL, que permitieron acceder a más de 70.000 mensajes de correo que fueron hechos públicos [69] [70] [71]. El contenido de algunos de estos mensajes obligó a Barr a dimitir a las pocas semanas[72]. La empresa también recibió duras críticas, muy desestabilizadoras, hasta el punto de que fue absorvida por ManTech International unos meses después.

---

[68] Spamhaus. https://www.spamhaus.org/ (Ú.a.: 07/09/2015)
[69] Brian Krebs. "HBGary Federal Hacked by Anonymous". Krebs-on-Security. 07/02/2011. http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/ (Ú.a.: 07/09/2015)
[70] Kim Zetter. "Anonymous Hacks Security Firm Investigating IT; Releases E-mail". Wired. 07/02/2011. http://www.wired.com/2011/02/anonymous-hacks-hbgary/ (Ú.a.: 07/09/2015)
[71] BBC News. "Anonymous hackers attack US security firm HBGary". 07/02/2011. http://www.bbc.com/news/technology-12380987 (Ú.a.: 07/09/2015)
[72] Andy Greenberg. "HBGary Federal's Aaron Barr Resigns After Anonymous Hack Scandal". Forbes. 01/03/2011. http://www.forbes.com/sites/andygreenberg/2011/02/28/hbgary-federals-aaron-barr-resigns-after-anonymous-hack-scandal/ (Ú.a.: 07/09/2015)

Por otro lado, desde enero de 2011, Anonymous comenzó a prestar su apoyo a la Primavera Árabe, poniendo en marcha la Operación Túnez. Inicialmente se trataba de proteger el acceso al sitio principal de Wikileaks en Túnez, posteriormente la necesidad de difusión de información por parte de la población hizo que se generara una intensa actividad en redes sociales, especialmente en Twitter, haciendo causa común con manifestantes locales y periodistas internacionales. Los objetivos sin embargo degeneraron cuando las protestas contra el régimen tunecino de Ben Alí se convirtieron en disturbios con decenas de muertos, que comenzaron con la inmolación a lo bonzo de Mohamed Bouazizi.

Anonymous se atribuyó una decisiva participación en el éxito de la "Revolución de los Jazmines" en Túnez, pero está sin acreditar. No obstante a través de AnonNews llamó sucesivamente a la movilización en Egipto, Arabia Saudí, Argelia, Libia, Bahrein, Siria, Jordania, Yemen y Marruecos. Estos llamamientos fueron seguidos de ataques para deformar sitios web oficiales.

En enero de 2012 Anonymous abrió un nuevo frente con la Operación Blackout (apagón), para protestar contra el proyecto de ley SOPA (Stop Online Piracy Act)[73]. La iniciativa presentada por el diputado republicano por Texas, Lamar Smith, tenía por objeto mejorar la protección de la propiedad intelectual en Internet, combatiendo el tráfico de contenidos sujeto a derechos de autor, actuando contra el sitio que aloje estos contenidos, y bloqueando el acceso a la publicidad, a las redes de pago que provean al sitio de beneficios y a los enlaces que permitan acceder a él. La ley incluía la posibilidad de que los proveedores de servicio bloqueen el acceso al sitio considerado infractor en caso de que se encuentre en el extranjero. Este punto resultó especialmente conflictivo, porque el procedimiento que permitiría ese bloqueo, obligaría a identificar las IP de los clientes y obligar a los proveedores a participar de una inspección profunda de paquetes, consistente en analizar todo el contenido transmitido de y hacia el usuario, violando la privacidad y planteando un problema de seguridad. Esta inspección ya había sido rechazada en 2003 por el Congreso al suprimir el programa TIA, aunque una cobertura legal de un método de inspección profunda de paquetes es posiblemente la mayor aspiración de los servicios de cibervigilancia norteamericanos.

Las empresas productoras de contenidos apoyaron inmediatamente el proyecto, y se sumaron las empresas farmacéuticas, encabezadas por Pfizer (fabricante de Viagra), que se consideraban perjudicadas por la distribución a través de Internet de productos farmacéuticos falsificados. En contra se levantó una enorme diversidad de opositores, entre los que figuraban la práctica totalidad de proveedores de acceso y grandes empresas de Internet , así como otras tecnológicas,

[73] SOPA. https://es.wikipedia.org/wiki/Stop_Online_Piracy_Act (Ú.a.: 07/09/2015)

pero también organizaciones defensoras de la libertad de expresión. La protesta se hizo global cuando Wikipedia decidió realizar un apagón del site [74].

Figura 12: *162 millones de internautas vieron el "apagón" de Wikipedia, realizado en sintonía con la Operación Blackout convocada por Anonymous para protestar contra SOPA. (Fuente: https://en.wikipedia.org/wiki/File:Wikipedia_Blackout_Screen.jpg. Ultimo acceso: 17/09/2015)*

Durante semanas Anonymous atacó sucesivamente a Sony, Fox News, la red de televisiones PBS, Nintendo, Gawker Media, y a especialistas de seguridad que colaboraban de forma habitual con el FBI. Algunos de estos ataques al parecer fueron liderados por el grupo escindido Gn0sis, muy activo y formado por hackers de nueva generación, más motivados por la diversión de mal gusto (lulz) que por el activismo. Durante los meses siguientes desplegaron una gran actividad en los canales IRC bajo el nombre de Lulz Security (LulzSec), desmarcándose de Anonymous con agrias polémicas y enfrentamientos, y realizando multitud de acciones de pirateo. Una de estas acciones incluyó un intento de control de AnoNews.org. Durante los cuatro meses siguientes 650 hackers vinculados con esta facción fueron identificados y denunciados por la policía. Su lider Sabu permanece en prisión desde 2011. Podría especularse con la idea de una depuración, pero no está totalmente acreditado.

[74] Wikipedia: Protesta contra SOPA. https://es.wikipedia.org/wiki/Wikipedia:Protesta_contra_SOPA (Ú.a.: 17/09/2015)

La corriente principal de Anonymous se centró en otros objetivos (#OperationGreenRights[75]), incrementando la actividad y el número de ataques. A raiz del accidente de la planta nuclear de Fukushima en Japón, varias empresas eléctricas fueron objeto de ataques, entre ellas ENEL, General Electric, EDF y Endesa. A ello se sumaron los ataques a Monsanto y Bayer, y empresas del sector petrolífero, Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil, The Royal Bank of Scotland o The Canadian Association of Petroleum Producers.

En enero de 2012 el cierre del site Megaupload desató una nueva ola de ataques a sitios de empresas del sector de la producción de contenidos. El cierre coincidió además con el debate sobre el Acuerdo Comercial Anti-falsificación (ACTA, siglas en inglés de Anti-Counterfeiting Trade Agreement), provocando ataques muy virulentos contra sitios oficiales de varios gobiernos [76].

La ausencia de estructura y el anonimato hacen de Anonymous más una idea que un grupo. Cualquiera puede proponer un objetivo, y, una diversidad de usuarios de Internet en todo el mundo, puede decidir sumarse y promover un ataque. En cambio otras operaciones pueden no pasar de bromas de mal gusto (lulz), o convertirse en operaciones quasimafiosas, si hablamos del robo de datos bancarios.

Del mismo modo no son inusuales las falsas atribuciones, desmentidos, desinformación y paranoia, llegando incluso a atribuir las acciones de Anonymous a los servicios secretos de los gobiernos, en una acción de control social muy calculada[77].

El 9 de agosto de 2011 se publicó un video en YouTube, atribuido a Anonymous, en el que se anunciaba el fin de Facebook para el 5 de noviembre, fecha de la muerte de Guy Fawkes, una condena motivada por la falta de respeto de Facebook a la privacidad de los usuarios. En las fechas siguientes se publicaron varios desmentidos, pero hasta el 6 de noviembre, en que Facebook siguió operando normalmente, no pudo confirmarse qué mensajes eran atribuibles a Anonymous. Podrían haberlo sido todos o ninguno. De hecho cualquier grupo de hackers suficientemente motivado hubiera podido aceptar el reto. El fake por cierto se repitió en 2014 [78].

La diversidad de motivaciones es muy ámplia. No dejan de incorporarse nuevos hackers a la comunidad, en tanto los más antiguos adquieren una conciencia más política y evolucionan a cometidos más específicos para mejorar la comunicación, desarrollar un periodismo

[75] #OperationGreenRights. http://operationgreenrights.blogspot.com.es/ (Ú.a.: 08/09/2015)
[76] "Anonymous takes down government sites in massive anti-ACTA attack". RT. 17/02/2012. http://www.rt.com/usa/anonymous-fff-consumer-acta-609/ (Ú.a.: 08/09/2015)
[77] Frank Mason. "AnonNews.org run by United States government". Internet Chronicle. 06/03/2011. http://chronicle.su/2011/03/06/anonnews-org-run-by-united-states-government/ (Ú.a.: 07/09/2015)
[78] Cinco Días. "La vieja amenaza de Anonymous a Facebook que terminó en nada". 04/11/2014. http://cincodias.com/cincodias/2014/11/03/lifestyle/1415038380_253498.html (Ú.a.: 08/09/2015)

participativo, similar a Wikipedia (lo que Anonymous denomina *periodismo de masas*), desarrollar métodos para realizar operaciones más sofisticadas, que incluyan una estrategia que incorpore a activistas y ciberactivistas, e incluso sumar expertos en derecho y abogados, que promuevan la legalización de algunas formas de ataques DDoS.

Un ejemplo paradigmático del desarrollo de la filosofía ciberocupa lo hemos tenido en España, a raíz de la aparición del movimiento 15M. El 15 de mayo de 2011, coincidiendo con la Primavera Árabe, el movimiento de los indignados, surgido tras la publicación del manifiesto ¡Indígnaos![79] (Indignez-vous!, en el original francés), del escritor Stèphane Hessel, convocó una manifestación para protestar por las consecuencias sociales de la crisis económica, la corrupción institucionalizada y promover una democracia más participativa. La convocatoria consiguió un éxito de movilización. Parte de ese éxito se produjo por el soporte del ciberactivismo. Sin embargo, es a partir de las acampadas en la Puerta del Sol en Madrid, cuando la coordinación entre activistas, muchos de ellos con perfil político, y ciberactivistas se vuelve más íntima, y el uso de las tecnologías se desarrolla de forma natural para la consecución de los objetivos del movimiento.

El 20 de febrero de 2011 se había creado la "Plataforma de coordinación de grupos pro-movilización ciudadana", un grupo de Facebook formado por representantes de colectivos con el fin de convocar la manifestación masiva del 15M y la redacción de un manifiesto. Y el mismo 16 de marzo, el grupo de Facebook se transforma en la plataforma Democracia Real Ya[80], donde se activa una web con un manifiesto y propuestas políticas para España.

En lo que afecta a nuestro país hemos de hablar propiamente de transformación social.

Lo que está por ver en los próximos años, dada la convergencia que se ha producido de activismo y ciberactivismo, e igual que el activismo ha accedido a los recursos del poder para desarrollar sus propuestas de acción política, es si el nuevo legislador, y la totalidad de la sociedad, es capaz de superar la brecha tecnológica intergeneracional y adopta las tecnologías de la información como recurso esencial del ejercicio democrático. Hablaríamos entonces de ciberdemocracia.

Pero todas estas motivaciones que se han señalado, conducidas dentro de los parámetros de la ética hacktivista, no pueden distraer del hecho de que existen hackers, y grupos de hackers, como los ciberguerreros, con otras motivaciones, que pueden malograr el ciberactivismo como resultado de un aumento de la criminalización y el recelo de los gobiernos, que temen por las

[79] ¡Indignaos!. https://es.wikipedia.org/wiki/%C2%A1Indignaos! (Ú.a.: 18/09/2015)
[80] ¡Democracia Real YA!. http://www.democraciarealya.es/ (Ú.a.: 08/09/2015)

actividades económicas y las infraestructuras críticas. Algunos autores plantean la posibilidad de que estemos al borde de una guerra civil digital.

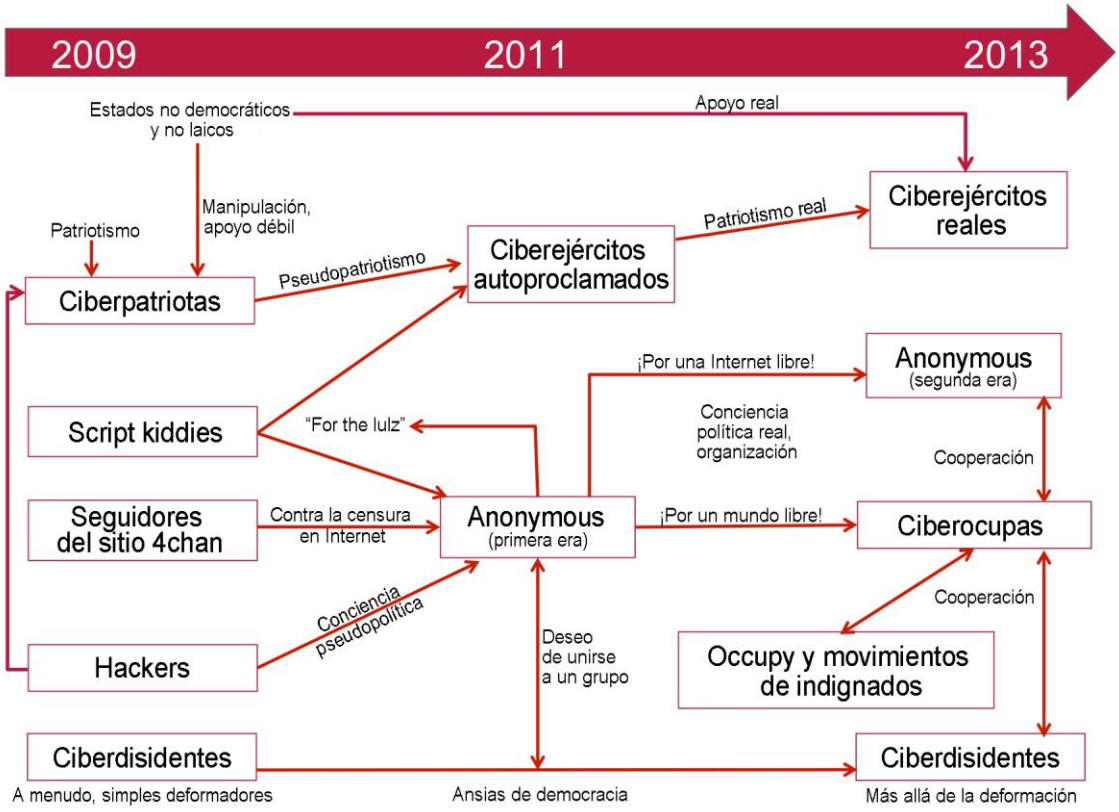

Figura 13: *Evolución del ciberactivismo en función de las motivaciones que Anonymous y otros grupos han expresado en sus acciones. Fuente: François Paget. "Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas". McAfee Labs, 2012. (p.31).* http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf?view=legacy *(Último acceso: 08/09/2015)*

2.3 Ciberespacio e Internet.

Internet es el conjunto de redes de comunicación que se interconectan utilizando los protocolos IP, de forma que, pese a su heterogeneidad, funciona como una red única de alcance global. En principio las redes que la conforman son redes de ordenadores, que acceden a servicios ofrecidos por una enorme diversidad de servidores. El servicio más universal es sin duda la web. Conforme las redes de telefonía han ofrecido servicio de acceso a datos, y han aumentado las capacidades de los dispositivos móviles, incorporando sistemas operativos que pueden ejecutar aplicaciones diversas, internet se ha ido ampliando y absorviendo otras redes. Muchos servicios

han migrado de sus redes específicas a utilizar internet, como es el caso de la telefonía IP (VoIP). Esta tendencia es más acentuada en entornos empresariales, sujetos a costes elevados de comunicaciones. En septiembre de 2015 ha entrado en vigor en España el proyecto CORA, el megacontrato de la Administración del Estado con Telefónica para que esta empresa sea su proveedor exclusivo de comunicaciones de la red multiservicio, servicios móviles e internet (lotes 1, 2 y 3). Este contrato afecta a todos los ministerios, inicialmente se incorporan a CORA los ministerios de Fomento y Ciencia y Tecnología, pero conforme terminen sus actuales contratos el resto de ministerios, se irán sumando al proyecto CORA. En enero de 2017 se sumará el Ministerio de Hacienda y Administraciones Públicas, que actualmente tiene contrato de exclusividad de sus comunicaciones con BT. Con la incorporación de este ministerio, que soporta todos los organismos de la Administración Periférica del Estado, quedará establecida una red de comunicaciones integral y toda la Administración del Estado pasará a utilizar telefonía IP. Las comunicaciones internacionales serán gestionadas por BT (lote 4).

La demanda de contenidos multimedia ha ocasionado que también otros medios hayan ido convergiendo hacia internet, como la televisión (IPTV) y las SmartTV, o las videoconsolas para juegos en línea. Pero más allá de internet existe aún todo un conjunto de redes que teóricamente están separadas de ella, redes transaccionales de flujos de dinero, operaciones del mercado de valores, transacciones de las tarjetas de crédito, redes de control de servicios, transporte, seguridad, redes dotadas de dispositivos de sensorización y control. El conjunto de todas estas redes conforman el ciberespacio.

Poco a poco muchas de estas redes también han ido conectando sus dispositivos para poder gestionarlos remotamente haciendo uso de internet, la mayoría de dispositivos domóticos y de seguridad son dispostivos activos que ofrecen acceso por protocolo http para su gestión remota. En este momento tecnológico hablamos ya de una faceta de internet a la que denominamos como *internet de las cosas* (IoT, Internet of Things).

El primero de este tipo de dispositivos conectado directamente a internet fue una máquina de Coca-Cola, situada en la Carnegie Mellon University en 1982[81], situada actualmente en la sexta planta del edificio Gates. Informaba sobre la disponibilidad de cada tipo de bebida y si ya se habían enfriado las que se reponían. Después llegó la avalancha. Ya no son sólo dispositivos que ofrecen servicios a las personas comunicándose por internet, sino que toda una diversidad de objetos cotidianos dotados de procesadores, se comunican entre sí, operan conjuntamente o son gestionados por otros dispositivos de forma remota.

[81] CMU SCS Coke Machine. https://www.cs.cmu.edu/~coke/ (Ú.a.: 18/09/2015)

Según Wikipedia, fue Bill Joy quién imaginó en primer lugar la comunicación D2D (del inglés: Device to Device, dispositivo a dispositivo), en 1999 en el Foro Económico Mundial de Davos. Sin embargo fue Kevin Ashton quien propuso por primera vez el término, en el Auto-ID Center del MIT en 1999, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores.

Sin embargo, conforme ha ido creciendo el ciberespacio, y se han incrementado las posibilidades de gestión de estas redes desde internet, se han incrementado las vulnerabilidades. La mayoría de fabricantes de dispositivos han favorecido en sus diseños los servicios de conectividad, sin preocuparse de la seguridad, lo que provoca que cada vez más redes sean vulnerables a ataques de hackers.

Samsung, el fabricante lider mundial de SmartTV, declaró recientemente su renuncia de responsabilidad ante la posibilidad de que la webcam integrada en sus televiores pudiera ser accesible por usuarios remotos, como demostraron SeungJin 'Beist' Lee y Seungjoo Kim, investigadores del CIST (Center for Information Security Technlogies) de la Korea University en la convención Black Hat de 2012[82] [83]. El profesor Seungjo Kim es además consultor habitual del gobierno en temas de e-Government y de los servicios nacionales de inteligencia coreanos, NISK (National Intelligence Service of Korea).

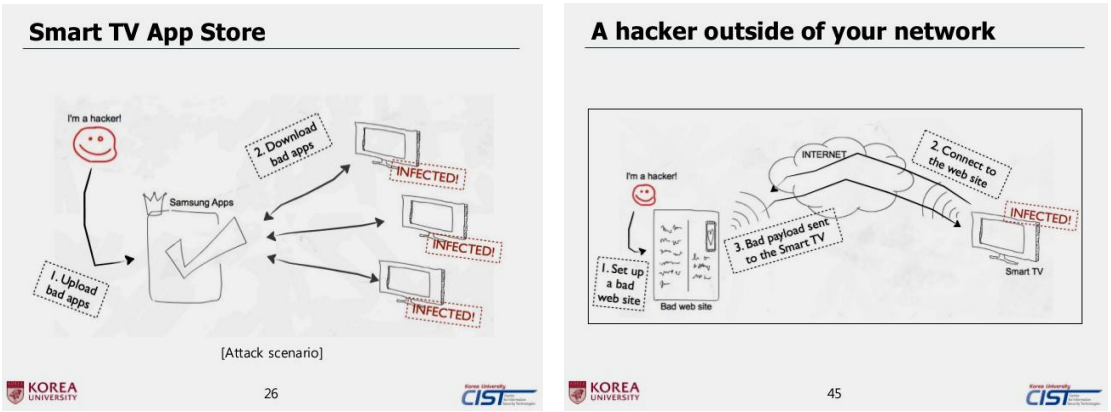

Figura 14: *Métodos de ataque a las SmartTV de Samsung probados por SeungJin Lee y Seungjoo Kim. Fuente: Presentación "Smart TV Security. 1984 in 21st century". (p.26 y 45)* *http://www.slideshare.net/skim71/smart-tv-security-1984-in-21st-century (Último acceso 17/09/2015).*

[82] 'Ms. Smith'. "Black Hat: Smart TVs are the 'perfect target' for spying on you". Network World. 02/08/2013. http://www.networkworld.com/article/2225091/microsoft-subnet/black-hat--smart-tvs-are-the--perfect-target--for-spying-on-you.html (Ú.a.: 10/09/2015)

[83] SeungJin 'Beist' Lee y Seungjoo Kim. "Smart TV Security". 08/03/2013. CIST. Korea University. http://www.slideshare.net/skim71/smart-tv-security-1984-in-21st-century (Ú.a.: 17/09/2015)

Estos televisores equipan el SO Tyzen, basado en el kernel de Linux. Existen algunas vulnerabilidades conocidas para los que están disponibles diferentes exploits en el mercado negro[84]. La autenticación es muy débil. El protocolo es muy simple en términos de autenticación y el paquete de autenticación sólo necesita una dirección IP, una dirección MAC y un nombre de host para la autenticación. Pero no es capaz de manejar valores Null, con lo que el protocolo se puede romper fácilmente, cualquier dispositivo con valor Null en su dirección MAC se puede conectar a la SmartTV.

Por otro lado, un hacker puede hackear e instalar malware a través de las API de la televisión como File.Unzip o Skype, que pueden ser usadas para copiar archivos o instalar una puerta trasera.

Por último un hacker podría intentar un ataque MIM (Man-in-the-Middle) proporcionando un certificado falsificado, porque el software no comprueba la autenticidad de los certificados del software descargado desde los servidores de Samsung.

Las SmartTV de LG, que también utilizan OS de código abierto, en este caso WebOS, adolecerían de vulnerabilidades similares. Muy probablemente, como señala el International Institute of Cyber Security, no tardaremos en encontrar noticias sobre desarrollo de malware específico y ataques a este tipo de dispositivos, que además no disponen por el momento de ninguna solución antivirus o antimalware.

Si bien la violación de la privacidad es una consecuencia muy grave para el usuario, las consecuencias de un ataque malicioso pueden llegar mucho más allá. Se han descrito ataques sobre dispositivos electrodomésticos a los que se ha hecho fallar y cortocircuitar provocando su encendido y apagado a frecuencias a partir de 200 veces por segundo[85]. La comodidad de encender el horno microondas antes de llegar a casa puede traducirse en un incendio de la vivienda.

Alex Drozhzhin, analista de seguridad de Kaspersky Daily, ha recopilado multitud de ataques a los dispositivos más variopintos[86]. Según describe en su artículo, David Jacoby demostró en

[84] "Cómo hackear fácilmente su SmartTV: Samsung y LG". Noticias de Seguridad Informática. 07/07/2015. http://noticiasseguridad.com/tecnologia/como-hackear-facilmente-su-smart-tv-samsung-y-lg/ (Ú.a.: 10/09/2015)
[85] Ciberseguridad. "Así pueden 'hackearte' cualquier aparato conectado a Internet". El País. 23/07/2015. http://tecnologia.elpais.com/tecnologia/2015/07/10/actualidad/1436539664_188672.html (Ú.a.: 10/09/2015)
[86] Alex Drozhzhin. "El Internet de las Cosas Inútiles". Kaspersky Labs. 19/02/2015. https://blog.kaspersky.es/internet-de-las-cosas-inutiles/5423/ (Ú.a.: 10/09/2015)

varias InfoSec como hackear su propia casa domótica[87]. Billy Rios de Laconiclt se atribuye el hackeo de un túnel de lavado a través de la mensajería de Facebook. Vasilis Hiuorios, un experto en seguridad de Kaspersky Labs, mostró en la Cumbre de Analistas de Seguridad 2015 (The SAS 2015), como piratear un sistema de vigilancia policial. Otro experto de Kaspersky, Roman Unucheck, demostró el hackeo de una pulsera de fitness en la misma cumbre de seguridad, lo que permitiría conocer la ubicación exacta de su propietario.

HP presentó a finales de 2014 un informe sobre seguridad de los dispositivos IoT[88], resultado del análisis de un ámplio abanico de dispositivos de numerosos fabricantes, entre los que se encontraban SmartTVs, webcams, termostatos caseros, bases de enchufes eléctricos controlados remotamente, controladores de sistemas de incendios, smarthubs caseros para control de múltiples dispositivos, cerraduras automatizadas, alarmas domésticas, básculas electrónicas, puertas de garage automatizadas…, todos ellos dispositivos que disponían de alguna forma de acceder a servicios en la nube y que incluían Apps para controlarlos o acceder remotamente desde dispositivos móviles.

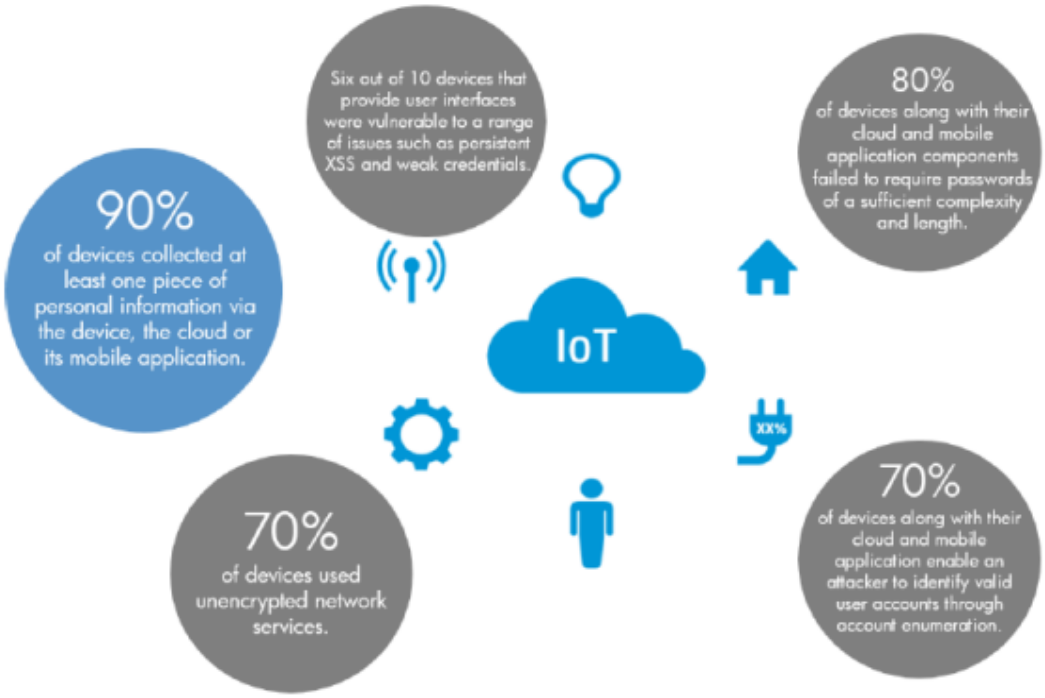

Figura 15: *Conclusiones del informe HP sobre seguridad de los dispositivos IoT. Fuente: Gary Audin. "Hacking IoT". No Jitter. 15/08/2014.* http://www.nojitter.com/post/240168874/hacking-iot *(Último acceso: 17/09/2015).*

[87] Dennis Fisher. "David Jacoby on Hacking His Home". ThreatPost. 24/09/2014. https://threatpost.com/david-jacoby-on-hacking-his-home/108517/ (Accedido a través de Kaspersky Labs http://t.co/0tDXbMBvxi). (Ú.a.: 10/09/2015)

[88] "Internet of Things Research Study". Hewlett Packard, Septiembre de 2014. http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf (Ú.a.: 17/09/2015).

La investigación indicó que el 80% de los dispositivos disponían de procedimientos de autenticación muy débiles. El 70% de los dispositivos no encriptaban la información al transmitirla por internet. El 60% de los interfaces con las webs accedidas eran inseguras, disponían de un sistema de credenciales muy débil y eran vulnerables a ataques. Todo el firmware y el software implementado en los dispositivos era extremadamente sencillo e inseguro. Por último, el 90% de los dispositivos recolecta algún tipo de información personal, a través del propio dispositivo, la conexión a internet o la aplicación en el móvil.

TrendMicro por otro lado identificó varios tipos de ataques que podían aprovechar las vulnerabilidades de los dispositivos IoT[89]:

- Ataques con sniffers, dispositivos capaces de leer y robar la información no encriptada que se transmite a través de una red de comunicación (vía internet, WiFi, bluetooth), y que permitirían a un atacante acceder posteriormente y controlar los dispositivos u obtener cualquier información.

- Ataques de denegación de servicio, que permitirían a un atacante bloquear el acceso a un dispositivo o a la aplicación que lo controla, inutilizando alarmas y dispositivos de seguridad o control.

- Ataques que aprovechen la debilidad de los procedimientos de encriptado, accediendo a la información, las claves, y posteriormente comprometiendo los sistemas.

- Ataques que vulneren los procedimientos de autenticación, obteniendo las claves de acceso a las redes y dispositivos, dado que la mayoría de dispositivos utilizan claves maestras que los usuarios no se preocupan de cambiar, o muy sencillas de obtener por procedimientos de fuerza bruta.

- Ataques Man-in-the-Middle (MiM), donde el atacante suplanta al servidor o web al que se conecta el dispositivo aportando certificados falsificados, o que no son comprobados por el dispositivo.

Ante estos riesgos, además de recomendar a los fabricantes que incrementen la seguridad y fiabilidad del software de sus dispositivos y Apps, TrendMicro recomienda a los usuarios domésticos de tecnologías IoT, que habiliten todas las opciones de seguridad en todos los dispositivos (incluidas redes domésticas por Bluetooth), disponer siempre de las últimas

[89] "The Internet of Everything: Layers, Protocols and Possible Attacks". TrendMicro. 23/09/2014. http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/ioe-layers-protocols-and-possible-attacks (Ú.a.: 17/09/2015).

actualizaciones de firmware en los dispositivos, bloquear todos los puertos y protocolos de comunicación que no se utilicen tanto en los dispositivos IoT como en los smarthubs que les proporcionan la conectividad, usar claves robustas, instalar parches para las vulnerabilidades existentes, tan pronto como estén disponibles, y encriptar siempre las comunicaciones.

El mundo de las videoconsolas tampoco está exento de incidentes. Posiblemente el más sonado haya sido el ataque masivo que sufrió la red PSN, Play Station Network de Sony, en 2011, en el que quedaron expuestos los datos de todos los clientes de la red, nombres, fechas de nacimiento, direcciones de correo electrónico, preguntas de seguridad y detalles de las tarjetas de crédito. En principio Sony achacó la caida de la red a una extensión de los ataques de Anonymous contra la compañía, pero posteriormente y por el tipo de información comprometida, se hizo evidente que el ataque había sido mucho más sofisticado que un ataque DDoS, posiblemente se utilizaron técnicas de inyección SQL, o alguna vulnerabilidad del firmware de las videoconsolas PS3. Lo que quedó también al descubierto es que Sony, incomprensiblemente, no encriptaba la información de sus clientes, ni las passwords ni los datos de las tarjetas de crédito. El objetivo no era provocar la falta de servicio a los clientes de Sony, sino obtener datos valiosos de los clientes[90]

Sin embargo, y aunque derechos fundamentales de los usuarios ,como la privacidad, se vean comprometidos, el verdadero riesgo, que lo convierte en una cuestión de estado, lo representan los sistemas de control de infraestructuras críticas. Richard A. Clarke y Robert K. Knake, en su libro “Guerra en la Red”[91], recopilan varios casos de ataques a sistemas de supervisión, control y adquisición de datos (SCADA) de varias redes de suministro de servicios básicos.

Según un estudio sobre seguridad de las redes eléctricas en EE.UU., un 20% de los dispositivos de control son accesibles mediante señales de radio, entre el 40% y el 80% están conectados a las redes de control interno de las compañías eléctricas, y cerca del 50% dispone de conexión a internet.

En 2003, el gusano Slammer logró infiltrarse en los sistemas SCADA de la red de suministro eléctrico y relentizó los controles. Un árbol caido en una línea de Ohio provocó un repentino aumento de tensión, y los dispositivos que debían impedir un efecto cascada fallaron. El resultado fue que ocho estados, dos provincias canadienses y 50 millones de usuarios quedaron sin servicio eléctrico. El apagón afectó secundariamente al acueducto de Cleveland. Aunque no fue un ataque directo, sin embargo en 2007, se utilizó el mismo procedimiento para atacar deliberadamente la red de suministro eléctrico en Brasil.

[90] Kevin Poulsen. “Play Station Network Hack. Who did it?”. Wired. 27/04/2011. http://www.wired.com/2011/04/playstation_hack/ (Ú.a.: 15/09/2015)
[91] Richard A. Clarke y Robert K. Knake. “Guerra en la red. Los nuevos campos de batalla”. Ed. Planeta, 2011. (pp. 131 – 142)

Para probar si un ataque podría provocar daños más graves, se realizó el experimento Aurora (The Aurora Generator Test[92]), en una red aislada en Idaho con generadores síncronos diesel de 2,5MW controlados desde un sistema SCADA con conexión remota. Los hackers participantes se hicieron con el control del sistema, encontraron el programa que gestionaba los interruptores de conexión a la red y los relés de protección (que actúan al cabo de unos 15 ciclos), y variaron sus parámetros, abriéndolos y cerrándolos fuera de sincronía (por debajo de los 15 ciclos). Cada vez que se cerraban los interruptores sin que llegaran a actuar los relés de protección, el choque provocado por el par de sincronización era tan brusco que el rotor del generador no lo soportaba. El efecto es equivalente al que produce en un automóvil, meter la marcha atrás cuando se circula a gran velocidad por una autopista, o acelerarlo a tope en punto muerto y meter bruscamente una marcha. El generador explotó y se desintegró al cabo de tres minutos.

Figura 16: *El generador diesel utilizado en el experimento Aurora humeando y sacudiéndose al salir de régimen. (Fuente: Wikipedia. https://en.wikipedia.org/wiki/Aurora_Generator_Test (Último acceso 17/09/2015)*

Como consecuencia, la Comisión Federal de Regulación de la Energía (FERC), exigió en 2010 que las compañías eléctricas norteamericanas desarrollaran planes de contingencia y medidas de seguridad específicas para proteger sus infraestructuras ante este tipo de vulnerabilidades,

[92] The Aurora Genarator Test. Wikipedia. https://en.wikipedia.org/wiki/Aurora_Generator_Test (Ú.a.: 17/09/2015)

penalizando desde 2012 a aquellas que no hayan tomado medidas preventivas. Como resultado de las actividades de auditado y protección de los sistemas SCADA de la red de distibución eléctrica, se descubrió que una enorme cantidad de sistemas habían sido infectados y se les había instalado puertas traseras y bombas lógicas, que en caso de ser activadas hubieran provocado daños cuantiosos e irreversibles en toda la red, inhabilitándola de forma permanente. Los auditores de seguridad especularon entonces con la posibilidad de que un ataque hacker menos malicioso, o incluso una maniobra de los operadores de los sistemas, hubiera podido activar accidentalmente las bombas lógicas, provocando fortuitamente sus devastadores efectos.

Aunque no se pudo atribuir quiénes fueron los autores del hackeo de la red eléctrica, un precedente del uso de este tipo de software malicioso podría ofrecer algunas pistas.

En la década de los 80, los servicios secretos soviéticos estuvieron muy interesados en adquirir información sobre varias tecnologías occidentales de carácter comercial e industrial, en especial para su industria de gas y petróleo. Un agente soviético que desertó a Francia entregó a los servicios secretos de este país un listado de todas estas tecnologías. Las actividades para obtenerlas continuaron durante años, mientras el contraespionaje occidental facilitaba a los soviéticos el acceso a diseños modificados. Uno de los diseños obtenidos por los rusos de una firma canadiense fueron los automatismos y software de control de las bombas y válvulas de su red de gasoductos, que se extiende desde Siberia hasta sus clientes en Europa Occidental. El software de estos automatismos funcionó inicialmente de forma correcta, sin embargo después de un tiempo comenzó a funcionar mal (no está acreditado si con conocimiento de la administración del presidente Ronald Reagan). El software hizo que en un tramo del gasoducto una de las bombas trabajara a máxima potencia, mientras que se cerraba la válvula hacia la que se dirigía el flujo. La presión del gas provocó una explosión de más de tres kilotones (tres veces la potencia de la bomba lanzada en Hiroshima), y está considerada la detonación no nuclear más potente de la Historia[93].

2.4. Ciberdelincuencia y Ciberterrorismo.

A finales de la pasada década, y con más intensidad desde 2007, se observó entre los administradores de sistemas y servicios de alerta de seguridad en tecnologías de la información, una estabilización en el número de incidentes y vulnerabilidades que se reportaban. No se trataba de que los sistemas informáticos fueran más seguros o que los administradores hubieran

[93] Thomas Reed. “At the Abyss: An Insider's History of the Cold War”. Wikipedia. https://en.wikipedia.org/wiki/At_the_Abyss (Ú.a.: 17/09/2015)

dado con la clave para mantener sus sistemas a salvo de ataques. Lo que estaba ocurriendo era consecuencia de la generación de un mercado negro, muy bien pagado, interesado en adquirir las vulnerabilidades al tiempo que se iban descubriendo, y a precios que a los ciudadanos corrientes les parecerían mareantes.

Esas vulnerabilidades no se notifican a los responsables de desarrollo y seguridad para que las corrijan y emitan sus actualizaciones y parches de seguridad, y se utilizan para diseñar software malicioso con el que atacar los sistemas que queden expuestos. Es lo que se denomina vulnerabilidades de día 0.

Según informaciones publicadas por el Instituto Nacional de Ciberseguridad (INCIBE[94], antiguo INTECO)[95], algunas empresas, como TippingPoint, filial de HP, en un tono muy reivindicativo, ya habían propuesto en 2005 la Zero Day Initiative, para adquirir vulnerabilidades a investigadores en múltiples productos de software, ofreciéndoles una gratificación en función de la gravedad de la vulnerabilidad y del producto que se trate. El objetivo que se persigue por parte de la iniciativa es incorporar los datos de estas vulnerabilidades de día 0 a los productos de seguridad perimetral de TippingPoint, ofreciendo un nivel de seguridad extra a sus clientes.

Existen más modelos de negocio como son los programas de recompensas, donde se siguen otras estrategias para que los investigadores de seguridad puedan obtener beneficios por sus descubrimientos dentro de un mercado legal. Estos programas de recompensas, o *bug bounty programs*, son concursos ad-hoc o programas estables que diferentes compañías realizan para premiar a investigadores que reportan vulnerabilidades de día 0 sobre sus productos.

Existen compañías que ofrecen retribuciones económicas como por ejemplo Google, Facebook, Samsung SmartTV o Mega. Otras que ofrecen el reconocimiento público del investigador en su página web por su labor de ayuda a la compañía junto con un pequeño regalo, como Dropbox, Amazon o United Airlines, que ofrece millas gratis; y otras compañías que solo ofrecen el reconocimiento público a través de su página web, como puede ser el caso de Twitter, Microsoft, Apple o Tuenti.

En agosto de 2013, según publica el canal de noticias ruso RT[96], un estudiante de informática palestino, que se identificó como Khalil, utilizó un exploit para publicar un mensaje en Facebook en el timeline del perfil de Mark Zuckerberg. Según declaró este hacker, había intentado reportar esta vulnerabilidad utilizando el bug bounty program de Facebook, pero la

[94] INCIBE. https://www.incibe.es/home/instituto_nacional_ciberseguridad/ (Ú.a.: 28/08/2015)
[95] "Mercado legal de vulnerabilidades 0day". INCIBE. 04/04/2013. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/mercado_legal_vulnerabilidades_0day (Ú.a.: 28/08/2015)
[96] "Hacker posts Facebook bug report on Zuckerberg's wall". RT. 17/08/2013. http://on.rt.com/2ylp9k (Ú.a.: 30/08/2015)

respuesta del equipo de desarrollo fue que esta vulnerabilidad no era de hecho un error. En una entrevista a CNET, Ryan McGeehan, exdirector del equipo de respuesta de seguridad de Facebook, reconoció que los investigadores que encuentran y reportan este tipo de errores de seguridad son raros. India tiene el segundo mayor número de cazadores de bugs del mundo, y de hecho encabeza el programa de recompensa de bugs de Facebook, con el mayor número de bugs válidos reportados, y un promedio 1.300 dólares por bug. Le siguen Rusia (cuyos cazadores de bugs obtienen un promedio de 4.000 dólares por bug, por su alta calidad), EE.UU., Brasil y Reino Unido.

Varias páginas web como Bugcrowd[97] o NibbleSecurity mantienen un listado actualizado y completo de todas las empresas de productos o servicios que ofrecen algún tipo de salida en un mercado legal a todos los investigadores de nuevas vulnerabilidades, ya sea en forma de bug bounty sobre sus propios productos y servicios, o en forma de compra directa para posteriormente utilizarse en servicios de seguridad de valor añadido.

El mercado legal sin embargo no es motivador para absorver la totalidad de las vulnerabilidades descubiertas. En general en el mercado legal se pagan entre 250 y 15.000 dólares, dependiendo de la gravedad del error descubierto. El mercado negro puede pagar cualquier cantidad, multiplicando las cifras del mercado legal por 100 o por 1000, dependiendo de la vulnerabilidad.

Según declaraciones de Félix Muñoz, Director General de Innotec System, publicadas en El País, una vulnerabilidad de iPhone se vende en el mercado negro por 300.000 euros, y de Microsoft por 500.000 euros.

Puede resultar desconcertante pensar que alguien esté interesado en adquirir esos datos técnicos y pagar por ellos millones de dólares, desarrollar un virus, y dañar unos cuantos sistemas. Está claro que inmediatamente será detectado, y se desarrollará una vacuna que se distribuirá con premura anulando sus efectos nocivos. Pero el objetivo del malware que hace uso de estas vulnerabilidades es pasar desapercibido, sin producir ningún efecto dramáticamente llamativo en los sistemas que los alojan. Eso los distingue de los virus tradicionales. Se trata de gusanos muy sofisticados, auténticas maravillas de ingeniería del software condensadas en unas pocas líneas de código. Se ocultan y modifican el sistema lo justo para no ser detectados y permitir que usuarios externos accedan y tomen el control, de un modo transparente al administrador del sistema.

[97] The Bug Bounty List. Bugcrowd. https://bugcrowd.com/list-of-bug-bounty-programs/ (Ú.a.: 30/08/2015)

El símil no puede ser más perfecto. Como un pequeño gusano en una manzana, es capaz de abrir una pequeña brecha en su piel, atraviesa su carne alimentándose de ella hasta llegar a su corazón, y allí permanece escondido, reproduciéndose, mientras pudre la fruta desde su interior, accediendo a la información o corrompiéndola.

Las políticas de seguridad están haciendo que el alojamiento de determinadas webs de reputación dudosa sea cada día más complicado. Lo mismo ocurre con la contratación de los dominios en internet. También la intervención y filtrado de las comunicaciones electrónicas es cada día más eficiente, así como el control de los mercados de tecnología estratégica. Todo ello dificulta la actividad delictiva, pero como sabemos, no sólo las mafias no dejan de operar sino que su número, volumen y áreas en las que operan, cada vez son mayores. Según datos de UNODC, United Nations Office on Drugs and Crime, el volumen de dinero que mueve, por ejemplo, el narcotráfico sólo en México, puerta de entrada del tráfico de drogas a EE.UU., estimado en cerca del billón de dólares -800.000 millones de dólares- en 2012, lo situaría entre los quince países con el PIB más alto del mundo. La gestión de esa actividad, que en poco se distingue de la de una gran multinacional, requiere de capacidad de proceso de la información y de comunicaciones eficientes. Y si no es posible adquirir sistemas, dominios o capacidad de proceso de un modo legal, quizá sí sea posible obtenerlos por otras vías.

El parque de ordenadores personales domésticos y redes públicas tampoco ha dejado de crecer, y la capacidad potencial de proceso que encierran es increíblemente elevada. Parte de esa capacidad ya intentó ser explotada con propósitos científicos para procesar la enorme cantidad de información que genera el proyecto SETI de la NASA, mediante la iniciativa SETI@home[98]. En varias universidades desde hace años que se han ensayado métodos para poder emplear la capacidad de proceso de las redes de ordenadores personales.

A finales de 2007 la policía de Nueva Zelanda, en colaboración con el FBI, detuvo en Hamilton a un cracker, conocido como Akill[99], que había podido construir una red de 1,3 millones de ordenadores personales, lo que se denomina una botnet o red zombi, de los cuales había conseguido obtener el control mediante un gusano desarrollado por él mismo, y aprovechaba su capacidad de proceso para vender una plataforma desde la que era posible realizar spam. Los propietarios de los ordenadores, distribuidos por todo el mundo, no sospechaban que estaban siendo utilizados. Únicamente con la generación de correo electrónico y accesos a su propio sitio web desde la red zombi, se calculó que había generado unos ingresos de más de 20 millones de dólares.

[98] SETI@home. http://setiathome.ssl.berkeley.edu/ (Ú.a.: 01/09/2015)
[99] "Arrests made in botnet crackdown". BBC News. 30/11/2007. http://news.bbc.co.uk/2/hi/technology/7120251.stm (Ú.a.: 30/08/2015)

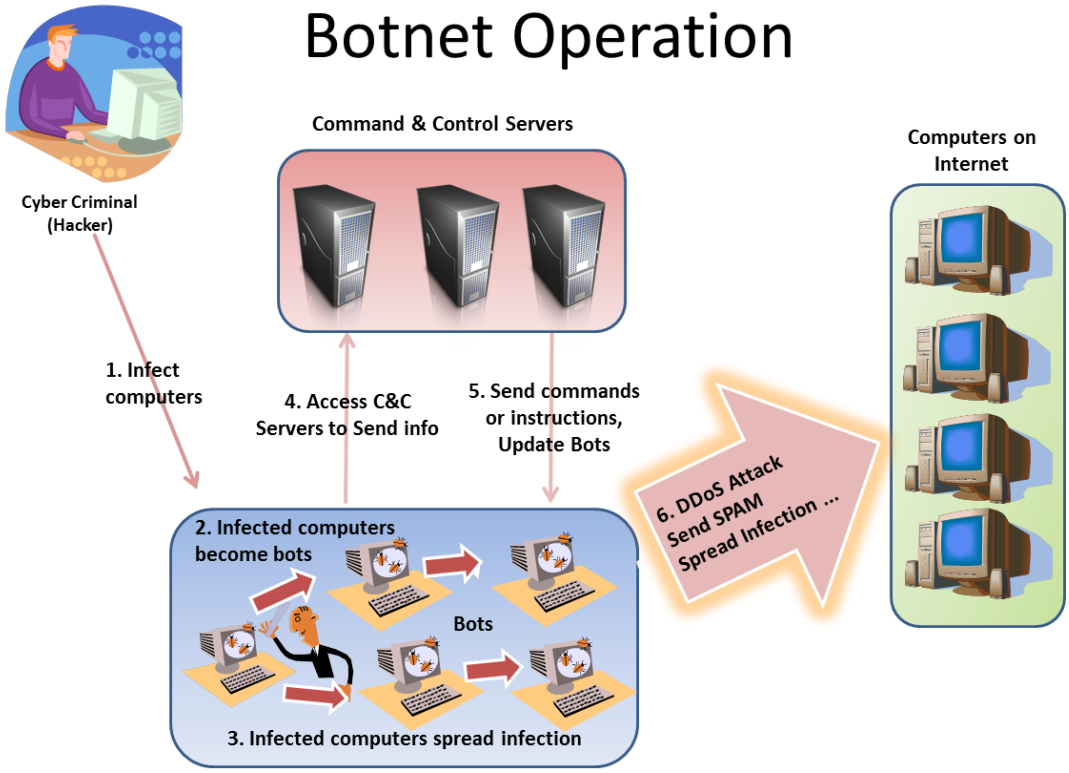

Figura 17: *Infografía en la que se muestra cómo operan las botnets o redes zombi. El proceso de monetarización de la plataforma incluiría al spammer, que contrataría los servicios de la botnet para distribuir su spam. (Fuente: Web de Motherboard a través de Google Images. http://4.bp.blogspot.com/-hD2qFH886bs/Tlfo8zmz-DI/AAAAAAAAAV0/hGjW5OINgbk/s1600/Botnet+Operation.png. Último acceso el 17/09/2015)*

En diciembre de 2009, en una acción coordinada de la Guardia Civil, el FBI y varias empresas de seguridad informática, se desactivó en España una red zombi de 13 millones de ordenadores infectados (200.000 en España) aunque, días más tarde, los detenidos consiguieron recuperar el control y lanzaron un ataque de represalia contra Defense Intelligence, dejando inoperativos sus servidores. La Guardia Civil optó entonces por poner el caso en conocimiento de la Audiencia Nacional, que ordenó la detención de los tres ciudadanos españoles responsables de la red, Netkairo, OsTiaToR y Johnyloleante. La trama había logrado robar datos personales y bancarios de más de 800.000 usuarios e infectar ordenadores de 500 grandes empresas y más de 40 entidades bancarias. La red Mariposa, desarticulada por el Grupo de Delitos Telemáticos de la

Guardia Civil, en colaboración con el FBI y la empresa Panda Security, tenía supuestamente capacidad para perpetrar ataques de ciberterrorismo mucho más virulentos.[100]

Si bien los éxitos en la deshabilitación de redes zombi tuvieron un gran impacto mediático, lo cierto es que entre 2007 y 2010, el spam se convirtió en uno de los grandes azotes de internet. Según los informes cuatrimestrales sobre amenazas y seguridad informática elaborados por Kaspersky y Symantec, entre 2009 y 2010 más del 90% de todo el tráfico de internet generado por el correo electrónico, lo constituían mensajes de spam, y cerca del 77% de ese tráfico se generaba en redes zombi.

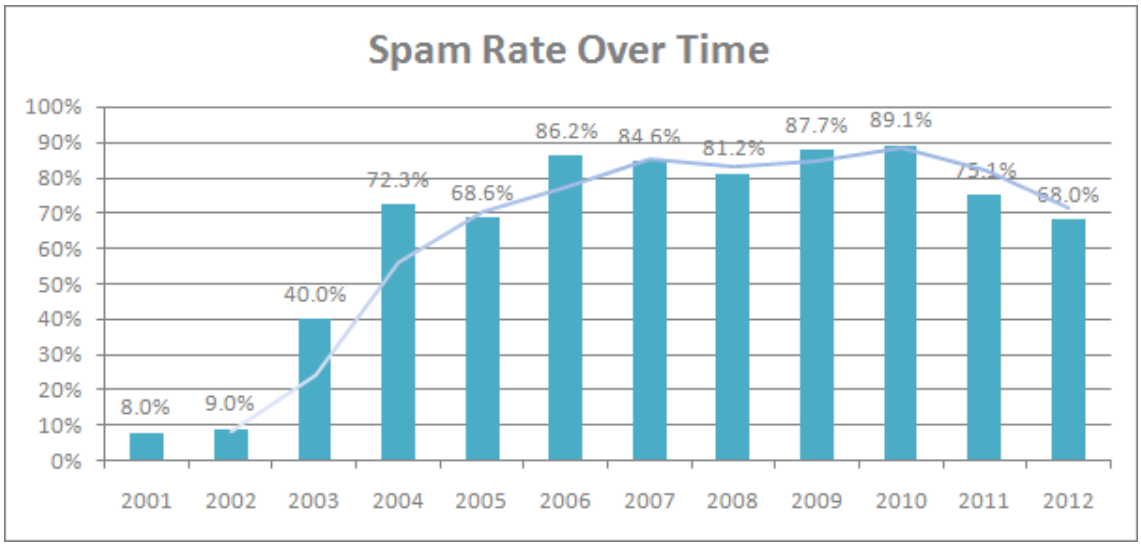

Figura 18: *Porcentaje anual de spam sobre el total de correos electrónicos. Fuente: Joanne Pimanova. "Email Spam Trends at a Glance: 2001-2012". EmailTray. 05/06/2012. http://www.emailtray.com/blog/email-spam-trends-2001-2012/ (Último acceso: 18/09/2015). (Accedido vía Google Images. Originamente publicado por Symantec en su informe anual sobre spam de 2011: "February 2012 Symantec Intelligence Report").*

Desde que existen las listas negras de dominios, que son filtrados y censurados cuando se detecta que desde ellos se realizan envíos de spam, los administradores de sistemas dan de baja sin contemplaciones a los usuarios que realizan estas prácticas. Si ésto no ocurre, el dominio entero corre el riesgo de ser suspendido. Cabe preguntarse consecuentemente de dónde surge pués la ingente actividad marginal de internet. E inmediatamente es posible hacerse una idea del mercado que las redes zombis pueden llegar a mover.

[100] EFE. "Tres españoles dirigían la mayor red de ordenadores 'zombis' del mundo". La Vanguardia. 04/03/2010. http://www.lavanguardia.com/sucesos/20100303/53896548728/tres-espanoles-dirigian-la-mayor-red-de-ordenadores-zombis-del-mundo.html (Ú.a.: 30/08/2015)

Según informaciones de Symantec a la BBC, en el segundo semestre de 2010 tres de los mayores productores de spam redujeron repentinamente su actividad. Uno de ellos, conocido como Rustock, responsable desde sus botnets rusas de la mitad del spam mundial, cayó a sólo el 0,5% del tráfico generado unos meses antes. Spamit por su parte anunció también que cesaba su actividad debido a varios acontecimientos negativos, sin especificar oficialmente más (posteriormente trascendió que se habían presentado cargos en Rusia contra Igor Gusev, considerado el mayor spammer a nivel mundial y promotor de Spamit y GlavMed, proveedor de pseudo-Viagra, que fué finalmente procesado).

El volumen global de spam se redujo de 250.000 millones de mensajes diarios, a 30.000 millones de mensajes. Independientemente de que los spammers pudieran sentirse cada vez más acosados, y su negocio haberse vuelto más volátil, las razones de esta drástica reducción no hay que buscarlas sin embargo en cambios en los protocolos de seguridad implementados por los gobiernos, que pudieran afectar a la contratación de servicios y a la actividad de los canales alegales, provocando el cierre de varias botnets; o en un cambio de modelo de negocio, trasladando el spam del correo electrónico a las redes sociales, aunque el cambio estaba en proceso; sino en los cambios estructurales del negocio del spam.

Varios informes y análisis para Kaspersky[101] y Symantec[102] relacionaron la actividad del spam en el mercado ruso con la salud de la actividad financiera y la crisis económica, y resultaban tremendamente indicativos, dado que hasta un 60% del spam estaba dominado por ese mercado.

La primera caída significativa del spam se registró en agosto de 2008, cuando se inició la crisis económica en Rusia. Una segunda caída se produjo en la primavera de 2009, cuando la crisis tocaba fondo. Estas caídas drásticas en el negocio forzaron a los spammers a establecer estrategias compensatorias nuevas, mediante los llamados programas de afiliación o asociación. En esta modalidad el spammer cobra no por correo enviado, sino, asociado al vendedor, por compra realizada. Ésto aún hizo que el spam resultara más sensible a la disponibilidad financiera de los clientes, y ayudó a globalizar la correlación de las fluctuaciones financieras con las de este mercado, de modo que se reflejan con precisión extrema.

Durante el primer semestre de 2010 se había apreciado una estabilización, con tendencia al alza, del mercado del spam en sus diversas modalidades, y una mayor diversificación de su origen, lo que se había asociado a una ligera recuperación de la base del cliente de spam, el pequeño y mediano negocio, y el mercado inmobiliario en la parte vendedor.

[101] Elena Bondarenko, Darya Gudkova, Maria Namestnikova. “Spam in the Third Quarter of 2010”. Kaspersky Lab. 10/11/2010. https://securelist.com/analysis/quarterly-spam-reports/36330/spam-in-the-third-quarter-of-2010/ (Ú.a.: 30/08/2015)
[102] Jacob Nitohiwa. “Spam reduction reports questionable”. ITWeb. 14/06/2011. http://www.itweb.co.za/index.php?option=com_content&view=article&id=40159 (Ú.a.: 30/08/2015)

Figura 19: *Caida del spam a finales de 2010 debido a la desactivación de varias botnets rusas. Fuente: Arantxa Asián. "El spam cae sorpresivamente". MuySeguridad.net. 07/01/2011. http://muyseguridad.net/2011/01/07/el-spam-cae-sorpresivamente/ (Último acceso: 18/09/2015). (Accedido via Google Images. Originamente publicado por Symantec en su informe anual sobre spam de 2011: "February 2012 Symantec Intelligence Report").*

El descenso en la actividad del mercado del spam en los últimos meses del año (del 85% del total del tráfico generado por el correo electrónico a menos de un 50%) coincide con el cierre en noviembre de la botnet Pushdo/Cutwail/Bredolab, y también con las incertidumbres planteadas por la economía norteamericana, el aumento del coste de la energía, las peores noticias económicas para el euro y el retraimiento de los clientes.

Durante 2011, con el colapso de las botnets rusas, EE.UU. tomó el relevo como principal generador del spam mundial, con un 20% de cuota. Le seguían India (7%) y Brasil (5%). Se produjeron también cambios importantes en el modelo de negocio. Por un lado los gestores de botnets diversificaron su oferta de servicios tratando de captar nuevos clientes, y dando lugar a la aparición de un mercado de servicios asociados a todo tipo de actividades delictivas. Por otro lado los spammers se hicieron también más maliciosos, conforme el mercado emergente se consolidaba.

En 2012, la empresa de seguridad TrendMicro publicó un informe de Max Goncharov[103] en el que se recopilaba la oferta de nuevos servicios ofrecidos en el mercado negro ruso del cibercrimen:

1. Servicios de encriptación de malware.
2. Hosting.
3. Servicios de proxy anónimo (con soporte de protocolos http, https, ftp, socks, cgi).
4. Servicios de VPN (redes privadas virtuales).
5. Servicios de infección por descarga de malware (waterholing). Se contrata por infección, pay-per-install (PPI), y los precios varían por país, dependiendo de la calidad de su tráfico web y la facilidad para alojar malware en las webs más probables.
6. Servicios de programación y/o venta de software (malware)
7. Servicios de ataques distribuidos de denegación de servicio (DDoS), por cualquier procedimiento, incluidos inundación por paquetes UDP, TCP, TCP SYN, Smurf, ICMP
8. Servicios de spam, incluido spam telefónico o por mensajería SMS
9. Alquiler e implementación de botnets, incluyendo centros de mando a través de web, por canal IRC, mensajes instantáneos (IM), u otros métodos más exóticos.
10. Servicios de comprobación de malware contra diverso software de seguridad
11. Venta de troyanos
12. Venta de rootkits
13. Servicios de ingeniería social
14. Servicios de hacking. Estos servicios pueden contratase por varios procedimientos: fuerza bruta (obtención de contraseñas usando diccionarios), obtención de respuestas a preguntas de seguridad, haciendo uso de vulnerabilidades de los sitios (empleando SQL injection, Cross-Site Scripting, o ambos), usando sniffers, troyanos, phishing, o ingeniería social.
15. Venta de copias de documentos escaneados (útiles para comprobación de cuentas bancarias con el máximo anonimato)
16. Servicios de fraude vía SMS (aunque este tipo de fraude es raro, se ofrecen servicios para envio de SMS utilizando números falsos o para activar otros servicios a través de SMS)

[103] Max Goncharov. "Russian Underground 101". Trend Micro. 2012. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf (Ú.a.: 30/08/2015)

17. Servicios de extorsión a través de ransomware
18. Venta de claves de activación de software
19. Venta y servicios de desarrollo de exploits
20. Falsificaciones (fakes asociadas a la contratación de servicios de phishing)
21. Venta de tráfico (los servicios de tráfico pueden generarse desde las plataformas de spam, sistemas infectados o hackeados, de diferentes paises y sistemas, para propósitos diversos).
22. Servicios de posicionamiento SEO para webs con contenido malicioso

Según informa la empresa, la inversión necesaria para convertirse en cibercriminal es mínima. Los precios del mercado para los servicios mínimos como DDoS cuesta entre 30 y 70 dólares al día, mientras que los servicios VPN oscilan entre los 50 o 55 dólares online con duración de tres meses. Las redes zombi también tienen precio: 35 dólares para el host propio y 40 para el de un tercero. Los precios que generalmente se pagan por las tecnologías, herramientas y servicios más sofisticados son mucho más altos (superando los 50 dólares). Para estar por delante de las soluciones del mercado de la seguridad online, los hackers también procuran ofrecer la opción de probar sus productos contra software de seguridad.

En 2013 Kaspersky informó de un descenso del spam tradicional por primera vez por debajo del 70%, debido a la desvinculación del comercio legal con el spam. Del mismo modo creció el spam con malware adjunto, preferentemente para el robo de contraseñas. Posiblemente se debió a una estrategia complementaria a los ataques de phishing, que también tuvieron más presencia en redes sociales y en el correo electrónico, disminuyendo los ataques diseñados para la obtención de datos de cuentas bancarias, ya que, como consecuencia de las políticas de adquisiciones, las passwords de las cuentas de correo electrónico de sitios como Google, Yahoo, Microsoft o Facebook, se vincularon a una amplia diversidad de servicios, redes sociales, mensajería, alojamiento de datos e incluso datos de tarjetas de crédito.

Los mensajes maliciosos se hicieron menos ingenuos, tratando de alcanzar a usuarios con más experiencia en el uso de medios digitales, y con conocimiento de algunos recursos en materia de seguridad informática, así se observaron envíos masivos de spam malicioso asociado a falsas actualizaciones de antivirus. La actualización en realidad volcaba un troyano de la familia Zeus/Zbot, destinado a obtener la información confidencial del usuario. La novedad de la distribución es que el troyano no recibía instrucciones de un centro de administración o de una web, sino que utilizaba el protocolo P2P para recibir informaciones de otros equipos infectados. Kaspersky catalogó también una ingente cantidad de spam, someramente dirigido al sector

turístico, agencias de viajes, hoteles, etc., que tenía el objeto de lavar dinero obtenido de estafas y tarjetas de crédito robadas[104].

China y EE.UU. fueron el origen del 50% de este tipo de spam malicioso generado en el mundo. A distancia se situaron países con una legislación laxa anti-spam, como Corea del Sur, Taiwán, Kazajistan, Bielorrusia, Ucrania o Canadá.

Los ataques dirigidos han sido estos dos últimos años los protagonistas en el escenario de las ciberamenazas, y su precisión ha ido incrementándose con el tiempo. Se han difuminado también las fronteras entre ciberdelincuentes, ciberactivistas y ciberespías, marcando una convergencia de intereses y métodos de actuación, y usandose indistintamente unos a otros.

En esta línea, Kaspersky desveló en octubre de 2012 la existencia de un malware que podía haber estado operando en todo el mundo durante al menos desde 2007, y al que se denominó Octubre Rojo[105]. Este malware se habría difundido ampliamente a nivel internacional y habría sido el responsable de la obtención de informaciones de un amplio espectro que variaban desde información diplomática de carácter secreto a informaciones personales de los teléfonos móviles. El vector principal de distribución fueron mensajes muy dirigidos que contenían adjuntos capaces de explotar varias vulnerabilidades de Microsoft Word y Excel. Este phishing dirigido, o spear phishing, se caracterizaba por el uso de adjuntos del tipo "Diplomatic Car for Sale.doc".

[104] Kaspersky Security Bulletin. El spam en 2013. "Criminalización del spam de carácter comercial". Viruslist. 23/01/2014. http://www.viruslist.com/sp/analysis?pubid=207271242#03 (Ú.a.: 16/09/2015)
[105] GReAT, Kaspersky Lab's Global Research & Analysis Team. "The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies". Securelist. 14/01/2013. https://securelist.com/blog/incidents/57647/the-red-october-campaign/ (Ú.a.: 16/09/2015)

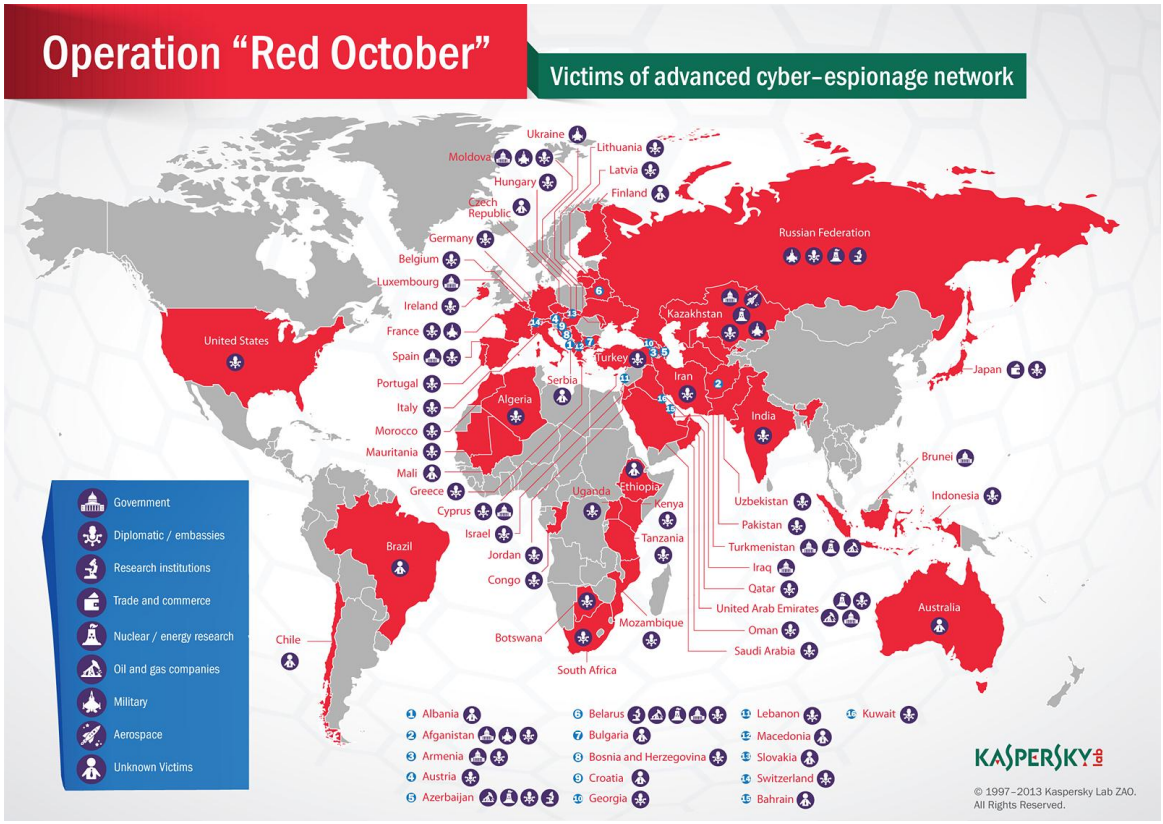

Figura 20: *Países afectados por la red "Octubre Rojo", y perfil de las víctimas. (Fuente: GReAT, Kaspersky Lab's Global Research & Analysis Team. "The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies". Securelist. 14/01/2013. https://securelist.com/blog/incidents/57647/the-red-october-campaign/. Último acceso: 16/09/2015)*

Posteriormente el malware mutó y apareció en varias webs para aprovechar vulnerabilidades del plugin de Java de los navegadores. Los destinatarios de los ataques fueron en su mayoria usuarios de perfil gubernamental, tanto de estados como de organizaciones internacionales de carácter diplomático, pero también usuarios de perfil científico, vinculados con organismos e instituciones de investigación. Con posterioridad a la publicación del informe de Kaspersky revelando la existencia de Octubre Rojo, más de 60 dominios usados por los creadores del malware para recibir la información obtenida, fueron dados de baja y cesó su actividad. SecureList anunció sin embargo en diciembre de 2014 la posibilidad de que se hubieran rediseñado algunas de las herramientas utilizadas y se hubieran retomado las actividades de

ciberespionaje. Descubrieron muchas similitudes entre Octubre Rojo y el malware Mevade, aparecido a finales de 2013[106]. A esta nueva oleada se le asignó el nombre "Cloud Atlas".

Según manifestaban los investigadores de Kaspersky en Securelist, el "modus operandi" de los cibercriminales y ciberespías presenta perfiles diferentes. Los primeros manifiestan más nerviosismo y aversión a la exposición de sus actividades, desaparecen incluso por años, y nunca utilizan la misma herramienta ni técnica. Los segundos borran sus huellas, relocalizan sus operaciones y siguen con ellas, como si nada hubiera ocurrido. Este parece ser el caso de Octubre Rojo.

Más allá, los exploits aparentaban haber sido creados por hackers de origen chino, y el malware Octubre Rojo en sí por desarrolladores de habla rusa. Ambos indicios no apuntaban necesariamente a los servicios secretos de ninguno de los dos estados, dado que la información conseguida habría sido de interés para cualquier postor, y por tanto la operación de ciberespionaje podría haber sido realizada por cualquier organización cibercriminal.

En febrero de 2014, la empresa de seguridad G-Data descubrió una nueva red de ciberespionaje, activa desde, al menos, 2012. En un principio no se pudo identificar el vector de infección, fue desvelado posteriormente por investigadores de Kaspersky, que bautizaron la infección como Epic-Turla[107], pero otras empresas, como Symantec, también estaban siguiendo la campaña y comprobaron la existencia de otros vectores[108].

El ataque había sido dirigido a una amplia variedad de objetivos, pero de forma muy eficiente, incluyendo gobiernos (departamentos de interior, industria y comercio, asuntos exteriores, defensa y agencias de inteligencia), embajadas, centros educativos y de investigación y empresas farmacéuticas, en 45 países, con más incidencia en Oriente Medio y Europa, entre ellos España, aunque se detectaron víctimas en otras regiones, incluidos EE.UU. y Rusia. El país más afectado fue Francia.

Se utilizaron vulnerabilidades de día 0 para desarrollar exploits con los que infectar a las víctimas a través de vectores diferentes. Por un lado, con técnicas de ingeniería social se intentaba conseguir que la víctima ejecutara archivos infectados, proporcionados a través de spear phishing. Se identificaron archivos PDF con exploits, instaladores de malware con

[106] GReAT, Kaspersky Lab's Global Research & Analysis Team. "Cloud Atlas: RedOctober APT is back in style". SecureList. 10/12/2014. https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/ (Ú.a.: 16/09/2015)
[107] GReAT, Kaspersky Lab's Global Research & Analysis Team. "The Epic Turla Operation". SecureList. 07/08/2014. https://securelist.com/analysis/publications/65545/the-epic-turla-operation/ (Ú.a.: 16/09/2015)
[108] Symantec Security Response. "Turla: Spying tool targets governments and diplomats". Symantec. 07/08/2014. http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats (Ú.a.: 16/09/2015)

extensión .scr, a veces comprimidos con RAR, y falsos Flash Player. Por otro lado se utilizaron técnicas de "waterhole" (literalmente "abrevadero"), que consisten en identificar webs vulnerables que las víctimas pudieran considerar de confianza para infectarlas, de modo que se redirija a los visitantes a webs desde las que descargar y distribuir el exploit, en este caso a través de vulnerabilidades de Flash Player, Java y de los navegadores Internet Explorer de Microsoft, versiones 6, 7 y 8 (fingerprinting). Se encontraron infecciones de Turla en más de un centenar de webs, la mayoría de Rumanía, Francia, EE.UU., Irán y Rusia, pero también se localizaron webs infectadas por Turla en España[109].

Figura 21: *Países afectados por la red Epic-Turla. (Fuente: Kaspersky Labs. "The Epic Snake: Unraveling the mysteries of the Turla cyber-espionage campaign". 07/08/2014. http://www.kaspersky.com/about/news/virus/2014/Unraveling-mysteries-of-Turla-cyber-espionage-campaign. Último acceso: 18/09/2015)*

[109] Christian Bautista. "Spy agencies compromised by 'Epic Turla' cyber espionage operation". Tech Times. 09/08/2014. http://www.techtimes.com/articles/12455/20140809/spy-agencies-compromised-by-epic-turla-cyber-espionage-operation.htm (Ú.a.: 16/09/2015)

Una vez la víctima se ha infectado, inmediatamente Turla se comunica con su centro de control, abriendo una puerta trasera en el sistema infectado y obteniendo información del sistema y de la víctima. Con el sistema ya comprometido, los atacantes entregan un lote de archivos, con un script que actúa sobre varias carpetas y las conexiones de red del sistema, y se incluye un keylogger, el archivador RAR y una serie de utilidades que servirán al atacante para identificar otros sistemas con los que se comunique la víctima; y suministrar backdoors por las que el sistema infectado pueda pasar a ser controlado por otros centros de control, al parecer en caso de que se identifique que la víctima es de alto nivel. Este segundo despliegue más sofisticado es conocido como Cobra/Carbon, o pfinet.

Respecto a la autoría, Kaspersky identificó que algunos de los exploits y backdoors utilizan terminología de habla rusa, así como la página de códigos 1251, que representa caracteres cirílicos.

Si los ataques a organismos gubernamentales han demostrado que pueden resultar muy desestabilizadores para los estados, y son potenciales generadores de conflictos reales, no lo son menos los ataques a entidades financieras y medios de pago. La cibervigilancia de los servicios secretos ha podido obtener información de las redes financieras, de las bases de datos de usuarios de banca o de operaciones con medios de pago, como hemos visto, pero se ha cuidado mucho de interferirlas, inclusive las cuentas de narcotraficantes, terroristas y dictadores, y provocar la pérdida de confianza en estas instituciones y en sus procedimientos, porque puede resultar eventualmente catastrófica para la economía internacional[110].

Como parte de la Estrategia de Seguridad Nacional, aprobada en Consejo de Ministros en mayo de 2013 y entre cuyos objetivos figura garantizar la seguridad económica y financiera, el Gobierno se ha dotado de un Consejo de Seguridad Nacional cuyas reuniones preside el Presidente del Gobierno, y en el que se integran, entre otros, el jefe del Alto Estado Mayor de la Defensa (JEMAD) y el director del CNI. Prueba también de la importancia que se le otorga al sector, y del alcance que pueden tener los riesgos de que es objeto, son las actuaciones del Servicio de Inteligencia Económica del CNI, que evalúa el riesgo político de los países (orientando el análisis a la inversión empresarial española), y realiza el análisis macroeconómico (estabilidad económica, seguimiento de sectores estratégicos) con especial atención a su incidencia en la economía española, para prevenir cualquier riesgo o amenaza que afecte a la independencia e integridad de España.[111]

[110] Richard A. Clarke y Robert K. Knake. "Guerra en la red. Los nuevos campos de batalla". Ed. Planeta, 2011. (pp. 318 – 319)
[111] Claudi Pérez. "El CNI investiga las presiones especulativas sobre España". El País. 14/02/2010. http://elpais.com/diario/2010/02/14/economia/1266102005_850215.html (Ú.a.: 19/09/2015)

Sin embargo el cibercrimen no se autolimita en sus objetivos, y es una amenaza muy real para las instituciones financieras, y en consecuencia para los estados.

A principos de 2015 se reveló la existencia de una campaña de ataques a entidades financieras, que aún continúa, y que se bautizó como Carbanak[112]. El objetivo de esta campaña, que la diferencia de las anteriores, es que el atacante no busca información, sino dinero, hablamos propiamente de ciberdelincuencia, pura y dura. Otro aspecto que diferencia a Carbanak de otros ataques es que los ciberatacantes hasta el momento siempre habían actuado contra los clientes de las entidades bancarias, obteniendo sus números de cuenta o mediante fraudes sobre los medios de pago, pero en este caso, la víctima es directamente la institución financiera, a través de transferencias por la red SWIFT (lo que ubica este ataque en el contexto de este proyecto), utilizando múltiples recursos para conseguir el robo de cantidades al parecer prefijadas. Una vez conseguido el objetivo, la víctima es abandonada y se eliminan los rastros.

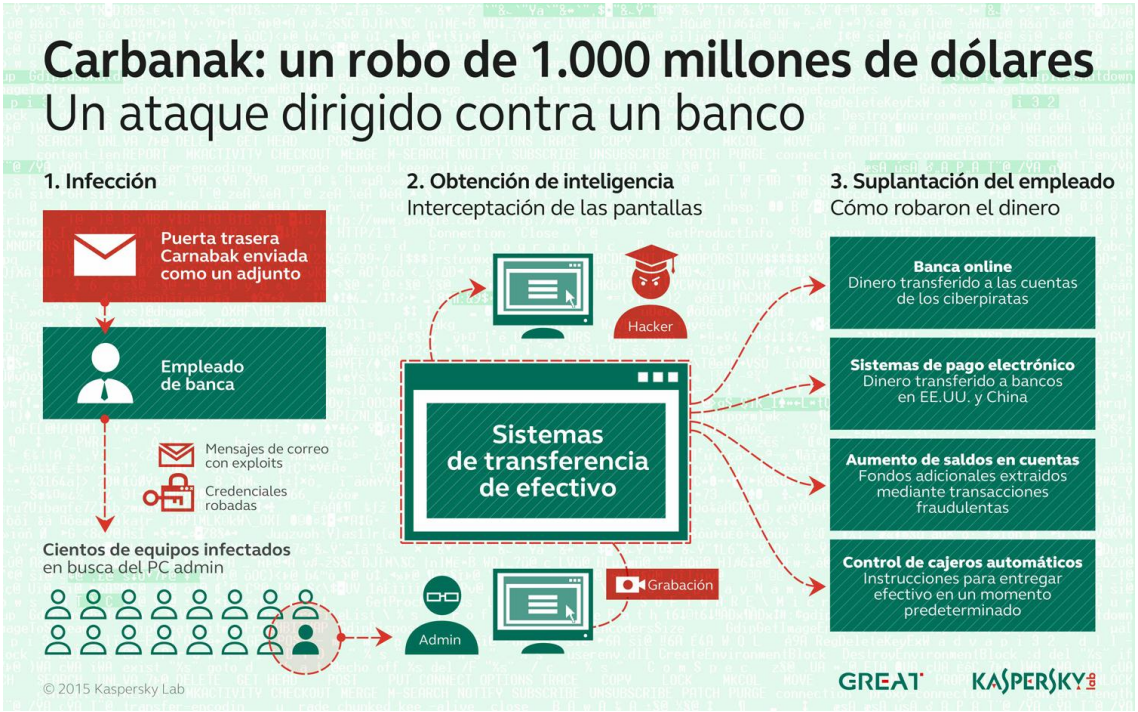

Figura 22: *"Modus operandi" de la red Carbanak. (Fuente: GReAT, Kaspersky Lab's Global Research & Analysis Team. "El gran robo de banco: el APT Carbanak". VirusList. 16/02/2015. http://www.viruslist.com/sp/weblog?weblogid=208189052 Último acceso: 16/09/2015)*

[112] GReAT, Kaspersky Lab's Global Research & Analysis Team. "El gran robo de banco: el APT Carbanak". VirusList. 16/02/2015. http://www.viruslist.com/sp/weblog?weblogid=208189052 (Ú.a.: 16/09/2015)

Las primeras infecciones se detectaron en diciembre de 2013. Un banco ruso alertó a investigadores de Kaspersky de que se estaban produciendo envíos de datos desde su dominio hacia China. La operación pudo ser seguida en vivo y localizado el malware que infectaba los ordenadores corporativos, lo que permitió un análisis forense detallado.

Muchas de estas redes utilizan como vector de infección el correo electrónico. Se realiza una intensa actividad de ingeniería social para recopilar información del organigrama y del personal de las entidades a atacar. Las redes sociales, especialmente Facebook, Twitter y Linkedin, se han convertido en una mina inagotable de información. A continuación se elabora una operación dirigida a infectar al objetivo, haciéndole llegar correos electrónicos fraudulentos que la víctima pueda considerar de fuentes fiables y cercanos a sus intereses, y con adjuntos infectados que instalarán en su sistema el malware diseñado por el atacante para cumplir sus objetivos. Este tipo de infección se denomina *spear fishing* (o pesca con arpón), y se distingue del phishing común en que no es indiscriminado.

Una vez se ha accedido a uno de los ordenadores corporativos, se extiende la infección al resto de la red, y se analiza el perfil de los usuarios en busca de los administradores de los sistemas, es lo que se denomina *movimiento lateral*, localizando información de estos nuevos "usuarios interesantes" para acceder a sus claves. Ocasionalmente se ha llegado a grabar en video a los usuarios para conocer en detalle su operativa. El atacante no necesita conocer previamente el funcionamiento interno del banco, de hecho todos son diferentes, pero acaban encontrando el punto desde el que es posible extraer dinero. La metodología por tanto puede variar. Los ataques de Carbanak se han concretado en transacciones internas a cuentas de los ciberdelincuentes, que posteriormente se cancelaron, transferencias a cuentas de EE.UU. y China mediante pagos electrónicos, aumentos de saldos mediante transacciones fraudulentas, y entregas de efectivo en cajeros automáticos de la red del banco, que son recogidos por "mulas" de la red de ciberdelincuentes.

Por el momento Carbanak ha atacado a más de 100 instituciones financieras en casi 30 países. Los países más afectados son Rusia y EE.UU, hay que considerar también que son los más grandes y cuentan con el mayor número de objetivos. Les siguen en incidencia China, Ucrania, Bulgaria, Alemania, Hong Kong y Taiwan. Otros países que se han visto afectados han sido Brasil, Canadá, Marruecos, España, Islandia, Gran Bretaña, Francia, Suiza, Noruega, República Checa, Polonia, Pakistán, India, Nepal y Australia.

Las AA.PP. en España son también objeto de constantes ataques que utilizan técnicas de phishing y spear phishing. En los últimos tres años han sido varias las campañas de phishing indiscriminado a usuarios del dominio seap.minhap.es, que utiliza los usuarios de la Secretaría de Estado de Administraciones Públicas (SEAP), dependiente del Ministerio de Hacienda y

Administraciones Públicas, y que concentra los servicios de inspección del Estado en todas las áreas funcionales, según establece la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado[113], en su Título II, Capítulo II, Sección 3ª. Además de las competencias en materia de inspección, estos órganos asumen también los registros generales de la AGE, bases de datos de inversiones, protocolos de protección civil, información de coordinación en materia de política interior, incluyendo la gestión de procesos electorales, bases de datos de sanciones administrativas, bases de datos de extranjería, inspecciones de mercancías conjuntamente con los servicios de aduanas, etc.

Las primeras campañas tuvieron lugar a partir de 2011, eran muy indiscriminadas, y consistían en correos electrónicos que simulaban comunicaciones de supuestos servicios TIC genéricos, solicitando credenciales de acceso a los usuarios para evitar el bloqueo de estos servicios. La sintaxis no era muy buena, era bastante evidente que se había utilizado una herramienta de traducción automática para redactarlos. Aún así, en parte debido a la novedad, la falta de protocolos de seguridad y la confianza de los usuarios por trabajar en el entorno seguro de la intranet administrativa, algunos usuarios de nivel directivo facilitaron sus credenciales, comprometiendo los sistemas.

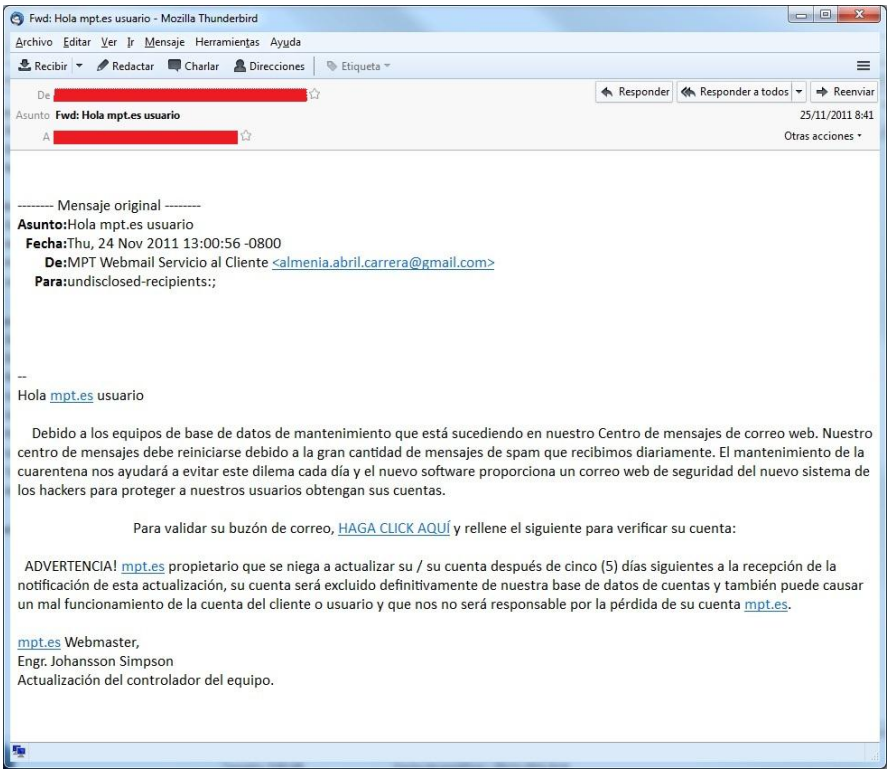

Figura 23: *Captura de pantalla de phishig típico en las campañas de 2011 contra la SEAP (en esa fecha integrada en el Ministerio de Política Territoria (dominio mpt.es).*

[113] BOE. "Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado". 15/04/1997. https://www.boe.es/buscar/doc.php?id=BOE-A-1997-7878 (Ú.a.: 21/09/2015)

Desde el Área de Seguridad de Red de la División de Sistemas (DSIC) se bloquearon los remitentes y los documentos Google Docs a los que dirigía el enlace remitido. No obstante se realizó una campaña informativa interna para promover la actualización de credenciales, ayudar a los usuarios a reconocer los ataques de phishing y notificarlos para acotar sus efectos.

En sucesivas campañas se comprobó que la sofisticación aumentaba, mejorando también el lenguaje, la apariencia oficial, y también el conocimiento de la red de la SEAP y sus servicios.

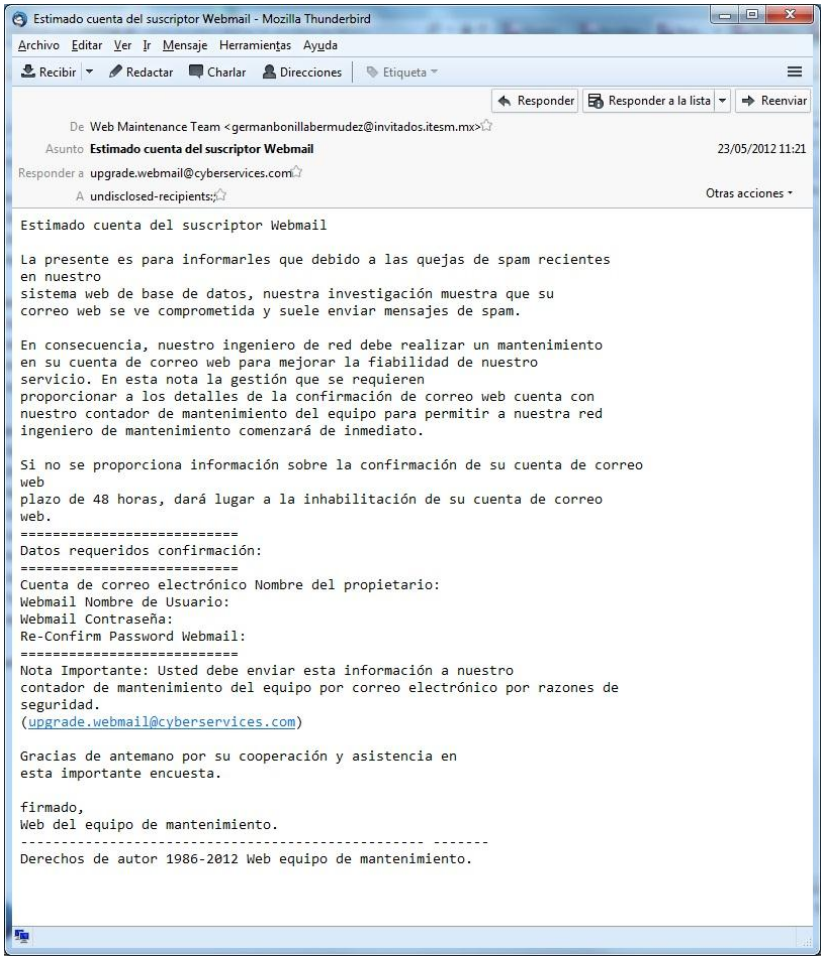

Figura 24: *Captura de pantalla de phishig típico en las campañas de 2012 contra la SEAP, se observa que el atacante conoce la existencia de servicios corporativos de webmail.*

Las campañas de 2013 mostraron que los phishing ya no eran indiscriminados, sino que se trataba de ataques centrados en conseguir credenciales de usuarios de la red de la SEAP, dominio seap.minhap.es, y los remitentes se enmascaraban tras direcciones de dominios falsos.

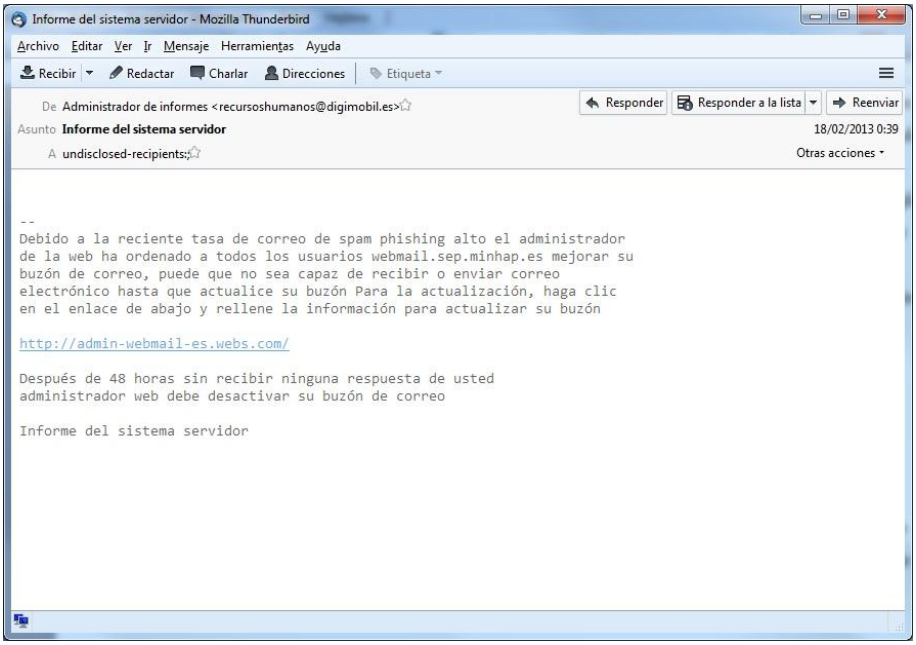

Figura 25: *Captura de pantalla de phishig típico en las campañas de 2013 contra la SEAP, el atacante se dirige expresamente a usuarios del dominio seap.minhap.es.*

Al editar las cabeceras se podía comprobar, a través de las direcciones IP de los remitentes, el origen real del dominio atacante.

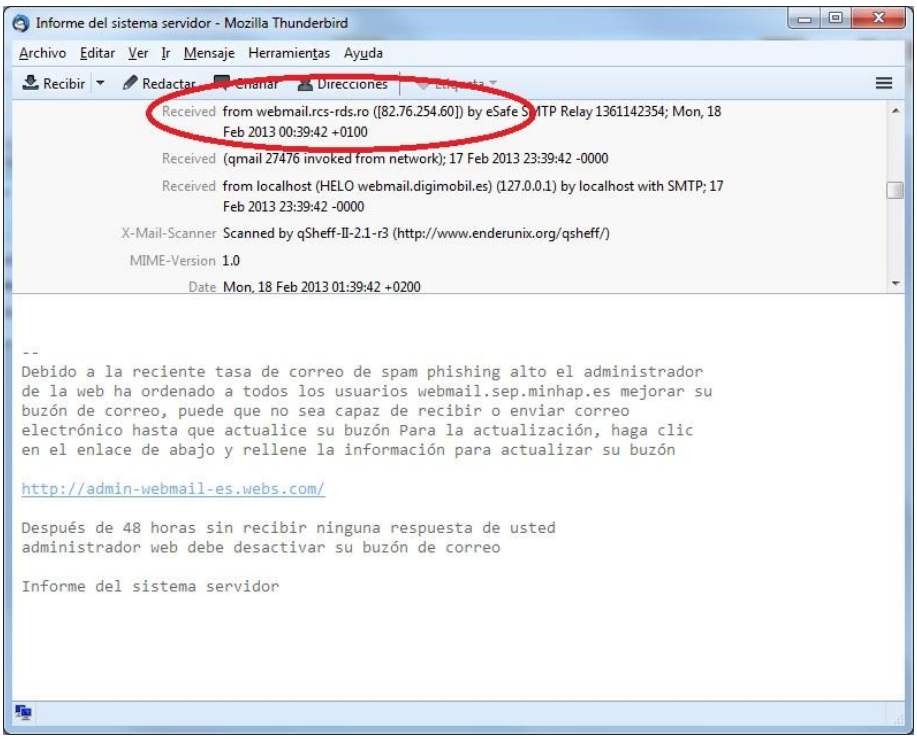

Figura 26: *Captura de pantalla en la que se observa la cabecera editada del correo de phishing, donde aparece en claro la ruta de entrega real y las correspondientes IPs.*

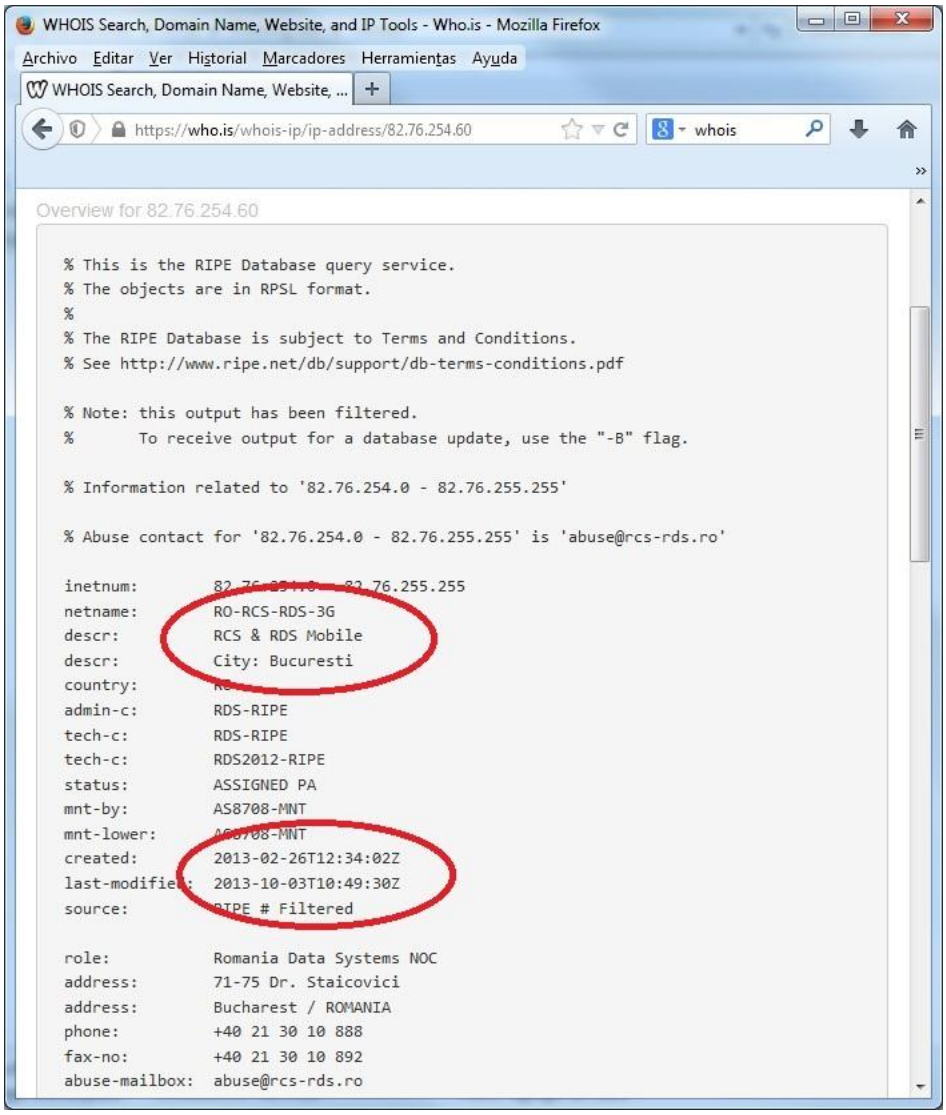

Figura 27: *Captura de pantalla de la consulta a RIPE sobre la identidad del remitente. En este caso se realizaba el phishing desde un dominio rumano, que se habilitó para este objetivo y posteriormente fue abandonado por el atacante.*

Las campañas de 2014 se intensificaron, y el número de incidentes y notificaciones de los usuarios aumentaron en más de un 400%.

En el siguiente phishing que inundó la SEAP, los atacantes, actuando desde un dominio en India, mostraron un correcto uso del idioma, pero también un conocimiento pormenorizado de los procedimientos internos de renovación de las credenciales por el gestor interno automatizado (Identity Manager). La experiencia previa y las campañas de formación resultaron en una prevención efectiva.

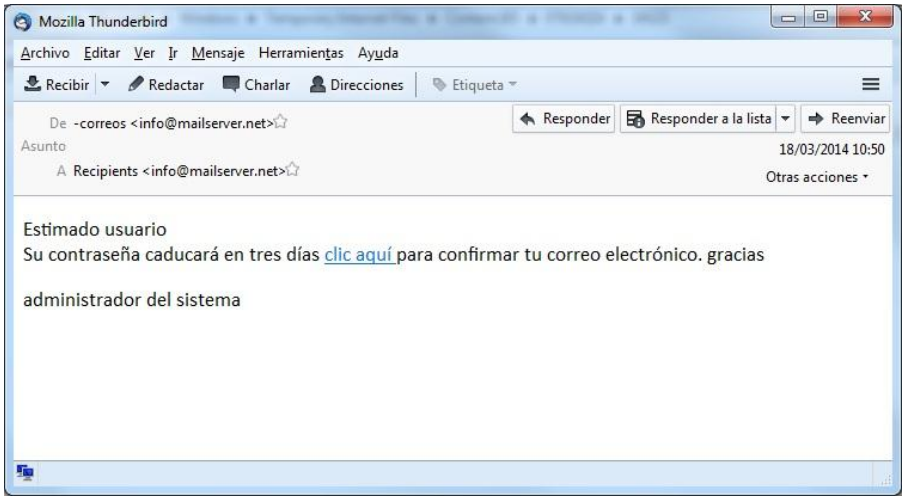

Figura 28: *Captura de pantalla de phishig de origen indio contra la SEAP en 2014.*

Este otro phishing en cambio, desde un dominio sueco, resulta menos creible, y apunta a una campaña basada en información de menor calidad y menos elaborada.

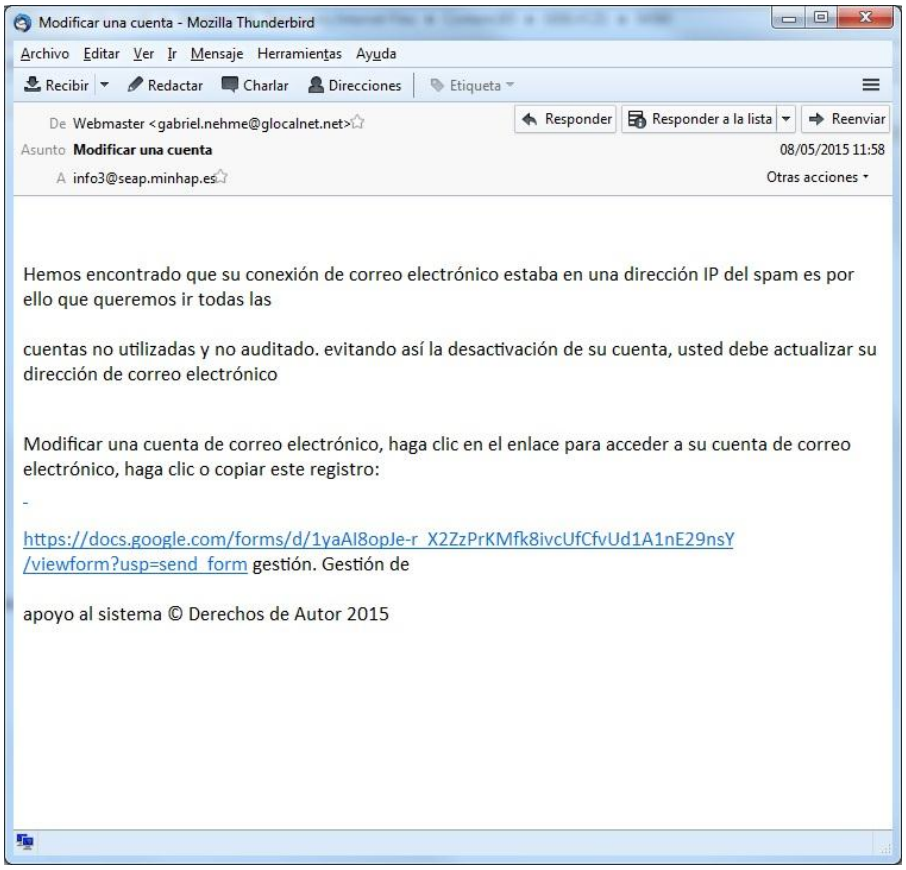

Figura 29: *Captura de pantalla de phishig de origen sueco contra la SEAP en 2014.*

La campaña más sofisticada tuvo lugar en marzo de 2015. Se observó que los correos fueron dirigidos con exclusividad a usuarios de nivel directivo, lo que implicaba un conocimiento profundo de la estructura de la organización, y la sistemática recopilación de información de este perfil de usuarios. Hablamos por tanto de una campaña de spear phishing. También el dominio del idioma mejoró significativamente. Por último el enmascaramiento del remitente mostró un nivel de sofisticación importante.

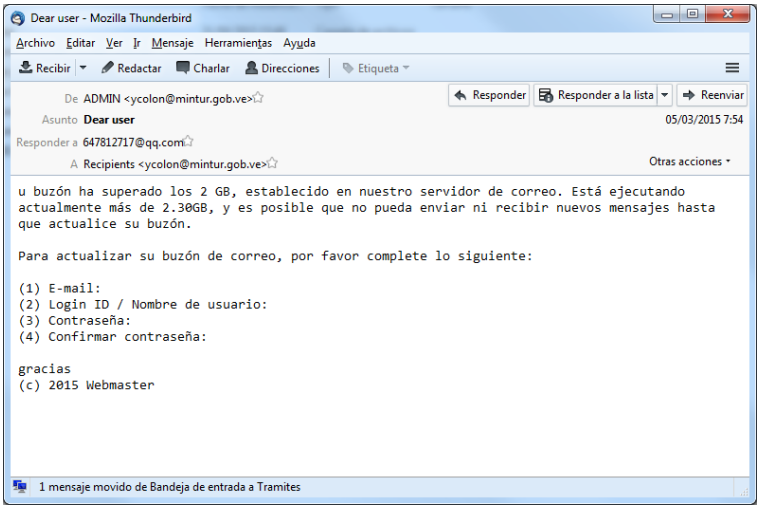

Figura 30: *Captura de pantalla de phishig contra la SEAP en 2015.*

El remitente aparentemente utilizaba un dominio gubernamental venezolano, sin embargo, al editar las cabeceras, se pudo comprobar que el mensaje fue entregado por servidores correspondientes a una red ubicada físicamente en Lagos, Nigeria.

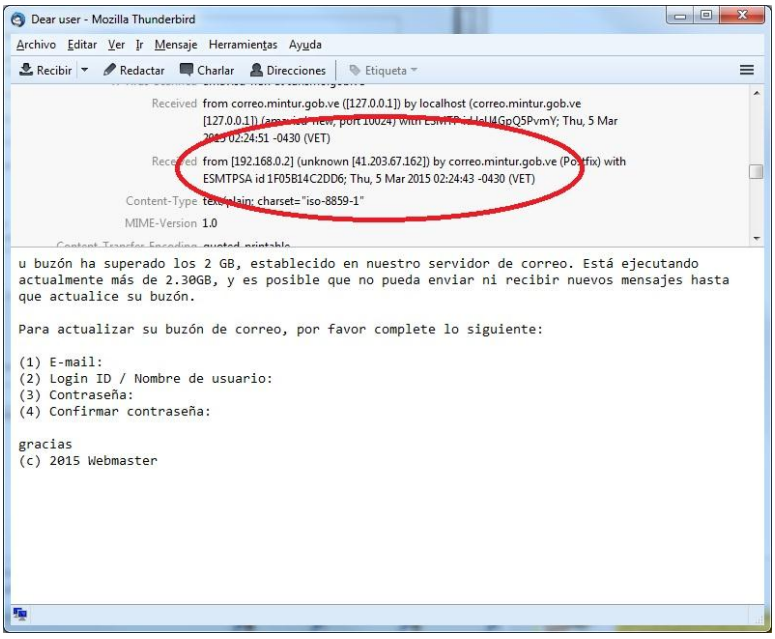

Figura 31: *Captura de pantalla de las cabeceras del phishing de 2015.*

Lo llamativo del phishing es que la información suministrada por la víctima no se dirigía al remitente nominal ni al enmascarado, se recepcionaba en un buzón de correo de un dominio .com diferente. Se pudo comprobar que la IP de destino estaba asociada a una red ubicada físicamente en Shenzhen, provincia de Guangdong, China. La red del grupo chino Tenzent aparece en la blacklist de CleanTalk como origen de 92 nodos activos de spam[114].

La precisión del ataque, el perfil gubernamental de las víctimas, el enmascaramiento del atacante, el refinamiento en el uso del idioma, el hecho de que haya coincidido con una renovación tecnológica en los sistemas de la SEAP, que implica también cambios en el software base y la implantación de mayores medidas de seguridad derivadas del ENS, que pueden haber acabado con vulnerabilidades prévias, hace pensar que se trata de una operación que ha podido prolongarse en el tiempo, ser persistente, y puede entrar en una fase de ataques más sofisticados.

No es extraño en cambio que estos phishing utilizaran plataformas nigerianas para su distribución. De hecho durante los últimos años las estafas electrónicas llevadas a cabo por las máfias subsaharianas a través del correo electrónico han caracterizado un tipo de fraude conocido como timo nigeriano, o 419 scam (estafa en inglés, pero también un juego de palabras, spam criminal).

Según indica el FBI norteamericano en su web oficial[115], los fraudes de la carta de Nigeria combinan la amenaza del fraude de suplantación de identidad con un tipo de estafa de cobro de cuotas por adelantado. Los estafadores envían un correo electrónico o carta por correo tradicional desde Nigeria que ofrece al destinatario la oportunidad de compartir un porcentaje de los millones de dólares que, según el autor de la carta (quien afirma ser un oficial del gobierno o un funcionario de banca), está intentando transferir fuera de Nigeria de forma ilegal.

Se solicita al destinatario que envíe información personal al autor de la carta, copias de documentación personal que será utilizada para falsificar documentos, nombre de bancos y números de cuentas bancarias, así como otro tipo de información útil para elatacante y que le permitirá refinar su estafa. Los estafadores son muy persistentes, posiblemente actúan en grupos organizados y especializados que mantienen la comunicación con la víctima en función del pefil que exprese. El éxito de la estafa depende de convencer a una víctima dispuesta que envíe dinero al autor de la carta en Nigeria, en forma de pagos parciales cada vez mayores, y con

[114] CleanTalk.org. Blacklist. https://cleantalk.org/blacklists/AS45090 (Ú.a.: 22/09/2015)
[115] "Fraude de carta de Nigeria sigue defraudando". FBI. 2015. https://www.fbi.gov/espanol/historias/fraude-de-carta-de-nigeria-sigue-defraudando (Ú.a.: 25/09/2015)

motivos diversos. Un 7% de los receptores de los envíos masivos en EE.UU. responde a esta estafa, y de ellos, un 20% llega a pagar alguna cantidad a los estafadores[116].

Las implicaciones legales son muchas. La mayoría de estados tipifican los delitos de evasión de capitales y blanqueo de dinero. En el caso de España, varias víctimas de este delito tuvieron que hacer frente a denuncias de la Fiscalís del Estado por estos cargos, ya que entregaron sus daos bancarios, efectivamente se realizaron transferencias a sus cuentas, pero estas no cesaron, las cuentas se utilizaron como parte de una ruta de transferencias internacionales en cantidades cada vez mayores, hasta que llamaron la atención de los servicios de inspección, que denunciaron el caso.

Nigeria por su parte no es condescendiente con las víctimas de la estafa, ya que implica colaboración con la organización criminal, fraude y evasión de capitales, que van en contra de las leyes nigerianas. Las estafas violan la sección 419 del código penal de Nigeria[117], de la que recibe el nombre este tipo de estafa.

Al respecto tengo la experiencia personal de haber recibido correos de más de 70 campañas de estas mafias nigerianas entre 2002 y 2009, a raiz de solicitar un certificado de identidad electrónica de Thawte a través de la Cámara de Comercio de Johannesburgo. La más elaborada y persistente desde enero de 2008 hasta diciembre de 2009, que llegó a involucrar a supuestos funcionarios de banca, incluido el CBM, Cental Bank of Nigeria, falsos funcionarios del FBI norteamericano, diplomáticos de Costa de Marfil o Sudáfrica, y compañías de seguros sudafricanas. Y de hecho, sigo siendo el único y legítimo heredero universal de una fortuna de 6 millones de dólares de Mr. Albert J. Fracas[118].

Las estafas por internet son prácticamente infinitas y van más allá de la estafa a través de envíos de spam malicioso. Uno de los métodos más agresivos de extorsión y estafa se consigue a través de la difusión de ransomware (o software de rescate), un malware catalogado como muy dañino, que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Según McAfee Labs el ransomware es originario de Rusia, pero existen más de 250.000 variantes, y desde 2013 ha tenido una expansión explosiva por todo el mundo. Las primeras

[116] Merce Molist. "El fraude del nigeriano". El País. 23/11/2006. http://elpais.com/diario/2006/11/23/ciberpais/1164252267_850215.html (Ú.a.: 25/09/2015)
[117] ICFNL. International Centre for Nigerian Law. "Código Penal Nigeriano. Part 6. Division 1. Chapter 38". Nigeria. http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm (Ú.a.: 25/09/2015)
[118] Foro de afectados por 419 scam. 419.bitten us.com. http://419.bittenus.com/7/11/MRALBERTJFRACAS.html (Ú.a.: 25/09/2015)

campañas se basaban en el malware Reveton, basado en el troyano Citadel, a su vez basado en el troyano Zeus[119]. Su vector de infección es a través de adjuntos de correos electrónicos y páginas webs de contenido pornográfico, que insertan código malicioso que la víctima se descarga al acceder. Su funcionamiento se basa en desplegar a través del payload un mensaje perteneciente a los cuerpos y fuerzas de seguridad, preferentemente del país de la víctima. Por este motivo se le empezó a conocer como "virus de la Policía", debido a que el mensaje alega que el sistema atacado ha sido utilizado para realizar actividades ilícitas, como el pirateo de software o traficar con pornografía infantil. Para dar verosimilitud al mensaje, se muestran la IP y datos de geolocalización del sistema. El troyano además muestra una advertencia informando que el sistema ha sido bloqueado como consecuencia de esta violación de la ley y el usuario debe pagar la correspondiente multa para poder desbloquearlo. Este pago debe realizarse por transferencia, o a través de cualquier otro medio electrónico.

Figura 32: *Captura de pantalla de la imagen de bloqueo mostrada por el ransomware Reveton. (Fuente: "Nueva variante de troyano REVETON (virus de la Policia)". Blog de SatInfo. 23/04/2013. http://www.satinfo.es/blog/2013/nueva-variante-de-troyano-reveton-virus-de-la-policia-cazado-por-la-heuristica-del-elistara/ Último acceso: 25/09/2015)*

[119] Ransomware. Wikipedia. https://es.wikipedia.org/wiki/Ransomware (Ú.a.: 25/09/2015)

En septiembre de 2013 la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, junto a la Fiscalía de la Audiencia Nacional desarrollaron desde el complejo policial de Canillas, una operación conducente a la detención de los responsables de la red criminal, que concluyó con la detención en Madrid de dos hackers ucranianos que vendían el acceso a los servidores de más de 21.000 empresas de 80 países, más de 1.500 de ellas en España, y eran responsables de blanquear los beneficios obtenidos de las víctimas del "virus de la Policía", para lo que habían ideado un método totalmente virtual. Este sofisticado entramado blanqueaba 10.000€ diarios a través de diferentes sistemas de pago electrónico y divisas virtuales (como Bitcoin, Linden Dolars, Webmoney o Perfect Money) entre las que el intercambio era constante para tratar de dificultar la trazabilidad de la procedencia ilícita[120].

También a finales de 2013 apareció una variante que encriptaba el sistema de archivos generando un par de claves RSA de 2048 bits practicamente imposibles de descifrar, denominada CryptoLocker. El rescate, equivalente a 1 bitcoin, debía realizarse en el plazo de 3 días, o en caso contrario se incrementaba el coste. En junio de 2014 se intervino la botnet GameOverZeuS (GOZ), y se pudo aislar el ransomware CryptoLocker. El Departamento de Justicia de EE.UU. presentó entonces cargos contra el hacker ruso Evgeniy Bogachev como responsable de dicha botnet, y de la estafa CryptoLocker, que generó pérdidas de cientos de millones de dólares y afectó a más de un millón de sistemas en todo el mundo. Se calcula que 235.000 víctimas realizaron el pago del rescate, la mitad de ellos en EE.UU., directamente a cuentas de Bogachev, generando una recaudación de más de 30 millones de dólares entre septiembre y diciembre de 2013[121].

En 2014 se anunció una nueva campaña de ransomware en España, que tuvo mucha incidencia entre usuarios de las AA.PP. El vector de infección era de nuevo el envío masivo de spam que distribuía una nueva variante de ransomware detectada como Trj/RansonCrypt.B. El mensaje mostrado suplantaba la identidad de la Sociedad Estatal de Correos y Telégrafos, y, al seguir los enlaces, dirigía a una web fraudulenta donde se solicitaba al usuario la introducción de un código captcha. Este paso tenía un doble propósito, descargar el ransomware e infectar a la víctima, e impedir el escaneado robotizado que permitiera obtener y aislar una copia del malware mutado[122].

[120] Nota de prensa. "Desarticulada la rama económica responsable del 'virus de la Policía' y que había comprometido la seguridad de 1.500 empresas en España". Cuerpo Nacional de Policía. http://www.policia.es/prensa/20130927_1.html (Ú.a.: 25/09/2015)
[121] "GameOver Zeus (GOZ) Malware and Botnet Architecture". FBI. Junio de 2014. https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/documents/gameover-zeus-and-cryptolocker-poster-pdf (Ú.a.: 25/09/2015)
[122] Marta López. "¡Atención! ¡Oleada de Ransomware simulando ser Correos!". Panda Mediacenter. 24/03/2015. http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/ (Ú.a.: 25/09/2015)

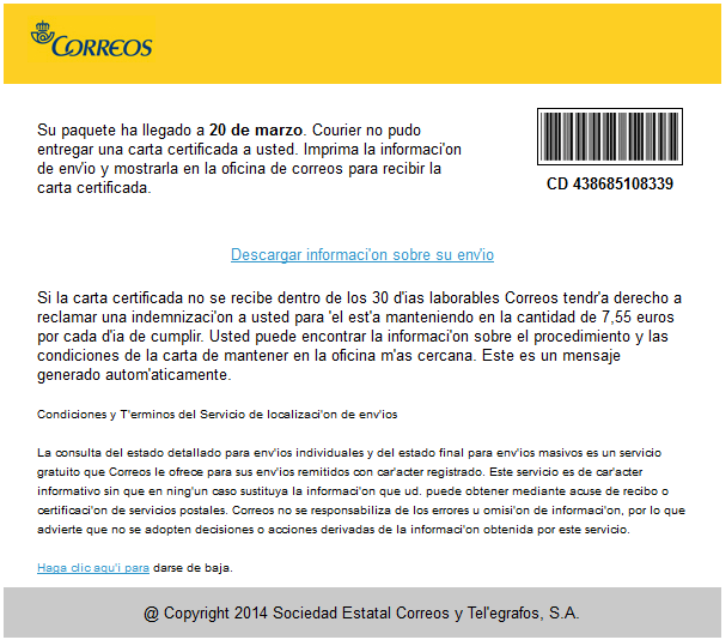

Figura 33: *Mensaje de spam fraudulento de suplantación de identida (fase 1). (Fuente: Marta López.Panda Mediacenter. 24/03/2015.* [*http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/*](http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/) *Último acceso: 25/09/2015)*

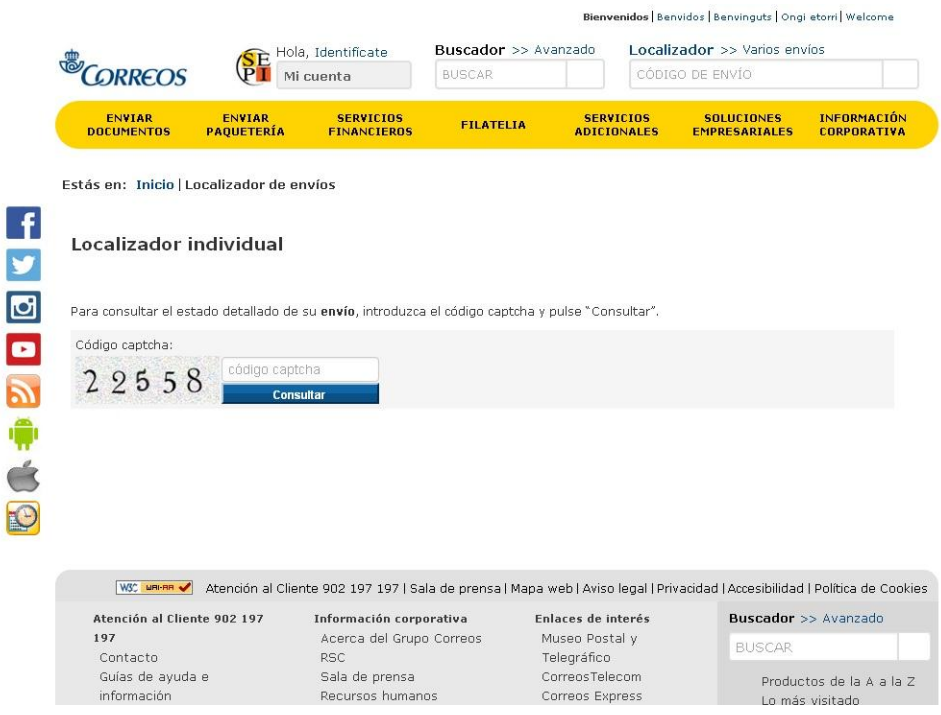

Figura 34: *Captura de pantalla de la web fraudulenta desde la que se produce la infección por ransomware (fase 2). (Fuente: Marta López.Panda Mediacenter. 24/03/2015.* [*http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/*](http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/) *Último acceso: 25/09/2015)*

Según McAfee Labs, el primer trimestre de 2015 estuvo marcado por la proliferación de nuevo ransomware, que creció un 165%, y por el malware diseñado para atacar a Adobe Flash Player, cuya incidencia aumentó un 317%[123] [124].

Los desarrollos implementados con el software de Adobe, para su ejecución en webs utilizando los plugins de Flash Player para el navegador, experimentaron un enorme crecimiento desde 2005, ya que aportaban un gran dinamismo y posibilidades de diseño ilimitadas a los diseñadores gráficos y desarrolladores de webs, con una gran calidad visual, convirtiéndose en el estándar multimedia de internet. Sin embargo han pasado a ser el elemento más vulnerable, tanto de las webs que alojan estos contenidos, o la publicidad desarollada con esta tecnología, como de los navegadores de usuarios a través de los plugins, siendo el vector de ataque preferido por los diseñadores de malware para atacar los sistemas[125]. Ésto ha provocado que las últimas versiones de varios navegadores, entre ellos Mozilla Firefox, inhabiliten por defecto el plugin de Adobe, y requieren la activación manual del usuario bajo su responsabilidad. Adobe ya anunció que abandonaba los desarrollos de Flash para plataformas móviles, y está condenado a ser sustituido también en otras plataformas por desarrollos en el estándar HTML5.

Estas vulnerabilidades son también las que aprovecha Equation, como se ha denominado al malware y, por extensión, al grupo que opera la red de ciberespionaje detectada en febrero de 2015[126]. Este malware, aún escasamente analizado, infectaría a sus víctimas a través de Flash utilizando el gusano Fanny, que a su vez descargaría uno o varios exploits desde los que modificar el Firmware de los dispositivos de almacenamiento del sistema, lo que permitiría mantener el control incluso aunque se modifique o se actualice el software base.

Equation al parecer desde 2001 ha infectado a decenas de miles de sistemas en más de 30 países, y sus víctimas pertenecen a los sectores gubernamental y diplomático, defensa, telecomunicaciones, tecnología aeroespacial, energía, investigación nuclear, petroleo y gas, nanotecnología, activismo islámico, medios de información, transporte, instituciones financieras y compañías de desarrollo de tecnologías de encriptación.

---

[123] CSO. “Se dispara el ransomware y el malware dirigido contra Adobe Flash”. ComputerWorld. 11/06/2015. http://cso.computerworld.es/tendencias/se-dispara-el-ransomware-y-el-malware-dirigido-contra-adobe-flash (Ú.a.: 25/09/2015)

[124] McAffee Labs. “Informe sobre amenazas. Mayo 2015” (p.5). Intel Security. http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2015.pdf?view=legacy (Ú.a.: 23/09/2015)

[125] CSO. “Nueva vulnerabilidad de día cero en Flash, la tercera en dos semanas”. Computerworld. 03/02/2015. http://cso.computerworld.es/alertas/nueva-vulnerabilidad-de-dia-cero-en-flash-la-tercera-en-dos-semanas (Ú.a.: 25/09/2015)

[126] Virus News. “Equation Group: The Crown Creator of Cyber-Espionage”. Kaspersky Lab. 16/02/2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage (Ú.a.: 25/09/2015)

Según Kaspersky, durante la fase de infección los operadores de Equation pueden utilizar hasta diez tipos diferentes de exploits, que a su vez explotan vulnerabilidades y métodos diferentes, sin embargo de forma sistemática, si no tienen éxito al tercer intento, abandonan el sistema sin infectarlo. Lo que hace único a Equation, y lo diferencia de las campañas descritas anteriormente es su increíble persistencia y sigilo, al quedar instalado el malware en el firmware del sistema (se ha detectado firmware modificado de discos SATA y de estado sólido de Western Digital, Samsung, Maxtor, Toshiba, IBM y Seagate)[127]; la capacidad de crear una zona de almacenamiento oculta en el disco físico, que aprovecha para exfiltrar enormes cantidades de información; su capacidad para actuar desde redes aisladas (air-gapped networks), ya que puede infectar un sistema desde una memoria USB, y aprovechar cualquier conexión de uno de estos dispositivos para exfiltrar la información; y por último la habilidad del malware para aprovechar cualquier medio de infección, incluso tecnologías muy clásicas, como propagar la infección a través de CDs, que a su vez resultaron infectados por métodos desconocidos.

Por sus características, algunos investigadores se refieren a Equation como una APT (Advanced Persistent Threat, o Amenaza Persistente Avanzada), y señalan la existencia de indicios de que los operadores de la red interactúen o tengan algún tipo de relación o vinculación con los operadores de Stuxnet, Duqu y Flame, generalmente desde una posición de superioridad jerárquica y operativa. Uno de estos indicios es que el gusano Fanny usado por Equation utilizaba en 2008 dos vulnerabilidades de día 0 que fueron introducidas en Stuxnet en junio de 2009. Una de estas vulnerabilidades explotadas por Stuxnet es un módulo de Flame.

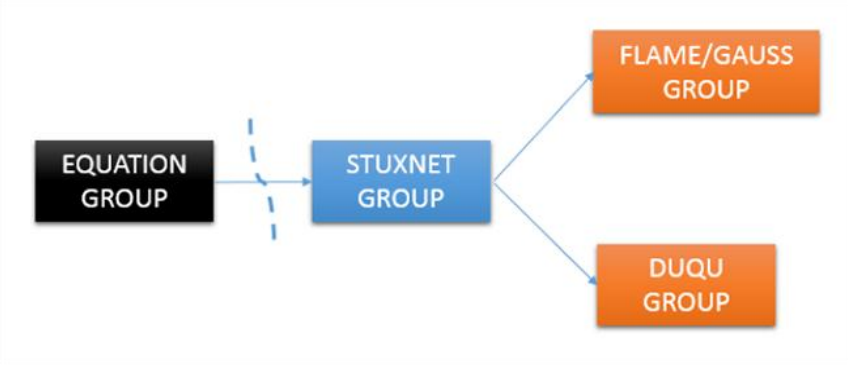

Figura 35: *Relación jerárquica supuesta entre grupos de ciberdelincuencia. (Fuente: "Equation Group: The Crown Creator of Cyber-Espionage". Kaspersky Lab. 16/02/2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage Último acceso: 25/09/2015)*

[127] McAffee Labs. "Informe sobre amenazas. Mayo 2015" (p.9). Intel Security. http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2015.pdf?view=legacy (Ú.a.: 23/09/2015)

Stuxnet apareció en 2009 como responsable del sabotaje a las centrifugadoras utilizadas por Irán para enriquecer uranio en el marco de su programa de fabricación de armamento nuclear. No se ha podido atribuir hasta la fecha la autoría, por lo que no se puede hablar propiamente de acto de ciberguerra, no obstante Stuxnet sí tiene la consideración de ciberarmamento.[128] El malware infectó los sistemas de control de las centrifugadoras y varió sus parámetros hasta dejarlas inoperativas.

Un poco después, a finales de 2011, el Laboratorio de Criptografía y Seguridad de Sistemas (CrySyS Lab) de la Universidad de Tecnología y Economía de Budapest, aisló y analizó un malware al que denominó Duqu, por los prefijos ~DQ de los ficheros que creaba[129]. Symantec, que continuó la investigación fue quien descubrió sus similitudes con Stuxnet. La infección por Duqu aparentemente fue muy controlada, afectó fundamentalmente a Hungría, Francia, Sudan e Irán, utilizando siempre técnicas de ingeniería social como vector de infección. Los atacantes parecían estar buscando información de sistemas de control industrial y comercial de organizaciones concretas[130]. No se registró actividad de Duqu desde 2012, y, excepto por sus similitudes con Stuxnet no parecía un malware de entidad. Hasta su reaparición en 2015[131].

Tan solo unos meses después del descubrimiento de Duqu, apareció Flame. Su descubrimiento fue anunciado en mayo de 2012 por MAHER (el Equipo de Respuesta ante Emergencias Informáticas de Irán), Kaspersky Lab y CrySyS Lab[132]. Flame se reveló como una compleja e inusual plataforma de ciberataque. Una vez aislado se comprobó que la infección había afectado a unos mil objetivos repartidos por todo el mundo, preferentemente de Oriente Medio, entre ellos Irán, Israel, Siria, Libano, Arabia Saudita, Egipto y Sudan, y con menos intensidad a EE.UU., Canadá, Rusia, varios países centroamericanos y, en mayor o menor medida, la totalidad de los países europeos. El vector de infección era un gusano capaz de autodistribuirse a través de internet o infectando memorias USB. Su funcionamiento era modular (con un tamaño extremadamente grande para un malware, 20MB) y muy complejo, haciendo uso de varias vulnerabilidades de Windows, que le permitían grabar audio, conversaciones de Skype, capturas de pantalla, pulsaciones de teclado y tráfico de red, y puede controlar la interfaz Bluetooth para intentar obtener información de los dispositivos Bluetooth cercanos.

---

[128] GReAT, Kaspersky Lab's Global Research & Analysis Team. "Stuxnet: Zero victims. The identity of the companies targeted by the first known cyber-weapon". ScureList. 11/09/2014. https://securelist.com/analysis/publications/67483/stuxnet-zero-victims/ (Ú.a.: 25/09/2015)
[129] Duqu. Wikipedia. https://en.wikipedia.org/wiki/Duqu (Ú.a.: 25/09/2015)
[130] Ryan Naraine. "Duqu FAQ". SecureList. 19/10/2011. https://securelist.com/blog/incidents/32463/duqu-faq-33/ (Ú.a.: 25/09/2015)
[131] GReAT, Kaspersky Lab's Global Research & Analysis Team. "The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns". SecureList. https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/ (Ú.a.: 25/09/2015)
[132] Flame. Wikipedia. https://es.wikipedia.org/wiki/Flame_%28malware%29 (Ú.a.: 25/09/2015)

Esta información, junto con los documentos almacenados en el ordenador, eran enviados a uno o varios servidores dispersos alrededor del mundo. Se localizaron al menos 80 sites diferentes que actuaban como centro de control en América del Norte, Asia y Europa. El perfil de las víctimas estaba muy definido: gubernamental, académicos e investigadores, y personas muy concretas. Se especuló mucho sobre su origen. Aunque no estaba directamente relacionado con Stuxnet, ni programado de la misma manera (Flame usa un lenguaje interpretado a base de scripts e incluye en su estructura modular la máquina virtual que lo ejecuta), hacía uso de similares vulnerabilidades de Windows, lo que llevó a Kaspersky a plantear que pudiera tratarse de un desarrollo paralelo controlado por los mismos creadores de Stuxnet. Al igual que Duqu, cesó su actividad en 2012[133].

Existe al menos otro derivado de Stuxnet descubierto también en las mismas fechas. Gauss llegó a afectar a más de 2.500 ordenadores y concentró sus ataques en el Líbano, Israel y territorios palestinos. Su principal objetivo era recabar información de las instituciones bancarias, transacciones comerciales y otros datos.

No está claro quien está detrás de estos malware. Sí parece que existe una relación entre los equipos de desarrollo de cada uno de ellos. Sin embargo, tras la aparición simultánea de Equation y Duqu 2.0 este año, se ha podido comprobar que existen infecciones mixtas, lo que daría a entender una cierta competencia entre los operadores de ambos grupos por la misma información.

La existencia de este tipo de malware plantea además muchas incognitas. Su uso como ciberarmamento, como ocurrió con Stuxnet, implica también su exposición, y la posibilidad por tanto de que sea reproducido.

Es bastante difícil que grupos terroristas con implantación en los paises más afectados por estos malware, como Al Qaeda o el Estado Islámico, pese a su interés, puedan aislar y hacerse con copias de algún derivado de Stuxnet, pero, aunque remoto, existe el riesgo de que organizaciones terroristas en algún momento se doten de ciberarmamento operativo, o lo adquieran en el mercado negro de la ciberdelincuencia, con la determinación de usarlo contra infraestructuras críticas[134].

Hasta la fecha no hay evidencias de que ningún grupo terrorista disponga de capacidad para atentar a través de internet, o de que se haya producido ningún incidente, y se les atribuye un

[133] Alexander Gostev. "The Flame: Questions and Answers". SecureList. 28/05/2012. https://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/ (Ú.a.: 25/09/2015)
[134] Emma Graham-Harrison. "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?". The Guardian. 12/04/2015. http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race (Ú.a.: 25/09/2015)

riesgo bajo de que puedan producir ciberataques. En todo caso, grupos yihadistas han ejecutado ciberataques a pequeña escala (esencialmente, desfiguraciones de páginas web y ataques DDoS), generalmente en respuesta a pretendidas hostilidades contra intereses islámicos, y que habría que encuadrarlos propiamente como acciones de ciberactivistas.

Más frecuente es la utilización de Internet con fines de financiación, coordinación, propaganda y reclutamiento[135]. Internet ofrece a las organizaciones terroristas un medio de fácil acceso, con poco o ningún control, que les permite el máximo anonimato, un rápido flujo de información, con altísimo impacto, escaso riesgo, barato e indetectable. Como expone el Grupo de Trabajo sobre Derecho y Cibercrimen del Observatorio para la Cibersociedad[136], ésto hace que se haya convertido en medio para procurar el reclutamiento de nuevos miembros, proporcionar adiestramiento a los integrantes de las distintas células, comunicarse, coordinar y ejecutar acciones, encontrar información, adoctrinar ideológicamente, promocionar sus organizaciones y desarrollar una guerra psicológica contra el enemigo.

Algunos grupos terroristas, como el IRA, Hamas, a través de la Fundación Tierra Santa para la Ayuda, o grupos terroristas chechenos, han divulgado por la red el número de cuentas bancarias a través de las que recaudar fondos de sus simpatizantes.

También se está usando internet como instrumento de guerra psicológica. Los terroristas utilizan este medio sin censura para propagar informaciones equivocas, amenazar o divulgar las imágenes de sus atentados. Los videos de las torturas, o incluso el asesinato, de rehenes y periodistas, han saltado de internet a los medios tradicionales de masas. El objetivo de estas grabaciones, que buscan deliberadamente el horror obsceno, refuerzan la sensación de indefensión de las sociedades occidentales, pero además sirven para cuestionar sus políticas, achacándoles la responsabilidad última de la violencia. Por otro lado, internet les permite también a estos grupos divulgar imágenes y videos de ataques soportados por civiles en varias zonas en conflicto, aunque sin acreditar y sin permitir que periodistas u observadores puedan contrastar las informaciones, tratando de incitar a la rebelión y a la lucha armada, y justificar a sus combatientes.

Aunque el reclutamiento tradicional de los grupos terroristas es a través del contacto directo y las relaciones de confianza, grupos como el Estado Islamico hacen uso de foros de internet para reclutar hombres que sirvan como combatientes y mujeres que estén dispuestas a asumir sus

[135] CCN-CERT-IA-09/15. "Ciberamenazas 2014. Tendencias 2015. Resumen ejecutivo". CCN. 09/04/2015. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html (Ú.a.: 23/09/2015)

[136] IV Congreso de la Cibersociedad (2009). Grupo de trabajo C-24: Derecho & cibercrimen. "Internet: Un espacio para el cibercrimen y el ciberterrorismo". Observatorio para la Cibersociedad. http://www.cibersociedad.net/congres2009/es/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610/ (Ú.a.: 25/09/2015).

postulados políticos y religiosos. Utilizan la información que sus sites proporcionan de los visitantes a sus webs, en las que explican como servir mejor a la Yihad, para contrastar su interés e implicación, y contactan posteriormente con los perfiles que mejor se adaptan a sus objetivos.

Los miembros de grupos terroristas han demostrado tambien una gran creatividad para aprovecharse de las capacidades de comunicación que les ofrece internet y el correo electrónico, evitando la intercepción de sus mensajes. Utilizan por ejemplo técnicas como la estenografía (que permite el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia), la encriptación y los semáforos rojos (que consiste en establecer un código de signos y convenciones, como el cambio de color de una imagen, que esconden un significado, una orden de ataque, la fecha y el lugar para una reunión, etc.). Aunque entre todos los métodos que emplean el más creativo sea establecer comunicaciones a través de cuentas de correo electrónico con nombres de usuarios y claves compartidas, de modo que las comunicaciones pueden establecerse usando borradores, como hicieron los terroristas de Al Qaeda para cordinar sus atentados de 2001 en EE.UU.

Internet es también una fuente inagotable de información, donde un terrorista puede obtener una enorme variedad de detalles acerca de sus posibles objetivos (mapas, horarios, detalles precisos sobre su funcionamiento, fotografías, visitas virtuales, etc.), la creación de armas y bombas, las estrategias de acción, etc. Pero, además, en algunos foros y páginas se distribuyen manuales operativos donde se explica como construir armas químicas y bombas, cómo huir, qué hacer en caso de detención policial, cómo realizar secuestros, o documentos críticos en los que se intenta extraer lecciones de conflictos pasados. Por ejemplo, los terroristas de los atentados de 2005 en Londres (7J), fabricaron los explosivos con fórmulas obtenidas a través de internet.

En algún momento varios grupos terroristas han dispuesto de páginas webs, como el Ejército Republicano Irlandés (IRA), el Ejército de Liberación Nacional Colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC), Sendero Luminoso, ETA o Hizbollah, que dispone habitualmente de varios mirrors, a fin de que si alguno cae, se pueda mantener la información y la cadena de legitimidad en los otros.

Pese a todo, algunos investigadores sostienen que algun grupo terrorista se sumará a una escalada ciberbélica en algún momento del futuro más próximo, y es sólo cuestión de tiempo que se produzca un ataque con consecuencias impredecibles[137].

[137] Samuel Gibbs. "Eugene Kaspersky: major cyberterrorist attack is only matter of time". The Guardian. 01/05/2014. http://www.theguardian.com/technology/2014/may/01/eugene-kaspersky-major-cyberterrorist-attack-uk (Ú.a.: 25/09/2015).

2.5. Ciberguerra y ciberarmamento.

La mayoría de autores coinciden en señalar que el concepto de ciberguerra se refiere al desplazamiento de un conflicto cuyo teatro de operaciones pasa a ser el ciberespacio, tiene como actores principales a los Estados, y se caracteriza por sus motivos políticos[138].

Tres aspectos del ciberespacio hacen posible la ciberguerra: el diseño de internet, los fallos y vulnerabilidades de hardware y software, y la tendencia a poner en línea cada vez más sistemas críticos.

Existen al menos seis vulnerabilidades en el diseño mismo de internet: el sistema de nombres de dominio (DNS); el enrutamiento entre ISP (Internet Service Provider), denominado BGP (Border Gateway Protocol); la falta de un gobierno de Internet; la transmisión de información ocurre en abierto sin codificar, y basta un packet sniffer para acceder a todo (snoop); la capacidad para propagar malware; y su diseño descentralizado[139].

Los fallos en hardware y software quizá sean el aspecto más importante. Se ha comentado la existencia de un mercado de adquisición de vulnerabilidades asociado al cibercrimen, pero no es menos importante la pérdida de control en la cadena de suministro de componentes hardware de los sistemas conectados a Internet. Los desarrolladores de hardware y software pueden introducir caballos de troya en el diseño de sus sistemas, que les habiliten el acceso, o incluso, un paso más allá insertar una bomba lógica. Esta estrategia es lo que se denomina *preparación del terreno*, y ningún estado la obvia cuando se plantea potenciales escenarios bélicos.

En su forma más básica una bomba lógica es un procedimiento de borrado de la información, pero en sus formas más avanzadas pueden primero ordenar al hardware hacer algo que lo dañe, como ordenar a la red eléctrica un aumento de tensión que funda transformadores y equipos, o aumentar puntualmente la presión de una red de distribución de gas, como ya se ha visto, confundir el sistema de señales de la red de trenes de alta velocidad, u ordenar a las superficies de control de un avión que lo pongan en picado, y, a continuación, borrarse y eliminar toda prueba.

El concepto de ciberguerra y el uso del ciberespacio como medio para el desarrollo de operaciones, tiene su precedente en la guerra electrónica y el uso y control del espectro

[138] Guerra informática. Wikipedia. https://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica (Ú.a.: 26/09/2015).
[139] Richard A. Clarke y Robert K. Knake. "Guerra en la red. Los nuevos campos de batalla". Ed. Planeta, 2011. (pp. 108 – 123).

electromagnético. Durante la Guerra Fría las dos potencias enfrentadas aprovecharon los conflictos declarados en varias zonas geográficas para tratar de extender sus zonas de influencia. Estos conflictos permitieron desarrollar y ensayar nuevos armamentos y técnicas. Algunos de estos conceptos fueron por ejemplo la guerra electrónica (EW), que se hizo habitual en muchos ejércitos como cobertura y apoyo táctico a sus tropas. El objetivo es impedir al enemigo el uso del espectro de emisiones electromagnéticas, confundiéndole o bloqueándole, mientas se conserva y defiende el uso propio. Las capacidades de guerra electrónica se mostraron muy útiles como apoyo a la inteligencia, esencial en las operaciones de penetración. Se desarrollaron conceptos como la inteligencia de comunicaciones (COMINT), inteligencia electrónica (ELINT) e inteligencia de señales (SIGINT).

La Segunda Guerra del Golfo, conocida también como Tormenta del Desierto, supuso un cambio de mentalidad en las reticencias de las cúpulas militares al empleo de técnicas informáticas para inhabilitar al enemigo antes de iniciar las llamadas operaciones cinéticas. El General Norman Schwarzkopf, al mando de las tropas de la coalición liderada por EE.UU., había rechazado en 1991 durante la Primera Guerra del Golfo, el plan propuesto por el Mando de Operaciones Especiales para infiltrar en Irak a un grupo de hackers que inhabilitaran su sistema de defensa. En 2003 sin embargo la situciación fue muy diferente. Los militares iraquíes pudieron comprobar las fehas previas a la invasión que sus redes de defensa habían quedado comprometidas. Miles de oficiales iraquíes recibieron correos electrónicos en los que el Mando Central norteamericano (CENTCOM) les comunicaba directamente sus planes para invadir Irak y sus recomendaciones para evitar bajas del lado iraquí. Se les informaba también que las unidades y fuerzas del ejército iraquí serían recompuestas tras el cambio de régimen.

A la imposibilidad de mantener la red de mando iraquí se sumó la inundación del espacio con señales electrónicas equívocas, que imposibilitaban no solo la detección del enemigo, sino reaccionar ante sus acciones y le otorgaban superioridad aérea. La campaña se inició con bombardeos de precisión sobre estaciones de transmisión y de radar, lo que obligó a los iraquíes a desactivar su sistema de alerta temprana y defensa, continuó con centros de mando, bases aéreas, y otros objetivos estratégicos utilizando misiles de crucero lanzados desde barcos situados en el Maditerráneo y el Golfo Pérsico, y desde aviones dotados de capacidades furtivas (invisibilidad al radar o stealth).

Cuando se inició la invasión terrestre muchos oficiales iraquíes optaron por obedecer las órdenes del CENTCOM, y las tropas de la coalición se encontraron con escasa oposición. Muchas unidades iraquíes habían aparcado sus blindados de forma ordenada a las afueras de sus bases, lo que facilitó su destucción a la aviación norteamericana.

A la administración Bush no le interesó actuar del mismo modo con los activos financieros del régimen de Sadam Hussein, evitando el precedente de violar las redes financieras, por temor a las consecuencias de un ciberasalto bancario.

En 2007 tuvo lugar un incidente significativo. En febrero de ese año el Parlamento de Estonia decidió la retirada de los símbolos de la ocupación soviética que aún quedaban en el país, entre ellas el memorial al soldado del Ejército Rojo construido por los soviéticos en Tallin. Estos memoriales se encuentran en las capitales de todos los países "liberados" por el ejército soviético durante la Segunda Guerra Mundial, y en muchos casos están protegidos por tratados internacionales bilaterales. Rusia presentó una protesta diplomática formal ante lo que consideró una afrenta ignominiosa por la profanación de las tumbas de los soldados soviéticos muertos en la Segunda Guerra Mundial, y situadas bajo el monumento, que dió pie a protestas de los estonios de origen ruso. En abril el gobierno estonio decidió el traslado de la estatua a un recinto militar y esto incendió a los medios más nacionalistas rusos y a la Duma, el Parlamento ruso.

Figura 36: *Memorial al soldado del Ejército Rojo en Tallin. (Fuente: "In pictures: A year in technology". BBC. 28/10/2007. http://news.bbc.co.uk/2/hi/in_pictures/7129507.stm Último acceso: 26/09/2015)*

El conflicto saltó entonces al ciberespacio. Los servidores de las páginas web más utilizadas de Estonia, incluidas webs gubernamentales y medios de comunicación, comenzaron a recibir severos ataques DDoS procedentes de Rusia y se bloquearon. Las dimensiones del ataque, en el que participaron varias botnets, con decenas o cientos de miles de ordenadores cada una, lo convirtieron en el más grande realizado hasta la fecha. Los estonios pensaron que se trataba de obra de hacktivistas rusos descontentos, sin embargo el ataque continuó hacia servidores DNS,

control de la red telefónica y el sistema de verificación de tarjetas de crédito. En ese momento más de un millón de ordenadores participaban del ataque DDoS. El Hansapank se vió comprometido y dejó de operar y se interrumpieron muchas de las transacciones comerciales y las comunicaciones del país. En acciones previas desarrolladas por hacktivistas los ataques DDoS duraban varios días. En el caso de Estonia fue diferente, centenares de sitios clave fueron atacados durante semanas, paralizando el país sin tiempo para recuperarse, hasta que Estonia elevó el asunto al Consejo de la OTAN[140].

Un equipo de expertos de la OTAN respondió al ataque con contramedidas, y se identificaron equipos pertenecientes a las botnets atacantes, que fueron sometidas a vigilancia hasta que se comunicaron para llegar a los centro de control. Éstos se localizaron finalmente en Rusia y se comprobó que el software empleado en las botnets había sido desarrollado en cirílico[141].

Estonia invocó el Tratado de Asistencia Legal Mutua con Rusia (MLAT) para que se investigara el origen del ataque, sin embargo la Duma rechazó la petición al considerar que el MLAT no era de aplicación.

Como resultado del incidente la OTAN creó un centro de ciberdefensa en Tallin, al que se le asignaron las funciones que actualmente desempeñan los CERT[142].

Rusia atribuyó el ataque a una campaña de hacktivistas y patriotas que actuaron en respuesta a la provocación estonia. El análisis de los objetivos implicaba un conocimiento importante de las redes y servidores estonios y el acceso a información que no es de dominio público. La coordinación y profundidad de las acciones tampoco respondía al patrón de ataques indiscriminados. Por último el ataque utilizó como vector varias botnets con control centralizado. Los expertos de la OTAN sugirieron que estos grupos debieron actuar bajo las directrices de los servicios secretos rusos. El ataque a Estonia tuvo un enorme impacto en los medios de comunicación, pero alertó de la posibilidad de actos de ciberguerra entre dos estados, evidenció la vulnerabilidad de las sociedades tecnológicas e ilustró los efectos que puede tener un ataque organizado.

En septiembre de 2007 los medios de comunicación de varios países[143] [144] atibuyeron a la aviación de Israel la destrucción de la planta nuclear siria en construcción en Al Kibar, cerca de

[140] Ricardo Martínez de Rituerto. "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE". El País. 18/05/2007. http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html (Ú.a.: 26/09/2015).
[141] Ian Traynor. "Russia accused of unleashing cyberwar to disable Estonia". The Guardian. 17/05/2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia (Ú.a.: 26/09/2015).
[142] EFE. "Estonia protegerá sus instituciones de ataques informáticos con ayuda de la OTAN". El Mundo. 18/05/2007. http://www.elmundo.es/navegante/2007/05/18/tecnologia/1179478759.html (Ú.a.: 26/09/2015).

la frontera turca, parte supuestamente de un programa secreto sirio, desarrollado en colaboración con técnicos norcoreanos, para obtener plutonio y fabricar armas nucleares. El gobierno israelí tardó un mes en reconocer la autoría, y no hizo declaraciones oficiales sobre la operación, como sí lo hizo en 1981 cuando destruyó la planta nuclear iraquí de Osirak[145]. La operación se conoce como Operación Orchard[146].

Las reacciones internacionales fueron muy confusas. Siria informó que habían respondido con fuego antiaéreo a un bombardeo israelí a instalaciones militares abandonadas en el desierto, y negó categóricamente que técnicos norcoreanos participaran en un proyecto de carácter nuclear. Extremo que corroboró el gobierno norcoreano. Inspecciones posteriores a cargo de la OIEA (Organismo Internacional de la Energía Atómica), dependiente de Naciones Unidas, y de inspectores del ISIS (Institute for Science and International Security), certificaron la existencia en el lugar del ataque de material radiactivo procesado procedente del reactor nuclear de Yongbyon, en Corea del Norte[147], lo que suponía de hecho la violación del Tratado de No Proliferación Nuclear.

Lo que llamó la atención de esta operación fue la capacidad de la aviación israelí para penetrar el espacio aéreo sirio durante varias horas con aviones sin capacidades furtivas (stealth), alcanzar su objetivo y bombardearlo con precisión sin que la aviación siria reaccionara. Rusia e Irán en particular se sintieron muy concernidos. Rusia había vendido a Siria los sistemas de defensa de última tecnología Tor-M1 y Pechora-2A, e Irán estaba interesado en su adquisición para proteger su propio programa de desarrollo nuclear. Rusia no podía explicar porqué su sistema había quedado ciego durante el ataque, lo que quedó claro a los rusos es que su sistema de última tecnología había sido objeto de un ciberataque inhabilitante.

Diversos analistas especularon sobre cómo había podido desarrollarse este ataque. Tres teorías se han mantenido como plausibles. Un comando de fuerzas especiales se infiltró en Siria y localizó los tendidos de fibra óptica de la red de defensa antiaérea siria, que se extiende por todo el país, y logró unirse a ella, hackeándolo in situ o instalando algún dispositivo que permitiera,

---

[143] David E. Singer; Mark Mazzetti. “Israel Struck Syrian Nuclear Project, Analysts Say”. The New Yory Times. 14/10/2007. http://www.nytimes.com/2007/10/14/washington/14weapons.html?_r=0 (Ú.a.: 26/09/2015).
[144] Erich Follath; Holger Stark. “The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor”. Der Spiegel. 02/11/2009. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html (Ú.a.: 26/09/2015).
[145] Daveed Gartenstein-Ross; Joshua D. Goodman. “The Attack on Syria's al-Kibar Nuclear Facility”. The Jewish Policy Center (2009). http://www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility (Ú.a.: 26/09/2015).
[146] Operación Orchard. Wikipedia. https://en.wikipedia.org/wiki/Operation_Orchard (Ú.a.: 26/09/2015).
[147] David Albright; Paul Brannan. “Syria Update III: New information about Al Kibar reactor site”. ISIS. 24/04/2008. http://isis-online.org/uploads/isis-reports/documents/SyriaUpdate_24April2008.pdf (Ú.a.: 26/09/2015).

mediante un enlace satélite, dar acceso remoto al sistema para hackearlo. Se trata de una operación complicada y arriesgada, pero no imposible. Según una segunda teoría los servicios secretos israelíes pudieron hackear el software ruso de los sistemas de control durante su desarrollo, incorporando algún troyano capaz de actuar al recibir una señal, y abrir una ventana en el sistema para no responder a ningún evento durante ese tiempo. Implicaría un esfuerzo considerable de los servicios secretos israelíes, o de algun otro país con el que colaborasen, así como una enorme capacidad de anticipación, pero no es imposible. Una tercera teoría proponía la posibilidad de usar las emisiones de radar para hackear los sistemas de control de los radares. Según esta teoría el ejercito israelí pudo hacer uso de un avión no tripulado con tecnología furtiva que habría penetrado el espacio sirio sin ser detectado, pero sí habría podido leer las emisiones del sistema de radar, y habría utilizado esta frecuencia para responder a los sistemas ejecutando una inyección de código que permitió descargar un gusano con instrucciones para dejar el sistema en el estado descrito anteriormente. Ninguna teoría ha sido confirmada o probada[148].

A finales de 2007 el Ministerio de Interior del gobierno chino denunció que hackers extranjeros, desde Taiwan y EE.UU. fundamentalmente, habían accedido sus sistemas y habían estado robando información de áreas clave en China. En particular se hizo mención de una campaña que afectó a la intranet de China Aerospace Science & Industry Corporation (CASIC). El vector de ataque al parecer habría sido un spyware que habría estado actuando desde 2006. La afirmación resultaba sorprendente entre numerosas acusaciones de Corea del Sur, Japón, EE.UU., India y varios paises europeos, entre ellos Francia, Alemania y Reino Unido, que denunciaban los constantes ataques chinos contra sus empresas y las constantes violaciones de los derechos de propiedad intelectual e industrial. Estas denuncias se incrementaron a lo largo de 2008. China a su vez se ha quejado siempre de lo grosero y poco profesional que resultan las acusaciones sin aportar evidencias.

Entre las muchas denuncias por ciberespionaje a China[149], el Departamento de Defensa de EE.UU. afirma que la tecnología del caza furtivo de 5ª generación Shenyang J-31, fue obtenida de forma ilegítima de los desarrollos del Lockheed Martin F-35 Lightning, a través de la Oficina China de Información Técnica con sede en la provincia de Chengdu, y de allí fueron suministrados a la corporación estatal aeronáutica china, encargada de filtrar la información y suministrarla a empresas de los sectores aeroespacial y tecnológico, lo que facilitó a los chinos un salto tecnológico de dos generaciones y varias décadas de desarrollos.

[148] Richard A. Clarke y Robert K. Knake. "Guerra en la red. Los nuevos campos de batalla". Ed. Planeta, 2011. (pp. 17 – 26).
[149] "Las acusaciones de EE UU a China por espionaje". El País. 19/05/2014. http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html (Ú.a.: 27/09/2015).

Figura 37: *El Shenyang J-31 y el Lockheed Martin F-35 Lightning. (Fuente: "China shows off new J-31 stealth fighter". AsianTown.com, 2014. http://news.asiantown.net/r/41040/china-shows-off-new-j-stealth-fighter Último acceso: 27/09/2015)*

En agosto de 2008 la situación política en Georgia era muy inestable. Las provincias con mayoría de población rusa al norte del país, Abjasia y Osetia del Sur, controladas por rebeldes prorusos desde 1992, provocaron un conflicto con el ejército georgiano al realizar varios ataques con misiles. La respuesta georgiana fue la invasión de Osetia del Sur. Ciberatacantes rusos entraron inmediatamente en acción lanzando ataques DDoS contra las webs del gobierno y medios de comunicación georgianos, y, tomando el control de los routers rusos y turcos por los que circula el tráfico de internet georgiano, mediante ataques de DNS bloquearon el acceso a otras fuentes de información externa, siguiendo el mismo patrón que unos meses antes se utilizó en Estonia. Al mismo tiempo Rusia inició los bombardeos en la región, la invadió con enorme facilidad y ocupó un territorio georgiano que no estaba en disputa para crear una zona de interposición. Abjasia aprovechó también la confusión y la falta de información para expulsar a los georgianos con apoyo del ejército ruso, que tomó otra parte del territorio georgiano para crear una nueva zona de interposición, lo que además ofreció a Rusia el control de la zona nororiental del Mar Negro.

Georgia intentó contrarrestar los ataques DDoS, pero los ciberatacantes frustraron cada movimiento[150]. Al intentar bloquear el tráfico ruso, los ciberatacantes modificaron sus paquetes para simular que procedían de China. Aunque el centro de control de las botnets estaba en Moscú, los atacantes comenzaron a utilizar máquinas canadienses, turcas, e irónicamente estonias. Cuando Georgia perdió el control de su dominio .ge, sus servidores institucionales se tuvieron que trasladar al extranjero, pero los atacantes respondieron creando webs falsas y redirigiendo el tráfico. La banca georgiana apagó sus servidores para proteger la información, pero los ciberatacantes rusos hicieron que hasta seis de sus botnets iniciaran un ataque DDoS contra webs bancarias internacionales simulando un ataque georgiano. La respuesta automatizada fue un bloqueo de las comunicaciones con Georgia que afectó a tarjetas de crédito y telefonía móvil[151].

Como en el caso de Estonia el gobierno ruso afirmó que se trataba de una respuesta popular espontánea antigeorgiana, y que sus operaciones militares habían tenido el propósito exclusivo de asegurar la paz. Es cierto en cualquier caso, como afirmó Gadi Evron, Director del CERT israelí, que los rusos hubieran podido destruir cinéticamente la infraestructura de acceso a internet de Georgia.

A mediados de 2009 Corea del Sur denunció que había sido objeto de un ciberataque desde Corea del Norte[152], que se desarrolló entre el 4 y el 9 de julio, y había afectado a varios organismos gubernamentales, incluyendo la red del NISK (National Inteligence Service of Korea). El ataque al parecer se había implementado infectando a 86 websites en 16 países, entre ellos EE.UU. Guatemala, Japón y China, que a su vez habían distribuido el código malicioso para construir una botnet para ejecutar ataques DDoS. Tras el análisis del código malicioso el NISK acusó a Corea del Norte de estar detrás de estos ataques.

Los casos de Estonia y Georgia están considerados por una mayoría de analistas como los dos primeros casos efectivos de ciberguerra. Sin embargo se trataron de ataques cuya tecnología se ha utilizado ampliamente por grupos de ciberactivistas. En 2010 Iran informó de un ciberincidente que marcó un antes y un después en las operaciones de ciberguerra.

[150] Tom Spiner. "Georgia accuses Russia of coordinated cyberattack". CNet. 11/08/2008. http://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/ (Ú.a.: 26/09/2015).
[151] Cyberattacks during the Russo-Georgian War. Wikipedia. https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War (Ú.a.: 26/09/2015).
[152] Associated Press. "North Korea launched cyber attacks, says south". The Guardian. 11/07/2009. http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks (Ú.a.: 26/09/2015).

Según indicó la agencia oficial iraní IRNA[153], varios ordenadores personales en las instalaciones nucleares iraníes habían resultado infectados por el gusano Stuxnet[154]. Posteriormente trascendió que la infección no había afectado únicamente a los ordenadores del personal directivo, sino que se había esparcido por los sistemas que controlaban más de un millar de centrifugadoras de enriquecimiento de uranio en varias instalaciones asociadas al programa nuclear iraní. Irán responsabilizaba de este ataque directamente a Israel[155].

Como ya se ha comentado, el gusano mostró la capacidad de actuar contra estos sistemas, reprogramar los parámetros de funcionamiento e inhabilitarlos de forma pemanente. Kaspersky Lab, Symantec, CrySyS Lab, y el MAHER (el Equipo de Respuesta ante Emergencias Informáticas de Irán), han estado analizando Stuxnet y otro malware posterior, encontrando características comunes entre todos ellos, especialmente entre las familias Stuxnet, Duqu/Gauss Flame, y el reciente Equation[156].

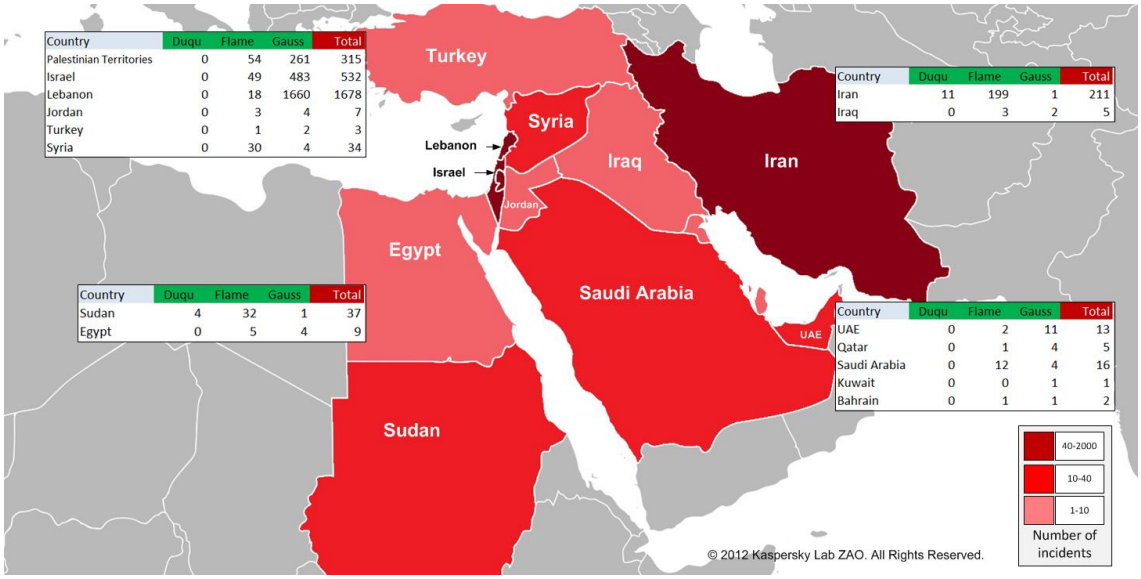

***Figura 38**: Incidentes ocasionados por Duqu, Flame y Gauss en Oriente Medio (Fuente: "Equation Group: The Crown Creator of Cyber-Espionage". Kaspersky Lab. 16/02/2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage Último acceso: 25/09/2015)*

[153] "Stuxnet worm hits Iran nuclear plant staff computers". BBC. 26/09/2010. http://www.bbc.com/news/world-middle-east-11414483 (Ú.a.: 26/09/2015).
[154] Stuxnet. Wikipedia. https://en.wikipedia.org/wiki/Stuxnet (Ú.a.: 26/09/2015).
[155] EFE, Teherán. "Irán reconoce un ataque informático masivo contra sus sistemas industriales". El Mundo. 27/09/2010. http://www.elmundo.es/elmundo/2010/09/27/navegante/1285571297.html (Ú.a.: 26/09/2015).
[156] "Equation Group: The Crown Creator of Cyber-Espionage". Kaspersky Lab. 16/02/2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage Ú.a.: 25/09/2015)

Kaspersky, en su boletín de seguridad de diciembre de 2012 mostraba las conclusiones de la recopilación de miles de incidentes relativos a infecciones por este malware capaz de actuar sobre el mundo físico, y su expansión en toda la zona de Oriente Próximo, una dinámica que consideraba un reflejo exacto de los procesos políticos en la región, que le llevó a afirmar que todo ello le permitía clasificarlos como uso de armas cibernéticas[157].

En 2013 se cruzaron acusaciones de ciberataques entre dos países tradicionalmente enfrentados, Pakistan e India. Según informaciones de Symantec[158], varios investigadores habían estado recopilando incidentes que catalogaron dentro de una operación bautizada como Hangover. Los afectados, mayoritariamente en países de Medio Oriente y Sudeste asiático, tenían perfiles gubernamentales. El vector de ataque eran campañas de spear phishing infectadas con un exploit, conducente a provocar la descarga de un troyano que permitía una comprobación inicial del sistema y el perfil de la víctima. En su caso se descargaba un payload completo para realizar una exfiltración de información más profunda. El análisis del malware mostró que aprovechaba vulnerabilidades de día 0 asociadas al uso de Windows de los ficheros de formato TIFF[159]. Symantec apuntaban a un origen indio de la operación.

Por las mismas fechas FireEye y ThreatConnect informaron de la operación Arachnophobia[160], una serie de ataques dirigidos utilizando mutaciones del malware Bitterbug, y aparentemente organizados desde Pakistán. Aunque los ataques se controlaban desde servidores virtuales ubicados en máquinas ubicadas en EE.UU., los analistas encontraron que las mutaciones de Bitterbug utilizadas contenían cadenas de texto que pudieron asociar a la empresa de seguridad pakistaní Tranchulas (tarántula).

En 2014 se produjo otra cadena de incidentes significativa. Tras el anuncio del estreno de la película "The Interview", una parodia del lider norcoreano Kim Jong-un, la productora Sony Pictures hizo público que estaba siendo objeto de un ciberataque de un grupo autodenominado #GOP, que posteriormente se identificó como Guardians of Peace (Guardianes de la Paz)[161]. El ataque provocado por el malware Destover inutilizó las redes de Sony durante semanas. Varios

[157] Alexander Gostev. "Kaspersky: Boletín de seguridad 2012. Las armas cibernéticas". VirusList. 18/12/2012. http://www.viruslist.com/sp/analysis?pubid=207271197 (Ú.a.: 24/09/2015).
[158] "Operation Hangover: Q&A on Attacks". Symantec. 20/05/2013. http://www.symantec.com/connect/blogs/operation-hangover-qa-attacks (Ú.a.: 27/09/2015).
[159] Gregg Keizer"'Operation Hangover' hackers exploit latest Windows zero-day". ComputerWorld. 07/11/2013. http://www.computerworld.com/article/2485693/malware-vulnerabilities/-operation-hangover--hackers-exploit-latest-windows-zero-day.html (Ú.a.: 27/09/2015).
[160] Pierluigi Paganini. "Operation Arachnophobia, targeted attacks from Pakistan". Security Affairs. 21/08/2014. http://securityaffairs.co/wordpress/27666/intelligence/operation-arachnophobia-pakistan.html (Ú.a.: 27/09/2015).
[161] "The Interview: A guide to the cyber attack on Hollywood". BBC. 29/12/2014. http://www.bbc.com/news/entertainment-arts-30512032 (Ú.a.: 27/09/2015).

analistas de AlienVault Labs, Symantec y Karspersky Lab, señalaron que el malware había sido escrito en coreano, y atribuyeron el origen de estos ataques a Corea del Norte[162]. Anonymous responsabilizó también al gobierno de Pyongyang de los ataques, contrarios a la libertad de expresión, e hizo pública su intención de responder con un contraataque. El Director de Inteligencia Nacional de EE.UU., James Clapper, describió el ataque como el más grave realizado a empresas e intereses norteamericanos, atribuyéndolo a Corea del Norte[163]. El propio Presidente de EE.UU., Barak Obama, declaró que daría una respuesta proporcionada al ataque norcoreano[164]. En diciembre la agencia de noticias china Xinhua informó que las comunicacines de internet en Corea del Norte llevaban varios días completamente paralizadas[165]. No ha trascendido por el momento cómo se produjo este bloqueo, y continúa la confusión sobre la atribución de los ataques.

A lo largo de 2015 se han ido sucediendo multitud de noticias relacionadas con ciberincidentes, y acusaciones de varios estados atribuyendo su origen a actuaciones de los servicios de inteligencia, unidades específicas de ciberguerra o grupos organizados de otros estados.

En marzo Turquía sufría un apagón eléctrico que afectó a más de 40 millones de personas. El gobierno turco acusó a Irán de ser el responsable del ciberataque que lo provocó, como respuesta por las acciones contra el régimen sirio de Bashar alAsad, y el apoyo turco a los rebeldes de Yemen[166]. En caso de confirmarse se trataría de un acto de ciberguerra.

Días después la televisión francesa TV5Monde anunció que había sido objeto de un ciberataque[167] que se atribuyó al Estado Islamico (IS), a través de un autodenominado "CyberCaliphate". El ataque aparentemente fue contratado por el IS a través del mercado negro

[162] Tom Fox-Brewster. "Sony Pictures hack: how much damage can North Korea's cyber army do?". The Guardian. 05/12/2014. http://www.theguardian.com/technology/2014/dec/05/sony-pictures-hack-north-korea-cyber-army (Ú.a.: 27/09/2015).
[163] Andrew Buncombe. "Sony Pictures hack: US intelligence chief says North Korea cyberattack was 'most serious' ever against US interests". The Independent. 07/01/2015. http://www.independent.co.uk/news/world/americas/us-intelligence-chief-sony-hack-was-most-serious-attack-against-us-interests-9963504.html (Ú.a.: 27/09/2015).
[164] David Carr. "How the Hacking at Sony Over 'The Interview' Became a Horror Movie". The New York Times. 21/12/2014. http://www.nytimes.com/2014/12/22/business/media/hacking-at-sony-over-the-interview-reveals-hollywoods-failings-too.html?_r=0 (Ú.a.: 27/09/2015).
[165] Reuters/Europa Press. "La conexión a Internet en Corea del Norte está paralizada por completo, según medios oficiales chinos". Europa Press. 27/12/2014. http://www.europapress.es/internacional/noticia-conexion-internet-corea-norte-paralizada-completo-medios-oficiales-chinos-20141227155330.html (Ú.a.: 27/09/2015).
[166] Pierluigi Paganini. "Iran accused of the blackout that paralyzed the Turkey". Security Affairs. 04/05/2015. http://securityaffairs.co/wordpress/36536/cyber-warfare-2/iran-accused-blackout-turkey.html (Ú.a.: 27/09/2015).
[167] Don Melvin; Greg Botelho. "Cyberattack disables 11 French TV channels, takes over social media sites". CNN. 09/04/2015. http://edition.cnn.com/2015/04/09/europe/french-tv-network-attack-recovery/ (Ú.a.: 27/09/2015).

ruso[168]. De confirmarse representaría un precedente de ciberterrorismo con consecuencias impredecibles[169].

China ha sido centro permanente de atención y protagonista de muchos titulares, como origen de permanentes oleadas de ciberataques[170] y contínuas acusaciones de ciberespionaje por parte de EE.UU. y otros países occidentales[171]. Estas acusaciones han sido siempre rechazadas por el gobierno chino[172]. La acusación formal contra militares chinos, anunciada en Washington en mayo de 2014 por el fiscal general Eric Holder, titular del Departamento de Justicia de EE.UU., representa la primera vez que se presentan imputaciones criminales contra funcionarios gubernamentales de otro país por ciberespionaje[173]. Según una estimación citada por The Washington Post, el ciberespionaje comercial cuesta a EE UU entre 24.000 y 120.000 millones de dólares al año (entre 17.500 y 88.000 millones de euros).

La acusación fue motivada por la presentación a finales de 2013 del informe de la consultora de seguridad Mandiant, "APT1. Exposing One of China's Cyber Espionage Units"[174], que revolucionó el sector de la seguridad informática. En este informe, resultado de una investigación iniciada en 2004, se exponía la actividad de la Unidad 61398 del Ejécito Popular de Liberación chino, se identificaba a algunos de sus integrantes, y se mostraban pruebas que permitían atibuirles la autoría de numerosos actos de ciberespionaje llevados a cabo desde 2006.

El informe popularizó el concepto de APT, Advanced Persistent Threat, como el conjunto de actividades y técnicas que permiten mantener una campaña de ciberespionaje de manera sigilosa y persistente. Además revelaba la existencia de una estrategia militar global centrada en el concepto de guerra asimétrica, por el que China se planteaba el escenario de un futuro

---

[168] John Lichfield. "TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link". The Independent. 10/06/2015. http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html (Ú.a.: 27/09/2015).

[169] Pablo Romero. "'Es una cuestión de tiempo que los 'ciberataques' tengan un impacto real en el mundo físico'. Entrevista a James Lyne, responsable de investigación de Sophos". El Mundo. 31/05/2014. http://www.elmundo.es/tecnologia/2014/05/31/5386f33de2704e99648b456e.html (Ú.a.: 27/09/2015).

[170] "Oleada de ciberataques desde China". El País. 07/03/2011. http://tecnologia.elpais.com/tecnologia/2011/03/07/actualidad/1299492061_850215.html (Ú.a.:27/09/2015).

[171] "Las acusaciones de EE UU a China por espionaje". El País. 19/05/2014. http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html (Ú.a.:27/09/2015).

[172] Macarena Vidal. "China considera "irresponsables" las acusaciones de ciberespionaje". El País. 05/06/2015. http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433503775_500727.html (Ú.a.:27/09/2015).

[173] Marc Bassets. "Washington acusa a cinco militares chinos de ciberespionaje industrial". El País. 19/05/2014. http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html (Ú.a.:27/09/2015).

[174] "APT1. Exposing One of China's Cyber Espionage Units". Mandiant, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (Ú.a.:05/03/2015).

enfrentamiento armado con EE.UU. impidiéndole utilizar su fuerza militar y provocándole un daño inhabilitante atacando sus infraestructuras críticas. El desarrollo de esta estrategia se basa en el zhixinxiquan, el "dominio de la información", y la Unidad 61398 sería la encargada de asumir esta función.

Desde la publicación del informe Mandiant, varias empresas de seguridad informática han anunciado la existencia de otra APTs, caracterizándolas por su ciclo de vida y distinguiéndolas de otro tipo de amenazas.

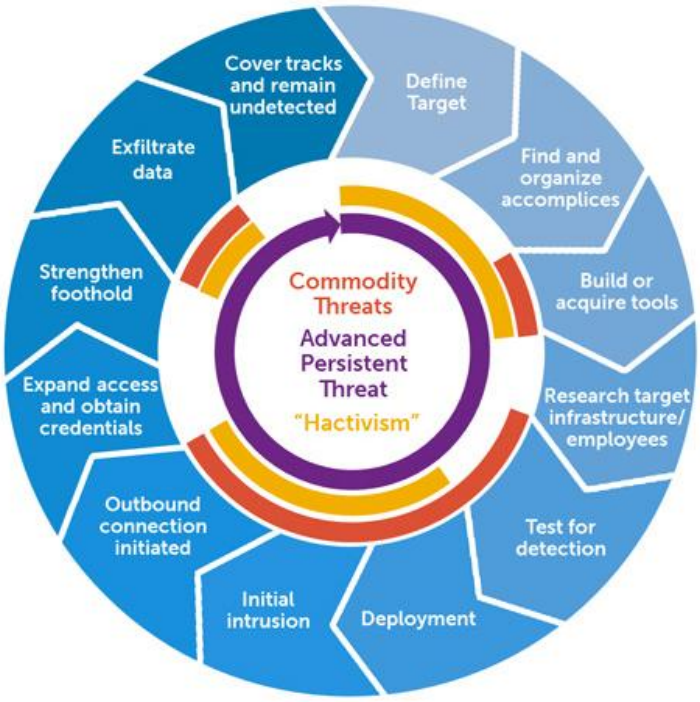

***Figura 39**: Ciclo de vida de una APT (Fuente: Advanced persistent threat. Wikipedia. https://en.wikipedia.org/wiki/Advanced_persistent_threat Último acceso: 25/09/2015)*

SecureList dispone de una base de datos interactiva donde pueden consultarse todas las APTs descubiertas hasta la fecha, Targeted CyberAttaks LogBook[175], construida en base a toda la información recopilada por Kaspersky Labs desde 2004,.

España no es ajena al uso de estas tecnologías y a principios de año trascendió que el gobierno español podía estar detrás del troyano Careto, que había infectado ordenadores en Marruecos, Brasil, Cuba, Gibraltar y País Vasco, al menos desde 2006 y hasta que fue descubierto por Kaspersky[176].

[175] Kaspersky Lab. Targeted CyberAttaks LogBook. https://apt.securelist.com/ (Ú.a.:05/03/2015).
[176] Ignacio Cembrero. "Un 'troyano' español espiaba en Marruecos". El Mundo. 15/02/2015. http://www.elmundo.es/espana/2015/02/15/54dfb6d3e2704e5a7f8b456c.html (Ú.a.:05/03/2015).

En 2009, en los peores momentos de la crisis económica y de la incertidumbre sobre el futuro del euro, también Francia espió a España[177], valiéndose del troyano Babar para tratar de determinar las decisiones que el gobierno de Rodríguez Zapatero tomaría al respecto. La información trascendió a través de las revelaciones de Edward Snowden, que fueron publicadas por Le Monde. Se atribuía a la DGSE francesa el desarrollo de Babar inicialmente para espiar a Irán, al igual que ocurrió con Stuxnet.Posteriormente sin embargo el troyano apareció en algunos otros países, entre ellos España, Canadá, Noruega, Grecia, Argelia y Costa de Marfil.

Recientemente el CNI hizo pública la contratación de 50 expertos en ciberguerra.[178]

Sin embargo no todo son ataques y amenazas, también ha habido movimientos en otros sentidos, como el Pacto de no ciberagresión entre China y Rusia. Según publica el INCIBE, China y Rusia han firmado un pacto por el que se comprometen a no realizar ataques informáticos entre si. Además se comprometen a colaborar para contrarrestar conjuntamente tecnología que pueda desestabilizar el ambiente político y socio-económico interno, alterar el orden público o interferir en los asuntos internos del Estado. Los dos países acordaron el intercambio de información entre las diferentes agencias encargadas del cumplimiento de la ley, el intercambio de tecnología y de garantizar la seguridad de las infraestructuras de información[179].

Aunque los términos ciberarmamento y ciberguerra resultan muy polémicos para los expertos, lo cierto es que todos los estados están tratando de dotarse de esta tecnología, incluso antes de establecer una política de ciberdefensa que pueda paliar los efectos de su uso[180]. La dependencia tecnológica va en aumento, las vulnerabilidades crecen, al igual que los incidentes, y también un cierto estado de paranoia.

Hay otros aspectos relativos a la seguridad del estado que representan graves vulnerabilidades. Como hemos visto Rusia aparentemente ha tratado de dominar los medios de comunicación de internet mediante ataques muy dirigidos, acompañando a sus operaciones en Georgia o recientemente en Ucrania. El dominio de las redes sociales y foros de intenet representa una gran ventaja táctica para movilizar simpatizantes y rebeldes, o, en su caso para acallar disidentes.

---

[177] Ignacio Cembrero. "'Babar', un 'gusano' francés para España". El Mundo. 15/02/2015. http://www.elmundo.es/espana/2015/02/15/54dfbc73e2704e7c7f8b456e.html (Ú.a.: 27/09/2015).
[178] Joaquín Gil. "'Hackers' de Rusia y China lanzaron ataques contra cuatro ministerios". El País. 14/12/2014. http://politica.elpais.com/politica/2014/12/13/actualidad/1418472065_191091.html (Ú.a.:27/09/2015).
[179] "China y Rusia firman un pacto de no "ciberagresión" mutua". INCIBE. 08/05/2015. https://www.incibe.es/technologyForecastingSearch/CERT/Alerta_Temprana/Bitacora_de_ciberseguridad/China_Rusia_pacto_no_ciberagresion (Ú.a.: 27/09/2015).
[180] Pablo Romero. "Armados para la 'ciberguerra' fría". El Mundo. 15/02/2015. http://www.elmundo.es/espana/2015/02/15/54dfb898e2704e5b7f8b456b.html (Ú.a.: 27/09/2015).

Este aspecto tampoco le pasa desapercibido a China, que desarrolló una intensa campaña de ataques contra Google, a través de lo que se ha denominado Operación Aurora[181], hasta que en enero de 2010 Google anunció el abandono de sus operaciones en China. Todo el tráfico que circula desde y hacia China es filtrado, y en su caso censurado, por el llamado Great FireWall (en referencia a la Gran Muralla, Great Wall en inglés y los dispositivos firewall de seguridad perimetral de redes). China puede de este modo dominar la información, siguiendo su política del zhixinxiquan, pero también se ha dotado de una poderosa arma de ciberdefensa, ya que es el único país del mundo que podría aislar completamente sus redes nacionales protegiéndolas ante un eventual estado de ciberguerra, manteniendo total o parcialmente su capacidad de respuesta.

Por último cabe plantearse otras situaciones, que no se tiene conocimiento que se hayan producido hasta el momento, pero que podrían representar graves amenazas, entre ellas un posible ciberataque a los procesos democráticos básicos del estado, por ejemplo un proceso electoral. Algunos países han realizado experiencias de voto electrónico, o incluso de votaciones a través de internet, como en el caso de EE.UU., Venezuela, Brasil, Bélgica, Estonia, India o Filipinas[182]. Muchos otros países han realizado estudios de implantación, entre ellos España, donde se han realizado varias experiencias piloto. Y algunos otros lo han prohibido o paralizado, como es el caso del Reino Unido, Irlanda, Holanda, Alemania o Finlandia[183].

En España hemos comprobado las consecuencias desestabilizadoras que puede tener un ataque terrorista durante los días previos a la jornada de votación en unas elecciones generales.

Aunque corresponde a las Juntas Electorales realizar y certificar el recuento de las votaciones, y las actas se firman pública y manualmente ante interventores de diferentes partidos políticos, la Subdirección General de Política Interior y Procesos Electorales (SGPIPE) del Ministerio del Interior, para favorecer la información pública ofrece a través de concurso público la informatización del proceso de recuento provisional en todas las elecciones celebradas hasta la fecha, en lo que se refiere a elecciones generales ha sido siempre INDRA la adjudicataria. De esta manera se ofrece información inmediata de los datos de participación y del recuento. Cabría plantearse el efecto de un ciberataque que afectase a los sistemas que dan soporte al proceso, en la transmisión del escrutinio o en la difusión de los resultados. La manipulación de la información tendría con toda seguridad gravísimos efectos políticos.

[181] Operation Aurora. Wikipedia. https://en.wikipedia.org/wiki/Operation_Aurora (Ú.a.: 27/09/2015).
[182] "Países con implantación de voto electrónico". Departamento de Seguridad del Gobierno Vasco. http://www.euskadi.net/botoelek/otros_paises/ve_mundo_impl_c.htm (Ú.a.: 27/09/2015).
[183] "Países con voto electrónico legalmente prohibido o paralizado". Departamento de Seguridad del Gobierno Vasco. http://www.euskadi.net/botoelek/otros_paises/ve_mundo_paralizado_c.htm (Ú.a.: 27/09/2015).

2.6. Amenazas de otros actores.

En los informes sobre ciberamenazas emitidos por el CCN, CCN-CERT-IA-09/15[184], se hace referencia a otros tipos de agentes y actores que pueden representar una amenaza y que merece la pena considerar, porque sus acciones pueden provocar las mismas consecuencias que un ciberataque perpetrado por cibercriminales u otros estados.

Cibervándalos y script kiddies. Los cibervándalos son individuos que poseen significativos conocimientos técnicos y actúan para demostrar públicamente que son capaces de hacerlo. Los script kiddies (o crios de los scripts) por el contrario poseen conocimientos limitados, hacen uso de herramientas construidas por terceros, y perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones conscientes de sus consecuencias.

A este respecto algunos analistas, como McAffee[185], han detectado en los últimos años un incremento de su actividad y la aparición de incidentes con malware desfasado[186].

Actores internos. También llamados *insiders*, son aquellas personas que tienen o han tenido algún tipo de relación con una organización, incluyendo exempleados, personal temporal o proveedores. Pueden constituir una de las mayores amenazas y su motivación suele ser siempre similar: venganza, motivos financieros o políticos, etc. Se tarta de personal que es buscado con preferencia por mafias, organizaciones cibercriminales o servicios de inteligencia para encargarse de la infección preliminar de la red objetivo, o para la exfiltración de información de la misma.

Ciberinvestigadores. La comunidad de investigadores que persiguen el descubrimiento de las vulnerabilidades que pueden afectar a los sistemas, con la publicación de los resultados de sus investigaciones pueden ayudar a terceros malintencionados.

Las organizaciones privadas. Las motivaciones para perpetrar ciberataques también se encuentran en organizaciones privadas cuando, movidas por el interés económico que supone poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial. La aparición y explosivo crecimiento del *cibercrimen-como-servicio* hace pensar que este tipo de actores crecerán en importancia en el futuro más próximo.

---

[184] CCN-CERT-IA-09/15. CCN. 09/04/2015. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html (Ú.a.: 27/09/2015).

[185] Robert Sicilano. ""Old" Malware Attacks Rising Significantly". McAffee Blog Central. 05/06/2013. https://blogs.mcafee.com/consumer/q1-threat-report/ (Ú.a.: 27/09/2015).

[186] Anthony diBello. "Malware retro alimenta la nueva ola de amenazas". Information Week México. 08/12/2014. http://www.informationweek.com.mx/columnas/malware-retro-alimenta-la-nueva-ola-de-amenazas/?utm_source=outbrain&utm_medium=social-cpc (Ú.a.: 27/09/2015).

2.7. Timeline.

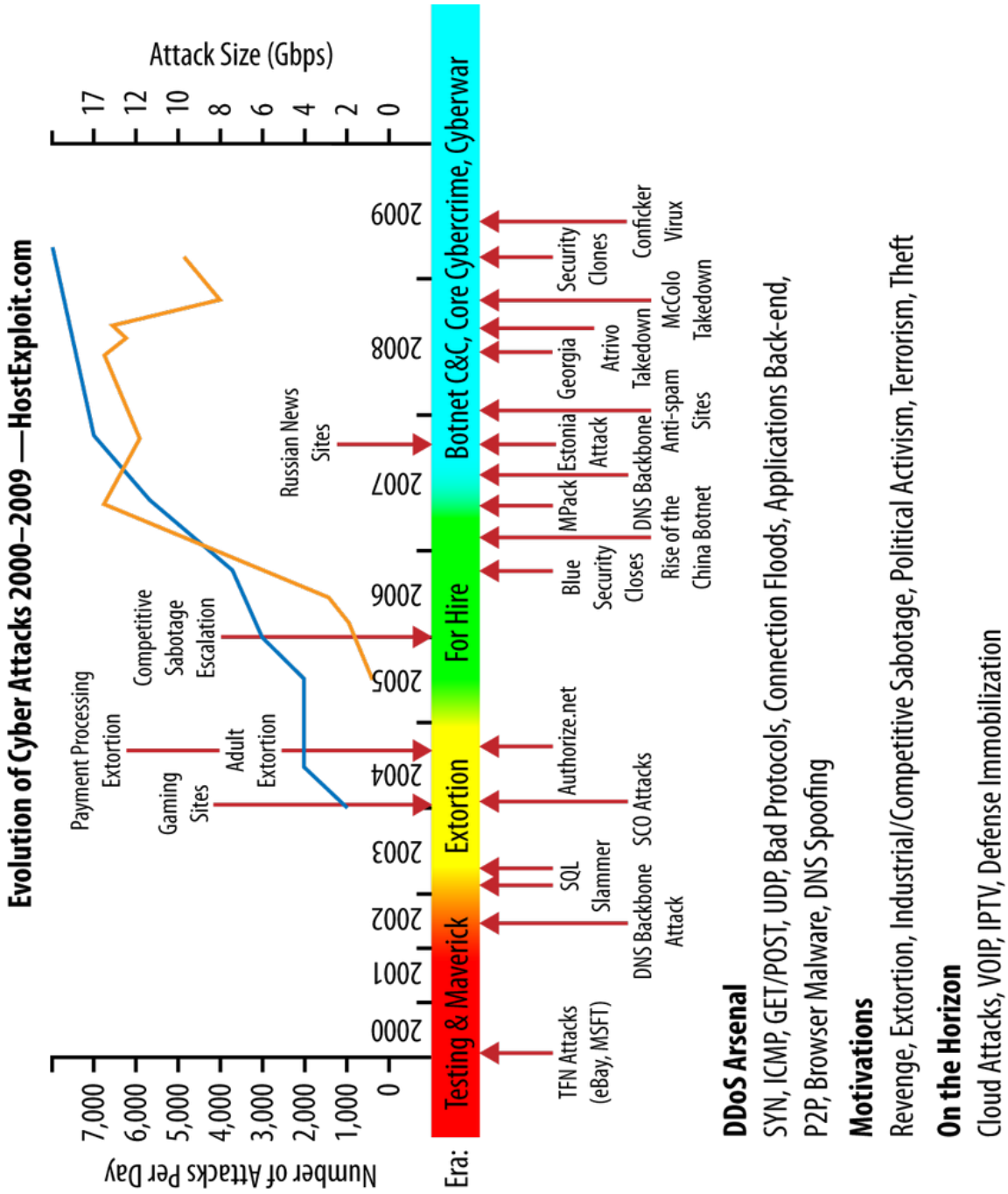

Figura 40: *Evolución de los ciberataques. (Fuente: Carr, Jeffrey (2011). Imagen obtenida vía Google Images. http://cdn.oreillystatic.com/oreilly/booksamplers/9780596802158-sampler.pdf Último aceso: 25/09/2015)*

3. Descripción de herramientas y métodos de intrusión y ataque.

La Estrategia de Ciberseguridad Nacional, de la que emana el Esquema Nacional de Seguridad (ENS), en el desarrollo de su Línea de Acción 2, "Seguridad de los Sistemas de Información y Telecomunicaciones que soportan a las AA.PP.", confiere al Centro Criptológico Nacional, un papel central en el desarrollo del ENS, a través del Equipo de Respuesta ante Emergencias Informáticas (CERT). Entre las funciones del CCN destacan las de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sitemas de información, según se establece en el RD 421/2004, de 12 de marzo, por el que se regula su estructura y funcionamiento.

En febrero de 2015 el CCN emitió la Guía CCN-STIC-817, titulada "Esquema Nacional de Seguridad. Gestión de Ciberincidentes". En este documento se elaboran una serie de criterios para clasificar las tipologías de ciberincidentes. Estos criterios se establecen atendiendo a una serie de factores:

- El tipo de amenaza, malware, intrusiones, exfiltración de información, abuso, fraude…
- El origen de la amenaza, si es interna o externa.
- La categoría de seguridad de los sistemas afectados, que queda definida en el Anexo I del ENS, como veremos más adelante.
- El perfil de los usuarios afectados, y qué privilegios de acceso disponen a información confidencial o sensible.
- El número y tipología de los sistemas afectados
- El impacto en la organización, desde el punto de vista de la protección de la información, la prestación de servicios, la conformidad legal o la pérdida de reputación.
- Los requerimientos legales

La combinación de uno o varios de estos factores es determinante a la hora de describir un incidente, establecer su peligrosidad, analizarlo y actuar para solucionar las consecuencias.

Atendiendo al vector de ataque el CERT del CCN establece la siguiente clasificación:

Tipo de Incidente	Descripción	Método

Tipo de Incidente	Descripción	Método
Contenido Abusivo	Ataques dirigidos a dañar la imagen de la organización, o a utilizar sus medios para otros usos ilícitos.	Spam
		Acoso y extorsión
		Actividades asociadas a la pederastia (alojamiento y transmisión de contenidos), violencia y ciberdelito en general
Código dañino	Software cuyo objetivo es infiltrarse o dañar u sistema, sin el conocimiento del responsable o del usuario, y con finalidades diversas.	Virus
		Gusanos
		Troyanos
		Spyware
		Rootkit
		Ransomware
Recogida de información	Ataques dirigidos a recabar información que permita elaborar ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	Identificación de vulnerabilidades (susceptibles de ser utilizadas en Ataques Zero-Day)
		Sniffing
		Ingeniería social
Intrusión	Ataques dirigidos a la explotación de vulnerabilidades de diseño o configuración de diferentes tecnologías, para introducirse en los sistemas de la organización.	Compromiso de cuenta de usuario
		Defacement
		Cross Site Scripting (XSS)
		Cross Site Request Forgery (CSRF)

Tipo de Incidente	Descripción	Método
		SQL Injection
		Spear Phihing
		Pharming
		Ataque de fuerza bruta
		Inyección de ficheros remota
		Explotación de vulnerabilidad software
		Explotación de vulnerabilidad hardware
Disponibilidad	Ataques dirigidos a impedir que los sistemas presten servicio, provocando daños en la productividad o en la reputación de la organización.	Ataques DoS/DDoS
		Fallo del hardware o software
		Error humano
		Sabotaje
Política de seguridad	Incidentes relacionados con la violación de las políticas internas de la organización en materia de seguridad.	
Confidencialidad, exfiltración, integridad o compromiso	Incidentes relacionados con el acceso, modificación o fuga de información clasificada.	Acceso no autorizado a información clasificada
		Modificación no autorizada de la información
		Publicación no autorizada de información
		Exfiltración de información
		Violaciones de Derechos de Propiedad Intelectual o

Tipo de Incidente	Descripción	Método
		Industrial
Fraude y suplantación	Incidentes relacionados con acciones derivadas de una suplantación fraudulenta de identidad.	Spoofing
		Phishing
		Uso no autorizado de recursos
		Uso ilegítimo de credenciales
Otros	Otros incidentes no clasificados.	

Tabla 1: *Clasificación de Tipos de incidentes en función del vector de ataque. Fuente: Carlos Galán; Jose Antonio Mañas; Innotec System. Guía de seguridad CCN-STIC-817. CCN-CERT (2015).* https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html *(Ú.a.: 14/04/2015)*

Generalmente la detección de los incidentes se realiza utilizando herramientas automatizadas, lo que se denomina IDS/IDP (Intrusion Detection Systems e Intrusion Prevention Systems), o sistemas de detección de intrusiones. Existen dos tipos de sistemas, según su ámbito de actuación:

- NIDS (Network IDS), o sistemas de red de detección de intrusiones, generalmente se trata de un sensor virtual, como un sniffer, que realiza un análisis heurístico pormenorizado del tráfico de red, que es comparado con firmas de ataques conocidos, buscando patrones, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El NIDS no sólo analiza el tipo de tráfico, sino que también revisa el contenido y su comportamiento. Normalmente esta herramienta se integra con un firewall, y se configura, o bien pasivamente, facilitando al administrador informes de las anomalías detectadas para ayudar en la toma de decisiones; o reactivamente, reprogramando el firewall de forma automática al detectar actividad sospechosa para cortar el tráfico de la supuesta red atacante. La programación reactiva implica respuestas inmediatas y aparentemente más seguras, sin embargo puede llegar a suponer un problema cuando se ejecutan aplicaciones en entorno Java que requieren una permanente actualización de la información y accesos constantes a bases de datos

remotas. Este tipo de tráfico puede ser eventualmente interpretado por el NIDS como un ataque.

- HIDS (Host IDS), o IDS de servidor. Se trata de un sistema de sondas software que tratan de detectar cualquier anomalía revisando la actividad de la máquina, pueden ser analizadores de bases de datos de objetos, de checksum, que emitirán una alerta cuando se haya producido un intento de desbordamiento de búfer contra de un servidor de base de datos, ante la presencia de un nombre de archivo con caracteres inusuales; herramientas antivirus, que revisan cada fichero, incluso durante su ejecución en memoria buscando patrones de amenazas; o analizadores de logs, que puedan detectar un cambio no previsto en la configuración de un host, en los logs de una aplicación, o advirtiendo de reiterados intentos fallidos de login desde un sistema externo desconocido, etc.

Pero también tienen una gran importancia las incidencias notificadas por los usuarios, que experimentan anomalías o las consecuencias directas del ataque. Por ello, la elaboración de una normativa clara, la implantación de herra mientas que favorezcan la comunicación interna, y la formación permanente de todos los usuarios en materia de seguridad es esencial en cualquier organización para prevenir y detectar cualquier ciberincidente de forma eficiente.

Aún así, muchos ciberincidentes son muy difíciles de detectar, como es el caso de las APTs (Advanced Persisten Threats), o Amenazas Persistentes Avanzadas, que utilizan técnicas y métodos, o combinaciones de ellos, muy sofisticados, de ocultación, anonimato y persistencia. En mayo de 2003, el CSIRT-CV, Centre de Seguretat TIC de la Comunitat Valenciana, conjuntamente con el INCIBE, Instituto Nacional de Ciberseguridad (antiguo INCIBE), presentaron un informe denominado “Detección de APTs”, en el que exponían los metodos de ataque de este tipo de amenazas, y las recomendaciones para su detección, que se tratan al final de este capítulo.

Toda la información recopilada se estructura en *precursores*, indicios de que puede ocurrir un ciberincidente, e *indicadores*, indicios de que ha ocurrido o puede estar ocurriendo un incidente. La mayoría de ataques no tienen otros precursores identificables que el anuncio por parte de un CERT de la detección de un exploit capaz de aprovechar una vulnerabilidad presente en el sistema, o el anuncio por parte de un grupo de hacktivistas de una campaña de ataques contra la organización.

Herramientas de gestión de los ciberincidentes en comunicación permanente con los CERT, como es el caso de la Herramienta LUCIA, desarrollada por el CERT del CCN, y que se analiza en el siguiente capítulo, pueden incrementar de forma efectiva la capacidad de anticipación y

respuesta, dado que permitirá recibir información categorizada de incidentes en curso y su nivel de peligrosidad o criticidad.

En la siguiente tabla se elabora el Nivel de Peligrosidad de los Ciberincidentes, atendiendo a la repercusión que pueda tener en los sistemas la materialización de la amenaza:

Nivel de peligrosidad	Amenazas subyacentes	Vector de ataque	Características potenciales del ciberataque
CRÍTICO	Ciberespionaje.	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
MUY ALTO	Interrupción de los servicios IT. Exfiltración de datos. Compromiso de los servicios.	- Códigos dañinos confirmados de Alto Impacto (RAT, rootkit). - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	Toma de control de los sistemas. Robo y publicación o venta de información sustraída. Ciberdelito. Suplantación.	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL. - Spear phising / pharming	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	Logro o incremento significativo de capacidades ofensivas. Desfiguración de páginas web. Manipulación de información.	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	Ataques a la imagen / menosprecio. Errores y fallos.	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

Tabla 2: *Nivel de peligrosidad de los ciberincidentes, en función de los efectos del incidente. Fuente: Carlos Galán; Jose Antonio Mañas; Innotec System. Guía de seguridad CCN-STIC-817. CCN-CERT (2015).* https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html *(Ú.a.: 14/04/2015)*

Se han caracterizado los ciberincidentes desde el punto de vista del sistema y su integridad. Pero desde la perspectiva del ciberatacante su actuación responde a un ciclo de vida en varias fases. Según los objetivos en cada fase las herramientas y métodos a utilizar variarán.

Figura 41: *Fases del ataque.*

La información siguiente se ha recopilado de diversas fuentes de internet tomando como base los cuadros anteriores. Se ha recurrido a Wikipedia, comparando sus versiones en castellano y en inglés, dado que la terminología resulta muchas veces oscura. Se han consultado también páginas de fabricantes y desarrolladores de herramientas software. Se ha obtenido información de algunas de las técnicas a través de los informes de consultorías de ciberseguridad, como Mandiant[187], o los informes sobre ciberseguridad emitidos por el INCIBE, el CSIRT-CV, o el CCN-CERT, especialmente las series de informes de amenazas CCN-CERT-IA, y de informes ejecutivos CCN-CERT-IE, y el Glosario[188]. Para acceder a esta información ha sido imprescindible obtener usuario registrado en el CCN. Ha resultado también útil el Tutorial de Seguridad Informática on-line ofrecido por el Laboratorio de Redes y Seguridad de la UNAM[189]. Por último se han consultado varias fuentes bibiliográficas, como Marcelo Rodao (2003) y Walker (2006).

[187] Mandiant (2013). "APT1. Exposing One of China's Cyber Espionage Units". http://intelreport.mandiant.com/ (Ú.a.: 05/03/2015)
[188] GuíaCCN-STIC-401. Glosario y Abreviaturas. CERT-CCN (Agosto, 2015). https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html (Ú.a. 24/09/2015)
[189] Laboratorio de Redes y Seguridad. "Tutorial de Seguridad Informática. Capítulo 3. Identificación de ataques y técnicas de intrusión". UNAM (México). http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap3.html (Ú.a. 24/09/2015)

3.1. Obtención de información.

Se ha indicado la importancia de la información para los estados o para una organización, no es menos para los atacantes En una primera fase el atacante investigará y documentará toda la información posible relevante sobre la víctima: dónde se localiza físicamente, qué tipos de solicitudes de información realiza (si en sus anuncios de Linkedin aparece en búsqueda de un DBA de Oracle, muy posiblemente su base de datos esté desarrollada en esa plataforma), su dirección IP, su página web, sitios en redes sociales, búsquedas con nslookup para conocer datos de sus servidores, búsquedas de la empresa en directorios de internet. Si posee información valiosa del objetivo, puede trazar mejor su plan de ataque, identificará la plataforma, qué posibilidades de encontrar información valiosa existen atacando una IP concreta, si la información valiosa se encuentra en otra ubicación, e inclusive la topología de red de la víctima se puede obtener durante la fase de reconocimiento. La forma de obtener y proteger la información varía dependiendo del medio y de las técnicas y métodos usados.

3.1.1. Bases de datos públicas.

Una de las razones por las cuales las vulnerabilidades en las bases de datos están tan extendidas es el hecho de que la mayoría de las bases que existen en Internet han sido programadas para optimizar los tiempos de respuesta y dar dinamismo a sus páginas, sin preocuparse de las implicaciones de seguridad. El usuario que diseña y construye una base de datos, y la sube a su web, demasiado a menudo no es consciente de que un fallo de seguridad puede comprometer todo el servidor que la aloja. Y los webmaster que ofrecen servicios de hosting a sus clientes, no pueden hacer mucho para evitarlo, ya que no es posible supervisar todas las acciones de los usuarios. En consecuencia estas bases de datos se convierten en objetivos inmediatos, fuentes de información y plataformas de operación valiosas para los atacantes.

3.1.2. Web.

La web no es solamente una fuente inagotable de información. Al código html con el que están programadas las páginas, se han ido añadiendo más capacidades con la inclusión de procesos en lenguajes más sofisticados: php, Java, XML, SQL. Este tipo de ejecución puede prestarse para ocultar códigos maliciosos en las páginas, que son ejecutados por los usuarios sin notarlo, dejando expuesta la seguridad del sistema. Ésto convierte a internet, por su propio diseño, en cuanto a protocolos, lenguajes y carencia de control y normativa reguladora, en una herramienta en manos de los atacantes.

3.1.3. DNS cache poisoning.

El DNS (Domain Name Service) es un sistema que permite traducir el nombre de un dominio a su dirección IP y viceversa, permitiendo que los usuarios utilicen nombres intuitivos para

referenciar otros sistemas o redes, en lugar de las IP reales. El sistema funciona en tres niveles, cada máquina en una red ejecuta un cliente DNS, que genera peticiones de resolución de nombres de dominio a un servidor DNS, que generalmente le es proporcionado automáticamente a través de protocolo DHCP, junto con el resto de configuración de acceso a la red. Este servidor, si no dispone de una entrada para resolver la dirección solicitada, puede reenviar la petición a un servidor DNS de una zona de autoridad superior.

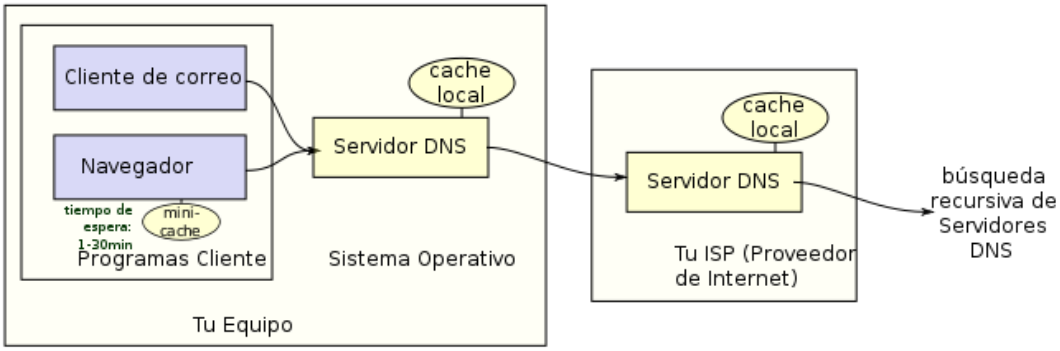

Figura 42: *El sistema DNS ante una petición de resolución de un nombre de dominio. Fuente: Wikipedia. https://es.wikipedia.org/wiki/Domain_Name_System (Ú.a.: 23/09/2015)*

Un atacante puede utilizar las tablas del DNS, que adolece de una arquitectura abierta, para realizar una suplantación de identidad, redirigir a la víctima a un dominio falsificado, y a partir de él obtener la información de su interés. Una vez que el atacante ha facilitado datos no autenticados el DNS los almacena (caché), y los facilita a su vez a otros servidores, por lo que se dice que la caché del DNS ha quedado envenenada. En su caso más grave, el atacante puede modificar el DNS de un ISP (Internet Service Provider), o proveedor de acceso a internet, que facilitará en cascada las tablas falsificadas a todos los servidores de DNS conectados a su red.

Una variante del ataque de envenenamiento DNS consiste en que el atacante responda una petición de resolución de nombre de dominio antes que el DNS legítimo, por ejemplo haciendo demorar la respuesta de este último. En este caso hablamos de falsificación de DNS, ó **DNS Forgery**.

3.1.4. Keylogger.

Un keylogger (keystroke logger, textualmente un registrador de teclado) es un tipo de software, o un dispositivo hardware, que puede registrar la actividad del teclado de un sistema. Aunque puede ser utilizado legalmente para registrar lo que hacen los usuarios al acceder al sistema o a una aplicación, en caso de una auditoría, para realizar una trazabilidad de las acciones del usuario, en caso de que se sospeche un sabotaje interno; generalmente es usado por un atacante

para obtener las contraseñas de sus víctimas sin su conocimiento. El keylogger almacena las pulsaciones en un fichero y posteriormente lo transmite por internet al atacante, a través de un website, un servidor ftp, o enviando un correo a una cuenta predefinida del atacante.

Los keylogger pueden trabajar a varios niveles, según su diseño. Los más potentes pueden ser instalados con un rootkit, con permisos de supervisor, o suministrados en un driver de teclado, y funcionan a muy bajo nivel, residiendo en el kernel (el núcleo del SO), por lo que son prácticamente indetectables. Algunos keyloggers pueden hacer uso del concepto de virtualización, y residir en una máquina virtual creada por un malware, ejecutándose por debajo del SO, como hace por ejemplo Blue Pill[190]. Existen keyloggers que se enganchan a una aplicación o a una App a través de sus APIs (Aplication Programming Interface), como por ejemplo las librerías de Windows GetAsyncKeyState( ) o GetForegroundWindow( ), que permiten sondear el estado o los eventos de teclado. Otro tipo de keylogger muy común es el basado en el método denominado inyección de memoria (MitB-Keylogger). Troyanos como Zeus y Spyeye, acceden directamente a las tablas de memoria asociadas al navegador u otras funciones del SO, para evitar al sistema de control de cuentas de usuario de Windows (Windows UAC, o User Account Control).

Existen también multitud de keyloggers hardware, instalables en PCs, cajeros automáticos, o incluso sensores para smartphones, pero su uso implica el acceso directo a los sistemas.

3.1.5. Ingeniería Social.

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social por lo general usará el teléfono, o el correo electrónico (entonces hablamos de phishing), para engañar a la gente y aprovechar su tendencia natural a ser empáticos, para llevar a su víctima a revelar información sensible, o bien a violar las políticas de seguridad de la organización. En otros casos el ingeniero social se hará pasar por técnico de una empresa de servicios, bombero, empleado de banca o desratizador. Es un procedimiento más inmediato que aprovechar agujeros de seguridad en los sistemas informáticos.

Algunos notables ingenieros sociales, como Kevin Mitnick (el más notable), Christopher Hadnagy (de hecho el primer teórico de la ingeniería social), los hermanos Ramy, Muzher y Shadde Badir (los tres ciegos de nacimiento, y autores de un extenso fraude telefónico en Israel en la década de los 90), Pete Herzog (un notable investigador en el campo de la ingeniería social y la neurología, y creador de ISECOM y la OSSTMM), Frank Abagnale (en quien se basó el personaje interpretado por Leonardo Di Caprio en la película “Atrápame si puedes”, de Steven

[190] Blue Pill. Wikipedia. https://en.wikipedia.org/wiki/Blue_Pill_%28software%29 (Ú.a.: 23/09/2015)

Spielberg), David Bannon (uno de los impostores más famosos del mundo, que se hizo pasar durante años por agente de la Interpol, llegando a publicar un libro de memorias, éxito de ventas, que finalmente le delató), Peter Foster o Steven Jay Rusell, coinciden en señalar que esta técnica se basa en encerrar a la víctima en una distorsión cognitiva, o sesgo cognitivo, que nos condiciona al interpretar la realidad. En España podríamos añadir a personajes como Francisco Gómez Iglesias (el pequeño Nicolás)[191].

Algunas de estas técnicas son por ejemplo:

Pretextos (blagging). Generalmente se construye un escenario semicreíble, al que se aporta verosimilitud utilizando información previa recopilada de la víctima, con objeto de obtener más información, más concreta o de más calidad.

Robo con engaño (diversion theft). El objetivo es persuadir a la víctima de que una entrega de información debe ser redirigida a un destinatario diferente pero aparentemente legítimo.

Phishing. En este caso la suplantación de identidad para la obtención de información confidencial de las víctimas, mediante la que el phisher (pescador) se hace pasar por una persona o empresa de confianza en una aparente comunicación, se realiza por correo electrónico. Generalmente el phishing tiene un carácter indiscriminado, y se apoya en envíos masivos de spam.

IVR phishing. En esta modalidad, se utiliza un IVR (Interactive Voice Response) telefónico, que simula el de una entidad legal asociado a un número 900, y mediante el cual se solicitan a la víctima datos sobre el PIN de sus tarjetas, u otra información bancaria.

Cebo (baiting). El atacante deja un soporte digital, como un CD o una memoria USB, infectado con un troyano, en un lugar muy visible, confiando que la víctima lo insertará en el sistema, por curiosidad o para descubrir al legítimo dueño. O puede etiquetarlo como documentación de un departamento interno, y esperar a que sea entregado a la víctima a través de una persona con la que existe una relación de confianza.

Quid pro quo. El atacante realiza llamadas al azar a los teléfonos corporativos de una organización identificándose como personal del departamento de soporte técnico, y eventualmente contactará con un usuario con un problema técnico, al que se le ayuda con su problema y, en el proceso, consigue que el usuario le proporcione acceso remoto o ejecute un malware.

[191] Martín Mucha y Javier G. Negre. "El niño que decía trabajar para Soraya y el CNI". El Mundo. 19/10/2014. http://www.elmundo.es/cronica/2014/10/19/54421cede2704e397c8b456b.html (Ú.a.: 23/09/2015)

Colarse (Tailgating o Piggybacking, que literalmente se traducirían como chupar rueda o llevar a cuestas). Para acceder a una zona físicamente restringida mediante algún tipo de control electrónico, o en la que es necesario el uso de acreditación, el atacante espera al paso de un usuario acreditado para colarse tras él, aprovechándose de su amabilidad o aportando cualquier excusa sobre su acreditación.

eMail spoofing, o spoofing por correo electrónico, consiste en una suplantación de identidad a través de la falsificación de los datos del remitente, podría considerarse también una técnica de ingeniería social. Es muy común en correos de phishing y spam.

3.1.6. Otros.

Jamming o Flooding (interferencia y saturación). Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla. En el caso de comunicaciones telefónicas se interfiere el espectro de radiofrecuencia para saturar el canal e inhabilitar al receptor. El dispositivo que permite este tipo de interferencias se denomina inhibidor o perurbador. Son técnicas muy comunes en escenarios de guerra electrónica (EW). El objetivo es aislar a la víctima e impedirle informarse de su situación.

Packet Sniffing, o análisis de paquetes. Muchas redes son vulnerables al *eavesdropping* (literalmete traducido como escuchar a escondidas), que consiste en la intercepción pasiva del tráfico de red. Generalmente el sistema en el que se instala hace funcionar a la tarjeta de red en modo promiscuo (se desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red son aceptados por la tarjeta como dirigidos al sistema). Existen sniffers para capturar cualquier tipo de información específica, contraseñas de acceso a cuentas si no están cifradas, números de tarjetas de crédito o direcciones de correo. El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). Los buenos Sniffers no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos[192]. El sniffer puede ser colocado tanto en un ordenador conectado a red, como en un router o en un gateway de conexión a internet o a una red de un mainframe. Así como un usuario legítimo, como un administrador de red, puede obtener información valiosa para detectar cuellos de botella, problemas de transmisión, o intrusiones, el propio intruso puede instalarlo en un sistema mediante un malware, y obtener acceso a toda la información transmitida por la red.

[192] Test de detección de sniffer. Wikipedia. https://es.wikipedia.org/wiki/Test_de_Detecci%C3%B3n_de_Sniffer (Ú.a.: 23/09/2015)

Algunos tipos de packet sniffers[193]:

- *Tcpdump*. Es una utilidad Unix, ejecutable desde la línea de comandos sólo con permisos de root, que muestra la cabecera de los paquetes que captura un interfaz de red, y permite monitorizar el tráfico de red en tiempo real. No es en cambio capaz de detectar anomalías. Está disponible en prácticamente todas las distribuciones Linux, pero requiere de las librerías libpcap. En cualquier caso ambas pueden descargarse desde la página oficial[194]. En entorno Windows se puede utilizar Windump, previa instalación de las librerías WinPcap, y descargables gratuitamente de su página oficial[195].

TCPDUMP **HACKPLAYERS.COM**

Opciones linea de comandos			
-A	Visualiza el paquete en modo ASCII	**-q**	Salir
-c <count>	Sale despues dcapturar n paquetes	**-r <file>**	lee los paquetes de un archivo
-D	Lista las interfaces disponibles	**-s <len>**	Captura "len" cantidad bytes/paquete
-e	Print link-level headers	**-S**	Muestra la secuencia absolita TCP
-F <file>	Use **file** as the filter expression	**-t**	No muestra timestamps
-G <n>	Rotate the dump file every n seconds	**-v[v[v]]**	Salida modo vervose
-i <iface>	Especifica interface de captura	**-w <file>**	Guarda captura en **"file"**
-K	No verifica TCP checksums	**-x**	Muestra los paquetes en HEX
-L	List data link types for the interface	**-X**	Imprime la trama en HEX y ASCII
-n	No convierte direciones en nombres	**-y <type>**	Specify the data link type
-p	No utliza modo promiscuo	**-Z <user>**	Drop privileges from root to **user**

Figura 43: *Comandos de tcpdump. Fuente: Hackplayers.com.*
http://www.hackplayers.com/2013/12/que-deberiamos-saber-sobre-tcpdump-1.html
(Ú.a.: 23/09/2015)

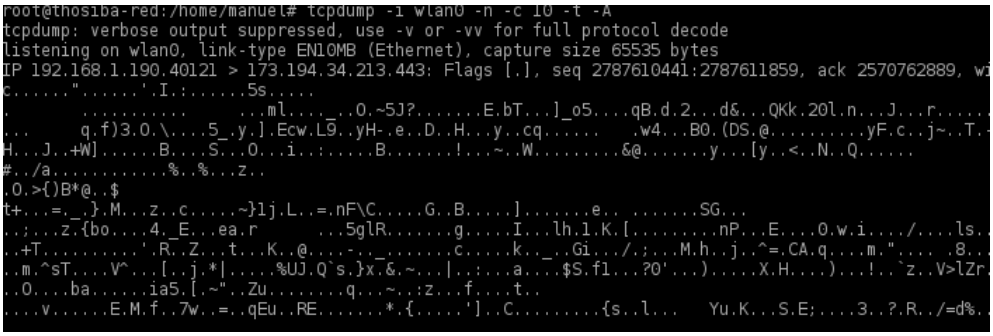

Figura 44: *Captura de pantalla de la salida de tcpdump. Fuente: Hackplayers.com.*
http://www.hackplayers.com/2013/12/que-deberiamos-saber-sobre-tcpdump-1.html
(Ú.a.: 23/09/2015)

[193] Tipos de packet sniffers. Wikipedia. https://es.wikipedia.org/wiki/Anexo:Tipos_de_packet_sniffers (Ú.a.: 23/09/2015)
[194] Tcpdump/Libpcap. http://www.tcpdump.org/ (Ú.a.: 23/09/2015)
[195] Librerías WinPcap. http://www.winpcap.org/ (Ú.a.: 23/09/2015)

- *Darkstat*. Es una herramienta sencilla para monitorizar una red, que analiza el tráfico y genera un informe estadístico en formato html. Es interesante porque ofrece información de los puertos usados por cada protocolo.

- *Traffic-Vis*. Es un demonio de los sistemas Unix que monitoriza el tráfico TCP/IP, y muestra la información en gráficos ASCII o en html. Requiere las librerías libpcap.

- *Ngrep*. Es un comando que extiende las características del grep de GNU a la capa de red, leyendo TCP, UDP e ICMP. Permite trabajar con el payload de los paquetes, es decir, con el cuerpo, no con sus cabeceras.

- *Snort*. Es un NIDS, un sistema de detección de intrusiones de red. Implementa un motor de detección de ataques y barrido de puertos, que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos de aprovechar alguna vulnerabilidad, análisis de protocolos, todo ello en tiempo real. Está disponible gratuitamente bajo licencia GPL, y funciona en plataformas Windows y Unix/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de diferentes CERTs. La versión 3.0 puede descargarse desde su página oficial[196]. Y hay disponible un buen tutorial de instalación y configuración en Sense.org.

[196] Snort.org. https://www.snort.org/ (Ú.a.: 23/09/2015)

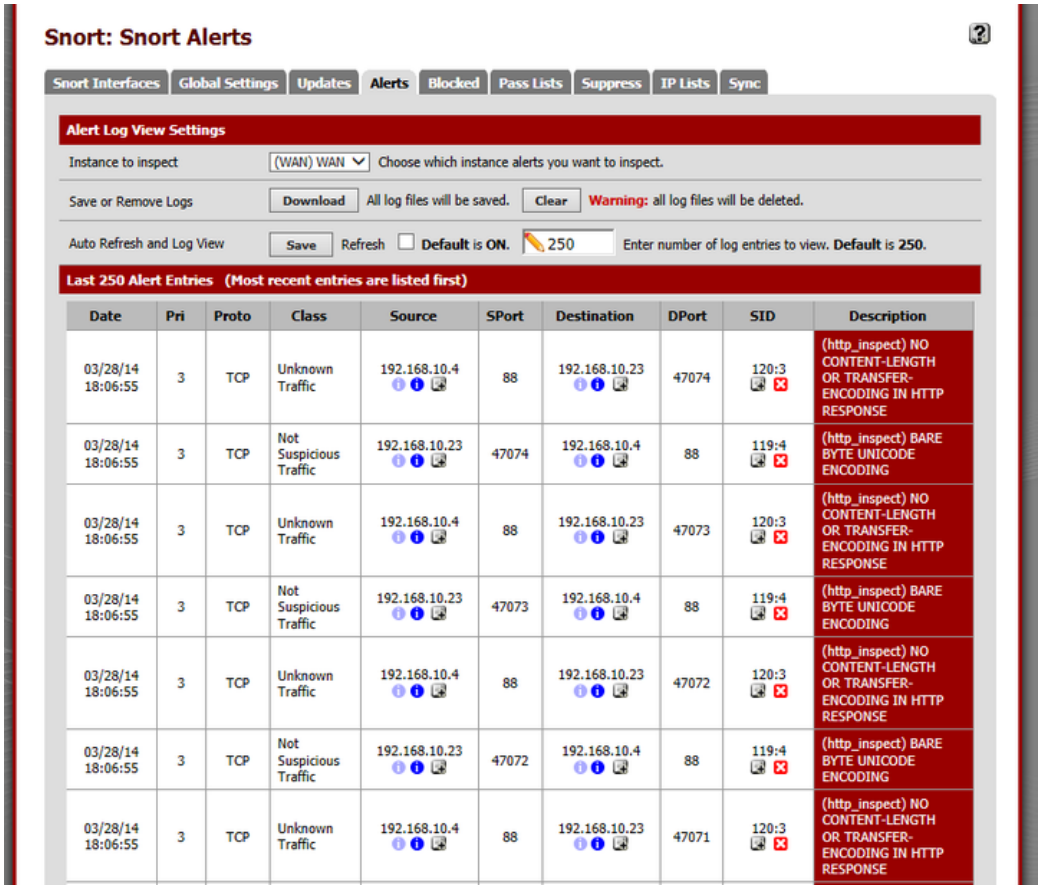

Figura 45: *Captura de pantalla de las alertas generadas por Snort. Fuente: Sense.org* https://doc.pfsense.org/index.php/Setup_Snort_Package *(Ú.a.: 23/09/2015)*

- *NWatch*. Es un analizador de puertos pasivo sobre tráfico IP en sistemas Unix. Permanece activo por defecto, monitorizando el interfaz por defecto del sistema (eth0) y siguiendo cada combinación de IP y puerto que identifica.

- *Wireshark* (antes Ethereal). Es un potente y extendido analizador de protocolos de licencia libre utilizado para realizar análisis y solucionar problemas en redes de comunicaciones en el desarrollo de software y protocolos, y como una herramienta didáctica para educación. Existe una versión ejecutable desde pendrive. Se encuentra disponible en su página oficial[197]

- *Ettercap*. Es un interceptor/sniffer/logger para LAN con switches. Soporta la disección activa y pasiva de varios protocolos (incluso aquellos cifrados, como SSH y https). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo, así como la intercepción de tráfico remoto, aún manteniendo la conexión

[197] Wireshark. https://www.wireshark.org/ (Ú.a.: 23/09/2015)

sincronizada a través de un proxy, lo que le permite establecer un ataque Man-in-the-Middle (MitM).

- *Kismet*. Es a la vez un sniffer y un NIDS, sistema de detección de intrusiones, para redes inalámbricas 802.11. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa funciona con Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. El cliente puede también funcionar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda.

- *Acrylic WiFi*. Es un sniffer gratuito de redes WiFi para sistemas Windows que funciona con la mayoría de tarjetas WiFi 802.11a/b/g/n/ac. Puede funcionar combinadamente con Wireshark, dandole soporte para analizar tráfico WiFi.

- *EtherDetect*. Es un sencillo analizador de paquetes pasivo basado en Windows capaz de filtrar cualquier protocolo en tramas TCP y UDP. Permite la visualización inmediata del contenido de las tramas en hexadecimal y en ASCII, el almacenamiento de todas las tramas de un nodo y la emisión de informes en formatos HTML y XML

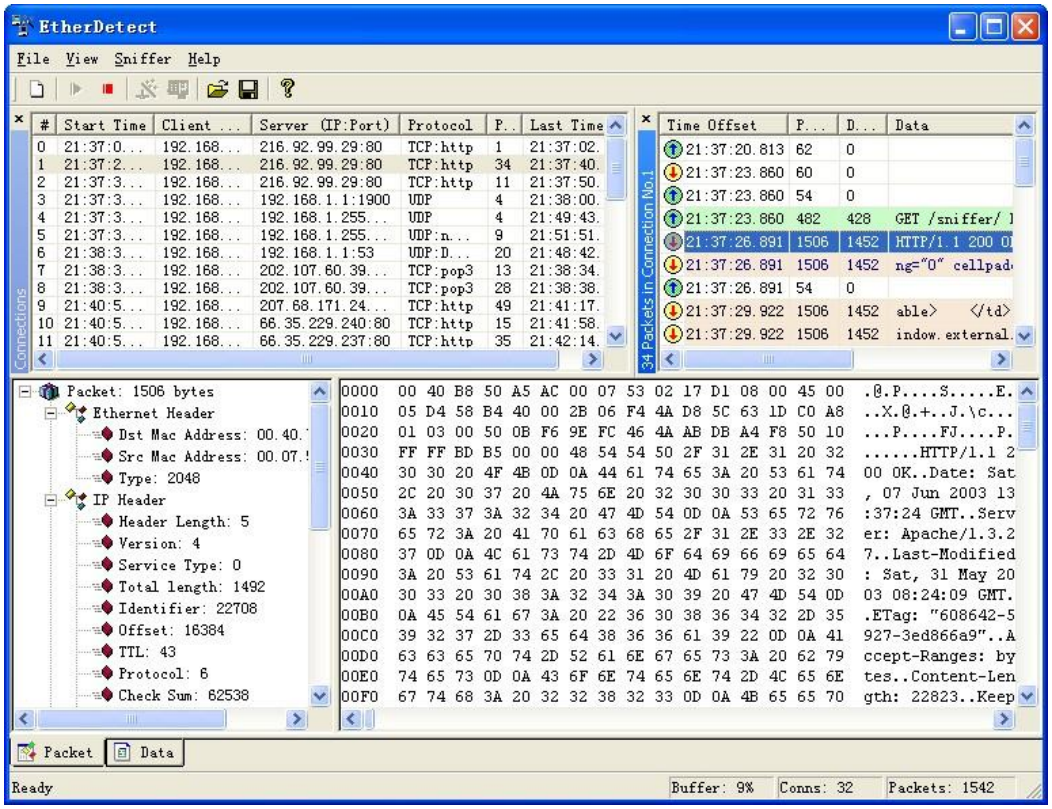

Figura 46: *Captura de pantalla de un packet sniffer. Fuente: EffeTech Network Monitoring Software. http://www.etherdetect.com/ (Ú.a.: 23/09/2015)*

Snooping (literalmente inspección). Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Para ello en este caso se hace uso de las capacidades de los switches para escuchar el tráfico producido por los protocolos de control IGMP (Internet Group Management Protocol), con lo que entonces hablamos de IGMP snooping[198], o inspección IGMP; o también por el protocolo DHCP, y en este caso se habla de DHCP snooping[199], o inspección DHCP. Generalmente los switches detectan qué puertos hacen uso de conexiones multicast, y las aislan dentro de su dominio de difusión sólo para esos nodos, de forma que no se inunde toda la red, lo que podría provocar una situación similar a un ataque DoS.

El DHCP snooping es un componente importante de la defensa contra ARP spoofing. El protocolo ARP (Address Resolution Protocol) comprueba la dirección IP en el campo Source Protocol Address de los paquetes ARP. Si la dirección IP no ha sido registrada por la inspección DHCP como una dirección en uso por un nodo o host conectado a uno de los puertos de entrada, entonces el paquete ARP se elimina. Sin embargo un atacante puede añadir su propio servidor DHCP (rogue DHCP, o DHCP pícaro) y controlar la inspección DHCP. Además de interceptar el tráfico de red, el atacante accede a los documentos, correos electrónicos u otra información almacenada, realizando en la mayoría de los casos la descarga de la información a la máquina remota atacante.

Tampering o Data Diddling. Modificación intencional y no autorizada de datos, o la alteración del software base instalado en un sistema, incluyendo borrado de archivos. Puede ser llevada a cabo por atacantes externos o internos, con lo que hablaríamos de sabotaje, generalmente con propósitos de fraude y estafa, o para dejar fuera de servicio a un competidor. La utilización de troyanos entra también dentro de esta categoría cuando su objeto es la consumación de acciones fraudulentas, como es el caso de Back Orifice y NetBus. En internet existen diversas fuentes que hacen referencia a este tipo de ataques utilizando esta misma terminología[200] [201] [202], por lo que se ha considerado interesante referenciarlo. En realidad hablamos de la modificación directa de la información por motivos de fraude y sabotaje.

[198] IGMP snooping. Wikipedia. https://es.wikipedia.org/wiki/IGMP_snooping (Ú.a.: 24/09/2015)
[199] DHCP snooping. Wikipedia. https://en.wikipedia.org/wiki/DHCP_snooping (Ú.a.: 24/09/2015)
[200] Tampering o Data Diddling. IMC, Independent Media Center. Barcelona. http://barcelona.indymedia.org/newswire/display/337061/index.php (Ú.a.: 24/09/2015)
[201] Ives Ledermann, Cristian Mendoza y otros. "Hackers y Seguridad". UDEC (Colombia). http://www2.udec.cl/~crmendoz/8.htm (Ú.a.: 24/09/2015)
[202] Carlos Gómez. "Legislación para ingenieros electrónicos". Google Blogger. http://carloslegislacion.blogspot.com.es/2012/11/definicion-de-diversos-delitos.html (Ú.a.: 24/09/2015)

3.2. Identificación de vulnerabilidades.

Etimológicamente la palabra vulnerabilidad está conformada por tres partes latinas: el sustantivo vulnus, que puede traducirse como "herida"; la partícula –abilis, que es equivalente a "que puede"; y el sufijo –dad, que es indicativo de "cualidad". De ahí que vulnerabilidad pueda determinarse como "la cualidad que tiene una entidad para poder ser dañada". En el ámbito de la informática y la tecnología en general, se emplea para referirse a todos los puntos débiles que existen en un sistema y pueden ser aprovechados para dañar el sistema o sus objetivos. Hemos visto en el capítulo 2 el interés que tienen, tanto los desarrolladores como los ciberdelincuentes, en descubrir nuevas técnicas o fallos en los sistemas que puedan ser aprovechados para planificar tanto la defensa como el ataque. Es muy difícil detectar un ataque por medio de una vulnerabilidad si de entrada se desconoce su existencia, de ahí el esfuerzo de atacantes y administradores de sistemas para identificarlas.

3.2.1. Ataques a redes de telefonía o Phreacking.

El hecho de que las nuevas redes telefónicas corporativas estén unidas a las redes de datos corporativas, como vimos en el Capítulo 2 en lo que se refiere al proyecto CORA de las AA.PP. en España, convierte a estas redes en un objetivo muy atractivo para los atacantes, que pueden emplearlas como una vía de entrada a los sistemas informáticos. Desde ahí, es posible acceder a la información corporativa, escuchar conversaciones y crear confusión en el sistema debido al desconocimiento de la procedencia del ataque.

La principal amenaza y forma de ataque a las redes telefónicas, es la intercepción de la información, aunque también la instalación de terminales no autorizadas supone un problema importante en este medio de comunicación. Es relativamente sencillo en casos de terminales inalámbricos, donde un scaner de frecuencias puede identificar rápidamente la presencia y frecuencia a la que transmite una base de telefonía inalámbrica. También se llegan a presentar casos donde el servicio queda no disponible, ya sea a causa de una sobresaturación del medio de transmisión o incluso daños a la infraestructura.

El phreaking (phone freak hacking) o hacking telefónico, como ataque clásico a dispositivos multifrecuencia, está no obstante en desuso. En EE.UU. no existen terminales multifrecuencia desde 2006, y es una tendencia mundial. Pero ha aparecido lo que se dennomina *VoIP phreaking*[203], que utiliza las redes de telefonía VoIP (Voice over IP) como cualquier otra red de ordenadores, ya que adolece de las mismas vulnerabilidades. Las redes VoIP generalmente se configuran sobre una VLAN (LAN virtual) específica definida en los switches y routers

[203] Ofir Arkin. "E.T. Can't Phone Home. Security Issues with VoIP". @Stake (Symantec). Obtenido a través de BlackHat.com. http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt

corporativos, y hacen uso de protocolos SIP (Session Initiation Protocol). Si un atacante consigue acceder hasta uno de estos dispositivos a través de la conexión del terminal, que a todos los efectos es un ordenador más, puede ganarse el control de la red utilizando técnicas de ARP spoofing.

El VoIP phreaking puede tener otras motivaciones para el crimen organizado. Existen proveedores comerciales de telefonía IP y tarjetas que han sido objeto de ataques y estafas. Al conseguir el acceso a la red IP, los phreakers pueden realizar llamadas a redes de telefonía RTC y móviles desde cualquier localización, cargando los costes de la comunicación al proveedor de acceso VoIP que actúa de pasarela hacia las redes RTC y móviles[204].

3.2.2. Ataques a redes de telefonía móvil.

La telefonía móvil es blanco de numerosos ataques de intercepción de información, aunque tant las redes como los términales puedan parecer seguros debido a las técnicas de encriptación y transmisión de datos que usan, cada vez se descubren más formas para infringir la seguridad de estos sistemas.

La cobertura de las redes de telefonía móvil se establece dividiendo el territorio en celdas o células, atendidas desde antenas repetidoras y estaciones base, unidas a través de la red terrestre convencional. Estas antenas, o las propias estaciones base pueden ser interceptadas, lo que permite al atacante realizar una triangulación para determinar la posición de un dipositivo activo conectado a la red móvil, o interceptar sus comunicaciones.

Esta intercepción no está limitada a escuchar las llamadas telefónicas, también se pueden interceptar los números telefónicos que se marquen y otro tipo de datos (como información de transacciones financieras) que puedan manejarse durante una operación telefónica. Estos ataques se valen de recursos diferentes, como algoritmos y programas de desencriptado, equipos de hardware especializados, programas maliciosos e ingeniería social.

El parque de terminales y smartphones conectados a redes 2/3/4G es cada vez más ámplio, los dispositivos son más potentes, y disponen de mayor diversidad de aplicaciones, ésto hace que los teléfonos sean mas prácticos y versátiles, pero al mismo tiempo los hace más vulnerables y susceptibles a todo tipo de ataques. Existen virus, troyanos, spyware y otro tipo de malware diseñados específicamente para los SO de los smartphones, y pueden transmitirse a través de tecnologías y servicios como Bluetooth, mensajes de texto, mensajería instantánea, correo electrónico, redes WiFi, puertos USB, audio y vídeo (WhatsApp, Skype), y el acceso a internet.

[204] Skeeve Stevens. “VoIP hacking is phreaking expensive”. CSO. 08/11/2011. http://www.cso.com.au/article/406675/voip_hacking_phreaking_expensive/ (Ú.a.: 24/09/2015)

Las redes 2G son muy inseguras, pero las redes 3/4G también tienen vulnerabilidades que permiten diversos tipos de ataques[205]:

IMSI Catcher. Consiste en hacerse pasar por la operadora del usuario para recabar su código IMSI (International Mobile Subscriber Identity, o Identidad Internacional del Abonado a un Móvil). Este código de identificación es único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, permitiendo su identificación a través de las redes GSM y UMTS, y permite identificar al propietario. Las redes GSM no se identificaban ante el móvil, y éstos eran muy vulnerables a este tipo de ataque. En las redes 3G la red debe identificarse ante el móvil con una clave encriptada, pero si el atacante fuerza el protocolo puede solicitarle al móvil su identificación, y este contesta con su IMSI.

Localización geográfica. La geolocalización ilegítima en redes 3G es también posible gracias al código IMSI que permite abrir un canal con el móvil el tiempo suficiente para triangular su posición.

DoS. Una falsa red puede suplantar a la operadora y enviar un código de rechazo antes de que se produzca la autenticación con la red legítima y las comunicaciones estén cifradas. De este modo el móvil pierde la cobertura 3G y no la recupera hasta que se produzca un reinicio.

Downgrade selectivo. Tras el ataque DoS descrito, eventualmente el móvil se conectará a través de la red 2G, quedando sus comunicaciones expuestas a otros tipos de ataques que permitirían la instalación de troyanos, extracción de información, etc.

Las guías CCN-STIC-45x[206] ofrecen una información muy completa sobre las características de los diferentes SO en el mercado, amenazas, vulnerabilidades y el modelo de arquitectura de seguridad para estos dispositivos, y ponen a disposición de los usuarios finales un amplio abanico de recomendaciones para configurar de forma segura la enorme variedad de servicios disponibles.

3.2.3. Barrido de puertos.

El barrido o escaneo de puertos consiste en verificar qué puertos están disponibles para ser explorados en uno o más equipos de la red. Por sí solo, el barrido de puertos es una actividad normal que frecuentemente es usado para mejorar los servicios de seguridad y rendimiento de una red, pero también puede utilizarse de forma maliciosa. Generalmente las aplicaciones

[205] David G. Ortiz. "Investigadores españoles demuestran que las redes 3G se pueden 'hackear' al menos de cuatro formas". eldiario.es. 08/03/2014. http://www.eldiario.es/hojaderouter/seguridad/root2G-3G-ataques-David_Perez-hacking-Jose_Pico-Layakk-redesed_con-seguridad_informatica_0_275772476.html (Ú.a.: 24/09/2015)
[206] Guías CCN-STIC-4xx. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias-generales.html CERT-CCN. (Ú.a.: 24/09/2015)

utilizan puertos específicos bien conocidos, la disponibilidad de un puerto por tanto va asociada a la presencia de la aplicación en el sistema, de la que pueden ser conocidas determinadas vulnerabilidades y ser utilizadas para ganarse el acceso al sistema.

En otros casos el sistema puede tener varios puertos abiertos, con desconocimiento del encargado de seguridad, y en consecuencia estos puertos no son vigilados, convirtiéndolos en una vulnerabilidad del sistema.

Puede ser consecuencia de una mala configuración de los sistemas de seguridad (por ejemplo los firewalls). Los administradores de los sistemas se despreocupan de la configuración de los puertos de las máquinas, que dejan abiertos para servicio de las aplicaciones de la red interna, confiando en que el firewall se encargará de filtrar cualquier intento de acceder a esos puertos desde internet, pero una mala configuración del firewall, que puede dejar por defecto puertos abiertos, o por una eventual apertura para proporcionar un servicio concreto, puede dejar desprotegidos a los sistemas.

3.2.4. Identificación de Firewalls.

Un firewall, o cortafuegos, es un dispositivo de seguridad de red diseñado para bloquear los accesos no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Permite o limita el tráfico, lo cifra o descifra, y filtra los paquetes de datos a partir de una serie de reglas y criterios definidos por el administrador de la red. Este dispositivo puede ser una maquina específicamente diseñada y construida para esta función, pero también un software instalado en un ordenador, que opera antes de distribuir el tráfico a la red. Por otro lado cada ordenador de la red puede equipar su propio firewall para autoprotegerse. También es frecuente conectar el cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

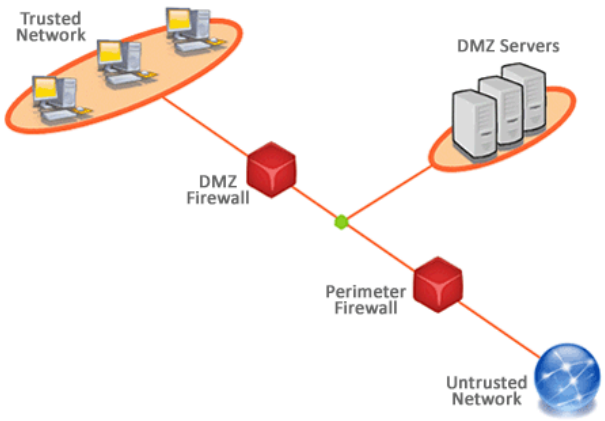

Figura 47: *Configuración de firewall y DMZ. Fuente: iWebGate Technology, a través de webcindario.com. http://zubiri-sad-03.webcindario.com/ (Ú.a.: 24/09/2015)*

Los atacantes pueden saltar la seguridad de un firewall aprovechando puertos eventualmente abiertos. Un método común para descubrir los puertos vulnerables es enviando una serie de paquetes de datos defectuosos (por ejemplo dirigidos a una IP que no existe en la red), el firewall los interceptará y no permitirá su enrutamiento, pero si el puerto no está siendo filtrado, permitirá pasar el paquete y al no poder enrutarlo correctamente, el firewall mandará un mensaje de error a través del protocolo ICMP (Internet Control Message Protocol), lo que evidenciará que el paquete no fue filtrado. Se puede crear así un listado de puertos que no están siendo filtrados a partir de los mensajes de error que se generen con este proceso.

Interpretación de reglas y filtros. Las reglas de filtrado son una serie de condiciones que un usuario, equipo de la red o paquete de datos, debe cumplir a partir de las políticas de seguridad de la información implantadas en la organización, para tener acceso a un equipo a través de los puertos protegidos por un sistema de seguridad (en este caso el firewall). Desde el punto de vista del atacante, la interpretación de filtros implica descifrar las condiciones necesarias que se necesitan para pasar información a través de los firewalls sin ser un usuario autorizado. Estos procedimientos incluyen ataques de fuerza bruta e incluso ingeniería social.

3.2.5. OS fingerprinting.

OS fingerpriting (la huella del Sistema Operativo) es el proceso de recopilación pasiva de información que lleva a identificar el sistema operativo de una máquina remota. Esta identificación se basa en los atributos de configuración que diferencian a cada uno de los sistemas de los demás: distintas implementaciones de la pila TCP/IP (algunas fuentes de hecho lo referencian como TCP/IP stack fingerprinting[207]), diferentes comportamientos ante el envío de paquetes que presentan una conformación especial, distintas respuestas en función del protocolo utilizado (TCP, ICMP, ARP), etc[208].

El objetivo de esta técnica no sólo se limita a identificar el sistema operativo remoto, también se puede obtener información de cómo funciona, en caso de tratarse de un sistema personalizado o que no esté documentado. El OS fingerprinting tiene aplicaciones legítimas, pero, como la mayoría de este tipo de recursos, también puede usarse para un ataque, siendo la identificación del SO remoto, uno de los primeros pasos necesarios para llevarlo a cabo, de forma que puedan identificarse vulnerabilidades, confeccionar exploits, inventariar los recursos de red, identificar dispositivos peligrosos, etc. Se pueden distinguir dos métodos:

[207] Fyodor. "Remote OS detection via TCP/IP stack fingerprinting". NMAP.org. http://www.insecure.org/nmap/nmap-fingerprinting-article.html (Ú.a.: 24/09/2015)
[208] Antonio Rana. "Intrusion Detection FAQ". SANS. https://www.sans.org/security-resources/idfaq/amap.php (Ú.a.: 24/09/2015)

Fingerprinting activo: este tipo de identificación del SO se basa en analizar la respuesta del servidor que se quiere identificar cuando se le envían determinados paquetes TCP y UDP.

El Fingerpriting activo tiene la ventaja de que se puede experimentar enviando diversos tipos de paquetes para forzar diferentes respuestas por parte del sistema, lo que aporta una mayor variedad de resultados a la hora de ser analizados. Su mayor desventaja es que es fácil de detectar e interceptar por parte de los dispositivos de seguridad (por ejemplo firewalls) implementados en la red donde esté el sistema analizado.

La herramienta más popular parece ser *Nmap*. Algunas de las técnicas que se utilizan pueden ser primitivas, pero otras son bastante complejas y requieren un conocimiento profundo de los protocolos TCP/IP para configurar las pruebas e interpretar los resultados. Nmap actúa en tres pasos: un escaneo inicial de puertos, que proporciona un listado de cuales están abiertos o cerrados; envío de paquetes construidos "ad hoc"; y análisis de las repuestas obtenidas que se contrastan contra una base de datos de conocimiento de SO (fingerprints).

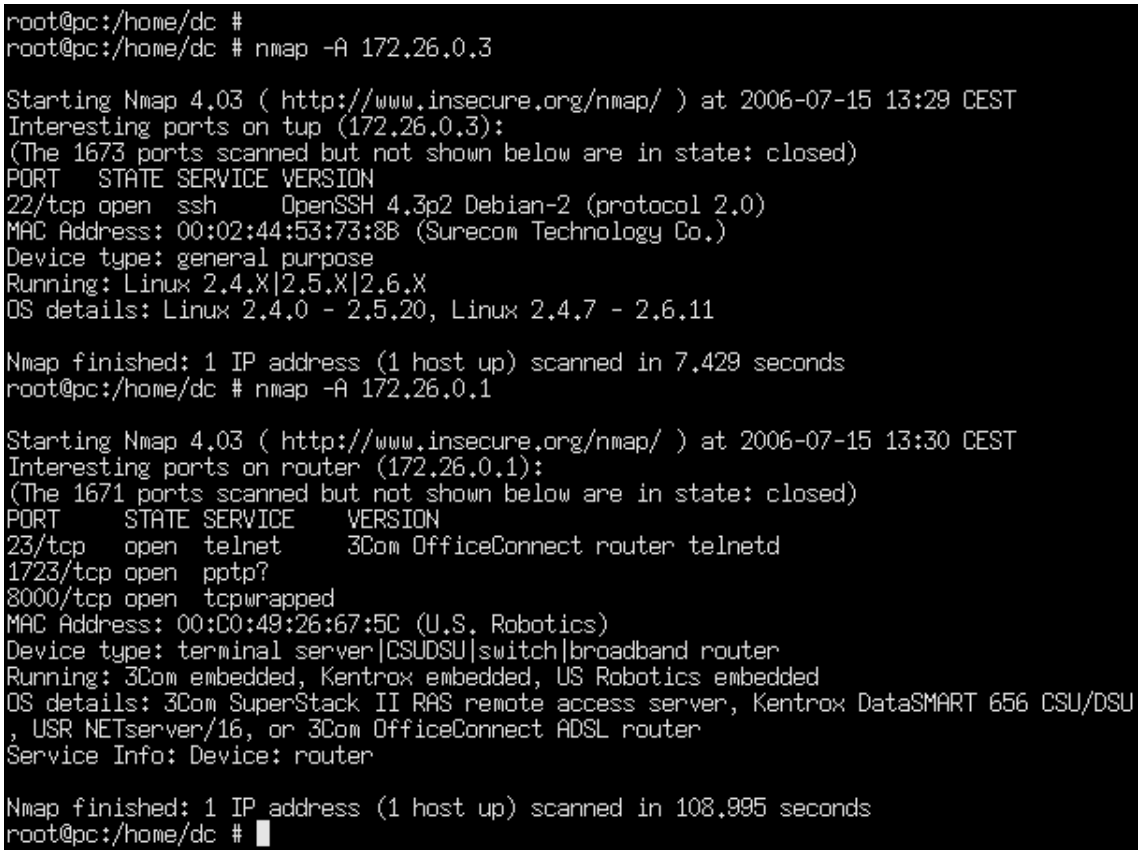

Figura 48: *Captura de pantalla de la ejecución de Nmap contra dos direcciones IP, en el primer caso se ha detectado un sistema Debian Linux, y en el segundo un router con un SO propietario, 3Com SuperStack. Fuente: Wikipedia. "Identificación de SO según pila TCP/IP". https://es.wikipedia.org/wiki/Implementaciones_de_TCP (Ú.a.: 24/09/2015).*

Fingerpriting pasivo[209]**:** el fingerpriting pasivo es un sniffing, consiste en capturar paquetes de datos provenientes del sistema remoto y analizarlos.

Igual que en el caso de la identificación activa, la pasiva se basa en el principio de que todas las tramas IP aportan información sobre las características del SO. Analizando los paquetes capturados e identificando dichas diferencias se puede determinar el SO de la máquina remota. Hay cinco parámetros particularmente útiles:

- El valor del campo TTL (Time to Live) de la cabecera de las tramas IP
- El tamaño de ventana inicial de la cabecera TCP.
- El valor del bit DF (Don't Fragment bit) de la cabecera IP
- El valor del campo Tipo de Servicio, TOS (Type of Service) en la cabecera IP
- Los tipos de opciones usados en las tramas TCP (si las hay)

Esta información puede contrastarse en una base de datos sencilla de huellas de SO[210].

3.2.6. Escaneo de redes WiFi.

Una red inalámbrica es un conjunto de dispositivos informáticos comunicados entre sí por medios no tangibles. Si conectarse de forma ilegítima a las redes cableadas es complicado -habría que conectarse físicamente mediante un cable-, en el caso de las redes inalámbricas esta tarea es sencilla.

El primer paso para conectarse a una red inalámbrica es detectar primero su presencia, así como recabar información sobre su configuración. El método más simple para detectar una red es utilizar la propia herramienta de redes inalámbricas que incorpora el sistema operativo o que incluye el fabricante de la tarjeta inalámbrica. Esta herramienta permite realizar una exploración de las redes disponibles, mostrando una lista con indicación del nombre SSID (Service Set IDentifier) de la red, y tipo de red (si esta cifrada o no, y el método de cifrado) de cada uno de los puntos de acceso (WAP, Wireless Access Point) detectados. Existen también herramientas como Netslumber, que explora de forma continua el espectro radioeléctrico en busca de redes inalámbricas disponibles.

Si una red no esta cifrada, se dice que es una red abierta, pero no significa que está desprotegida, ya que puede estar usando un sistema de protección distinto al cifrado WEP/WPA.

---

[209] Honeynet Project. "Know Your Enemy: Passive Fingerprinting". 04/03/2002. http://old.honeynet.org/papers/finger/ (Ú.a.: 24/09/2015)
[210] Honeynet Project. "Lists of fingerprints for passive fingerprint monitoring". 20/05/2000. http://old.honeynet.org/papers/finger/traces.txt (Ú.a.: 24/09/2015)

Estos datos son suficientes para conectarse a una red propia, pero para entrar a una red a la que no se está autorizado se necesita recopilar más datos. Las herramientas que pueden usar los atacantes utilizan dos métodos para recopilar información:

Pasivo. Estos sistemas se limitan a escuchar e interpretar la información que reciben, la más inmediata la identificación SSID de la red. Los ataques pasivos afectan a la confidencialidad pero no influyen en la integridad de la información.

Activo. En este caso los sistemas no se limitan a escuchar, sino que interactúan de una u otra forma, con la red. Por ejemplo, si no reciben el nombre SSID, recabarán la información del punto de acceso o de los sistemas unidos a la red. Los ataques activos pueden llegar a modificar, eliminar o inyectar tráfico a la red.

La información que se puede conseguir utilizando estos métodos es por ejemplo:

- Nombre SSID, aunque el punto de acceso lo tenga oculto
- Esquema de direccionamiento IP de la red.
- Marca y modelo del hardware.
- Versión del software.
- Tipo de cifrado utilizado.
- Clave de cifrado WEP.
- Puertos IP abiertos.
- Información intercambiada.

Toda esta información no puede conseguirse en un solo ataque o con una sola herramienta, por lo que el atacante deberá recopilar la información en diversos pasos sin ser descubierto y usar todo tipo de herramientas y métodos, incluyendo la ingeniería social de ser necesaria.

3.2.7. Instalaciones físicas.

La seguridad física se implementa mediante la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Comprende todos los controles y mecanismos de seguridad interior y perimetral del CPD (Centro de Proceso de Datos), así como los medios de acceso remoto hacia y desde el mismo, implementados para proteger el hardware y los medios de almacenamiento de datos.

Las principales amenazas que se prevén en cualquier estudio de riesgos, o en los planes de contingencia, relativos a la seguridad física de las instalaciones de un CPD, son: la probabilidad

de que desastres naturales, incendios accidentales, tormentas e inundaciones, afecten a los sistemas de información, así como también la falta de instalaciones apropiadas para afrontarlas; y las amenazas ocasionadas por el hombre, ésto es, robos, disturbios, sabotajes internos o externos.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

Control de Accesos. El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector, dentro de las instalaciones de una organización. Los controles de acceso incluyen la utilización de personal de seguridad, dispositivos electrónicos de acceso y verificación, cerraduras manuales y electrónicas, e implantación de políticas y normas de seguridad aplicables al personal.

Una intrusión en las instalaciones físicas generalmente está protagonizada por los mismos empleados, que conocen y tienen acceso directo a las instalaciones y pueden eventualmente saltarse los protocolos de seguridad implantados. En casos muy excepcionales se da por personas totalmente ajenas, como por ejemplo ladrones, espías y terroristas. Pero el riesgo existe, y los incidentes, aunque raros, se producen.

3.2.8. Configuración de servicios y servidores.

Existen muchos casos en que los riesgos pueden reducirse simplemente por verificar la configuración de todos los servicios que forman parte de un sistema.

Todos los servicios se instalan con una configuración estándar que pueden permitir una puesta en producción rápida y un uso fácil, lo que resulta muy conveniente desde el punto de vista de la productividad, pero no suele ser la más apropiada desde el punto de vista de la seguridad.

En general las organizaciones de tamaños grande o muy grande, estructuran sus servicios y servidores en dos entornos: un entorno de producción y otro de preproducción. Los nuevos servicios o servidores se instalan en el entorno de preproducción, y se configuran al tiempo que se les somete a pruebas con datos simulados, o subconjuntos de datos reales, y con usuarios reales, antes de pasarlos al entorno de producción. En general la configuración se ajusta para que responda a los requerimientos de ejecución con el menor impacto posible en la organización, lo que implica muchas veces mantener configuraciones muy similares a las existentes, provocando una propagación de las vulnerabilidades.

Muchas veces un servicio mal configurado se convierte en una grave vulnerabilidad que será detectada y aprovechada por los atacantes potenciales. Por ello cuando se implanta un servicio o

dispositivo dentro de una red, es necesario realizar una configuración personalizada que cumpla con las políticas de seguridad, estableciendo un compromiso entre la funcionalidad del sistema y su seguridad.

3.2.9. Software.

El software ofrece una versatilidad absoluta como herramienta de ataque desde cualquier punto de vista. Por un lado un atacante puede aprovechar diferentes vulnerabilidades de un software (bugs, errores de diseño, mala configuración…) para acceder a una red o sistema. También existe software que sin ser necesariamente malicioso, puede ser usado para romper la seguridad, existen numerosas aplicaciones que han sido creadas para ayudar en la mejora continua de la seguridad, la administración de sistemas o facilitar la conectividad de una red, pero que también son herramientas que pueden utilizarse de forma ilegítima para atacar los sistemas, como hemos visto con Nmap. Y existe software personalizado, creado por los mismos atacantes con el propósito de ayudar a penetrar la seguridad de los sistemas.

3.3. Acceso a los sistemas y redes.

Cada sistema o red tiene puntos vulnerables que pueden ser aprovechados por los atacantes para acceder al sistema, a esta actividad se le conoce como intrusión o explotación del sistema, y puede ser llevada a cabo por personas externas o los mismos usuarios internos.

La explotación de sistemas no se limita al aprovechamiento de errores de programación o puertos abiertos, con ingenio también se puede sacar provecho de las características correctamente configuradas del sistema mismo. Esta práctica puede ser ejecutada por distintos medios, por tanto para combatirla es necesario hacer uso de distintas tecnologías, estrategias y políticas de seguridad, y desarrollar sistemas con técnicas de programación segura, referenciada también como programación defensiva. La metodología para la programación segura es un suplemento de la metodología de seguridad OSSTMM (Open Source Security Testing Methodology Manual)[211] [212].

A continuación se indican las formas más comunes de explotación de sistemas.

3.3.1. Promiscuidad en redes.

En una red de ordenadores, la información se transmite en una serie de paquetes con la dirección física (o dirección MAC) del emisor y del destinatario, de manera que cuando

[211] Pete Herzog. Open Source Security Testing Methodology Manual (OSSTMM). ISECOM. http://www.isecom.org/research/osstmm.html (Ú.a.: 24/09/2015)
[212] Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). Junta de Andalucía. http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551 (Ú.a.: 24/09/2015)

transmitimos un fichero, éste se divide en un número de paquetes de tamaño predeterminado, y el receptor es el único que captura los paquetes identificados con su dirección.

En modo promiscuo, un nodo intermedio captura todos los paquetes, que normalmente desecharía, incluyendo los paquetes destinados a él mismo y al resto de las máquinas. El modo promiscuo resulta muy útil para ver qué paquetes atraviesan la red. Por otro lado también es útil para realizar ataques contra redes, instlando un sniffer que hará funcionar la máquina en este modo para capturar toda la información que se transmita. Este término se usa también para describir técnicas de ataque a redes WIFI cifradas.

Existen herramientas para la detección de interfaces de red que se encuentren en modo promiscuo. Se basan en el envío de paquetes que nadie responderá, salvo los equipos en modo promiscuo[213].

Detección de Latencia en paquetes ICMP: Este método lanza muchas peticiones TCP erróneas para que ningún equipo las tenga en consideración. A continuación se envía ping a todas las máquinas. La máquina en modo promiscuo tardará en responder ya que está ocupada procesando los paquetes. El atacante podría bloquear la entrada de peticiones ICMP en el firewall de su equipo para evitar ser descubierto.

Detección mediante paquetes ping ICMP: Se lanza un ping a una máquina sospechosa, con la MAC del paquete erronea. Si la máquina está en modo promiscuo, responderá sin comprobar que la MAC es errónea. El atacante de nuevo podría bloquear la entrada de peticiones ICMP en el firewall de su equipo para evitar ser descubierto.

Detección mediante paquetes ARP: Se envía un paquete de petición ARP con destino a la dirección IP de la máquina sospechosa y a una dirección MAC inexistente. Si el equipo está en modo promíscuo, procesará dicha consulta ARP y responderá. Este proceso se suele repetir para todas las IPs válidas en el rango de direcciones de la red local para comprobar todos los equipos. El atacante podría usar una distribución Linux modificada para no responder a este tipo de consultas y evitar así ser descubierto por este método.

Detección en base a resoluciones DNS: Muchos programas de captura de tramas de red que funcionan en modo promíscuo suelen tener por defecto activada la opción de resolver las IP de los equipos remitentes y destinatarios de los paquetes capturados. Un programa de detección puede enviar paquetes desde una IP inexistente a otra para comprobar si posteriormente se

[213] Detección de máquinas en modo promiscuo en la red. Wikipedia. https://es.wikipedia.org/wiki/Modo_promiscuo#Detecci.C3.B3n_de_m.C3.A1quinas_en_modo_promiscuo_en_la_red (Ú.a.: 24/09/2015)

realizan las correspondientes resoluciones de DNS. El atacante por su parte podría deshabilitar las resoluciones de DNS en el programa de captura de tramas para evitar ser descubierto.

Un sniffer adecuadamente configurado puede pasar inadverido en una red, pese a los intentos del administrador por rastrear su presencia, y acceder a toda la información transmitida.

3.3.2. Robo de identidad.

Un ataque de robo de identidad se produce cuando un usuario ilegítimo se hace pasar por otro legítimo, con el propósito de ganar acceso a la red, obtener privilegios administrativos o realizar operaciones fraudulentas. El atacante puede robar la identidad usando directamente el equipo de la víctima, obteniendo sus credenciales de acceso, falsificando identificaciones digitales o certificados de identidad y firma electrónica, o por tantas vías como le sugiera la imaginación[214].

Una variante del robo de identidad es el robo de sesión, como el nombre indica, consiste en apropiarse de la sesión iniciada por otro usuario, teniendo acceso a todos los recursos a los que la víctima tiene acceso. También suplantar una dirección IP, para intentar hacer pasar un equipo por otro, es un robo de identidad. Este tipo de suplantación es posible al modificar manualmente la configuración de red del equipo.

La mayoría de las personas no se enteran que han sido víctimas del robo de identidad hasta que aparecen cobros misterisoso en sus facturas de crédito

3.3.3. Engaño a firewalls y detectores de intrusos.

Al describir las técnicas de detección de firewalls, barrido de puertos y fingerprinting, ya se han mencionado algunos ejemplos de cómo penetrar estos sistemas de seguridad, el robo de identidad también es una forma de pasar a través de un firewall, utilizando una sesión autorizada, y los detectores de intrusos (IDS) no pueden verificar que el usuario sea realmente quien dice ser.

Incluso con políticas de seguridad proactivas, si un atacante consigue engañar a un firewall[215], pasará tiempo hasta que el CISO encuentre indicios de la presecia de un intruso, posiblemente cuando la extracción de información ya sea un problema muy grave.

3.3.4. Vulnerabilidades en el software.

[214] Techniques for obtaining and exploiting personal information for identity theft. Wikipedia. https://en.wikipedia.org/wiki/Identity_theft#Techniques_for_obtaining_and_exploiting_personal_information_for_identity_theft (Ú.a.: 24/09/2015)
[215] Serg Vergara. "Saltando la seguridad de un Firewall". 15/04/2011. https://sergvergara.wordpress.com/2011/04/15/tratando-de-saltar-la-seguridad-de-un-firewall/ (Ú.a.: 25/09/2015)

Las vulnerabilidades en el software pueden ser errores de programación, configuración, análisis, diseño o implantación, y pueden presentarse en los programas de seguridad, navegadores, gestores de bases de datos, aplicaciones varias, o en el mismo sistema operativo.

La forma en que un atacante aproveche estas vulnerabilidades para entrar a un sistema varía dependiendo del sistema, software y herramientas con las que cuenta, de modo que cada caso es diferente. Pero el primer paso es siempre reunir toda la información posible sobre el sistema objetivo.

Seguido se reseñan algunas de las vulnerabilidades de software que generalmente se usan para atacar la seguridad de un sistema:

Buffer Overflows[216]. Se trata de un error de programación en el que un proceso intenta guardar datos más allá de los límites asignados de memoria. El resultado es la escritura de datos en direcciones cercanas de memoria correspondientes a otros procesos, provocando resultados incorrectos o la interrupción de la ejecución del programa (aborto).

Este error también puede ser forzado por la ejecución de código malicioso y es la causa de muchas vulnerabilidades de software, ya que puede ser aprovechado para corromper la ejecución de un programa produciendo una sobreescritura de la dirección de retorno de una función y haciendo que apunte directamente hacia un código concreto (generalmente un shell) logrando que se ejecute.

Heap Overflows. Es otro tipo de buffer overflow que causa una modificación en los datos contenidos de una pila o heap (zona de memoria dinámica) en vez de modificar la dirección de retorno, logrando alterar la lógica de funcionamiento de un proceso, que responderá como si las condiciones de entrada fueran diferentes.

Format String Bugs (Errores en las cadenas con formato)[217]. Este tipo de errores aparecen cuando se usa alguna de las funciones que admiten opciones de formato. El programador puede confundir por error *printf ("%s", buffer)* con *printf (buffer)*. La primera función muestra la cadena en pantalla, que es lo que el programador intenta. La segunda función, que no especifica el primer argumento, produce que la función espere una opción, entre las que se le puede añadir *%n* que escribe el número de bytes mostrados, con lo que un atacante podría formar una cadena con formato que incluyera datos aleatorios, y muy posiblemente el código que quiera ejecutar.

[216] Desbordamiento de Bufer. Wikipedia. https://es.wikipedia.org/wiki/Desbordamiento_de_b%C3%BAfer (Ú.a.: 27/09/2015)
[217] Errores en las cadenas con formato. Websecurity.es. http://www.websecurity.es/errores-las-cadenas-formato (Ú.a.: 27/09/2015)

Dicha opción, permite que se sobreescriba la memoria de forma arbitraria, y podría verse afectado el puntero de retorno, provocando la ejecución de código del atacante.

Race Conditions (Condición de Carrera)[218]. Múltiples procesos se encuentran en condición de carrera si el resultado de los mismos depende del orden de su ejecución. Si los procesos que están en condición de carrera no son correctamente sincronizados, o no resuelven correctamente la concurrencia, puede producirse una corrupción de datos, que puede ser aprovechada por exploits locales para vulnerar los sistemas.

SQL Injection[219]. Es un método que aprovecha una vulnerabilidad asociada a la validación de datos suministrados por el usuario, como parte de una operación sobre una base de datos. Una inyección SQL consiste en suministrar código malicioso dentro de una consulta SQL. Al ejecutarse esa consulta por el gestor de base de datos, el código SQL inyectado también se ejecutará, con lo que se puede insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar código malicioso en el sistema.

Cross-Site & Cross-Domain Scripting (Secuencias de órdenes en sitios/dominios cruzados).

Cross-Site-Scripting (XSS)[220]. Es una vulnerabilidad típica de las aplicaciones Web. Permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript, o en otro lenguaje similar, evitando medidas de control como la Política del mismo origen.

Dicho código malicioso se compone de cadenas de datos cuyo contenido son scripts completos contenidos en enlaces o ejecutados desde formularios. En caso de que sea ejecutado, lo hará con todos los privilegios permitidos por las políticas de seguridad configuradas en el navegador del usuario o del sitio visitado. El atacante oculta el hipervinculo malicioso tras un texto con apariencia de enlace, dirige al usuario al sitio e inyecta en el site la información que le interesa, como si suministrara información de una cookie.

Cross Domain. Esta vulnerabilidad se basa en el elemento OBJECT, permitido en HTML 4, y que es usado para incluir objetos externos dentro de una página Web. Estos objetos pueden ser cualquier control ActiveX como WebBrowser, además de imágenes, applets y otros.

Los controles WebBrowser (controlan diversas acciones en el navegador), incluidos en esta etiqueta pueden eludir las restricciones de seguridad ordinarias aplicadas para otros elementos del código HTML. Esto literalmente significa que se puede ejecutar código malicioso al visitar

[218] Condición de carrera. Wikipedia. https://es.wikipedia.org/wiki/Condici%C3%B3n_de_carrera (Ú.a.:27/09/2015)
[219] Inyección SQL. Wikipedia. https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL (Ú.a.: 27/09/2015)
[220] The Cross-Site Scripting (XSS) FAQ. CGISecurity. http://www.cgisecurity.com/xss-faq.html (Ú.a.:27/09/2015)

una página Web o al recibir un mensaje electrónico con formato HTML, tal como si fuera ejecutado en forma local, sin advertencia alguna del navegador.

Virus[221] y Gusanos[222]. Un virus es un código escrito con la intención expresa de replicarse. Un virus se adjunta a sí mismo a un programa huesped y, a continuación, intenta propagarse de un equipo a otro sin consentimiento del usuario. Adicionalmente puede contener una parte denominada payload que ejecutará una serie de acciones cuando se cumplan las condiciones especificadas. Un verdadero virus no se difunde sin la intervención humana, alguien debe compartir un archivo o enviar un mensaje de correo electrónico para propagarlo.

Un gusano, también llamado Worm, o iWorm (gusano de internet), al igual que un virus está diseñado para copiarse de un equipo a otro, pero lo hace automáticamente, tomando el control de las características del sistema que permiten transferir archivos o información. El gran peligro de los gusanos es su habilidad para replicarse, por ejemplo enviándose a todos los destinatarios de una libreta de direcciones o a todas las IP de una red. Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.

Certificados Digitales y entidades de certificación. Los certificados digitales permiten acreditar la legitimidad de un software o de una página web. Son esenciales en los sistemas operativos de 64 bits para reconocer el software del fabricante de un dispositivo, y también habilitan a los navegadores para securizar una operación de comercio electrónico. Un atacante puede utilizar estos certificados para suplantar una identidad y obtener acceso al sistema.

3.3.5. Ataques a contraseñas.

Un ataque a contraseña es toda acción dirigida a obtener, modificar o borrar las contraseñas de acceso de un sistema informático. Su eficacia depende de la debilidad de las contraseñas (limitadas en número y tipo de caracteres, palabras completas de un idioma, etc.). Por ello se recomienda usar combinaciones aleatorias de caracteres para conformar una contraseña robusta. Con la desventaja de que la mayoría de los usuarios no pueden recordarlas, y generalmente las anotan en otros medios (como un archivo de texto o una nota de papel), que pueden extraviar, o a los que otros usuarios pueden acceder.

Acceso a los ficheros de contraseñas. Una vulnerabilidad presente en cualquier sistema que no encripta los ficheros que contienen las contraseñas almacenadas, de forma que pueden ser localizados e interpretarse la información. Parece una obviedad, pero permitió obtener las contraseñas y datos económicos de los usuarios de PSN de Sony.

[221] Virus informático. Wikipedia. https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico (Ú.a.:27/09/2015)
[222] Gusano informático. Wikipedia. https://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico (Ú.a.:27/09/2015)

Ataque de diccionario[223]. Consiste en probar todas las palabras existentes en un diccionario (cualquier fichero con cadenas de texto probable o potencialmente usadas como contraseña). En este método también se pueden combinar las palabras para formar frases, alterar las combinaciones de cadenas, y usar diccionarios de idiomas extranjeros. Es un método muy efectivo cuando los usuarios tienen contraseñas débiles.

Fuerza bruta[224]. Se trata de combinar todos los posibles caracteres para formar combinaciones hasta obtener la contraseña correcta. Es el método mas laborioso y difícil, y solo puede ser logrado por maquinas con una elevada capadidad de proceso.

3.3.6. Debilidad de los protocolos de red[225].

Los protocolos de red son el conjunto de reglas formales que permiten el intercambio de datos entre entidades que forman parte de una red. Este intercambio de datos no se limita a la información contenida en bases de datos y ficheros, incluye también instrucciones y procesos. Por eso una debilidad en los protocolos de intercambio puede tener consecuencias que van desde la negación del servicio de red, a la pérdida y alteracion de información, robo de los recursos de la red e incluso permitir el control remoto de los sistemas. El protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), basado en el modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), está diseñado para encaminar la información y tiene un grado muy elevado de fiabilidad, pero no está exento de vulnerabilidades, incluidas algunas de diseño, como la que afecta al BGP (Border Gateway Protocol), que se emplea para el intercambio de información de enrutamiento y el mantenimiento de las tablas de direcciones IP, y que hace uso intensivo de las conexiones TCP, sin utilizar ningún tipo de autenticación.

3.3.7. Ataques a servicios.

Los ataques a los servicios tienen por objetivo colapsar un sistema o red para evitar que los servicios y recursos puedan ser utilizados por los usuarios. Un atacante puede realizar un ataque con el objeto de bloquear un servicio por varios medios:

- Ejecutar actividades que consuman una gran cantidad de recursos de las maquinas afectadas, provocando una reducción en su rendimiento y posteriormente la caída del sistema completo.
- Provocar el colapso de redes mediante la generación de grandes cantidades de tráfico, generalmente de múltiples equipos.

[223] Ataque de diccionario. Wikipedia. https://es.wikipedia.org/wiki/Ataque_de_diccionario (Ú.a.:27/09/2015)
[224] Ataque de fuerza bruta. Wikipedia. https://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta (Ú.a.:27/09/2015)
[225] Raúl Siles. "Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados". RedIRIS, 2002. http://www.rediris.es/cert/doc/segtcpip/Seguridad_en_TCP-IP_Ed1.html (Ú.a.:27/09/2015)

- Sabotear la red alterando las tablas de los routers para que proporcionen información falsa que impida el acceso a ciertas maquinas de la red.
- Transmisión de paquetes de datos malformados, o que no cumplan las reglas de protocolo.
- Incumplimiento de las reglas de un protocolo.

3.3.8. Ataques a redes WiFi.

Las técnicas de ataque a redes WiFi son conceptualmente similares a los ataques a otras redes, pero pueden presentar algunas diferencias específicas. Se puede distinguir entre ataques pasivos y activos. Los primeros no modifican la información, el atacante se limita a escuchar, obtener y monitorear la información (este tipo de ataque es muy difícil de detectar). En un ataque activo un usuario no autorizado puede modificar y/o denegar el acceso a la información.

Sniffing. El sniffing, como ya se ha comentado, es un ataque pasivo que consiste en que un usuario no autorizado se dedica a hacer un monitoreo de todos lo paquetes de información que circulan por la red mediante un sniffer. El tráfico de las redes inalámbricas puede espiarse más fácilmente que una red convencional, ya que el medio es accesible, y sólo se necesita una tarjeta de red inalámbrica y un equipo para empezar a interceptar los datos, independientemente de si están cifrados o no.

Análisis de tráfico. En este tipo de ataque pasivo el atacante obtiene la información que desea por medio de un exámen profundo del tráfico y sus patrones: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

Suplantación o enmascaramiento. Este tipo de ataque activo consiste en conseguir varias direcciones válidas mediante un sniffer y analizar el tráfico para saber a que hora poder conectarse para suplantar a un usuario de la red atacada. El atacante se apodera de la dirección del verdadero usuario tras su atenticación, pudiendo acceder a la información dentro de la red.

Access Point Spoofing. O asociación maliciosa, es otra forma de suplantación, en este caso el atacante se hace pasar por un access point y sus víctimas piensan estar conectándose a una red WLAN verdadera. Ataque común en redes ad-hoc.

Rogue Access Point[226]. No es realmente un ataque a una red WiFi, sino que el atacante utiliza un dispositivo de acceso WiFi conectado a una red segura sin conocimiento del administrador para acceder a ella de forma inalámbrica.

Modificación. El atacante borra, manipula, añade o reordena mensajes transmitidos.

[226] Rogue access point. Wikipedia. https://en.wikipedia.org/wiki/Rogue_access_point (Ú.a.:27/09/2015)

Denegación de Servicio (DoS). Éste método de ataque consiste en que el atacante de la red se ocupa de generar interferencias de variados tipos hasta que se produzcan tantos errores en la transmisión que la velocidad caiga abruptamente o que la red cese sus operaciones. Al ser ataques de corta duración es muy difícil defenderse de ellos ya que solo es posible detectarlos en el momento en que actúan.

Ataque de Hombre en Medio o Reactuación (Man-in-the-middle)[227]. Como ya se ha comentado, el atacante adquiere la capacidad de interponerse en una comunicación y leer, insertar y modificar a voluntad los mensajes entre las dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. Todo ello implica una manipulación externa de la información, así como un ataque adicional a nivel de intercepción de la comunicación (por ejemplo con Access Point Spoofing), y denegación de servicio.

ARP Poisoning[228]. También referenciado como ARP Spoofing. Suplantación de identidad por falsificación de la tabla ARP (Address Resolution Protocol, o Protocolo de resolución de direcciones). El ataque consiste en mandar un paquete del tipo "REPLY ARP" falso en el que otorgamos una dirección IP legítima a una MAC (Media Access Control, o Dirección de control de acceso al medio) ilegítima. La mayoría de los sistemas operativos no implementan estados en el protocolo ARP y por tanto aceptan el REPLY aún sin haber realizado ninguna petición.

WEP key-cracking. WEP (Wired Equivalent Privacy) es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes WiFi que permite cifrar la información que se transmite. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 ó 128 bits. Para atacar una red inalámbrica se utilizan los denominados packet sniffers y los WEP crackers.

Para llevar a cabo este ataque, se captura una cantidad de paquetes suficiente, lo cual será determinado por el número de bits de cifrado, mediante la utilización de un packet sniffer. A continuación, mediante un WEP cracker o key cracker, se trata de vulnerar el cifrado de la red. Un key cracker es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP, como BackTrack[229], AirCrack[230] o WEPCrack[231].

[227] Ataque Man-in-the-middle. Wikipedia. https://es.wikipedia.org/wiki/Ataque_Man-in-the-middle (Ú.a.:27/09/2015)
[228] ARP Spoofing. Wikipedia. https://es.wikipedia.org/wiki/ARP_Spoofing (Ú.a.:27/09/2015)
[229] Gina Trapani. "How to Crack a Wi-Fi Network's WEP Password with BackTrack". LifeHacker. 10/28/11. http://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack (Ú.a.:27/09/2015)
[230] AirCrack-ng. http://www.aircrack-ng.org/ (Ú.a.:27/09/2015)
[231] Anton T. Rager. WEPCrack. http://wepcrack.sourceforge.net/ (Ú.a.:27/09/2015)

3.4. Aseguramiento del acceso.

Una vez que el atacante ha logrado penetrar a un sistema, intentará mantener el acceso, para no tener que repetir el mismo proceso de infiltración cada vez, arriesgándose a una exposición y abandonando el sigilo, o porque las tareas de exfiltración de información se prolongarán en el tiempo.

3.4.1. Backdoors[232].

Una puerta trasera es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo de autenticación para acceder al sistema. Las más conocidas son Back Orifice y NetBus. En algunos casos estas puertas pueden tener su origen en una serie de servicios que se utilizan durante las fases de desarrollo de un sistema informático y que se mantienen por error o descuido.

3.4.2. Troyanos[233].

O Caballo de Troya (por la Odisea de Homero), es cualquier malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

3.4.3. Rootkits[234].

Un rootkit es un troyano que otorga privilegios de acceso y administración (root) a un sistema manteniendo su presencia oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. Se distinguen tres tipos de rootkits:

Rootkits binarios. Reemplazan a una herramienta del administrador del sistema, sustituyendo el fichero binario original por otro modificado que incluye nuevas utilidades.

Rootkits de kernel. Modifican el núcleo (kernel) del sistema operativo en el equipo infectado. De este modo consiguen manipular las respuestas del kernel para poder ocultar nuevos archivos, puertos abiertos, procesos, etc.

Rootkits de librerias. Reemplazan las librerías del sistema, incluyendo distintas funciones que son utilizadas por otros programas cuando se ejecutan en el sistema infectado. De esta manera las funciones del troyano pueden afectar a distintos programas que se estén ejecutando en el sistema.

---

[232] Puerta trasera. Wikipedia. https://es.wikipedia.org/wiki/Puerta_trasera (Ú.a.:27/09/2015)
[233] Troyano. Wikipedia. https://es.wikipedia.org/wiki/Troyano_%28inform%C3%A1tica%29 (Ú.a.:27/09/2015)
[234] Rootkit. Wikipedia. https://es.wikipedia.org/wiki/Rootkit (Ú.a.:27/09/2015)

3.5 Eliminación de Evidencias

El trabajo de un atacante no concluye con la intrusión. De su sigilo depende la efectividad y pesistencia de sus acciones y la gravedad del daño que puede causar. Para ello el atacante intentara eliminar toda evidencia de su actividad, esto es, cualquier información que puede ser rastreada y analizada para interpretar en qué ha consistido un incidente de seguridad, qué daños ha provocado, cuáles son sus consecuencias y quién pudo ser el responsable. Para ello se emplean algunos de los siguientes métodos.

3.5.1. Edición de ficheros log[235].

Un fichero log de sistema, es un registro de las actividades que ocurren en un sistema informático. La información registrada incluye incidentes, funcionamientos anómalos, existencia de fallos en la configuración de las aplicaciones, desconexión de los dispositivos del sistema, cambios realizados en la configuración de los equipos, la utilización de recursos sensibles por parte de los usuarios del sistema, etc.

Más aún, los logs pueden mostrar actividades poco habituales en ciertos usuarios, como: intentos de acceder a la cuenta del super usuario, violar mecanismos de seguridad o indagar en lugares del sistema a los que no tienen acceso. Son una herramienta útil para mantener la seguridad del sistema pero también presentan una serie de características que entorpecen su uso: redundancia de información, falta de correlación en los eventos registrados, baja legibilidad y poca seguridad.

Los logs del sistema pueden ser leídos y modificados por otras aplicaciones, y el acceso a estos ficheros no esta restringido ni supervisado, por lo que son un blanco fácil de atacar, siendo copiados, borrados o modificados. Incluso cuando los log del sistema pueden registrar cuando alguien modifica su contenido, no puede indicar qué información fue modificada por lo que su información deja de ser útil y fiable.

3.5.2. Ocultación de información.

En el contexto de la seguridad informática, ocultar la información puede ser un acto que tiene por propósito reforzar la seguridad de un sistema informático, o bien una táctica usada por el atacante para pasar a través de los medios de seguridad sin ser detectado.

Existen métodos para ocultar la información en un medio digital, tales como las firmas digitales (fingerprinting), y las marcas de agua digitales (watermarking), las cuales a su vez están basadas en la esteganografía.

[235] Log (registro). Wikipedia. https://es.wikipedia.org/wiki/Log_%28registro%29 (Ú.a.:27/09/2015)

3.5.3. Esteganografía[236]

La esteganografía es una disciplina que trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

Es un error común confundir la esteganografía con la criptografía, o bien pensar que la primera es una rama de la segunda. Tienen objetivos distintos, aunque se complementan perfectamente para incrementar la seguridad. Con la criptografía se intenta cifrar o codificar un mensaje de modo que sea ininteligible si no se posee el decodificador adecuado, pero la existencia del mensaje es conocida. En tanto que la esteganografía intenta ocultar el hecho mismo del envío, escondiendo el mensaje, que no necesariamente estará encriptado, dentro del portador que lo oculta.

En la esteganografía digital tanto el mensaje como el portador es, en términos generales, un objeto software cualquiera. Aunque los medios portadores preferidos (por sus características) son archivos multimedia (imágenes, audio y vídeo). Los mensajes ocultos con técnicas de estegangrafía, muchas veces son encriptados previamente. StegHide es un software esteganográfico que soporta cifrado y compresión. Trabaja con archivos JPEG, BMP, WAV y AU y tiene licencia GNU.

[236] Esteganografía. Wikipedia. https://es.wikipedia.org/wiki/Esteganograf%C3%ADa#Software_de_esteganograf.C3.ADa (Ú.a.:27/09/2015)

4. Estrategias de ciberdefensa.

Antecedentes.

La creciente dependencia de la sociedad del ciberespacio, y su fácil accesibilidad, hacen que cada vez sean más comunes y preocupantes las intrusiones en este ámbito. Los ciberataques, en sus diversas modalidades de ciberterrorismo, ciberdelito, ciberespionaje o activismo en la red, se han convertido en un potente instrumento de agresión contra todos los estamentos de la sociedad. La ausencia de legislación armonizada y el diseño de internet favorecen que estas amenazas se materialicen, y explican que sea un objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios básicos, así como la gestión de las infraestructuras críticas.

En 2013 el Consejo de Seguridad Nacional promovió la creación de una Estrategia de Ciberseguridad Nacional[237], al amparo de la Estrategia de Seguridad Nacional aprobada por el Consejo de Ministros el 31 de mayo de 2013, que contempla la ciberseguridad como uno de sus ámbitos de actuación. Con este documento España se sitúa al nivel de otros países que han revisado sus estrategias de seguridad nacionales para avanzar el desarrollo de un segundo nivel específicamente en el ámbito de la ciberseguridad[238].

Estrategia de ciberseguridad nacional.

El propósito de la Estrategia de Ciberseguridad Nacional, es fijar las directrices generales del uso seguro del ciberespacio.

En su segundo capítulo se establecen los principios rectores que la inspiran y que están en sintonía con los de la Estrategia de Seguridad Nacional (unidad de acción; anticipación y prevención; eficiencia y sostenibilidad en el uso de los recursos; y resiliencia o capacidad de resistencia y recuperación).

Los principios rectores que se han establecido para esta estrategia, y siempre respetando los derechos fundamentales establecidos en la Constitución, son: el liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional.

[237] Presidencia del Gobierno. "Estrategia de Ciberseguridad Nacional". Madrid (2013). http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf (Ú.a.: 28/09/2015)
[238] Caro Bejarano, Mª José. "Estrategia de Ciberseguridad Nacional". Instituto Español de Estdios Estratégicos. 09/12/2013. http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf (Ú.a.: 28/09/2015)

En cuanto a sus objetivos se ha establecido uno global, garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques; y seis objetivos específicos:

Ámbito	**Objetivo**
Administraciones Públicas	Garantizar que los sistemas TIC utilizados posean el nivel adecuado de seguridad y resiliencia.
Empresas e infraestructuras críticas	Impulsar la seguridad y resiliencia de los sistemas TIC empleados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular.
Ámbito judicial y policial	Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
Sensibilización	Concienciar a los ciudadanos, profesionales, empresas y AA.PP. de los riesgos del ciberespacio.
Capacitación	Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad.
Colaboración internacional	Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

***Tabla 3**: Objetivos específicos de la Estrategia de Ciberseguridad Nacional.*

Estos objetivos se pretenden alcanzar mediante varias líneas de acción, como son: incrementar las capacidades de prevención, detección, respuesta y recuperación ante las ciberamenazas, incluyendo potenciar las capacidades militares y de inteligencia para ejercer una respuesta legítima y proporcionada en el ciberespacio; garantizar la implantación del Esquema Nacional de Seguridad, reforzando las capacidades de detección y mejorando la defensa de los sistemas clasificados; impulsar la implantación de la normativa de protección de Infraestructuras Críticas, ampliar las capacidades del CERT de Seguridad e Industria, e impulsar la participación del sector privado; potenciar la investigación y persecución del ciberterrorismo y la

ciberdelincuencia, fortaleciendo la cooperación policial internacional, fomentando la cooperación ciudadana y articulando los instrumentos de intercambio y transmisión de información de interés policial; impulsar la segurida y resiliencia de las TIC del sector privado; promover la capacitación de los profesonales e impulsar el sistema de I+D+i en materia de ciberseguridad, e impulsar las actividades de certificación de ciberseguridad y medidas de protección de productos, servicios y sistemas; concienciar a la sociedad y promover la cultura de la ciberseguridad y el uso responsable de las tecnologías y servicios de la Sociedad de la Información; promover un ciberespacio internacional seguro y confiable.

Comparativa de ciberseguridad en Europa.

La política de ciberseguridad europea está unida tanto a un marco de regulación internacional como nacional, y se interpreta en un contexto de estructuras de varios niveles[239]. Los dos documentos más importantes son la Estrategia de Ciberseguridad de la UE de 2013[240] y la Directiva de Seguridad de las Redes y de la Información (NIS), presentada a trámite por la Comisión COM (2013) 48 [241], aprobada por el Parlamento Europeo en febrero de 2014 y pendiente de su aprobación por el Consejo.

Estas políticas sobre ciberseguridad comenzaron a plantearse en 2000, a partir de la Comunicación conjunta del Consejo y la Comisión (COM/2000/890 final), y ha sido prioritaria en la agenda europea desde entonces. En 2004 se creó la Agencia Europea para la Seguridad de las Redes y la Información, ENISA[242] (European Network and Information Security Agency). Después, en 2006 se creó el Programa Europeo de Protección de las Infraestructuras Críticas (EPCIP). Y en 2009 el Consejo fijó su decisión de establecer una política de ciberseguridad común, 2009/C 321/01.

El Parlamento Europeo ha establecido una Agenda Digital Europea para 2020[243] (Digital Agenda for Europe 2020) que sirve como marco para una serie de iniciativas de la UE para el desarrollo de una estrategia, una sociedad y una economía digital comunes. Las iniciativas de la

[239] Wegener, Henning. "La ciberseguridad en la Unión Europea". Instituto Español de Estudios Estratégicos. 14/07/2014. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf (Ú.a.: 28/09/2015)
[240] JOIN (2013) 1final. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". European Comision. Brussels. 07/02/2013. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 (Ú.a.: 28/09/2015)
[241] COM (2013) 48. "Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión". NIS Directive. European Comision. Brussels. 07/02/2013. http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive (Ú.a.: 28/09/2015)
[242] ENISA. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/ (Ú.a.: 28/09/2015)
[243] Digital Agenda for Europe 2020. European Comision. Brussels.. http://ec.europa.eu/digital-agenda/en (Ú.a.: 28/09/2015)

Agenda Digital Europea para el desarrollo de una sociedad digital se estructuran en 7 líneas de actuación o pilares (Pillars): Mercado Único Digital; Interoperabilidad y estandarización; Confianza y seguridad; Acceso a internet rápido y ultrarápido; Investigación e innovación; Mejora en la alfabetización, capacitación e inclusión digitales; y Beneficios basados en las TIC para la sociedad europea.

Las estrategias en materia de ciberseguridad se enmarcan en el Pillar III, Confianza y seguridad[244], y se concretan a través de diferentes acciones e iniciativas, que comprenden: la creación de una red integrada de CERTs (Computer Emergency Response Team, o Equipo de Respuesta ante Emergencias Informáticas); la organización de simulacros de ciberincidentes que sirvan para establecer protocolos de actuación y planes de contingencia; el desarrollo de la política de Protección de Infraestructuras de Información Críticas (CIIP), que debe permitir proteger a la UE de ciberataques e interrupciones a gran escala, aumentando la preparación, seguridad y resiliencia de las infraestricturas TIC vitales; el desarrollo de Directivas sobre ciberseguridad para un marco legislativo común; la colaboración entre todos los agentes interesados; favorecer la información a través de la Agencia Europea de Seguridad de la Información y las Redes, ENISA, y un CERT de nivel europeo (CERT-EU); y, por último, promover la colaboración internacional, a través del Grupo de Trabajo sobre Ciberseguridad y Cibercrimen establecido entre la UE y los EE.UU., pero también a través de la OCDE, ONU, ITU (International Telecommunications Union), OSCE (organización para la Seguridad y Cooperación en Europa) o el IGF (Internet Governance Forum).

La mayoría de los gobiernos europeos son conscientes de la necesidad de desarrollar una política de ciberseguridad y resiliencia propia, complementaria a las políticas comunes, lo que constituye el punto fuerte de las políticas europeas, y las diferencia de las de otros estados más centrados en la disuasión y la construcción de una capacidad de ataque. Sin embargo existen considerables diferencias en estas políticas a nivel de estado, en el desarrollo de un marco legal y las capacidades operacionales, de forma que existe una brecha considerable entre los diferentes paises.

Los 27 estados miembros de la UE disponen de CERT nacionales, pero las funciones y experiencia de cada uno son muy dispares, y la integración presenta muchas dificultades, por lo que la aplicación de la Directiva de Seguridad de las Redes y de la Información (NIS) planteada por el Parlamento Europeo en el marco de la Agenda Digital Europea para 2020, supondrá un esfuerzo muy elevado. La cooperación de los CERT nacionales con el sector privado de cada

[244] Cybersecurity Strategy of the European Union. Pillar III. European Comision. Brussels. http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security (Ú.a.: 28/09/2015)

país sólo está contemplada en cinco países, sin que el resto disponga de una herramienta de apoyo a muchas de sus infraestucturas críticas.

El grupo de trabajo internacional BSA/The Software Alliance presentó a primeros de año un estudio comparativo sobre la situación en los estados miembros de la UE en materia de ciberseguridad, "EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace"[245]. En este estudio se analizan 25 aspectos concretos referentes a los procesos de gestión de la ciberseguridad y la resiliencia en cada país, organizados en cinco bloques:

- Existencia de un marco legal actualizado, comprensible y basado en una estrategia de ciberseguridad nacional sólida. Este marco legal debe estar construido atendiendo a los siguientes principios: debe basarse en la determinación y jerarquización de riesgos; ser tecnológicamente neutral; factible; flexible; y respetuoso con la privacidad y las libertades de los ciudadanos.

- Existencia de organismos nacionales encargados de la prevención y gestión de ciberincidentes, y específicamente la existencia de un CERT.

- Existencia de planes específicos en el sector de la ciberseguridad

- Existencia de políticas que favorezcan la confianza y la colaboración entre el sector público y el privado, así como con otros organismos internacionales, en materia de ciberseguridad.

- Existencia de campañas de fomento de la educación y la concienciación sobre riesgos y ciberseguridad en materia de tecnlogías de la información.

El siguiente cuadro muestra el resultado del estudio, que ofrece una instantánea bastante nítida del desarrollo de las estrategias en ciberdefensa de todos los estados miembros de la UE a fecha 1 de enero de 2015[246].

[245] BSA/The Software Alliance (2015). "EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace". http://cybersecurity.bsa.org/index.html (Ú.a.: 28/09/2015)
[246] BSA/The Software Alliance. "EU Cybersecurity Dashboard. Countries". http://cybersecurity.bsa.org/countries.html (Ú.a.: 28/09/2015)

✔ Yes ✖ No ◑ Partial

#	QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
	LEGAL FOUNDATIONS																												
1.	Is there a national cybersecurity strategy in place?	✔	✔	✖	✖	✔	✔	✖	✔	✔	✔	✔	✖	✔	✖	✔	✔	✔	✔	✖	✔	✔	Draft	✔	✔	✖	✔	✖	✔
2.	What year was the national cybersecurity strategy adopted?	2013	2012	–	–	2013	2011	–	2014	2013	2011	2011	–	2013	–	2014	2014	2011	2013	–	2013	2013	–	2013	2008	–	2013	–	2011
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✖	✔	✔	◑	✖	✔	✖	◑	✖	◑	✔	✔	✖	✔	✔	✔	✔	✔	✔
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	✖	✖	✖	✖	✔	◑	✔	◑	✖	✖	◑	✔	✖	✖	✖	✖	✖	◑	◑	✖	✖	✖	◑	✖	✖	✔	◑
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	✖	✖	✖	✖	◑	✖	✔	✔	✖	Draft	✖	✖	✖	✖	✔	◑	◑	◑	◑	✖	◑	✖	✖	◑	◑	✖	✖
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	✖	✖	◑	✖	✔	✖	✔	✔	✖	Draft	✖	✔	✖	✔	✖	◑	✖	✖	✔	✖	◑	✖	◑	✖	✖	✖	◑
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	◑	✖	✖	✔	✔	✖	✔	✖	✖	✔	✖	✖	✖	✖	✔	✔	✖	✔	✖	✔	✖	◑	✖	✔	✖	✖	✖
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	✔	✔	✖	✖	✔	✔	✔	✔	✖	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	◑	N/A	N/A	N/A	◑	✔	✔	✔	◑	✔	✔	✔	N/A	✔	◑	◑	◑	N/A	✔	◑	N/A	◑	✖	N/A	✔	✔	◑
	OPERATIONAL ENTITIES																												
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2.	What year was the computer emergency response team (CERT) established?	2008	2008	2008	2009	–	2011	2009	2008	2014	2008	2012	2009	2013	–	2014	2006	2006	2011	2002	2012	2008	2008	2011	2009	2010	2008	2003	2014
3.	Is there a national competent authority for network and information security (NIS)?	◑	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
5.	Are national cybersecurity exercises conducted?	✔	✔	✔	◑	◑	◑	✔	✔	✔	✔	✔	✔	◑	✔	✔	✔	◑	◑	◑	✔	◑	◑	◑	✔	◑	◑	✔	✔
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	✖	◑	✖	✖	✔	◑	◑	✖	✖	✖	✖	✔	✖	✔	✔	◑	◑	✖	✔	✔	◑	◑	✖	✖	✔	◑	✔
	PUBLIC PRIVATE PARTNERSHIPS																												
1.	Is there a defined public private partnership (PPP) for cybersecurity?	✔	◑	◑	◑	◑	✖	✖	◑	◑	✖	✔	✖	◑	✖	◑	✖	✖	✖	◑	✔	✖	◑	✖	✖	✖	✔	◑	✔
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	✔	◑	✖	✖	✖	✔	◑	✔	✖	✔	✖	◑	✔	◑	✖	◑	✖	✖	✔	◑	✖	◑	◑	◑	✔	◑	✔
3.	Are new public private partnerships in planning or underway (if so, which focus area)?	✔	–	✖	✖	✖	◑	✖	✖	✖	◑	✔	✖	✖	✖	◑	◑	◑	◑	✖	–	✖	✖	✔	✖	✖	–	✖	–
	SECTOR SPECIFIC CYBERSECURITY PLANS																												
1.	Is there a joint public private sector plan that addresses cybersecurity?	✔	✖	✖	◑	◑	✖	✖	✖	◑	✔	✖	✖	◑	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✔
2.	Have sector specific security priorities been defined?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	◑
3.	Have any sector cybersecurity risk assessments been conducted?	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
	EDUCATION																												
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✔	◑	✖	✔	◑	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✖	✔	✖	✔

***Figura 49**: Estrategias de seguridad de los estados miembros de la UE. (Fuente: BSA/The Software Alliance (2015). "EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace". http://cybersecurity.bsa.org/index.html Ú.a.: 28/09/2015)*

Estado de la ciberseguridad de otros agentes internacionales.

La siguiente información se ha extractado del informe "Ciber-Resiliencia. Aproximación a un Marco de Medición", elaborado por el INTECO, Instituto Nacional de Tecnologías de la Información[247] (actualmente INCIBE).

Fuera de Europa son pocos los estados que han adoptado una estrategia nacional de ciberseguridad y un marco normativo: Australia, Canadá, China, Corea del Sur, EE.UU., India, Israel, Japón, Nueva Zelanda, Singapur, Sudáfrica y Turquía. Algunas de ellas, como las de Israel o China son secretas, aunque han trascendido algunas de las medidas que se han adoptado en el marco de sus respectivas estrategias. Rusia no parece estar interesada en desarrollar un marco legal para la ciberseguridad. En Latinoamérica comienzan a darse los primeros pasos en materia de ciberseguridad.

Canadá

Se presta especial importancia a la protección de las infraestructuras críticas, pero todo el concepto de ciberseguridad se enmarca bajo la visión global de resiliencia. Para Canadá es muy importante la colaboración Público-Privada, desde que se tiene constancia de que los riesgos y amenazas de los ciberataques tienen como objetivo a los sectores público y privado. Se promueven y apoyan a nivel estatal las iniciativas para mejorar la ciberresiliencia, incluyendo las de las infraestructuras críticas. Además también se implica la Administración en difundir el conocimiento necesario entre sus ciudadanos, para mejorar su propia protección.

Sin embargo, como en muchos otros casos, no se establece o se promueve un sistema coordinado y conjunto de gobernanza o apoyo a las métricas e indicadores para realizar una evaluación y seguimiento del estado de la ciberseguridad.

EE.UU.

Es unos de los países más avanzados en la definición y establecimiento de una Estrategia de Ciberseguridad[248] en todos los aspectos. Su visión global de la Ciberseguridad desemboca en

[247] Héctor R.Suárez; Juan D. Peláez Álvarez. "Ciber-Resiliencia. Aproximación a un Marco de Medición". INTECO. Mayo, 2014. https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf (Ú.a.:28/09/2015)

una división de responsabilidades de protección entre distintos organismos, por ejemplo, la división funcional y operativa entre NSA (National Security Agency), DHS (Department of Homeland Security), NIST (National Institute of Standards and Technology), CIS (Center for Internet Security), CCS (Council on CyberSecurity) y GHSAC (Governors Homeland Security Advisors Council). Sin embargo la estrategia propone un sistema nacional que mejore la ciberresiliencia a nivel nacional e internacional, mediante mecanismos de vigilancia y respuesta. Para ello se basa en reforzar el uso de estándares interoperables y seguros, y en la colaboración Público-Privada e interestatal, que así mismo sean eje para reforzar la seguridad de las infraestructuras críticas nacionales. Se plantea también una gobernanza de internet que sirva a las necesidades de todos los usuarios, y para ello realizan iniciativas mediante su CSIRT de nivel nacional para compartir información entre entidades públicas, sectores clave, IICC y otros organismos concernidos. Por ello se enfatiza que para asegurar la resiliencia de las redes y sistemas de información se requiere de acciones coordinadas y conjuntas a nivel nacional que abarquen la totalidad de la Administración, en colaboración con el sector privado y los ciudadanos.

Aunque se efectúa un acercamiento general, como en otros casos, no se establece o se promueve un sistema coordinado y conjunto de métricas e indicadores para realizar evaluación y seguimiento del estado de la Ciberseguridad.

Japón

En el caso japonés se presta especial atención a la protección de la información crítica, de los sistemas que las soportan, siendo los objetivos de dicha protección el identificar y asegurar dicha información crítica, y evitar riesgos a través de la innovación tecnológica. Para ello establecen claramente roles y responsabilidades entre Administración y sector privado, implicando a las empresas, instituciones educativas y centros de investigación, incluso en alguna iniciativa concreta. Por otra parte enfatizan las consecuencias, tanto económicas como personales con objeto de concienciar a todos los actores.

Estado actual de la ciberseguridad en España.

En el informe de actividad 2013-2014 emitido por el CCN a finales de agosto de 2015[249] se presentan los resultados del Informe sobre el Estado de la Seguridad (INES) obtenidos en ese

[248] Departement of Defense. "The Department of Defense Cyber Strategy". Abril, 2015. Washington. EE.UU. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Ú.a.: 28/09/2015)
[249] CCN-CERT. "Informe de Actividades 2013-2014". Centro Criptológico Nacional. https://www.ccn-cert.cni.es/documentos-publicos/1069-informe-actividad-ccn-2013-2014-enfrentadas/file.html (Ú.a.:28/09/2015)

periodo 2013-2014 a partir de la información recopilada a través de los formularios de la aplicación INES, descritos en la Guía CCN-STIC-824[250].

Por otro lado, la Guía CCN-STIC-817[251], "Esquema Nacional de Seguridad. Gestión de Ciberincidentes", describe con detalle cómo, a partir de la Estrategia de Ciberseguridad Nacional y en el marco del ENS, se han implementado los organismos y procedimientos para la gestión de ciberincidentes (que se describen en el punto siguiente), apoyándose en la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas), para poner en contacto a todos los organismos y actores concernidos en la gestión del ciberincidente.

Ambos documentos ofrecen una imagen del estado de la ciberseguridad en España, en lo que se refiere a la caracterización de los ciberincidentes tratados, y al marco normativo, organismos, procedimientos y recursos implementados para su gestión.

Ciberincidentes.

En el año 2014, el CCN-CERT, gestionó un total de 12.916 incidentes en las AA.PP. y en empresas de interés estratégico, de los cuales 132 fueron catalogados como críticos, una cifra que representa un incremento del 78% con respecto al año 2013, que ya se aumentó a su vez más del 150% con relación al 2012. Además, el número de incidentes con una *peligrosidad crítica* ascendió casi un 250%.

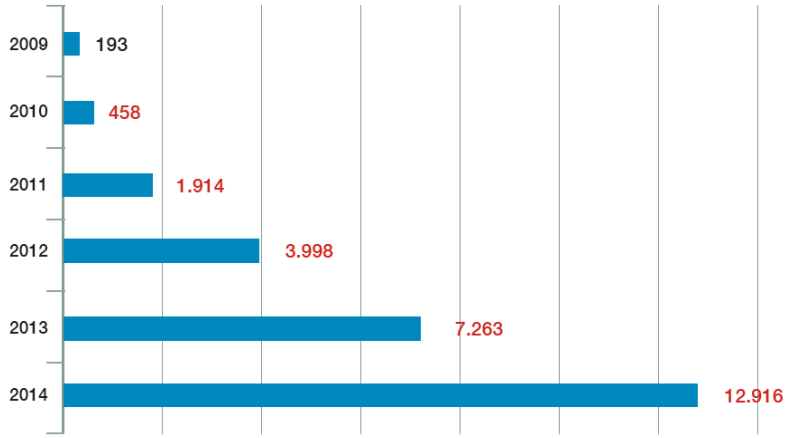

***Figura 50**: Ciberincidentes en España. (Fuente: CCN-CERT-IA-09/15. https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf Ú.a.:28/09/2015)*

[250] CCN-CERT. Guía CCN-STIC-824. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/542-ccn-stic-824-informaci%C3%B3n-del-estado-de-seguridad/file.html (Ú.a.:28/09/2015)

[251] CCN-CERT. Guía CCN-STIC-817. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html (Ú.a.:28/09/2015)

Atacantes y métodos utilizados.

Entre los atacantes, y según se indca en el informe de actividad, siguen destacando, por orden de importancia: las agencias de inteligencia y las unidades de ciberdefensa de las fuerzas armadas de diferentes países, la ciberdelincuencia, el hacktivismo y en menor medida los grupos terroristas y otros actores.

En España ha decaído la presencia hacktivista de grupos locales, manteniéndose 'La 9ª Compañía' como único referente operativo. En cambio, se ha observado un incremento leve de ataques de entidades hacktvistas marroquíes contra páginas web.

En cuanto a las herramientas y los métodos utilizados, el informe indica que se trata de ataques a todo tipo de dispositivos, pero con especial incremento en los móviles, y utilizando con preferencia técnicas de ingeniería social a través de las redes sociales, preferentemente spear-phishing, así como ataques contra servicios web o incidentes con ransomware, más agresivo que otros años y con especial incidencia en España. El malware en general se ha vuelto más complejo, se ha incrementado su número (alcanzando los 25 millones de muestras), se adapta y muta. De todo este código, la mayor parte corresponde a troyanos.

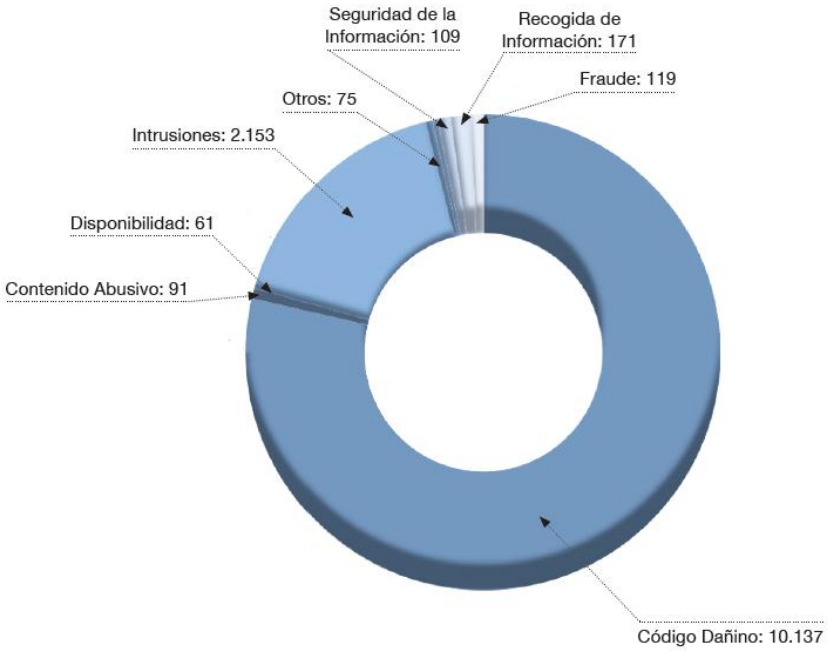

***Figura 51**: Categorías de incidentes gestionados en España. (Fuente: CCN-CERT-IA-09/15. https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf Ú.a.:28/09/2015)*

Incidentes que tienen su origen todos ellos en la falta de concienciación del usuario, la escasa vigilancia del tráfico de red y la protección inadecuada.

Según el informe del CCN estas amenazas, originariamente dirigidas a empresas e instituciones públicas, actúan también sobre personas individuales, incluyendo altos directivos de compañías y de organismos públicos, personajes notorios y responsables políticos. Entre las conclusiones del informe se indica que se observa, además, una tendencia a atacar a los elementos más débiles que formen parte de la *cadena de intercambio de datos* (por ejemplo, contratistas, proveedores, etc.), antes que hacerlo directamente contra los objetivos finales, que han mejorado significativamente sus estrategias y capacidades defensivas.

Atendiendo al perfil de las víctimas, en el sector público se ha experimentado un incremento significativo de incidentes de gravedad crítica relacionados con el ciberespionaje, y también incidentes de gravedad media y gravedad alta relacionados con el ciberdelito, en particular la sustracción de documentación y la interrupción de sistemas, respectivamente.

El sector privado ha sufrido un mayor incremento de incidentes relacionados con el ciberdelito y en menor medida por el hacktivismo, en concreto se produjeron incidentes relativos a la sustracción y manipulación de información, y la interrupción o toma de sistemas. También se produjo una alta incidencia de casos de ciberespionaje.

Por último, entre los ciudadanos y particulares, se ha experimentado un incremento significativo de incidentes de gravedad alta relacionados con el ciberdelito relativos a la sustracción y manipulación de información, y la interrupción o toma de sistemas.

Las organizaciones, por tanto, se enfrentan a un nuevo paradigma en el tratamiento de las amenazas contra los sistemas de información, que pasa por poner más énfasis en la detección de los ataques que en su prevención, en depender más de la cualificación de las personas, complementado con la tecnología, y en invertir suficientemente en estos campos de forma continuada. Concluye el informe resaltando la importancia de la confianza y el intercambio de información, tanto en el ámbito público como privado, con los Equipos de Respuesta encargados de la gestión de la ciberseguridad, CNI (Centro Nacional de Inteligencia), CCN[252] (Centro Criptológico Nacional), CCN-CERT[253] (Equipo de Respuesta ante Emergencias Informáticas del CCN), CERTSI[254] (CERT del Ministerio de Industria), INCIBE[255] (Instituto Nacional de Ciberseguridad) y CNPIC[256] (Centro Nacional para la Protección de las Infraestructuras Críticas).

[252] CCN. Centro Criptológio Nacional. https://www.ccn.cni.es/ (Ú.a.:28/09/2015)
[253] CCN-CERT. https://www.ccn-cert.cni.es/ (Ú.a.:28/09/2015)
[254] CERTSI. https://www.incibe.es/CERT/Infraestructuras_Criticas/ (Ú.a.:28/09/2015)
[255] INCIBE. Instituto Nacional de Ciberseguridad. https://www.incibe.es/home/instituto_nacional_ciberseguridad/ (Ú.a.:28/09/2015)
[256] CNPIC. http://www.cnpic.es/ (Ú.a.:28/09/2015)

5. El Esquema Nacional de Seguridad.

Antecedentes.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECS)[257], reconocía el derecho de los ciudadanos a relacionarse con las AA.PP. por medios electrónicos y regulaba aspectos básicos del uso de las TIC en las relaciones de las administraciones con los ciudadanos y empresas, así como de su propio funcionamiento interno, estableciendo la necesidad de asegurar la disponibilidad, el acceso, la integridad, autenticidad, confidencialidad y conservación de la información.

La LAECS, en su artículo 42, contemplaba la creación del denominado Esquema Nacional de Seguridad (ENS), como instrumento para asegurar las condiciones de confianza necesarias para el uso de los medios TIC, por medio de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las AA.PP, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Su creación se reguló a través del Real Decreto 3/2010, de 8 de enero. La implantación está siendo más lenta de lo previsto, aunque el ENS exige de las AA.PP. que inicien un proceso de adecuación de los servicios prestados a través de internet en el ámbito de la Administración Electrónica, para el cumplimiento de las medidas de seguridad previstas en su articulado. Aún así el desarrollo que ha experimentado el sector público desde su aprobación ha sido significativo, y, sitúa a España a la cabeza de los países europeos en desarrollo digital en este sector, según el DESI (Digital Economy and Society Index) de 2015[258].

El ENS pretende establecer *elementos comunes relativos a la seguridad* en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, al objeto de crear las condiciones necesarias para la confianza en el uso de los citados medios electrónicos que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En los artículos 36 y 37 del RD 3/2010, se señala que el Centro Criptológico Nacional (CCN) estará encargado de articular la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Response Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que

[257] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352 (Ú.a.:28/09/2015)
[258] Digital Public Service DESI 2015 for Spain. Digital Agenda for Europe. http://ec.europa.eu/digital-agenda/en/scoreboard/spain#5-digital-public-services (Ú.a.:28/09/2015)

pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Por su parte, la Estrategia de Ciberseguridad Nacional confiere al CCN-CERT un papel central en el desarrollo de su Línea de Acción 2: Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas, como actor imprescindible en la garantía de la plena implantación del ENS, mediante el refuerzo de las capacidades de inteligencia, detección, análisis y respuesta del CCN-CERT y de sus Sistemas de Detección y Alerta Temprana.

Le corresponde también al CCN la elaboración de las Guías de Seguridad CCN-STIC para mejor cumplimiento del ENS, de acuerdo al artículo 29 del RD 3/2010.

Las acciones de formación, en colaboración con el INAP, Instituto Nacional de Administración Pública, están previstas en la disposición adicional primer del RD 3/2010.

Todo ello convierte al ENS en una herramienta útil para poner en funcionamiento los principos básicos y requisitos mínimos para una protección adecuada de la información, que es su objeto, tal como se expresa en su artículo 1.

Estructura, contenido y objetivos del ENS.

El Esquema Nacional de Seguridad se estructura en 10 capítulos y 44 artículos, a lo largo de los cuales se determinan las obligaciones básicas que deben cumplir todas las Administraciones Públicas en materia de seguridad de la información. Siguen varias disposiciones adicionales y transitorias, y cinco anexos.

El primero desarrolla la meodologías de categorización de los sistemas, estableciendo sus niveles, y analiza cada una de las dimensiones de seguridad que establece el propio ENS.

- Disponibilidad [D].
- Autenticidad [A].
- Integridad [I].
- Confidencialidad [C].
- Trazabilidad [T].

El segundo anexo recoge el catálogo de medidas a aplicar en función de la categoría establecida para cada sistema, y que están divididas en tres grupos.

- Marco organizativo [org].

- Marco operacional [op].
- Marco de protección [mp].

Sus objetivos principales son los siguientes:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.
- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- Facilitar un tratamiento continuado de la seguridad.

En su articulado el ENS establece una serie de actuaciones a las AA.PP. y sectores críticos, entre ellas la creación de las Políticas de Seguridad internas de cada organización. Para implementarlas el ENS fija una metodología basada en el estudio de riesgos, y propone el uso de la Herramienta PILAR. De la determinación de los riesgos a los que están expuestos los sistemas y su información, se obtendrá la categorización del sistema y serán de aplicación las medidas que figuran en el ENS, que deberán ser desarrolladas por personal cualificado encargado de la gestión de la segurida de los sistemas (CISO).

Para ello en paralelo el ENS prevé la emisión de las Guías STIC y herramientas por parte del CCN, que desarrollará su capacidad de respuesta a través del CCN-CERT.

Los organismos deberán elborar en el marco de sus Políticas de Seguridad un Plan de Respuesta a Ciberincidentes, junto a los Procedimientos de Respuesta. En estas tareas se coordinaran con

el CCN-CERT, informando de los incidentes, y la evolución de su estado hasta su completa resolución (el ciclo de vida de rspuesta al ciberincidente se detalla en la Guía CCN-STIC-403). Para realizar esta comunicación el CCN facilita la herramienta LUCIA.

Por último los responsables de seguridad de los sistemas TIC tienen la obligación de adecuar sus sistemas al ENS y a su marco legal, que comprende la siguiente normativa:

- Estrategia de Ciberseguridad Nacional
- Ley 15/1999, de 13 de diciembre, LOPD[259]
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Esquema Nacional de Interoperabilidad
- Esquema nacional de Seguridad y normativa derivada
- Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

Metodologías y herramientas.

Las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones.

El art. 29 del ENS señala la utilidad de las Guías CCN-STIC. En concreto, dice: *"Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones."*

No se trata, por tanto, de normas imperativas, sino de la expresión de metodologías y recomendaciones para el adecuado cumplimiento de lo dispuesto en el ENS. Recomendaciones que tendrán especial significación para aquel organismo administrativo afectado por un incidente grave de seguridad, motivado por la inobservancia de las recomendaciones descritas.

MAGERIT v.3. Metodología de Gestión de Riesgos en las Tecnologías de la Información.

Podemos afirmar que el Análisis y la Gestión de Riesgos son la base de la Seguridad TIC. Las Directrices de seguridad de la OCDE, las normas internacionales ISO/IEC 27001/27002, las

[259] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE. http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750 (Ú.a.:28/09/2015)

normas NIST, etc., todas ellas sustentan su aplicación a un preceptivo análisis y ulterior gestión de riesgos.

Para obtener una información más completa de las prácticas europeas habituales en Gestión de Riesgos, puede consultarse la página web de ENISA[260].
Por este motivo, el art. 6 del ENS señala como obligatorio, para todos los sistemas afectados por el ENS, el desarrollo de un Análisis de Riesgos, al que deberá seguir el correspondiente proceso de Gestión de Riesgos (art. 13).

Realizar un Análisis y Gestión de Riesgos no es, por tanto, una medida opcional: es una exigencia de obligado cumplimiento.

El CCN propone y facilita MAGERIT, en su versión 3, asociada a la herramienta PILAR para realizar la evaluación obligatoria de riesgos de los sistemas de información.

También proporciona varias herramientas gratuitas para ayudar en la implementación del ENS, dar soporte a la transmisión de información entre las partes y ayudar a los responsables de seguridad a cumplr sus cometidos de forma estructurada y sistemática.

PILAR 5.4.1. Versión pública de la herramienta de Análisis de Riesgos PILAR.

Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si estimamos la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema.

Degradación y frecuencia califican la vulnerabilidad del sistema. El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.

PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

• ISO/IEC 27002 (2005, 2013)- Código de buenas prácticas para la Gestión de la Seguridad de la Información

• ENS - Esquema Nacional de Seguridad Más información sobre Magerit (3.0).

CLARA (Customized Local And Remote Analisys tool).

[260] ENISA. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/ (Ú.a.:28/09/2015)

CLARA es una herramienta para cumplimiento del ENS, permite verificar la aplicación de las plantillas de seguridad de las guías 850A, 850B, 851A y 851B.

La herramienta constituye un mecanismo para analizar las características de seguridad técnicas definidas a través del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. El análisis del cumplimiento está basado en las normas de seguridad que han sido proporcionadas a través de la aplicación de plantillas de seguridad, según las guías CCN-STIC de la serie 800: 850A, 850B, 851A y 851B.

Se tiene en consideración que los ámbitos de aplicación de este tipo de plantillas son muy variados y por lo tanto dependerán de su aplicación las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS. No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas habrán podido ser modificadas para adaptarlas a sus necesidades operativas.La herramienta para el análisis de cumplimiento es funcional exclusivamente en sistemas Windows

INES. Informe Nacional del Estado de la Seguridad.

El Esquema Nacional de Seguridad (ENS) establece la obligación de evaluar regularmente el estado de la seguridad de los sistemas por parte de las Administraciones Públicas. Su artículo 35 señala: "*El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente R.D., de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones Públicas*".

Asimismo, el ENS dispone la necesidad de establecer un sistema de medición de la seguridad del sistema, estableciendo un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

1. Grado de implantación de las medidas de seguridad.
2. Eficacia y eficiencia de las medidas de seguridad.
3. Impacto de los incidentes de seguridad.

Para cumplir con este mandato, el CCN ha desarrollado el proyecto INES (Informe Nacional del Estado de Seguridad). Este proyecto cuenta con una nueva plataforma que proporciona a las distintas Administraciones Públicas un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas.

Esta plataforma permite la recogida de información organizada, delegada y supervisada. El Responsable de la Seguridad aparece como el encargado de la interfaz con INES, proporcionando, validando y analizando la información de seguridad propia de su organismo y consolidada a nivel de Administración Pública.

Otra de las características de INES es la posibilidad de que cada organismo acceda, complete o consulte sólo sus datos que se clasificarán por años, para ver su evolución. Con el proyecto INES, al igual que con la Guía CCN-STIC 824 Informe del Estado de Seguridad se busca una estimación preventiva de la seguridad, vía análisis del cumplimiento de determinados aspectos que se han estimado críticos para cualquier organismo, una estimación de la eficacia y eficiencia de las actividades en materia de seguridad y una estimación del esfuerzo humano y económico dedicado a seguridad TI.

LUCIA. Herramienta de Gestión de Incidentes.

LUCIA, Listado Unificado de Coordinación de Incidentes y Amenazas, es el proyecto de implantación de la nueva herramienta de gestión de incidentes de seguridad del CCN-CERT, basada en el sistema de incidencias Request Tracker (RT) y en su extensión para equipos de respuesta a incidentes Request Tracker for Incident Response (RT-IR). Dichas herramientas han sido personalizadas para cumplir los requerimientos y procedimientos del CCN-CERT y alineadas con el cumplimiento del ENS.

Una de las mejoras más importantes que incorpora LUCIA es la posibilidad de interacción entre sistemas de gestión de incidentes, pudiendo llegar a crear una federación de sistemas, en la que el sistema del CCN-CERT establecería un canal con cada uno de los sistemas independientes, y a través de esté enlace seguro, se transmitirían incidentes de seguridad de los organismo adscritos al SAT o la metainformación de los incidentes entre las distintas organizaciones y el CCN-CERT (depende de la participación en el proyecto), facilitando por tanto la coordinación, intercambio y resolución de los incidentes de seguridad.

Aunque las incidencias de SAT-INET y SAT-SARA se podrán seguir gestionando por parte de los organismos adheridos, en su forma tradicional, es decir, accediendo a la herramienta, LUCIA proporcionará una nueva forma de atenderlas, para aquellos organismos que la desplieguen, debido a que la herramienta del CCN-CERT y la herramienta local del organismo se sincronizarán y compartirán la información del evento, ya no habrá necesidad de acceso al sistema central, sino que los organismos podrán realizar todas las operaciones de actualización sobre el sistema local.

Los beneficios directos que los organismos adscritos al proyecto podrán obtener son:

- Una herramienta de gestión de incidentes en el caso de que no dispongan ninguna o necesiten una específica.
- Cumplir los requisitos del Esquema Nacional de Seguridad (ENS) y la guía CCN-STIC 817 (Gestión de incidentes en el ENS),
- Ofrecer un lenguaje común de peligrosidad y clasificación del incidente en consonancia con las guías CCN-STIC 403 y CCN-STIC 817 basado en dos niveles y avalado por instituciones internacionales.
- Mejorar la coordinación entre el CCN-CERT y todos los organismos a los que ofrece sus servicios mediante la Integración de los incidentes de seguridad con el CCN-CERT.
- Mejorar el intercambio de información de incidentes de seguridad.
- Mantener la trazabilidad y seguimiento del incidente
- Mejora en los procesos de gestión
- Automatizar tareas y permitir su integración con otros sistemas
- Categorización del cierre y causas del incidente
- Construir bases de datos de conocimiento
- Mejora de gestión de los proyectos SAT-SARA y SAT-INET

LUCIA se basa en un sistema de software libre que no acarrea ningún coste de licencias por parte del organismo adscrito.

El sistema se encuentra virtualizado mediante VMware (compatible con KVM [http://www.linux-kvm.org]) y configurado sobre una plataforma linux Centos de 64 bits (en su versión 7 actualmente) por lo que su compatibilidad se encuentra asegurada para cualquier plataforma que disponga de un mínimo de 2 núcleos de procesador (no necesariamente 2 procesadores físicos), 4 GB de memoria y 200 Gb de disco duro. Al ser una máquina virtual los recursos pueden ampliarse según la plataforma a utilizar.

La comunicación entre sistemas LUCIA se realiza mediante comunicación HTTPS/REST/SOAP en un canal cifrado y autenticado.

Se distribuye una máquina virtual preconfigurada a los organismos federados para su sistema local.

Las actualizaciones de seguridad y cambio de versiones correrán a cargo del CCN-CERT, el cual enviará periódicamente a los organismos para su implementación. En el caso de personalizaciones concretas para ampliar o adaptar los servicios internos serán responsabilidad del organismo existiendo el buzón lucia@ccn-cert.cni.es para dirigir las dudas y consultas.

CARMEN 3.0. (Centro de Análisis de Registros y Minería de EveNtos).

CARMEN, Centro de Análisis de Registros y Minería de EveNtos, es un desarrollo del Centro Criptológico Nacional y la empresa S2Grupo para la identificación del compromiso por parte de amenazas persistentes avanzadas (APT), constituyendo la primera capacidad española, basada en conocimiento y tecnología nacionales, en este sentido.

CARMEN es una herramienta de adquisición, procesamiento y análisis de información para la generación de inteligencia principalmente a partir de los tráficos de una red. Se compone de agentes que recopilan los flujos de tráfico (elementos de adquisición), un motor de base de datos en el que se inserta la información y una aplicación web que permite la representación y consulta de la información obtenida, para que un analista trabaje con ella y tome decisiones a partir de los resultados proporcionados por la herramienta.

Los orígenes de datos que actualmente soporta CARMEN son:

- HTTP, tanto a partir de un proxy, como de forma pasiva.
- DNS, de forma pasiva.
- SMTP, de forma pasiva.
- IPC, de forma pasiva.

Sobre cada una de las fuentes de datos, CARMEN permite la aplicación de reglas predefinidas para la detección de usos indebidos y, especialmente, para la detección de anomalías significativas (estadísticas, cadenas de texto, series temporales y basadas en conocimiento) que puedan ser indicativas de un compromiso en la organización, así como la definición e integración de nuevo conocimiento en la herramienta, desde IOC hasta condiciones de anomalía. CARMEN está orientada a la identificación de movimientos externos (servidores de C&C y servidores de exfiltración) y movimientos laterales de una amenaza persistente avanzada. Las capacidades de adquisición y análisis de la herramienta permiten cubrir las principales vías de comunicación de estas amenazas con el exterior (navegación web, consultas DNS y correo electrónico) así como diferentes mecanismos de comunicación interna en la red comprometida. Adicionalmente a la etapa de persistencia, CARMEN aporta capacidades para la detección de la amenaza en su etapa de intrusión, principalmente condiciones de anomalía para la detección de mecanismos habituales de entrada, como watering hole o exploit kits, así como despliegue e integración de capacidades de sandboxing para la detección de spear phishing.

MARTA (Motor de Análisis Remoto de Troyanos Avanzados).

Herramienta de análisis de código dañino (en desarrollo)[261].

[261] GlobbTV. "InnoTec System colabora con el Centro Criptológico Nacional en la contención de ciberataques". http://www.globbtv.com/4383/noticias/innotec-system-colabora-con-el-centro-criptologico-nacional-en-la-contencion-de-ciberataques (Ú.a.:28/09/2015)

6. Consideraciones finales.

La OTAN, atendiendo a la calificación referente a conflictos y ciberconflictos establecida por la legislación internacional, no reconoce que los ciberincidentes puedan se rclasificados como actos de guerra. No obstante la amenaza es real, es un factor de inestabilidad, sucede instantáneamente, es global, y evita el campo de batalla, pero las consecuencias son potencial e igualmente devastadoras.

Prepararse para la ciberguerra, tanto en los aspectos de prevención, defensa y resiliencia como en las vertientes de disuasión, capacidad de ataque y respuesta táctica, es una estrategia ineludible para cualquier estado.

Por otro lado los avances tecnológicos permiten la intrusión en redes y dispositivos, la recogida de datos y su almacenamiento y análisis como nunca antes había sido posible. No se puede negar la oportunidad que representa para la defensa de una nación. Con toda certeza es un camino que adoptarán todas las naciones en un futuro próximo y cambiará las sociedades, obligando a establecer un nuevo balance entre seguridad y libertad.

El concepto de privacidad, tal como lo hemos conocido, está próximo a evolucionar, y es difícil que las leyes puedan contener una realidad tecnológica que se impone al ritmo que aceptamos nuevos servicios más interconectados. Si hasta la fecha podía pensarse que la privacidad se extendía, como enuncian las leyes, más allá de la individualidad biológica, hasta la diversidad de datos generados por una persona, y con independencia de dónde éstos estuvieran alojados, siendo un derecho fundamental de cada individuo el poder accederlos, modificarlos o cancelarlos a voluntad, hemos de asumir que una parte importante de ese extensión quedará excluida del concepto de privacidad.

Durante la elaboración de este PFC el CERT del CCN ha publicado varios informes y nuevas guías de seguridad, entre ellas, por ejemplo, la Guía CCN-STIC 817, titulada “ESQUEMA NACIONAL DE SEGURIDAD. GESTIÓN DE CIBERINCIDENTES”. En esta guía, muy centrada en la utilización de la Herramienta LUCIA, se desarollan los pasos que deben seguir los organismos de las AA.PP. en coordinación con el propio CCN, implantar el ENS y adecuarse al marco legal, crear sus propias Políticas de Seguridad, y dotarse de equipos de respuesta para gestionar adecuadamente los ciberincidentes que se produzcan con los sistemas informáticos del organismo.

En este mismo documento se intentan tipificar los ciberincidentes, en base a varios criterios, y se establece una categorización por su gravedad, utilizando varias aproximaciones para establecer una métrica. Esta métrica sería la base para implantar una estrategia de resiliencia.

Se hace mención también del desarrollo de herramientas automatizadas de red o de servidor IDS/IPS (Intrusion Detection Systems e Intrusion Prevention Systems), para la detección de ciberincidentes a partir del análisis de antivirus, la inspección de logs y la detección de indicios de actividad anormal.

Sería interesante poder proponer a los alumnos de la titulación la realización de próximos PFCs que desarrollen estos aspectos.

Bibliografía

- Aguilar Alcacer, Jordi; Oltra Gutiérrez, Juan Vicente (2007). "Phishing, vectores de ataque y técnicas de defensa". FI, UPV. Valencia.
- Caro Bejarano, Mª José (2013). "Estrategia de ciberseguridad nacional". Instituto Español de Estudios Estratégicos. Madrid.
- Carr, Jeffrey (2011). "Inside Cyber Warfare, 2nd Edition. Mapping the Cyber Underworld". O'Reilly Media. Sebastopol, CA. EE.UU.
- CCN-CERT (2015). "Ciberamenazas 2014. Tendencias 2015. Resumen ejecutivo". CERT del Cento Criptológico Nacional. Madrid.
- Clarke, Richard A.; Knake, Robert K. (2011). "Guerra en la red. Los nuevos campos de batalla". Planeta. Barcelona.
- Crespo Lorente, Rubén; Oltra Gutiérrez, Juan Vicente (2006). "Clasificación del movimiento hacker y sus implicaciones sociales y mediáticas: impacto en España". ETSIA, UPV. Valencia.
- Erickson Jon (2003). "Hacking: the art of exploitation". Wo Starch Press. San Francisco, EE.UU.
- Ferrer Vallet, María Isabel; Oltra Gutiérrez, Juan Vicente (2007). "Internet oscura: de los sniffers al phreaking". ETSIA, UPV. Valencia.
- Franco, Jean-Michel; EDS-Institut Promèthéus (1997). "El Data Warehouse. El Data Mining". Ed. Gestión 2000. Barcelona.
- García-Morán, Jean Paul; Fernández Hansen, Yago; Martínez Sánchez, Rubén; Ochoa Martín, Ángel (2011). "Hacking y seguridad en internet". RA-MA. Madrid.
- Gimenez Solano, Vicente Miguel; Oltra Gutiérrez, Juan Vicente (2011). "Hacking y ciberdelito". FI, UPV. Valencia.
- Ligh, Michael Hale; Adair, Steven; Hartstein, Blake; Richard, Matthew (2010). "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code". Indianapolis, EE.UU.

López Crespo, Francisco; Amutio Gómez, Miguel A.; Cantabrana González, Ricado (2005). “MAGERIT, metodología de análisis y gestión de riesgos. Herramienta PILAR”. Curso TIC0530-02. Instituto Nacional de Administración Pública. Madrid.

Marcelo Rodao, Jesús de (2003). “Piratas cibernéticos. Cyberwars, seguridad informática e internet” (2ª edición). RA-MA. Madrid.

Miguel Perez, Carlos; Matas García, Abel Mariano; Jimenez García, María Teresa;Hereda Soler, Ernest; Caballero Velasco, María Angeles (2012). “La biblia del hacker”. Anaya Multimedia. Madrid.

Northcutt, Stephen; Novak, Judy (2001). “Guía avanzada. Detección de intrusos” (2ª edición). Pearsons Educación S.A.. Madrid.

Presidencia del Gobierno (2013). “Estrategia de Ciberseguridad nacional”. Departamento de Seguridad Nacional de Presidencia del Gobierno. Madrid.

Rando, Enrique; Alonso, Chema (2013). “Hacking de aplicaciones Web: SQL injection” (2ª edición). Informática64. Madrid.

R.D. 3/2010 (2010). “Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (incluye corrección de errores publicada el 11 de marzo de 2010)”. Ministerio de la Presidencia. Madrid.

Schmid, Gerhard (2001). “Informe STOA sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON) (2001/2098(INI))”. Parlamento Europeo. Estrasburgo. Francia.

Sun Tzu. “El Arte de la Guerra (Versión de Thomas Cleary)”. Ed. EDAF. 31ª edición, enero 2007.

Vollnhalls, Otto (1999). “Multilingual dictionary of IT Security: english, german, french, spanish, italian”. K.G. Saur. Munich, Alemania.

Walker, Andy (2006). “Manual imprescindible de seguridad, spam, spyware y virus”. Anaya Multimedia. Madrid.

Webs referenciadas

[3] Nuclearfiles.org. “MAD Strategy”. http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-mutual-assured-destruction.htm (Ú.a.: 14/08/2015)

[4] HistoriaSiglo20.org. “Acuerdos SALT”. http://www.historiasiglo20.org/GLOS/SALT.htm (Ú.a.: 14/08/2015)

[5] HistoriaSiglo20.org. “Crisis de los Euromisiles”. http://www.historiasiglo20.org/GLOS/euromisiles.htm (Ú.a.: 14/08/2015)

[6] Alonso, Gustavo (1990). “La Iniciativa de Defensa Estratégica (SDI)”. GSI de la UPM. http://www.gsi.dit.upm.es/~fsaez/intl/libro_complejidad/16-iniciativa-de-defensa-estrategica.pdf (Ú.a.: 14/08/2015)

[7] National Security Agency. SIGINT. (2009). https://www.nsa.gov/sigint/ Fort Meade, Maryland EE.UU. (Ú.a.: 14/08/2015)

[8] Science and Technology Options Assessment. http://www.europarl.europa.eu/stoa/ STOA Secretariat, European Parliament. Bruselas (Bélgica) (Ú.a.: 14/08/2015)

[9] Informe STOA (2001/2098(INI)), de 11 de julio de 2001. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//ES (Ú.a.: 30/05/2015)

[10] Jerome Thorel. “Pourquoi l'affaire Echelon embarrasse Thomson-CSF”. ZDNet. 14/07/2000. http://www.zdnet.fr/actualites/pourquoi-l-affaire-echelon-embarrasse-thomson-csf-2060838.htm (Ú.a.:22/08/2015)

[11] Tratado de Lisboa. Innovaciones en materia de Política Exterior y de Seguridad Común (PESC). Eurogersinformation (2010). http://www.eurogersinfo.com/espagne/actes2209.htm (Ú.a.: 22/08/2015)

[12] ENFOPOL 55. Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services. 20/06/2001. http://www.statewatch.org/news/2001/sep/9194.pdf (Ú.a.: 22/08/2015)

[13] Gilles Tremlet. “US offers to spy on Eta for Spain”. The Guardian. 15/06/2001. http://www.theguardian.com/world/2001/jun/15/spain.usa (Ú.a.: 14/08/2015)

[15] JED (Jam Echelon Day). https://www.thing.net/~rdom/ecd/jam.html (Ú.a.: 19/08/2015)

[16] Wendy McAuliffe. "’Jam Echelon Day’ doomed to failure, say Experts”. ZDNet, 26/07/2001. http://www.zdnet.com/article/jam-echelon-day-doomed-to-failure-say-experts/ (Ú.a.: 19/08/2015)

[17] Wikileaks. The Spy Files. https://wikileaks.org/the-spyfiles.htm (Ú.a.: 28/07/2015)

[18] Alejandro López de Miguel. “La reacción de sorpresa de los estados de la UE ante el espionaje es hipócrita, puro teatro”. Público. 30/10/2013. http://www.publico.es/internacional/reaccion-sorpresa-estados-ue-espionaje.html (Ú.a.: 15/08/2015)

[19] SWIFT http://www.swift.com/index.page?lang=es (Ú.a.: 15/08/2015)

[20] Gregor Peter Schmitz. “SWIFT Suspension? EU Parliament Furious about NSA Bank Spying.”. Der Spiegel. 18/09/2013. http://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920.html (Ú.a.: 15/08/2015)

[21] Objetivos de Protect America Act. Departamento de Justicia de EE.UU. http://www.justice.gov/archive/ll/ (Ú.a.: 16/08/2015)

[22] Copia desclasificada del informe preceptivo sobre el PCP para la aprobación de la Ley FISA, elaborado por ponentes del Departamento de Justicia, Departamento de Defensa, CIA y NSA. https://oig.justice.gov/special/s0907.pdf (Ú.a.: 15/08/2015)

[23] Electrospaces. "What is known about NSA's PRISM program". 23/04/14 (Updated 06/06/15). http://electrospaces.blogspot.com.es/2014/04/what-is-known-about-nsas-prism-program.html (Ú.a.:14/08/2015)

[24] Frederic Lardinois. "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program". TechCrunch. 06/06/2013. http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/ (Ú.a.: 16/08/2015)

[25] BND. http://www.bnd.bund.de/EN/Scope_of_Work/Mission/Mission_node.html (Ú.a.: 16/08/2015)

[26] GCHQ. http://www.gchq.gov.uk/what_we_do/Pages/index.aspx (Ú.a.: 16/08/2015)

[27] American Civil Liberties Union. "What can the NSA do?". 2006. https://www.aclu.org/files/pdfs/eavesdropping101.pdf (Ú.a.: 16/08/2015)

[28] Hubert Gude, Laura Poitras and Marcel Rosenbach. "Transfers from Germany Aid US Surveillance". Der Spiegel. 05/08/2013. http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html (Ú.a.: 21/08/2015)

[29] Manuel Altozano. "La policía podrá usar troyanos para investigar ordenadores y tabletas". El País. 03/06/2013. http://sociedad.elpais.com/sociedad/2013/06/03/actualidad/1370289646_865495.html (Ú.a.:21/08/2015)

[31] Jacques Follorou et Franck Johannès. "Révélations sur le Big Brother français". Le Monde. 04/07/2013. http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (Ú.a.: 28/08/2015)

[32] Miguel A. Gallardo. OSEMINTI. 2006. http://www.miguelgallardo.es/oseminti/ (Ú.a.: 10/07/2015)

[34] Navegante. "El Parlamento Europeo aprueba la retención de datos contra el terrorismo". El Mundo. 14/12/2005. http://www.elmundo.es/navegante/2005/12/14/esociedad/1134560239.html (Ú.a.:05/09/2015)

[35] PrivacySOS. "NARUS, deep packet inspection and the NSA". 09/04/2015. https://www.privacysos.org/technologies_of_control/naurus (Ú.a.: 29/08/2015)

[36] Shane Harris. "Giving In to the Surveillance". The New York Times. 22/08/2012. http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html?_r=0 (Ú.a.:29/08/2015)

[37] James Bamford. "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". Wired. 15/03/2012. http://www.wired.com/2012/03/ff_nsadatacenter/all/ (Ú.a.: 29/08/2015)

[38] NSA Utah Data Center. https://nsa.gov1.info/utah-data-center/ (Ú.a.: 29/08/2015)

[39] BOE. http://www.boe.es/buscar/doc.php?id=BOE-B-2007-256021 (Ú.a.: 30/08/2015)

[40] "Sitel Requiere un control". Asociación de Internautas. 09/09/2009. http://www.internautas.org/html/5711.html (Ú.a.: 31/08/2015)

41 "Así funciona Sitel, el "Gran Hermano" de Zapatero". Libertad Digital. 15/10/2009. http://www.libertaddigital.com/nacional/asi-funciona-sitel-el-gran-hermano-de-zapatero-1276373188/ (Ú.a.: 31/08/2015)

42 Agencia Española de Protección de Datos. http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (Ú.a.: 01/09/2015)

43 Conclusiones de la Inspección de la AEPD sobre SITEL. AEPD. 19/01/2010. http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/enero/190110_np_conclusiones_sitel.pdf (Ú.a.: 01/09/2015)

44 LOPJ. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (Vigente hasta el 01 de Octubre de 2015). Noticias Jurídicas. http://noticias.juridicas.com/base_datos/Admin/lo6-1985.l1t1.html (Ú.a.: 01/09/2015)

45 LECrim. Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal (Vigente hasta el 28 de Octubre de 2015). Noticias Jurídicas. http://noticias.juridicas.com/base_datos/Penal/lecr.html (Ú.a.: 01/09/2015)

46 LOPD. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Noticias jurídicas. http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html (Ú.a.: 01/09/2015)

47 Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. BOE. http://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950 (Ú.a.: 11/09/2015)

48 Pablo Romero. "Así actuó la Policía para identificar a los supuestos 'líderes' de Anonymous". El Mundo. 27/06/2011. http://www.elmundo.es/elmundo/2011/06/24/navegante/1308937468.html (Ú.a.:31/08/2015)

49 Blog oficial de Anonymous Iberoamérica. http://anonopsibero.blogspot.com/2014/12/operacion-elaborada-por-la-policia-en.html (Ú.a.: 31/08/2015)

50 Wikipedia. "Hacktivismo". https://es.wikipedia.org/wiki/Hacktivismo (Ú.a.: 28/08/2015)

51 François Paget. "Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas". McAfee Labs, 2012. http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf?view=legacy (Ú.a.:17/09/2015)

52 Mercé Molist. "¿Cómo nació el 'Hacktivismo'?". El Mundo. 16/04/2015. http://www.elmundo.es/tecnologia/2015/04/16/552fc9a2ca4741be608b4578.html (Ú.a.: 28/08/2015)

53 Declaración Universal de los DD.HH. http://www.un.org/es/documents/udhr/ (Ú.a.: 16/09/2015)

54 Suelette Dreyfus, Julian Assange (2011), "Underground". Ed. Seix Barral. Barcelona. Versión electrónica libre del libro. www.underground-book.net (Ú.a.: 12/09/2015)

56 The Internet Operating System Counter. http://www.leb.net/hzo/ioscount/ (Ú.a.: 02/09/2015)

57 Mercé Molist. "Pequeña guía histórica de los primeros hackers españoles". El Mundo. 21/04/2014. http://www.elmundo.es/tecnologia/2014/04/20/53523c03ca474132388b456c.html (Ú.a.: 02/09/2015)

58 Mercé Molist. "Hackstory.es. La historia nunca contada del underground hacker en la Península Ibérica". 2012. http://hackstory.es/ebook/Hackstory%20-%20Merce%20Molist%20Ferrer.pdf (Ú.a.: 30/08/2015)

59 Hackstory.es http://hackstory.net/Hackstory.es_Index (Ú.a.: 02/09/2015)

[60] Mercé Molist. “El primer detenido por 'hacking' en España fue un madrileño de 19 años”. El Mundo. 01/02/2014. http://www.elmundo.es/tecnologia/2014/02/01/52eca305ca474133388b456d.html (Ú.a.: 02/09/2015)

[61] Iberhack. http://web.archive.org/web/19980201050415/http://iberhack.islatortuga.com/index.html (Ú.a.: 02/09/2015)

[62] JeCk’s Page. Lineas 900. 09/11/1999. http://jeck.8m.com/900.htm (Ú.a.: 03/09/2015)

[63] Almeida Asociados. “Caso Millenium: no concurre prueba concreta del proceso de defraudación”. 14/02/2005. http://www.bufetalmeida.com/54/caso-millenium-1-no-concurre-prueba-concreta-del-proceso-de-defraudacion.html (Ú.a.: 04/09/2015)

[64] Jonathan Jenkins. “Man trolled the web for girls: cops”. Sun Media. 7/12/2007. http://cnews.canoe.com/CNEWS/Crime/2007/12/07/4712680-sun.html (Ú.a.: 04/09/2015)

[65] Howard Dahdah. “'Anonymous' group declares online war on Scientology”. Computerwold. 08/02/2008. http://www.computerworld.com.au/article/206359/_anonymous_group_declares_online_war_scientology_/ (Ú.a.: 03/09/2015)

[66] Nick Carbone. “How Time Warner Profits from the ‘Anonymous’ Hackers”. Time. 29/08/2011. http://newsfeed.time.com/2011/08/29/how-time-warner-profits-from-the-anonymous-hackers/ (Ú.a.: 02/09/2015)

[67] Press Release. “Wikileaks empieza a publicar cables diplomáticos de la embajada de EE.UU.”. Wikileaks. 28/11/2010. https://wikileaks.org/Wikileaks-empieza-a-publicar.html (Ú.a.: 15/09/2015)

[68] Spamhaus. https://www.spamhaus.org/ (Ú.a.: 07/09/2015)

[69] Brian Krebs. “HBGary Federal Hacked by Anonymous”. Krebs-on-Security. 07/02/2011. http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/ (Ú.a.: 07/09/2015)

[70] Kim Zetter. “Anonymous Hacks Security Firm Investigating IT; Releases E-mail”. Wired. 07/02/2011. http://www.wired.com/2011/02/anonymous-hacks-hbgary/ (Ú.a.: 07/09/2015)

[71] BBC News. “Anonymous hackers attack US security firm HBGary”. 07/02/2011. http://www.bbc.com/news/technology-12380987 (Ú.a.: 07/09/2015)

[72] Andy Greenberg. “HBGary Federal's Aaron Barr Resigns After Anonymous Hack Scandal”. Forbes. 01/03/2011. http://www.forbes.com/sites/andygreenberg/2011/02/28/hbgary-federals-aaron-barr-resigns-after-anonymous-hack-scandal/ (Ú.a.: 07/09/2015)

[73] Wikipedia. “SOPA”. https://es.wikipedia.org/wiki/Stop_Online_Piracy_Act (Ú.a.: 07/09/2015)

[74] Wikipedia. “Wikipedia: Protesta contra SOPA.” https://es.wikipedia.org/wiki/Wikipedia:Protesta_contra_SOPA (Ú.a.: 17/09/2015)

[75] #OperationGreenRights. http://operationgreenrights.blogspot.com.es/ (Ú.a.: 08/09/2015)

[76] “Anonymous takes down government sites in massive anti-ACTA attack”. RT. 17/02/2012. http://www.rt.com/usa/anonymous-fff-consumer-acta-609/ (Ú.a.: 08/09/2015)

[77] Frank Mason. “AnonNews.org run by United States government”. Internet Chronicle. 06/03/2011. http://chronicle.su/2011/03/06/anonnews-org-run-by-united-states-government/ (Ú.a.: 07/09/2015)

[78] Cinco Días. "La vieja amenaza de Anonymous a Facebook que terminó en nada". 04/11/2014. http://cincodias.com/cincodias/2014/11/03/lifestyle/1415038380_253498.html (Ú.a.: 08/09/2015)

[79] Wikipedia. ¡Indignaos!. https://es.wikipedia.org/wiki/%C2%A1Indignaos! (Ú.a.: 18/09/2015)

[80] ¡Democracia Real YA!. http://www.democraciarealya.es/ (Ú.a.: 08/09/2015)

[81] CMU SCS Coke Machine. Carnegie Mellon University. https://www.cs.cmu.edu/~coke/ (Ú.a.: 18/09/2015)

[82] 'Ms. Smith'. "Black Hat: Smart TVs are the 'perfect target' for spying on you". Network World. 02/08/2013. http://www.networkworld.com/article/2225091/microsoft-subnet/black-hat--smart-tvs-are-the--perfect-target--for-spying-on-you.html (Ú.a.: 10/09/2015)

[83] SeungJin 'Beist' Lee y Seungjoo Kim. "Smart TV Security". 08/03/2013. CIST. Korea University. http://www.slideshare.net/skim71/smart-tv-security-1984-in-21st-century (Ú.a.: 17/09/2015)

[84] "Cómo hackear fácilmente su SmartTV: Samsung y LG". Noticias de Seguridad Informática. 07/07/2015. http://noticiasseguridad.com/tecnologia/como-hackear-facilmente-su-smart-tv-samsung-y-lg/ (Ú.a.: 10/09/2015)

[85] Ciberseguridad. "Así pueden 'hackearte' cualquier aparato conectado a Internet". El País. 23/07/2015. http://tecnologia.elpais.com/tecnologia/2015/07/10/actualidad/1436539664_188672.html (Ú.a.: 10/09/2015)

[86] Alex Drozhzhin. "El Internet de las Cosas Inútiles". Kaspersky Labs. 19/02/2015. https://blog.kaspersky.es/internet-de-las-cosas-inutiles/5423/ (Ú.a.: 10/09/2015)

[87] Dennis Fisher. "David Jacoby on Hacking His Home". ThreatPost. 24/09/2014. https://threatpost.com/david-jacoby-on-hacking-his-home/108517/ (Accedido a través de Kaspersky Labs http://t.co/0tDXbMBvxi). (Ú.a.: 10/09/2015)

[88] "Internet of Things Research Study". Hewlett Packard, Septiembre de 2014. http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf (Ú.a.: 17/09/2015).

[89] "The Internet of Everything: Layers, Protocols and Possible Attacks". TrendMicro. 23/09/2014. http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/ioe-layers-protocols-and-possible-attacks (Ú.a.: 17/09/2015).

[90] Kevin Poulsen. "Play Station Network Hack. Who did it?". Wired. 27/04/2011. http://www.wired.com/2011/04/playstation_hack/ (Ú.a.: 15/09/2015)

[92] Wikipedia. "The Aurora Genarator Test". https://en.wikipedia.org/wiki/Aurora_Generator_Test (Ú.a.: 17/09/2015)

[93] Thomas Reed. "At the Abyss: An Insider's History of the Cold War". Wikipedia. https://en.wikipedia.org/wiki/At_the_Abyss (Ú.a.: 17/09/2015)

[94] INCIBE. https://www.incibe.es/home/instituto_nacional_ciberseguridad/ (Ú.a.: 28/08/2015)

[95] "Mercado legal de vulnerabilidades 0-day". INCIBE. 04/04/2013. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/mercado_legal_vulnerabilidades_0day (Ú.a.: 28/08/2015)

[96] "Hacker posts Facebook bug report on Zuckerberg's wall". RT. 17/08/2013. http://on.rt.com/2ylp9k (Ú.a.: 30/08/2015)

[97] The Bug Bounty List. Bugcrowd. https://bugcrowd.com/list-of-bug-bounty-programs/ (Ú.a.: 30/08/2015)

[98] SETI@home. http://setiathome.ssl.berkeley.edu/ (Ú.a.: 01/09/2015)

[99] "Arrests made in botnet crackdown". BBC News. 30/11/2007. http://news.bbc.co.uk/2/hi/technology/7120251.stm (Ú.a.: 30/08/2015)

[100] EFE. "Tres españoles dirigían la mayor red de ordenadores 'zombis' del mundo". La Vanguardia. 04/03/2010. http://www.lavanguardia.com/sucesos/20100303/53896548728/tres-espanoles-dirigian-la-mayor-red-de-ordenadores-zombis-del-mundo.html (Ú.a.: 30/08/2015)

[101] Elena Bondarenko, Darya Gudkova, Maria Namestnikova. "Spam in the Third Quarter of 2010". Kaspersky Lab. 10/11/2010. https://securelist.com/analysis/quarterly-spam-reports/36330/spam-in-the-third-quarter-of-2010/ (Ú.a.: 30/08/2015)

[102] Jacob Nitohiwa. "Spam reduction reports questionable". ITWeb. 14/06/2011. http://www.itweb.co.za/index.php?option=com_content&view=article&id=40159 (Ú.a.: 30/08/2015)

[103] Max Goncharov. "Russian Underground 101". Trend Micro. 2012. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf (Ú.a.: 30/08/2015)

[104] Kaspersky Security Bulletin. El spam en 2013. "Criminalización del spam de carácter comercial". Viruslist. 23/01/2014. http://www.viruslist.com/sp/analysis?pubid=207271242#03 (Ú.a.: 16/09/2015)

[105] GReAT, Kaspersky Lab's Global Research & Analysis Team. "The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies". Securelist. 14/01/2013. https://securelist.com/blog/incidents/57647/the-red-october-campaign/ (Ú.a.: 16/09/2015)

[106] GReAT, Kaspersky Lab's Global Research & Analysis Team. "Cloud Atlas: RedOctober APT is back in style". SecureList. 10/12/2014. https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/ (Ú.a.: 16/09/2015)

[107] GReAT, Kaspersky Lab's Global Research & Analysis Team. "The Epic Turla Operation". SecureList. 07/08/2014. https://securelist.com/analysis/publications/65545/the-epic-turla-operation/ (Ú.a.: 16/09/2015)

[108] Symantec Security Response. "Turla: Spying tool targets governments and diplomats". Symantec. 07/08/2014. http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats (Ú.a.: 16/09/2015)

[109] Christian Bautista. "Spy agencies compromised by 'Epic Turla' cyber espionage operation". Tech Times. 09/08/2014. http://www.techtimes.com/articles/12455/20140809/spy-agencies-compromised-by-epic-turla-cyber-espionage-operation.htm (Ú.a.: 16/09/2015)

[110] Richard A. Clarke y Robert K. Knake. "Guerra en la red. Los nuevos campos de batalla". Ed. Planeta, 2011. (pp. 318 – 319)

[111] Claudi Pérez. "El CNI investiga las presiones especulativas sobre España". El País. 14/02/2010. http://elpais.com/diario/2010/02/14/economia/1266102005_850215.html (Ú.a.: 19/09/2015)

[112] GReAT, Kaspersky Lab's Global Research & Analysis Team. "El gran robo de banco: el APT Carbanak". VirusList. 16/02/2015. http://www.viruslist.com/sp/weblog?weblogid=208189052 (Ú.a.: 16/09/2015)

[114] Blacklist. "AS45090 Shenzhen Tencent Computer Systems Company Limited". CleanTalk.org. https://cleantalk.org/blacklists/AS45090 (Ú.a.: 22/09/2015)

[115] "Fraude de carta de Nigeria sigue defraudando". FBI. 2015. https://www.fbi.gov/espanol/historias/fraude-de-carta-de-nigeria-sigue-defraudando (Ú.a.: 25/09/2015)

[116] Merce Molist. "El fraude del nigeriano". El País. 23/11/2006. http://elpais.com/diario/2006/11/23/ciberpais/1164252267_850215.html (Ú.a.: 25/09/2015)

[117] ICFNL. International Centre for Nigerian Law. "Código Penal Nigeriano. Part 6. Division 1. Chapter 38". Nigeria. http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm (Ú.a.: 25/09/2015)

[118] Foro de afectados por 419 scam. 419.bitten us.com. http://419.bittenus.com/7/11/MRALBERTJFRACAS.html (Ú.a.: 25/09/2015)

[119] Ransomware. Wikipedia. https://es.wikipedia.org/wiki/Ransomware (Ú.a.: 25/09/2015)

[120] Nota de prensa. "Desarticulada la rama económica responsable del 'virus de la Policía' y que había comprometido la seguridad de 1.500 empresas en España". Cuerpo Nacional de Policía. http://www.policia.es/prensa/20130927_1.html (Ú.a.: 25/09/2015)

[121] "GameOver Zeus (GOZ) Malware and Botnet Architecture". FBI. Junio de 2014. https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/documents/gameover-zeus-and-cryptolocker-poster-pdf (Ú.a.: 25/09/2015)

[122] Marta López. "¡Atención! ¡Oleada de Ransomware simulando ser Correos!". Panda Mediacenter. 24/03/2015. http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/ (Ú.a.: 25/09/2015)

[123] CSO. "Se dispara el ransomware y el malware dirigido contra Adobe Flash". ComputerWorld. 11/06/2015. http://cso.computerworld.es/tendencias/se-dispara-el-ransomware-y-el-malware-dirigido-contra-adobe-flash (Ú.a.: 25/09/2015)

[124] McAffee Labs. "Informe sobre amenazas. Mayo 2015" (p.5). Intel Security. http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2015.pdf?view=legacy (Ú.a.: 23/09/2015)

[125] CSO. "Nueva vulnerabilidad de día cero en Flash, la tercera en dos semanas". Computerworld. 03/02/2015. http://cso.computerworld.es/alertas/nueva-vulnerabilidad-de-dia-cero-en-flash-la-tercera-en-dos-semanas (Ú.a.: 25/09/2015)

[126] Virus News. "Equation Group: The Crown Creator of Cyber-Espionage". Kaspersky Lab. 16/02/2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage (Ú.a.: 25/09/2015)

[127] McAffee Labs. "Informe sobre amenazas. Mayo 2015" (p.9). Intel Security. http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2015.pdf?view=legacy (Ú.a.: 23/09/2015)

[128] GReAT, Kaspersky Lab's Global Research & Analysis Team. "Stuxnet: Zero victims. The identity of the companies targeted by the first known cyber-weapon". ScureList. 11/09/2014. https://securelist.com/analysis/publications/67483/stuxnet-zero-victims/ (Ú.a.: 25/09/2015)

[129] Duqu. Wikipedia. https://en.wikipedia.org/wiki/Duqu (Ú.a.: 25/09/2015)

[130] Ryan Naraine. “Duqu FAQ”. SecureList. 19/10/2011. https://securelist.com/blog/incidents/32463/duqu-faq-33/ (Ú.a.: 25/09/2015)

[131] GReAT, Kaspersky Lab's Global Research & Analysis Team. “The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns”. SecureList. https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/ (Ú.a.: 25/09/2015)

[132] Flame. Wikipedia. https://es.wikipedia.org/wiki/Flame_%28malware%29 (Ú.a.: 25/09/2015)

[133] Alexander Gostev. “The Flame: Questions and Answers”. SecureList. 28/05/2012. https://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/ (Ú.a.: 25/09/2015)

[134] Emma Graham-Harrison. “Could Isis’s ‘cyber caliphate’ unleash a deadly attack on key targets?”. The Guardian. 12/04/2015. http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race (Ú.a.: 25/09/2015)

[135] CCN-CERT-IA-09/15. “Ciberamenazas 2014. Tendencias 2015. Resumen ejecutivo”. CCN. 09/04/2015. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html (Ú.a.: 23/09/2015)

[136] IV Congreso de la Cibersociedad (2009). Grupo de trabajo C-24: Derecho & cibercrimen. “Internet: Un espacio para el cibercrimen y el ciberterrorismo”. Observatorio para la Cibersociedad. http://www.cibersociedad.net/congres2009/es/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610/ (Ú.a.: 25/09/2015).

[137] Samuel Gibbs. “Eugene Kaspersky: major cyberterrorist attack is only matter of time”. The Guardian. 01/05/2014. http://www.theguardian.com/technology/2014/may/01/eugene-kaspersky-major-cyberterrorist-attack-uk (Ú.a.: 25/09/2015).

[138] Guerra informática. Wikipedia. https://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica (Ú.a.: 26/09/2015).

[140] Ricardo Martínez de Rituerto. “Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE”. El País. 18/05/2007. http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html (Ú.a.: 26/09/2015).

[141] Ian Traynor. “Russia accused of unleashing cyberwar to disable Estonia”. The Guardian. 17/05/2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia (Ú.a.: 26/09/2015).

[142] EFE. “Estonia protegerá sus instituciones de ataques informáticos con ayuda de la OTAN”. El Mundo. 18/05/2007. http://www.elmundo.es/navegante/2007/05/18/tecnologia/1179478759.html (Ú.a.: 26/09/2015).

[143] David E. Singer; Mark Mazzetti. “Israel Struck Syrian Nuclear Project, Analysts Say”. The New Yory Times. 14/10/2007. http://www.nytimes.com/2007/10/14/washington/14weapons.html?_r=0 (Ú.a.: 26/09/2015).

[144] Erich Follath; Holger Stark. “The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor”. Der Spiegel. 02/11/2009. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html (Ú.a.: 26/09/2015).

[145] Daveed Gartenstein-Ross; Joshua D. Goodman. “The Attack on Syria's al-Kibar Nuclear Facility”. The Jewish Policy Center (2009). http://www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility (Ú.a.: 26/09/2015).

[146] Operación Orchard. Wikipedia. https://en.wikipedia.org/wiki/Operation_Orchard (Ú.a.: 26/09/2015).

[147] David Albright; Paul Brannan. "Syria Update III: New information about Al Kibar reactor site". ISIS. 24/04/2008. http://isis-online.org/uploads/isis-reports/documents/SyriaUpdate_24April2008.pdf (Ú.a.: 26/09/2015).

[149] "Las acusaciones de EE UU a China por espionaje". El País. 19/05/2014. http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html (Ú.a.: 27/09/2015).

[150] Tom Spiner. "Georgia accuses Russia of coordinated cyberattack". CNet. 11/08/2008. http://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/ (Ú.a.: 26/09/2015).

[151] Cyberattacks during the Russo-Georgian War. Wikipedia. https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War (Ú.a.: 26/09/2015).

[152] Associated Press. "North Korea launched cyber attacks, says south". The Guardian. 11/07/2009. http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks (Ú.a.: 26/09/2015).

[153] "Stuxnet worm hits Iran nuclear plant staff computers". BBC. 26/09/2010. http://www.bbc.com/news/world-middle-east-11414483 (Ú.a.: 26/09/2015).

[154] Stuxnet. Wikipedia. https://en.wikipedia.org/wiki/Stuxnet (Ú.a.: 26/09/2015).

[155] EFE, Teherán. "Irán reconoce un ataque informático masivo contra sus sistemas industriales". El Mundo. 27/09/2010. http://www.elmundo.es/elmundo/2010/09/27/navegante/1285571297.html (Ú.a.: 26/09/2015).

[156] "Equation Group: The Crown Creator of Cyber-Espionage". Kaspersky Lab. 16/02/2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage (Ú.a.: 25/09/2015)

[157] Alexander Gostev. "Kaspersky: Boletín de seguridad 2012. Las armas cibernéticas". VirusList. 18/12/2012. http://www.viruslist.com/sp/analysis?pubid=207271197 (Ú.a.: 24/09/2015).

[158] "Operation Hangover: Q&A on Attacks". Symantec. 20/05/2013. http://www.symantec.com/connect/blogs/operation-hangover-qa-attacks (Ú.a.: 27/09/2015).

[159] Gregg Keizer"'Operation Hangover' hackers exploit latest Windows zero-day". ComputerWorld. 07/11/2013. http://www.computerworld.com/article/2485693/malware-vulnerabilities/-operation-hangover--hackers-exploit-latest-windows-zero-day.html (Ú.a.: 27/09/2015).

[160] Pierluigi Paganini. "Operation Arachnophobia, targeted attacks from Pakistan". Security Affairs. 21/08/2014. http://securityaffairs.co/wordpress/27666/intelligence/operation-arachnophobia-pakistan.html (Ú.a.: 27/09/2015).

[161] "The Interview: A guide to the cyber attack on Hollywood". BBC. 29/12/2014. http://www.bbc.com/news/entertainment-arts-30512032 (Ú.a.: 27/09/2015).

[162] Tom Fox-Brewster. "Sony Pictures hack: how much damage can North Korea's cyber army do?". The Guardian. 05/12/2014. http://www.theguardian.com/technology/2014/dec/05/sony-pictures-hack-north-korea-cyber-army (Ú.a.: 27/09/2015).

[163] Andrew Buncombe. "Sony Pictures hack: US intelligence chief says North Korea cyberattack was 'most serious' ever against US interests". The Independent. 07/01/2015.

http://www.independent.co.uk/news/world/americas/us-intelligence-chief-sony-hack-was-most-serious-attack-against-us-interests-9963504.html (Ú.a.: 27/09/2015).

[164] David Carr. "How the Hacking at Sony Over 'The Interview' Became a Horror Movie". The New York Times. 21/12/2014. http://www.nytimes.com/2014/12/22/business/media/hacking-at-sony-over-the-interview-reveals-hollywoods-failings-too.html?_r=0 (Ú.a.: 27/09/2015).

[165] Reuters/Europa Press. "La conexión a Internet en Corea del Norte está paralizada por completo, según medios oficiales chinos". Europa Press. 27/12/2014. http://www.europapress.es/internacional/noticia-conexion-internet-corea-norte-paralizada-completo-medios-oficiales-chinos-20141227155330.html (Ú.a.: 27/09/2015).

[166] Pierluigi Paganini. "Iran accused of the blackout that paralyzed the Turkey". Security Affairs. 04/05/2015. http://securityaffairs.co/wordpress/36536/cyber-warfare-2/iran-accused-blackout-turkey.html (Ú.a.: 27/09/2015).

[167] Don Melvin; Greg Botelho. "Cyberattack disables 11 French TV channels, takes over social media sites". CNN. 09/04/2015. http://edition.cnn.com/2015/04/09/europe/french-tv-network-attack-recovery/ (Ú.a.: 27/09/2015).

[168] John Lichfield. "TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link". The Independent. 10/06/2015. http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html (Ú.a.: 27/09/2015).

[169] Pablo Romero. "'Es una cuestión de tiempo que los 'ciberataques' tengan un impacto real en el mundo físico'. Entrevista a James Lyne, responsable de investigación de Sophos". El Mundo. 31/05/2014. http://www.elmundo.es/tecnologia/2014/05/31/5386f33de2704e99648b456e.html (Ú.a.: 27/09/2015).

[170] "Oleada de ciberataques desde China". El País. 07/03/2011. http://tecnologia.elpais.com/tecnologia/2011/03/07/actualidad/1299492061_850215.html (Ú.a.:27/09/2015).

[171] "Las acusaciones de EE UU a China por espionaje". El País. 19/05/2014. http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html (Ú.a.:27/09/2015).

[172] Macarena Vidal. "China considera "irresponsables" las acusaciones de ciberespionaje". El País. 05/06/2015. http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433503775_500727.html (Ú.a.:27/09/2015).

[173] Marc Bassets. "Washington acusa a cinco militares chinos de ciberespionaje industrial". El País. 19/05/2014. http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html (Ú.a.:27/09/2015).

[174] "APT1. Exposing One of China's Cyber Espionage Units". Mandiant, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (Ú.a.:05/03/2015).

[175] Kaspersky Lab. Targeted CyberAttaks LogBook. https://apt.securelist.com/ (Ú.a.:05/03/2015).

[176] Ignacio Cembrero. "Un 'troyano' español espiaba en Marruecos". El Mundo. 15/02/2015. http://www.elmundo.es/espana/2015/02/15/54dfb6d3e2704e5a7f8b456c.html (Ú.a.:05/03/2015).

[177] Ignacio Cembrero. "'Babar', un 'gusano' francés para España". El Mundo. 15/02/2015. http://www.elmundo.es/espana/2015/02/15/54dfbc73e2704e7c7f8b456e.html (Ú.a.: 27/09/2015).

[178] Joaquín Gil. "'Hackers' de Rusia y China lanzaron ataques contra cuatro ministerios". El País. 14/12/2014. http://politica.elpais.com/politica/2014/12/13/actualidad/1418472065_191091.html (Ú.a.:27/09/2015).

[179] "China y Rusia firman un pacto de no "ciberagresión" mutua". INCIBE. 08/05/2015. https://www.incibe.es/technologyForecastingSearch/CERT/Alerta_Temprana/Bitacora_de_ciberseguridad/China_Rusia_pacto_no_ciberagresion (Ú.a.: 27/09/2015).

[180] Pablo Romero. "Armados para la 'ciberguerra' fría". El Mundo. 15/02/2015. http://www.elmundo.es/espana/2015/02/15/54dfb898e2704e5b7f8b456b.html (Ú.a.: 27/09/2015).

[181] Operation Aurora. Wikipedia. https://en.wikipedia.org/wiki/Operation_Aurora (Ú.a.: 27/09/2015).

[182] "Países con implantación de voto electrónico". Departamento de Seguridad del Gobierno Vasco. http://www.euskadi.net/botoelek/otros_paises/ve_mundo_impl_c.htm (Ú.a.: 27/09/2015).

[183] "Países con voto electrónico legalmente prohibido o paralizado". Departamento de Seguridad del Gobierno Vasco. http://www.euskadi.net/botoelek/otros_paises/ve_mundo_paralizado_c.htm (Ú.a.: 27/09/2015).

[184] CCN-CERT-IA-09/15. CCN. 09/04/2015. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html (Ú.a.: 27/09/2015).

[185] Robert Sicilano. ""Old" Malware Attacks Rising Significantly". McAffee Blog Central. 05/06/2013. https://blogs.mcafee.com/consumer/q1-threat-report/ (Ú.a.: 27/09/2015).

[186] Anthony diBello. "Malware retro alimenta la nueva ola de amenazas". Information Week México. 08/12/2014. http://www.informationweek.com.mx/columnas/malware-retro-alimenta-la-nueva-ola-de-amenazas/?utm_source=outbrain&utm_medium=social-cpc (Ú.a.: 27/09/2015).

[187] Mandiant (2013). "APT1. Exposing One of China's Cyber Espionage Units". http://intelreport.mandiant.com/ (Ú.a.: 05/03/2015)

[188] GuíaCCN-STIC-401. Glosario y Abreviaturas. CERT-CCN (Agosto, 2015). https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html (Ú.a. 24/09/2015)

[189] Laboratorio de Redes y Seguridad. "Tutorial de Seguridad Informática. Capítulo 3. Identificación de ataques y técnicas de intrusión". UNAM (México). http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap3.html (Ú.a. 24/09/2015)

[190] Blue Pill. Wikipedia. https://en.wikipedia.org/wiki/Blue_Pill_%28software%29 (Ú.a.: 23/09/2015)

[191] Martín Mucha y Javier G. Negre. "El niño que decía trabajar para Soraya y el CNI". El Mundo. 19/10/2014. http://www.elmundo.es/cronica/2014/10/19/54421cede2704e397c8b456b.html (Ú.a.: 23/09/2015)

[192] Test de detección de sniffer. Wikipedia. https://es.wikipedia.org/wiki/Test_de_Detecci%C3%B3n_de_Sniffer (Ú.a.: 23/09/2015)

[193] Tipos de packet sniffers. Wikipedia. https://es.wikipedia.org/wiki/Anexo:Tipos_de_packet_sniffers (Ú.a.: 23/09/2015)

[194] Tcpdump/Libpcap. http://www.tcpdump.org/ (Ú.a.: 23/09/2015)

[195] Librerías WinPcap. http://www.winpcap.org/ (Ú.a.: 23/09/2015)

[196] Snort.org. https://www.snort.org/ (Ú.a.: 23/09/2015)

[197] Wireshark. https://www.wireshark.org/ (Ú.a.: 23/09/2015)

[198] IGMP snooping. Wikipedia. https://es.wikipedia.org/wiki/IGMP_snooping (Ú.a.: 24/09/2015)

[199] DHCP snooping. Wikipedia. https://en.wikipedia.org/wiki/DHCP_snooping (Ú.a.: 24/09/2015)

[200] Tampering o Data Diddling. IMC, Independent Media Center. Barcelona. http://barcelona.indymedia.org/newswire/display/337061/index.php (Ú.a.: 24/09/2015)

[201] Ives Ledermann, Cristian Mendoza y otros. "Hackers y Seguridad". UDEC (Colombia). http://www2.udec.cl/~crmendoz/8.htm (Ú.a.: 24/09/2015)

[202] Carlos Gómez. "Legislación para ingenieros electrónicos". Google Blogger. http://carloslegislacion.blogspot.com.es/2012/11/definicion-de-diversos-delitos.html (Ú.a.: 24/09/2015)

[203] Ofir Arkin. "E.T. Can't Phone Home. Security Issues with VoIP". @Stake (Symantec). Obtenido a través de BlackHat.com. http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt (Ú.a.: 24/09/2015)

[204] Skeeve Stevens. "VoIP hacking is phreaking expensive". CSO. 08/11/2011. http://www.cso.com.au/article/406675/voip_hacking_phreaking_expensive/ (Ú.a.: 24/09/2015)

[205] David G. Ortiz. "Investigadores españoles demuestran que las redes 3G se pueden 'hackear' al menos de cuatro formas". eldiario.es. 08/03/2014. http://www.eldiario.es/hojaderouter/seguridad/root2G-3G-ataques-David_Perez-hacking-Jose_Pico-Layakk-redesed_con-seguridad_informatica_0_275772476.html (Ú.a.: 24/09/2015)

[206] Guías CCN-STIC-4xx. CERT-CCN. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias-generales.html (Ú.a.: 24/09/2015)

[207] Fyodor. "Remote OS detection via TCP/IP stack fingerprinting". NMAP.org. http://www.insecure.org/nmap/nmap-fingerprinting-article.html (Ú.a.: 24/09/2015)

[208] Antonio Rana. "Intrusion Detection FAQ". SANS. https://www.sans.org/security-resources/idfaq/amap.php (Ú.a.: 24/09/2015)

[209] Honeynet Project. "Know Your Enemy: Passive Fingerprinting". 04/03/2002. http://old.honeynet.org/papers/finger/ (Ú.a.: 24/09/2015)

[210] Honeynet Project. "Lists of fingerprints for passive fingerprint monitoring". 20/05/2000. http://old.honeynet.org/papers/finger/traces.txt (Ú.a.: 24/09/2015)

[211] Pete Herzog. Open Source Security Testing Methodology Manual (OSSTMM). ISECOM. http://www.isecom.org/research/osstmm.html (Ú.a.: 24/09/2015)

[212] Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). Junta de Andalucía. http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551 (Ú.a.: 24/09/2015)

[213] Detección de máquinas en modo promiscuo en la red. Wikipedia. https://es.wikipedia.org/wiki/Modo_promiscuo#Detecci.C3.B3n_de_m.C3.A1quinas_en_modo_promiscuo_en_la_red (Ú.a.: 24/09/2015)

[214] Techniques for obtaining and exploiting personal information for identity theft. Wikipedia. https://en.wikipedia.org/wiki/Identity_theft#Techniques_for_obtaining_and_exploiting_personal_information_for_identity_theft (Ú.a.: 24/09/2015)

[215] Serg Vergara. "Saltando la seguridad de un Firewall". 15/04/2011. https://sergvergara.wordpress.com/2011/04/15/tratando-de-saltar-la-seguridad-de-un-firewall/ (Ú.a.: 25/09/2015)

[216] Desbordamiento de Bufer. Wikipedia. https://es.wikipedia.org/wiki/Desbordamiento_de_b%C3%BAfer (Ú.a.: 27/09/2015)

[217] Errores en las cadenas con formato. Websecurity.es. http://www.websecurity.es/errores-las-cadenas-formato (Ú.a.: 27/09/2015)

[218] Condición de carrera. Wikipedia. https://es.wikipedia.org/wiki/Condici%C3%B3n_de_carrera (Ú.a.:27/09/2015)

[219] Inyección SQL. Wikipedia. https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL (Ú.a.: 27/09/2015)

[220] The Cross-Site Scripting (XSS) FAQ. CGISecurity. http://www.cgisecurity.com/xss-faq.html (Ú.a.:27/09/2015)

[221] Virus informático. Wikipedia. https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico (Ú.a.:27/09/2015)

[222] Gusano informático. Wikipedia. https://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico (Ú.a.:27/09/2015)

[223] Ataque de diccionario. Wikipedia. https://es.wikipedia.org/wiki/Ataque_de_diccionario (Ú.a.:27/09/2015)

[224] Ataque de fuerza bruta. Wikipedia. https://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta (Ú.a.:27/09/2015)

[225] Raúl Siles. "Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados". RedIRIS, 2002. http://www.rediris.es/cert/doc/segtcpip/Seguridad_en_TCP-IP_Ed1.html (Ú.a.:27/09/2015)

[226] Rogue access point. Wikipedia. https://en.wikipedia.org/wiki/Rogue_access_point (Ú.a.:27/09/2015)

[227] Ataque Man-in-the-middle. Wikipedia. https://es.wikipedia.org/wiki/Ataque_Man-in-the-middle (Ú.a.:27/09/2015)

[228] ARP Spoofing. Wikipedia. https://es.wikipedia.org/wiki/ARP_Spoofing (Ú.a.:27/09/2015)

[229] Gina Trapani. "How to Crack a Wi-Fi Network's WEP Password with BackTrack". LifeHacker. 10/28/11. http://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack (Ú.a.:27/09/2015)

[230] AirCrack-ng. http://www.aircrack-ng.org/ (Ú.a.:27/09/2015)

[231] Anton T. Rager. WEPCrack. http://wepcrack.sourceforge.net/ (Ú.a.:27/09/2015)

[232] Puerta trasera. Wikipedia. https://es.wikipedia.org/wiki/Puerta_trasera (Ú.a.:27/09/2015)

[233] Troyano. Wikipedia. https://es.wikipedia.org/wiki/Troyano_%28inform%C3%A1tica%29 (Ú.a.:27/09/2015)

[234] Rootkit. Wikipedia. https://es.wikipedia.org/wiki/Rootkit (Ú.a.:27/09/2015)

[235] Log (registro). Wikipedia. https://es.wikipedia.org/wiki/Log_%28registro%29 (Ú.a.:27/09/2015)

[236] Esteganografía. Wikipedia. https://es.wikipedia.org/wiki/Esteganograf%C3%ADa#Software_de_esteganograf.C3.ADa (Ú.a.:27/09/2015)

[237] Presidencia del Gobierno. "Estrategia de Ciberseguridad Nacional". Madrid (2013). http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf (Ú.a.: 28/09/2015)

[238] Caro Bejarano, Mª José. "Estrategia de Ciberseguridad Nacional". Instituto Español de Estdios Estratégicos. 09/12/2013. http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf (Ú.a.: 28/09/2015)

[239] Wegener, Henning. "La ciberseguridad en la Unión Europea". Instituto Español de Estudios Estratégicos. 14/07/2014. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf (Ú.a.: 28/09/2015)

[240] JOIN (2013) 1final. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". European Comision. Brussels. 07/02/2013. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 (Ú.a.: 28/09/2015)

[241] COM (2013) 48. "Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión". NIS Directive. European Comision. Brussels. 07/02/2013. http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive (Ú.a.: 28/09/2015)

[242] ENISA. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/ (Ú.a.: 28/09/2015)

[243] Digital Agenda for Europe 2020. European Comision. Brussels.. http://ec.europa.eu/digital-agenda/en (Ú.a.: 28/09/2015)

[244] Cybersecurity Strategy of the European Union. Pillar III. European Comision. Brussels. http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security (Ú.a.: 28/09/2015)

[245] BSA/The Software Alliance (2015). "EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace". http://cybersecurity.bsa.org/index.html (Ú.a.: 28/09/2015)

[246] BSA/The Software Alliance. "EU Cybersecurity Dashboard. Countries". http://cybersecurity.bsa.org/countries.html (Ú.a.: 28/09/2015)

[247] Héctor R.Suárez; Juan D. Peláez Álvarez. "Ciber-Resiliencia. Aproximación a un Marco de Medición". INTECO. Mayo, 2014. https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf (Ú.a.:28/09/2015)

[248] Departement of Defense. "The Department of Defense Cyber Strategy". Abril, 2015. Washington. EE.UU. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Ú.a.: 28/09/2015)

[249] CCN-CERT. "Informe de Actividades 2013-2014". Centro Criptológico Nacional. https://www.ccn-cert.cni.es/documentos-publicos/1069-informe-actividad-ccn-2013-2014-enfrentadas/file.html (Ú.a.:28/09/2015)

[250] CCN-CERT. Guía CCN-STIC-824. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/542-ccn-stic-824-informaci%C3%B3n-del-estado-de-seguridad/file.html (Ú.a.:28/09/2015)

[251] CCN-CERT. Guía CCN-STIC-817. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html (Ú.a.:28/09/2015)

[252] CCN. Centro Criptológio Nacional. https://www.ccn.cni.es/ (Ú.a.:28/09/2015)

[253] CCN-CERT. https://www.ccn-cert.cni.es/ (Ú.a.:28/09/2015)

[254] CERTSI. https://www.incibe.es/CERT/Infraestructuras_Criticas/ (Ú.a.:28/09/2015)

[255] INCIBE. Instituto Nacional de Ciberseguridad. https://www.incibe.es/home/instituto_nacional_ciberseguridad/ (Ú.a.:28/09/2015)

[256] CNPIC. http://www.cnpic.es/ (Ú.a.:28/09/2015)

[257] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352 (Ú.a.:28/09/2015)

[258] Digital Public Service DESI 2015 for Spain. Digital Agenda for Europe. http://ec.europa.eu/digital-agenda/en/scoreboard/spain#5-digital-public-services (Ú.a.:28/09/2015)

[259] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE. http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750 (Ú.a.:28/09/2015)

[260] ENISA. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/ (Ú.a.:28/09/2015)

[261] GlobbTV. "InnoTec System colabora con el Centro Criptológico Nacional en la contención de ciberataques". http://www.globbtv.com/4383/noticias/innotec-system-colabora-con-el-centro-criptologico-nacional-en-la-contencion-de-ciberataques (Ú.a.:28/09/2015)

Figuras

Tablas

Glosario

11M	Acrónimo que hace referencia a los atentados terroristas contra trenes de cercanías perpetrados por yihadistas en Madrid el 11 de marzo de 2004.
15M	Acrónimo que hace referencia al Movimiento 15M, o de Indignados, surgido a raiz de las manifestaciones convocadas en la Puerta del Sol de Madrid el 15 de mayo de 2011 para protestar por los efectos sociales de la crisis económica.
AA.PP.	Administraciones Públicas. En España contempla el conjunto de las tres admnistraciones en las que se estructura el Estado: la Administración General del Estado (AGE), las administraciones autonómicas, y las administraciones de entidades locales (ayuntamientos, cabildos, diputaciones y corporaciones locales).
Adware	Acrónimo de Advertisement (anuncios) y software (programas), código que facilita la presentación de publicidad a un usuario durante la instalación o uso de un programa, o el acceso a una página web, con objeto de generar lucro a su autor. Muchos programas shareware incorporan la posibilidad de deshabilitar su adware si se adquiere una licencia.
AEPD	Agencia Española de Protección de Datos, organismo público creado en 1993 encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España.
Air-gapped	Medida de seguridad que consiste en mantener un sistema o una red segura aislada físicamente de redes inseguras o de internet.
API	Interfaz de programación de aplicaciones (del inglés Application Programming Interface), es el conjunto de facilidades que ofrece una biblioteca (o librería) de progamación para ser utilizada por otro software como una capa de abstracción.
App	Aplicación o programa (del inglés Application). Se refiere generalmente a aplicaciones desarrolladas para funcionar en tabletas y smartphones, o en un navegador (webapp), suelen ser dependientes de internet y más dinámicas que los programas tradicionales de entorno PC (cliente pesado).

APT	Acrónimo en inglés de Advanced Persistent Threat, o Amenaza Persistente Avanzada, es un conjunto de procesos informáticos sigilosos y continuos, dirigidos a penetrar la seguridad informática de una entidad específica, llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una APT. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas.
AWACS	Acrónimo en inglés de Airborne Early Warning and Control System, o Sistema Aerotransportado de Alerta Temprana y Control. Es un sistema de intercepción electrónica aerotransportado que permite un seguimiento táctico del teatro de operaciones facilitando SIGINT y ELINT.
Backdoor	Puerta trasera. Secuencia de código que permite evitar los algoritmos de autenticación para acceder a un sistema informático.
BBS	Bulletin Board System (Sistema de Tablón de Anuncios), software de red que permite a los usuarios remotos conectarse al sistema vía telnet y descargar software, intercambiar mensajes, etc.
Blacklist	Lista negra que recopila dominios de internet denunciados por haber desarrollado actividad maliciosa.
Bluebox	Dispositivo capaz de emitir tonos por la línea telefónica y que se utiliza para realizar phone phreaking o hacking telefónico.
Bluetooth	Especificación para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.
BND	Bundesnachrichtendienst, o Servicio Federal de Inteligencia alemán.
BGP	Border Gateway Protocol, protocolo de enrutamiento entre diferentes proveedores de acceso a Internet, o ISP (Internet Service Provider).
Bomba lógica	Código insertado intencionalmente en un programa informático, que permanece oculto hasta cumplirse una o más condiciones preprogramadas, momento en el que ejecuta una acción maliciosa.

Botnet	Acrónimo de bot, o robot, y net, red en inglés. También conocida como red zombi. El artífice de la botnet infecta con malware a sus víctimas para obtener sus recursos y puede controlar todos los ordenadores/servidores infectados de forma remota.
Bug	Error de programación del software.
Bug bounty	Programa de recompensas de los fabricantes de software para premiar a los investigadores que reportan vulnerabilidades de sus productos.
C2	También conocidos como C&C, Command and Control. Servidores que alojan las webs desde las que se realiza el control de los ordenadores infectados por gusanos y troyanos, y desde donde se les suministra instrucciones, o reciben los ficheros con la información recopilada.
Captcha	Completely Automated Public Turing test to tell Computers and Humans Apart (prueba de Turing completamente automática y pública para diferenciar computadoras de humanos). Se trata de una prueba desafío-respuesta utilizada para determinar cuándo el usuario es o no humano, generalmente se ofrece una imagen de un texto deformado que un humano puede reconocer. En otras ocasiones se muestran varias imágenes y se realiza una pregunta que lleva a relacionar o discriminar varias de ellas.
CD	Compact Disc, o Disco Compacto. Disco óptico utilizado para almacenar datos en formato digital.
CERT	Equipo de Respuesta ante Emergencias Informáticas (del inglés Computer Emergency Response Team), es un grupo de expertos que se encarga de evaluar el estado de seguridad global de redes y ordenadores, y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades, y ofrece información que ayude a mejorar la seguridad de estos sistemas.
CCN	Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (CNI).
Ciberactivista	Activista social o político que desarrolla su actividad en el ciberespacio.
Ciberbullying	Acoso virtual o ciberacoso, es el uso de información y medios de comunicación digitales para acosar a un individuo, mediante ataques

	personales, divulgación de información confidencial o falsa, entre otros medios.
Ciberespacio	Conjunto de todos los objetos e identidades que existen conectados por cualquier medio a una red informática mundial.
Ciberincidente	Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.
CISO	Chief Information Security Officer, Responsable de Seguridad de la Información.
Cracker	Acrónimo de “crack” (“romper” en inglés) y “hacker”, persona que viola la seguridad de un sistema informático y toma el control de éste provocando un daño: obtiene información protegida, borra datos, etc. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.
Crack	Software que realiza una modificación permanente o temporal sobre otro, o en su código, para obviar una limitación o candado impuesto a propósito por el programador original.
Creepware	Spyware que permite a los hackers, los depredadores en línea y los cibercriminales espiar el ordenador personal, tableta, ordenador portátil, smartphone u otro dispositivo (como un dispositivo IoT) de la víctima, que esté conectado a internet, y que por lo general dispone de una cámara web y un micrófono.
Data mining	Minería de datos. Procesos informáticos basados en la Teoría de la complejidad computacional que intentan descubrir patrones en grandes volúmenes de conjuntos de datos utilizando técnicas de inteligencia artificial, aprendizaje automático, estadística y sistemas de bases de datos.
Deep Web	También llamada Hidden Web, es la web profunda u oculta, no accesible a través de navegadores convencionales. Usualmente, se utilizan herramientas como TOR (The Onion Router) para acceder a ella.
DGSE	Direction Générale de la Securité Extérieure, del gobierno francés, con sede en París.

DNS	Domain Name Service, o Servidor de Nombres de Dominio, se encarga de realizar la traducción de un nombre de dominio a su IP.
DoS/DDoS	Ataque de Denegación de Servicio (del inglés Denial of Service), consiste en provocar en el sistema atacado la pérdida de la conectividad por consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos del sistema, lo que lleva a que un servicio o recurso sea inaccesible a los usuarios legítimos del sistema. Generalmente este tipo de ataques se ejecutan coordinadamente desde una red zombi o botnet, en ese caso se denominan ataques DoS Distribuidos, o DDoS. Cuando el sistema fracasa y se bloquea, un hacker puede llegar a tomar el control del sistema.
Domótica	Del latín domus (hogar), y automática. Conjunto de sistemas capaces de automatizar una vivienda, aportando servicios de gestión energética, seguridad, bienestar y comunicación, e integrados por medio de redes de comunicación interiores y exteriores, que permiten una gestión remota.
ELINT	Inteligencia electrónica (del inglés ELectronic INTelligence), o adquisición de información por medios electrónicos.
Encriptado	Procedimiento de cifrado o codificado destinado a alterar la representación de la información con el fin de hacerla ininteligible a receptores no autorizados.
ENFOPOL	Enforcement Police, o Refuerzo para la Policia, es un conjunto de requisitos técnicos elaborados a partir de 1995 por los Ministerios de Interior de los estados miembros de la UE, para que las operadoras de telefonía adecuasen sus sistemas, ante eventuales demandas de intervención de las comunicaciones telefónicas, internet, comunicaciones móviles u otras formas de comunicación.
ENS	Esquema Nacional de Seguridad.
EW	Guerra electrónica (del inglés Electronic Warfare), consiste en una actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso hostil de todos los espectros de energía, por ejemplo el electromagnético, por parte del adversario y a la vez conservar la utilización de dicho espectro en beneficio propio.
Exploit	Fragmento de software, datos, o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo (del inglés to exploit, explotar o aprovechar).

Fake	Literalmente “falso”. Se refiere a cualquier falsificación, una noticia falsa que se hace circular por internet, una falsificación de un site o parte de su información, etc.
Fingerprinting	También conocido como OS fingerprinting o TCP/IP stack fingerprinting. Técnica por la que se obtiene información del Sistema Operativo que ejecuta una máquina remota conectada a internet, y sus parámetros de configuración.
Firmware	Código que establece la lógica de más bajo nivel en un dispositivo. Está fuertemente integrado con la electrónica siendo el software que tiene directa interacción con el hardware.
Five Eyes	Five Eyes Intelligence Community, nombre con el que se conoce oficiosamente a los estados del acuerdo UKUSA. La comunidad de inteligencia ampliada a otros estados europeos ha recibido el nombre de Nine Eyes ó Fourteen Eyes, conforme ha ido creciendo.
Fuerza bruta	Obtención de las credenciales de acceso a un sistema por cualquier método que no implique el desencriptado de las claves: ingeniería social, técnicas de diccionario, uso de claves maestras, etc.
GCHQ	Gobernment Comunications Headquarters, Cuartel General de Comunicaciones, dependiente del Foreign Office del gobierno británico, y con sede en Blechley Park, Londres.
GPRS	General Packet Radio Service, o servicio general de paquetes vía radio, es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications, o GSM) para la transmisión de datos mediante conmutación de paquetes.
Grayware	Programa y fichero que no está infectado y que no es malicioso de una manera obvia, pero que puede ser molesto o incluso perjudicial para el usuario (por ejemplo, herramientas de hacking, accessware, spyware, adware, dialers y bromas).
Grooming	Textualmente “acicalar”. Conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él.

Guías STIC	Conjunto de normas desarrolladas por el CCN para la implementación del ENS (CCN-STIC-800) siendo de aplicación para las AA.PP. y teniendo como objeto la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.
Gusano	También llamado iWorm, es un malware capaz de replicarse a sí mismo, a diferencia de los virus, que requieren la intervención humana para infectar a otros sistemas.
Hacker	En su acepción más extendida, se denomina en los ambientes de seguridad informática a las personas que realizan entradas no autorizadas a los sistemas utilizando redes de comunicaciones. Esta acepción es la recogida por la RAE, aunque muy cuestionada desde la cultura hacker, que reivindica una acepción más ética, y distingue al cracker, que sería el cibercriminal, del hacker, que identifica a personas con talento y conocimiento en el mundo de los sistemas y su programación, las comunicaciones y su seguridad, y que promueven la idea de que toda información debe ser libre. Aquí se consideran ambas acepciones.
HackLab	Lugar físico donde gente con intereses en nuevas tecnologías, y artes digitales o electrónicas se puede conocer, socializar y colaborar. Suele utilizarse software libre y un sistema de organización y aprendizaje cooperativo, con una importante componente ideológica.
Hackmeetings	Reuniones organizadas por hackers para promover la colaboración, y el intercambio de información y experiencias. Pueden tener carácter local, nacional e incluso internacional.
Hacktivismo	Acrónimo de hacker y activismo. Utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Se conoce también como desobediencia civil electrónica.
Hosting	Servicio externalizado de alojamiento de información o de un site (web hosting).
H/P/A/V/C	Hacking/Phreaking/Anarchy/Virus/Cracking, término utilizado por los hackers para identificar zonas de descarga y foros de intercambio de herramientas.
ICBM	Misil balístico intercontinental (del inglés InterContinental Balistic Missile). Este tipo de armamento de destrucción masiva y de largo alcance equipa varias cabezas nucleares y pueden ser programados para atacar varios objetivos.

IDE	Iniciativa de Defensa Estratégica, conocida también por sus siglas en inglés (SDI, Strategic Defense Initiative), o popularmente como "Guerra de las Galaxias", consistió en una carrera armamentista promovida por la administración del Presidente norteamericano Ronald Reagan, conducente a la producción de armamento defensivo en superficie y en órbita, con el que poder interceptar misiles ICBM e el aire, antes de que alcanzasen sus objetivos.
INAP	Instituto Nacional de Administración Pública, es el organismo promotor de la formación contínua para el personal de las AA.PP.
INCIBE	Instituto Nacional de Ciberseguridad. Antiguo INTECO.
IoT	Internet de las cosas (del ingles, Internet of Things). Término que se refiere a la interconexión de objetos cotidianos con internet.
IP	Protocolo de Internet. Se refiere también a la dirección única que identifica a un dispositivo en Internet (dirección IP).
IRC	Internet Relay Chat, es un protocolo de comunicación en tiempo real, creado por Jarkko Oikarinen, que no requiere que el usuario inicie sesión o habilite la comunicación con otros usuarios, como con la mensajería instantánea. La comunicación es abierta a través de canales, en los que puede participar cualquier usuario desde una aplicación cliente (IRCd, o IRC daemon), que los gestiona.
JED	Jam Echelon Day, o Día del atasco de Echelon. Campaña propuesta por los hacktivistas a través de internet para provocar un bloqueo de los sistemas de la red de cibervigilancia ECHELON.
LOPD	Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
LOPJ	Ley Orgánica 6/1985 del Poder Judicial.
LEC ó LECrim	Ley de Enjuiciamiento Criminal.
Lulz	Derivación de LOL (Laugh out loud), y su contracción en una mala y chistosa ortografía con lust (lujuria). Es un término usado generalmente por los trolls, que identifica sus bromas de mal gusto, y cuya motivación es divertirse desestabilizando emocionalmente a sus víctimas ("for the lulz").
MAC	

MAD	Destrucción mutua asegurada (del inglés Mutual Assured Destruction), concepto utilizado en la creación de estrategias de respuesta ante un ataque nuclear durante la Guerra Fría.
Madware	Adware móvil, en un juego de palabras con mad (loco). Técnicas agresivas para colocar publicidad en los álbumes de fotos de un dispositivo móvil o en las entradas de la agenda, con el objeto de insertar mensajes en la barra de notificaciones. El madware puede llegar incluso a reemplazar un tono de llamada con un anuncio.
MAGERIT	Metodología de Análisis y Gestión de Riesgos en el ámbito de las IT (Information Technologies), elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las AA.PP. En su versión 3 el CERT del CCN la ofrece con la herramienta PILAR. Magerit etimológicamente es Madrid en castellano antiguo (del Magrit árabe).
Malware	Cualquier programa o fichero diseñado para provocar un daño. Incluye virus, gusanos, troyanos, exploits, etc.
MIM	Ataque Man-in-the-Middle, MiM, MitM, de intermediario o JANUS (dios romano de dos caras). Técnica de hacking consistente en proporcionar credenciales falsificadas al sistema atacado para que se comunique con el atacante como si lo hiciera con un sistema de confianza, interponiéndose en las comunicaciones sin que la víctima pueda apreciarlo.
Netstrike	Manifestación o sentada virtual, consiste en una acción de protesta en internet conducente a bloquear una web o un servicio electrónico. Se diferencia de un ataque DDoS en que los usuarios acceden conscientemente y en masa a los servicios de una web como harían ante una oficina real para colapsarla.
Nick	Abreviatura, alias o seudónimo (del inglés nickname) utilizado en Internet para identificar a una persona de modo alternativo a su nombre propio. En inglés se utiliza el acrónimo AKA (also known as, también conocido como) cuando el nick acompaña al nombre real.
NSA	National Security Agency, o Agencia de Seguridad Nacional del gobierno de los EE.UU., con sede en Fort Meade, Maryland.
OSEMINTI	Infraestructura de inteligencia semántica operacional. Sistema de la Agencia Europea de Defensa capaz de construir en tiempo real una representación

	semántica de un conjunto heterogéneo de informaciones, con objeto de ayudar a tomar decisiones en situaciones complejas.
Payload	Parte del código de un malware que provoca los efectos maliciosos.
PDA	Asistente digital personal (del inglés Personal Digital Assistant), originalmente se trataba de dispositivos de bolsillo con funciones de agenda electrónica, actualmente son teléfonos móviles inteligentes.
PILAR	
Pharming	Ataque informático que consiste en modificar o sustituir el archivo DNS cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria), de manera que en el momento en el que el usuario escribe su nombre de dominio en la barra de direcciones de su navegador, se le redirige automáticamente a una dirección IP ilegítima, donde se aloja una web falsa que suplantará la identidad de la entidad, obteniéndose de forma ilícita las claves de acceso de las víctimas.
Phishing	Técnica de suplantación de identidad para la obtención de forma fraudulenta de las credenciales de acceso a un sistema informático u otra información confidencial de las víctimas, mediante la que el phisher (pescador) se hace pasar por una persona o empresa de confianza en una aparente comunicación, generalmente por correo electrónico. El término phishing posiblemente deriva de password fishing (pesca de contraseñas). Cuando el procedimiento es muy dirigido a un usuario o un perfil de usuarios concretos, hablamos de spear phishing (pesca con arpón).
Phreaking	Acrónimo de phone break hacking, o hacking de las redes de telefonía.
Profiling	En criminología, obtención del perfil de un criminal a partir de indicios físicos y psicologicos. En ingeniería del software generalmente se refiere al análisis del rendimiento de un sistema.
Proxy	En una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor, lo que permite implementar una serie de funcionalidades: control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, mejorar el rendimiento, mantener el anonimato, proporcionar Caché web, etc

PSP	President's Surveillance Program, o Programa Presidencial de Vigilancia, estrategia aprobada en 2001 por el Presidente George Bush para dar cobertura legal a las actividades de cibervigilancia desarrolladas por los servicios secretos norteamericanos. El programa estuvo en vigor hasta 2007, en que se aprobó la ley PAA (Protect America Act).
RAT	Remote Access Tool, o herramientas de acceso remoto. Software que permite a un operador controlar a distancia un sistema. Las herramientas de acceso remoto tienen usos perfectamente legales, para administración remota o soporte técnico, pero puede asociarse a usos maliciosos, en estos casos el código puede instalarse usando un troyano.
RD	RD, Real Decreto. Norma jurídica con rango de reglamento que emana del poder ejecutivo. Se diferencia del RDL, o Real Decreto Ley, en que no precisa de validación por parte del poder legislativo.
Redes sociales	Medio de comunicación social que se centra en establecer un contacto con otras personas por medio de la Internet. Están conformadas por un conjunto de servicios, equipos y programas y sobre todo por personas que comparten alguna relación, en donde mantienen intereses y actividades en común, o se encuentran interesados en explorar los intereses y las actividades de otros usuarios.
Resiliencia	Capacidad de un sistema para anticiparse, proteger su integridad, defender su uso, resistir, recuperarse y evolucionar ante una crisis o un ciberataque.
RLOPD	Reglamento que desarrolla la LOPD.
Rootkit	Malware que otorga privilegios de acceso y administración a una computadora manteniendo su presencia oculta al control de los administradores (root) al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.
SALT	Acuerdo para la limitación de armamento estratégico (del inglés Strategic Arms Limitation Talks).
SCADA	Sistema de Supervisión, Control y Adquisición de Datos (del inglés Supervisory Control And Data Acquisition), software que permite controlar y supervisar procesos industriales a distancia.

Script kiddies	Término que hace referencia a personas con escasa habilidad técnica, sociabilidad o madurez, que utilizan scripts, programas o técnicas de otros hackers.
SGAE	Sociedad General de Autores de España.
Shareware	Modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales, hasta que adquiera una licencia de uso completo.
SIGINT	Inteligencia de Señales (del inglés SIGnal INTeligence), comprende el conjunto de técnicas de intercepción e interpretación de señales electromagnéticas.
Site	Website, ó web. Conjunto de páginas de un dominio que ofrecen servicios en Internet a través de protocolos http o https.
SITEL	Sistema Integral de Intercepción de las Comunicaciones Electrónicas, del Ministerio del Interior español, operado conjuntamente por la Policía Nacional, la Guardia Civil y el Servicio de Vigilancia Aduanera, y compartido cn el CNI.
Smart	Prefijo que identifica dispositivos inteligentes conectados a Internet, de forma que pueden acceder a servicios y suministrar información que permita una configuración personalizada que proporcione más comodidad y usabilidad al usuario, tales como SmartPhones, SmartTVs, smarthubs, etc.
Sniffer	Analizador de paquetes, es un programa de captura de las tramas de datos transmitidas en una red de ordenadores.
SOAP	Simple Object Access Protocol. Es un protocolo para acceso a servicios web que define como dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML (eXtensible Markup Language).
SOPA	Stop Online Piracy Act, también conocida como Ley H.R. 3261. Iniciativa legislativa norteamericana para luchar contra la piratería en internet.
SQL	Lenguaje de consulta estructurado (del inglés Structured Query Language), es un lenguaje declarativo de acceso a bases de datos relacionales.

SQL Injection	Inyección SQL, método de hacking que se vale de una vulnerabilidad en el nivel de validación de las entradas para realizar operaciones sobre una base de datos. Un incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene o genera código SQL, puede provocar que se infiltre código malicioso en el sistema.
Spam	Término que identifica a los envíos masivos por medios tecnológicos de mensajes no deseados, generalmente de contenido publicitario, y que perjudica de una o varias maneras al receptor, saturando su cuenta, restringiendo el ancho de banda o actuando como vector de entrada de malware. Se conoce también como correo basura. Al responsable de generar spam se le conoce como spammer.
Spoofing	Técnica de hacking por la que un atacante de un sistema informático conectado en red se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación. En función de la tecnología utilizada se habla de IP spoofing (el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se refiere a cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.
SSEUR	SIGINT Seniors Europe, comunidad de inteligencia formada por los estados europeos con programas y capacidades de cibervigilancia.
STOA	Scientific and Technological Options Assessment, es el servicio encargado de la realización de estudios e informes técnicos para la Dirección General de Estudios del Parlamento Europeo.
SWIFT	Society for Worldwide Interbank Financial Telecommunications, organismo que gestiona la red de comunicaciones interbancarias que permiten las transacciones internacionales.
Switch	Dispositivo de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los gateways, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.
Sysop	Acrónimo de System Operator. Responsable de la gestión de un sistema BBS, sería el equivalente actual del sysadmin (System Administrator), o el webmaster (gestor de un sitio web).

TIA	Total Information Awareness. Programa del gobierno de los EE.UU. basado en el concepto de la actuación policial predictiva. El objetivo de TIA era reunir información detallada acerca de las personas con el fin de anticipar y prevenir los delitos. El programa fue suspendido por el Congreso norteamericano en 2003.
TIC	Tecnologías de la Información y las Comunicaciones.
Troyano	O Caballo de Troya (por la Odisea de Homero), es cualquier malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
UKUSA	Acuerdo de seguridad del que participan los servicios secretos de EE.UU., Reino Unido, Canada, Australia y Nueva Zelanda.
UMTS	Universal Mobile Telecommunications System, o Sistema universal de telecomunicaciones móviles, es una de las tecnologías usadas por los teléfonos móviles de tercera generación (3G).
Virus	Malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.
VPN	Red Privada Virtual (del inglés Virtual Private Network).
Vulnerabilidad	En el ámbito de la informática y la tecnología en general, se emplea para referirse a todos los puntos débiles y condiciones de funcionamiento no contempladas en la programación, que se considera que tiene un sistema determinado y que pueden hacer que sea susceptible de fracasar en sus cometidos o ser atacado por malware de diversa tipología.
Waterholing	Literalmente abrevadero. Técnica de hacking que consiste en infectar a la víctima proporcionándole el malware desde websites de su confianza que puedan ser vulnerables al ataque del hacker.
Web	Término que identifica tanto a la World Wide Web (WWW) o red informática mundial, como a una cualquiera de las páginas asociadas a un dominio, o websites, que la conforman y ofrecen servicios en Internet a través de protocolos http y https.
Webcam	Acrónimo de web y cámara. Cámara de video con conexión a internet.

WiFi	Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica basados en el estándar IEEE 802.11.
XSS	Cross Site Scripting, o Secuencia de comandos en sitios cruzados, es un estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada. Suele utilizarse junto con CSRF (Cross-Site Request Forguery, o falsificación de petición en sitios cruzados) y SQL Injection (inyección SQL).
Zero-Day	Vulnerabilidades o ataque de día 0, 0-Day, ó Zero-Day, es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de malware gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas por el fabricante del producto. Se considera el método de ataque más peligroso.