Universidad Politécnica de Valencia

Resumen

Escuela Técnica Superior de Ingeniería Informática
Departamento de Informática de Sistemas y Computadores

Doctor en Filosofía
Ingeniería Informática

Modelado de Actores Hostiles Avanzados: caracterización, categorización y detección

Antonio Villalón Huerta

La información y los sistemas que la tratan son un activo a proteger para personas, organizaciones e incluso países enteros. Nuestra dependencia en las tecnologías de la información es cada día mayor, por lo que su seguridad es clave para nuestro bienestar. Los beneficios que estas tecnologías nos proporcionan son incuestionables, pero su uso también introduce riesgos que ligados a nuestra creciente dependencia de las mismas es necesario mitigar. Los actores hostiles avanzados se categorizan principalmente en grupos criminales que buscan un beneficio económico y en países cuyo objetivo es obtener superioridad en ámbitos estratégicos como el comercial o el militar. Estos actores explotan las tecnologías, y en particular el ciberespacio, para lograr sus objetivos.

La presente tesis doctoral realiza aportaciones significativas a la caracterización de los actores hostiles avanzados y a la detección de sus actividades. El análisis de sus características es básico no sólo para conocer a estos actores y sus operaciones, sino para facilitar el despliegue de contramedidas que incrementen nuestra seguridad. La detección de dichas operaciones es el primer paso necesario para neutralizarlas, y por tanto para minimizar su impacto.

En el ámbito de la caracterización, este trabajo profundiza en el análisis de las tácticas y técnicas de los actores. Dicho análisis siempre es necesario para una correcta detección de las actividades hostiles en el ciberespacio, pero en el caso de los actores avanzados, desde grupos criminales hasta estados, es obligatorio: sus actividades son sigilosas, ya que el éxito de las mismas se basa, en la mayor parte de casos, en no ser detectados por la víctima.

En el ámbito de la detección, este trabajo identifica y justifica los requisitos clave para poder establecer una capacidad adecuada frente a los actores hostiles

avanzados. Adicionalmente, proporciona las tácticas que deben ser implementadas en los Centros de Operaciones de Seguridad para optimizar sus capacidades de detección y respuesta. Debemos destacar que estas tácticas, estructuradas en forma de *kill–chain*, permiten no sólo dicha optimización, sino también una aproximación homogénea y estructurada común para todos los centros defensivos.

En mi opinión, una de las bases de mi trabajo debe ser la aplicabilidad de los resultados. Por este motivo, el análisis de tácticas y técnicas de los actores de la amenaza está alineado con el principal marco de trabajo público para dicho análisis, MITRE ATT&CK. Los resultados y propuestas de esta investigación pueden ser directamente incluidos en dicho marco, mejorando así la caracterización de los actores hostiles y de sus actividades en el ciberespacio. Adicionalmente, las propuestas para mejorar la detección de dichas actividades son de aplicación directa tanto en los Centros de Operaciones de Seguridad actuales como en las tecnologías de detección más comunes en la industria. De esta forma, este trabajo mejora de forma significativa las capacidades de análisis y detección actuales, y por tanto mejora a su vez la neutralización de operaciones hostiles. Estas capacidades incrementan la seguridad global de todo tipo de organizaciones y, en definitiva, de nuestra sociedad.