_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNWANTED SOFTWARE

Francisco José Sabater Estellés

Supervising Professor: Jaroslav Burčík

Supervising Professor on UPV: Antonio León Fernández

Czech Technical University, Faculty of Electrical Engineering

Course 2016/2017

ČVUT ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Prague, 12th of June 2017

Abstract

The objective of this work will be to know the evolution of malicious software over the years. Also make a detailed analysis of how these software work and have an idea of what their attack vectors are, and secondly, to know the solutions that have been applied and that have been carried out in order to get rid of the software successfully.

In the following Bachelor's Thesis, the main theme are the malwares, which are an unwanted software and malicious infection that affects the computer and takes information about the user. Malware is a general term which refers to all types of virus, trojans, worms, spyware, scareware and more unwanted software.

Acknowledgements

I want to thank to several persons and entities their collaboration in the elaboration of this bachelor thesis. First of all, I want to thank Czech Technical University in Prague, the department of Electrical and Mechanical Engineering for making it possible, providing me with the necessary tools to make the thesis. Thanks to my supervisor Jaroslav Burčík for accepting me to work with him and help me every time I had doubts. Thanks to my family for giving me the opportunity of living abroad for 6 months and supporting me in the mental and economic aspects. Finally, thanks to all the friends who have helped me during my Erasmus when sometimes you can feel alone.

Table of Contents

Introduction 6
Objectives 8
Infection 9
How Cyber Attacks Occur 9
What Cyber Attacks Look Like 10
Understanding Cyber Threats 10
Marketing 11
Methods of malware infection 13
Protection 16
How to Protect From Cyber Attacks 16
How to Scan a Computer Correctly 17
How to Get Rid of Persistent Malware 17
How to Remove a Virus When The Computer Won't Work 18
New Cyber security Threats 19
Development 20
Conclusions 26
References 31

Introduction

Malware, is a term for any sort of software designed with malicious intent, and it is a combination of the words malicious and software. It is sometimes called badware too, and is usually used synonymously with many of the common types of malware, listed below. And in legal documents, the malware term is often referred to as computer contamination. So as we can see, there are multiple ways to define malicious software, and then we will deepen in the subject and see a list of all the common types and their definitions.

That aim of a malware is often theft your private information or the creation of a backdoor to a computer so someone can gain access to it without permission. However, software that does *anything* that it didn't tell the owner it was going to do could be considered malware.

Usually, the intentions of the software creator is why that software is considered a malware, instead of its functions. In recent years, the creation of malware is increasing due to its rapid proliferation and the amount of money that is achieved thanks to these malicious software. At first malware were created as a joke or mockery, but today are used for vandalism and for the benefit of the creator.

There are several factors that make computers weaker against a malware attack. Among these defects are the design of the operating system, having all the computers in a network that run the same operating system, granting users many permissions or just by using the Windows operating system, which because of its popularity, programmers create more malware for this OS.

The reasons why our computer can be infected are several. It is quite common to happen accidentally when downloading a corrupted file with malware. Some malware also gets on our computers because of vulnerabilities in this and in the software it owns.

Another method of infection is that when downloading a file, such as a song, an image or a video, this is actually an executable that installs malware. But most of the time malware is introduced by ourselves because we do not look at what we are installing, and inadvertently install plug-ins that infect our computer.

The malwares includes all types of virus, trojans, worms, spyware, scareware and more unwanted software. There are a lot of differences between these unwanted software, each one have a purpose and a an attack vector.

In first place, the viruses, which commonly are confused with the big term malware, are a malicious infection that makes copies of themselves and travel between computers trough shared or copied files. These type of malwares are designed for make the computer useless and inoperable, and their attack erase and corrupt our computers, what means that destroy it.

Then we have the trojans, which name come from the "Trojan Horse", a horse that was supposed to be a gift of peace, but inside of it there were soldiers that attacked from the inside. That's the way how a trojan act in a computer, it attack the computer while the user thinks it is making another function. It carries a malicious code which creates a back door from where your computer can be controlled remotely.

The worms are other kind of malware that attack the net. They act on a network sending copies of themselves to other computers, using security holes to travel from one host to another host. They do it automatically propagating by the hosts that have the computer in the network.

The crimeware are a growing problem nowadays, this type of unwanted software is designed to access to users' computers and then steal funds from their accounts and complete unauthorized transactions that benefit the creator of this malware.

Finally, we can talk about the spywares and the scarewares. The spywares are malwares that collect information without the user knowing, and send this information to the creator of the malware. The purpose of this is not to destroy or make the computer unusable, but to obtain our information for their benefit. And then the scarewares, which are very young malwares, and they work warning you that you have been infected and forcing you to pay to free your computer of this infection. The handle is received by the creator of the scareware, and the user does not receive any solution.

As for ways to remove malware from our computer, removing the cases of the most powerful infections, most can be removed by a few steps to follow, although there are some that require a little more effort to be able to completely eliminate them from our computer. There are plenty of paths to do this. One of the simplest methods is just to access the control panel and uninstall the program containing the virus, in case we know what program it is.

There are other viruses that are not so easy to remove from the system, as rogue registry keys and unique files that can only be deleted manually. For these cases the best method is to use antimalware or specialized programs to perform these tasks.

As far as we are concerned with the protection of our computer against malware, the most effective method is to take precautions while being cautious at the time of downloading files, entering web pages, etc ...

The first step we should take to properly protect our computer would be to have an antivirus / antimalware program installed, and have it updated and configured for monitoring the sites that we visited and the files we download in search of a possible virus that can infect us and in this way cause damage to our computer.

Objectives

In this work what we want to achieve is to know better how malwares and also antivirus work. Everyone today knows the terms of malware and antivirus, with this work we can discover how they act and therefore, we can know better what to do if we face an infection, being able to repel this attack thanks to the use of antivirus, or simply remove this threat manually with our knowledge.

We will also focus on the history of such malware and antivirus. We will start from the beginning, when the first virus appeared. We will see how little by little the issue of infections to computers and computer networks worried many and for this reason appeared the first antivirus, which were also becoming obsolete by the advance of the complexity of viruses, as it also happens today.

In this work we will also see how has evolved the use of viruses, from being simple bugs or errors in some script of the program, to be totally intentional and with a specific purpose, either to create chaos, to steal information or to protest for something against which the creator disagreed.

We will be able to verify that the cybercrime is already integrated as if it were another sector of the IT industries. Institutions pay malware coders to write malicious code and thus use it to their advantage, harming or not, to other institutions. Within these malware coders, we have several types. There are hackers, who sell their services, spammers who use vulnerabilities in networks to fill the network of bulk emails. There are also those who steal the identities of people in order to access restricted sites that cannot be accessed by anyone.

To be able to protect yourself from these cases, the first thing to do is to have an antivirus that works in real time installed and working. You also need a malware removal program installed, and in addition to this, an emergency malware removal rescue boot disc / thumb drive.

The final objective is to give a conclusion about everything we are going to be talking about in this work. In this conclusion a detailed review of the history of malware and antivirus will be made, highlighting the occurrences of the most important viruses, the creation of new types of viruses, the effect they had worldwide, the way in which they could be dealt with viruses, and also the legal measures taken on its creators.

Infection

How Cyber Attacks Occur

Knowing when you are infected is very important, and so is understanding how cyber attacks act is essential part to be able to combat these attacks and know that to deal with one of them.

Most attacks are a combination of semantic tactics used syntactically or, in simpler terms, an attempt to change a computer user's behavior through some computer tactics. For example, phishing emails or cyber attack software, such as viruses and worms, are used to trick the user into providing information or downloading some kind of file that ends up being a code that infiltrates the computer and steals information from this. All this just mentioned, can be described as cyber attack.

When your anti-malware software finds a virus on your computer, this may be new malware. Your anti-virus software, using the methods for which it is programmed, it scans the computer and checks that it has eliminated any trace of malware. Being a new virus is updated to be more difficult to detect and even to be able to avoid being eliminated by any of the anti-virus software that they have in the market at that time. This infection is called persistent malware infection. As we mentioned before, these types of malware get that perseverance by hiding on computer and hard drive sites that may be inaccessible to the operating system, and thus prevent anti-virus software scanners from detect them.

In order to deal with persistent malware infection, there are some things we can take into account in order to be prepared to deal with this infection.

The first thing to do is to make sure that the anti-virus software that has the computer has the latest version installed, and that it is updated and running every few minutes to be able to detect any kind of malware. It is also important that we perform a full system scan, instead of performing the typical quick scan that is usually recommended every little time.

Another option is to install another anti-virus software on the computer, in order to have a second opinion in case the first anti-virus has not detected any malware and it is clear that there is some kind of malware in the computer for the fact that it is doing things outside of the normal.

And finally, and as a recommendation even if the computer that we handle is not at risk, it is always to have a back up of our most important data and files, in order to always be able to recover these documents in case the infection arrives to be serious and we cannot take control of the computer again.

What Cyber Attacks Look Like

The most common cyber attacks are those that come in a link that you can click on. It can be an email from your bank, your work, a friend, a relative, etc. By clicking on this link we are redirected to a webpage that was not what we expected is there when the infection starts. One way to avoid this is, if we know that we are at risk of an infection, place the pointer over the link that we want to access, and look at the screen in the bottom left corner of your screen. In this way we can see if the web that we are going to access is the one we hope for or is another and therefore we should be aware.

The infection can also come when you download a file that contains a malicious piece of code. These files can also be sent via e-mail, but they can also attack when downloading movies, books, music, applications, etc ... which are free. Hackers use these files, since people usually look for them so they do not have to pay for them. This is why the web is plagued with files uploaded by these criminals to infect as many computers as possible.

Finally, and as we mentioned above, another way to become infected is to enter a website which is programmed so that when you enter immediately infect the computer. These websites can seem very professional and even truthful, you can even browse the site perfectly and even buy or download some content, without having any idea that you are already infected.

Understanding Cyber Threats

As we can deduce from all this, one of the greatest enablers of cyber attacks is human behavior. Even the latest, strongest security can't protect you if you open the door and let the criminal in. That's why it's important to know what cyber threats are, how to spot a potential attack, and how to protect yourself.

When classifying cyber attacks, these are classified into two groups: the syntactic attacks and the semantic attacks.

Syntactic Cyber Attacks

The syntactic attacks are attacks that can manifest themselves in different types of malicious software, and that therefore can attack your computer by several channels.

The most common types of syntactic attacks are viruses, which are hooked to another program to be reproduced, and are in attachments, which on downloading activate the virus they carry with them, and it begins to replicate. Also on the other hand are the worms, which spread through the network and infect all computers in this one. They do not need to be attached to a file because they travel on the network, which is why they are more dangerous and can infect entire networks. And finally, to mention the most common malicious software syntactic attacks,

we have the trojan horses, which act in the background, while you are using a program, this may be infected by a Trojan and be acting behind your back without you not even realizing it.

Semantic Cyber Attacks

Semantic attacks are more about changing the perception or behavior of the person or organization that's being attacked. These attacks have much less to do with the use of software, but use the failures or innocence of people to be able to infect.

In this type of attacks, the most prominent are phishing attacks. These attacks are sent by creators of malicious malware to be able to get what they want from those who receive it, be it information, data, accounts, etc ... They are usually sent via e-mail, and this seems to be a normal e-mail, they can even imitate the company with which you do business or work, so it is your duty to answer or download what this e-mail contains. These phishing attacks may contain viruses, worms or trojans, but the main component is social engineering, as we said before, try to change the behavior of the person or company that receives it. This is why we can say that social engineering combines the two types of attacks, both syntactic and semantic.

On the other hand we also have the ransomware, which are malicious codes that take control of the system or the company network and ask for a ransom in exchange for a payment, in the form of information, data or simply digital money, for the network to be released . These attacks are usually directed towards companies, but can also target a specific person, if he has what cyber criminals want.

Finding a solution for these types of attacks is possible, the problem is that finding such a solution can take anywhere from hours to months. This is why, the more sophisticated attacks, reach a greater number of victims.

Marketing

Without going any further, a few months ago I was trying to get rid of malware that had affected my computer, and that no matter how many times I run the anti-virus, it could not detect it despite trying out several anti-virus and having them updated.

I started researching into the world of malware, and I was able to learn more about the intentions of hackers and malware writers. I saw, as I said before, that today's malware was not as easy to detect and remove from the computer as it was before, when you just had to activate the anti-virus, scan the computer, and get rid of the virus that infected it.

I also learned that malware creators have developed new methods of sophisticated malware such as that can be inserted into low-level drivers that load prior to your PC's operating system. Some of this malware can even be inserted into the computer's firmware, making them extremely hard to detect and remove even after completely cleaning and reloading the computer.

But, then the question came to me, what is the reason that motivates them to create all these malicious malware? I researched more deeply on these issues, and discovered that the motive was money and greed.

It is a new type of economy, the economy of the modern age, and is based on hackers and malware creators being paid to infect computers and networks. Once they have infected the network, they sell the use and control of it, and the buyers order what they have to do with them. Most commonly, networks and computers are used to attack the system, to damage or steal the information they contain, to extort for a rescue or even more.

Cyber criminals have marketing programs that give money to anyone who wants to infect a computer network with their malware. As I was able to find out, by visiting Kaspersky's Securelist, hackers and malware creators would pay between $ 250 and $ 500 for a thousand computers that have their malware installed and ready to run.

Each customer who joins this marketing campaign receives an identifying number that is linked to the malware installed. This identification number ensures that the purchaser who installed the malware on the victim's computer receives the money for the instalation, and in this way the creator of the malware has an idea of how much he has to pay for the service performed.

It can be enormously beneficial for malware creators to carry out their marketing programs, as it is for all those who want to install that malware on computer networks.

Since all this may seem a bit confusing, I will explain it with a simple example:

A malicious malware creator, such as a fake anti-virus software, pays its affiliates of the marketing program $ 250 for installing its malware on 1000 computers. Once the malware is extended, the creator of the malware gives the solution to the users of these computers, but for this they have to pay $ 50, this way he will remove the malware and everything will return to normal. Although only a quarter of those infected will accept the offer and will end up paying that $ 50 to free their computers, the cyber ciminal would reimburse $ 12,250 after paying the affiliates.

But this can be even bigger. If the creator of the malware combines another malware with its fake anti-virus program, it will be installed when it is executed, so that he can earn more money by infiltrating the malware of another malware creator, since it has combined as we have said before its malware with that of the other cyber criminal.

And even more, the creator of malware can sell control of computers that have infected with his malware, and get more and more money from people who have an interest in the information of these computers or want to make a botnet attack.

It is for all this, so I have realized that in these times, cyber criminalism, is more linked to marketing and business. Its use is no longer limited to attacks by contrariety of ideas or pure fun, but it has been seen in this a very profitable way to withdraw money.

After finding all this information, I tried to solve the problem and I got it. And as one day one of my teachers told me "Don't bring me a problem unless you bring a solution with you", so these are the methods I used to be able to deal with the computer infection.

The first step I took was to look for a possible undetected malware infection. Seeing that the browser constantly brought me to pages that I had not authorized to access, I started applications without permission and even applications I did not know or had installed, and that did not let me perform basic functions like opening a folder, I was clear which was facing an undetected malware infection.

As we have commented in other sections of this work, it is very important not to just have the opinion of a single anti-virus, so at least what we should do is with another anti-virus other than the one we use from normal, scan the computer in case it detects the undetected malware.

Another solution is to seek help from an expert, so tell us if you know a solution for the malware that has infected us or if you can tell us how to get rid of the infection. We do not have to physically go to a store, there are also online experts who can solve the problem. Another method is to consult in forums, since someone has been able to have the same problem as us and if them have found a solution to, have it hung on the network.

And if all else fails, what you have to do is a back up of all the important information that is available, and then reinstall the operating system on the computer, and when reinstalling pass the anti-virus again to know that there is no more threat.

Methods of malware infection

To conclude this section, we will discuss the most common methods of malware infection. It is advisable to avoid doing the following actions so that you are not infected by any malicious malware.

Firstly, a very common error is browsing the web with javascript enabled by default. Today's hackers use web sites to scatter their infected files. They can make these files to be uploaded constantly using tools that work automatically and repackage the binary in an attempt to bypass signature-based scanners. The choice of the web browser is helpful in these cases. Although all web browsers are just as susceptible to a malicious malware attack, it even includes the most famous ones such as Chrome, Firefox, Opera, etc ... disabling javascript makes browsing much safer .

On the other hand, we have another common error that if we do not correct can lead to an infection of our computer, and this error is using Adobe Reader and Adobe Acrobat with default settings. Adobe Reader and Adobe Acrobat always come pre-installed on computers as a PDF viewing tool, and even if you do not use this program, only the presence of this program on your computer already puts it at risk. In fact, vulnerabilities in Adobe Reader and Adobe Acrobat are one of the most common infection vectors, so it is advisable to keep it updated to the latest version, as well as to seek what settings you must have so that it does not cause us any problem.

Another common cause of infection is clicking unsolicited links in e-mail or IM. Many malicious or infectious links are sent via e-mail and IM, so they are vector for both malware and social engineering attacks. What is recommended in these cases is to read e-mails in plain text, in this way it is possible to identify infected links. Another option is to never click on any link from an e-mail or IM that we receive without prior notice, or from an unknown sender.

We also have the threat of clicking on pop-ups that claim your computer is infected. They are called rogue scanners, badly known as scareware. What they do is to camouflage themselves as if they were an anti-virus or any other security system, and they offer protection to the users with pop-ups that emerge in the screen of many websites, saying that their computer is infected and that only clicking they can solve it. It is best to avoid clicking all kinds of pop-ups, and more if the websites are not legit.

One mistake you should never make is that of logging into an account from a link received. Never loggin to an account after being redirected to the website from a link that you have received via e-mail, IM, or social network message (such as Facebook, Whatsapp, etc ...). The best in these cases is to close the link that has redirected you to the website, and open it again with the browser, using a link with which we can be safe from data theft.

Not applying security patches for all programs is a common buckler also. If we do not update and update program patches, there are hundreds of vulnerabilities in which malicious malware can be exploited. And this is not only important in Windows patches, but in all the programs that the computer has. There is even a program that helps you to check which of the computer programs need to be patched, the Secunia Software Inspector.

One mistake we have to protect our computer is that we think that with the anti-virus that we install and that is the best according to all the recommendations we are already fully protected, but this is not so. Even the best anti-virus on the market may not detect new malware coming out day by day. So it is best to always have a second anti-virus to be able to check with the two that the computer that we are scanning is not really infected.

An error that is not already so common these days, is not to use anti-virus. Many people think that just being cautious and visiting safe sites do not have to be infected and, therefore, do not have the need to install an anti-virus on their computer. Whichever web you visit, there is always a risk of infection, and if we are not protected, this infection will not have any difficulty entering our computer.

In the same way, there are people who think that using a firewall on their computer limits and is bad for it, and all they get is that infectious malware have the doors open to enter the computer without having to overcome any barrier.

Finally, we have the error of falling for phising or other social engineering scams. What malware creators do here is often to use promises of quick wealth and sad stories that become great using their product, so that they can hook victims who fall into their net. In this case, common sense is the best way to avoid these infections.

Protection

Every day thousands and thousands of viruses are discovered. In order to find a cure against these viruses, reverse engineering is used, and this can take from 5 minutes to more than a few months of work. This is why no antivirus is fully effective. Protection against viruses requires continuous monitoring with a layered approach with multiple packages.

When a cyber attack hits our computer, it can take many forms. It can steal personal information, control the computer, request a rescue for the computer to work again, etc ... And one of the reasons why these attacks reproduce so fast is because they are often very difficult to locate and remove of the system.

How to Protect From Cyber Attacks

Many people think that with an anti-virus and a good firewall has completely protected their computer, but that is not enough. New infectious malware can overcome these barriers without any problems. So you have to follow some guidelines when it comes to protecting our computer.

One of the first things we must change to protect our computer is our behavior. In no case should we share our personal information unless we are absolutely sure that the website is totally secure. One tip for these occasions is to look at the URL of the website we are on. An unsafe site will start with http:// while a safe site will start with https://.

Never download a file or click on a link if it is not something you expect in advance. If you are waiting for the mail of someone with a file or a link and you know very well what it contains because that person who sends you is legit. Even if the e-mail comes from a trustworthy company, it is worth visiting the website in search of the offer they offer you in a link, or even calling to make sure what they send you is a veridical offer and there is no what to worry about.

Of course, an indispensable requirement to protect our computer is to keep it always updated, with the latest security patches installed. A preventive measure is to activate the automatic updates, since in this way we make sure that our computer is always going to be updated. Hackers are looking for gaps in order to infect computers with their infectious malware and one of the first things they are looking for are computers lacking security updates, which is why keeping your computer always up to date is one of the most effective methods against cyber attacks.

It is good to always have insurance, that is why every week or month we should make a backup of our personal information and most important files. When all else fails, at least we can use this backup to return to normal as soon as possible. It is best to have this back up separately from the computer, for example using an external hard drive or we now have the option of the cloud, which makes everything much easier.

How to Scan a Computer Correctly

Scanning a computer completely in search of infectious malware is often a step that people do not know how to perform well. Scanning for viruses with the anti-virus does not always solve the infection of the computer.

Many malware that infects our computer creates problems in Windows and on the same computer as blue screens, DLL crashes, crashes, unauthorized activity of the hard disk, pop-ups when opening the browser, and many other serious problems . So it is important to always scan the computer very well to know and be sure that everything works properly.

In order to scan a computer properly, we must first download and run a Microsoft Windows Malicious Software Removal Tool. This tool to scan computers will help us to find specific malware. Before using it, make sure it is updated to the latest version, since it will not do anything against the new malware. One advice to make the scanning of the computer easier is to delete the temporary files we have in it, so the scanner does not stop at files which do not need to be scanned.

Next, what we must carry out is a complete scan of our computer. We should try not to run the default scan, because then you will be excluding very important parts of your computer, so try to make sure that the configuration of your anti-virus is done to do a full scan of your computer. Especially, make sure that it includes the master boot record, boot sector, and any application that is running in memory, as they are really sensitive parts that can carry the most dangerous malware. In addition, if you have an antimalware tool, you should also run it once the scan is done, for more security of the computer.

How to Get Rid of Persistent Malware

If your computer is still infected by malware after updating the anti-virus, having a complete scan of the computer, and even having performed a scan with a second anti-virus to ensure you, there are other options you can hold . For example, using an Offline Antimalware Scanner:

Virus scanners that run at the operating system level may not often detect some types of infectious malware, as these are hidden under the operating system level. This is why it is recommended to run an Offline Antimalware Scanner.

One of the first things you should try to be able to eradicate persistent malware is to run the Windows Defender Offline scanner. This works out of Windows, so you have more chances of detecting hidden malware, which are the most persistent malware.

This scanner must be installed from a computer that is not infected, and then stored in a USB flash drive or CD / DVD. Once we have it, insert the CD / DVD or connect the USB flash drive and reboot the infected computer.

To do this we must have previously configured the computer so that it can be turned on from the USB port or from the CD / DVD, this can be done in the system bios.

Once we have started the computer following these instructions and it has been executed, we should only follow the instructions that appear on the screen for a full scan of the computer. Once the scan is complete, reboot the computer normally.

How to Remove a Virus When The Computer Won't Work

It is possible that when our computer is infected, it reaches the point of being unusable and we cannot even access the operating system. These are the most dangerous malware, since they do not allow the operating system to start, but there is still a solution for these cases.

As many malware are stored in memory, the computer can start, and it is at that moment when we must act, booting the computer into Safe Mode. in this way we will not let the virus run and we can carry out the steps to get rid of it.

The best time to remove malware is when it's in a non active state. Booting into Safe Mode is one option, but isn't always the best option. Some malware will register as the file handler for a particular file type, so any time that file type is loaded, the malware is launched first. Your best bet for thwarting these type of infectors is to create a BartPE Recovery CD and use it to access the infected system.

Infectious malware, like any other program, needs to be executed in order to get into action and start to harm the computer. Once we have entered the safe mode and accessed the infected hard disk, we can start to investigate about the startup point for signs of the infection.

Many of today's malware what they do is block the access to the Task Manager or the Folder Options menu in Windows, or it makes other system changes that hamper discovery and removal efforts. Therefore, once you have eliminated the malware that infected the computer, you will need to regain control of it, and for this you have to reset the configuration in order to gain normal access. First we will have to regain access to the registry, and then re-enable the task manager. This way we can have normal control of the computer again.

New Cyber security Threats

Talking more about the current situation, there are some predictions that some have dared to do about new infectious malware and also some advice on how to protect ourselves so that we do not get caught unawares.

First we have the watches and the wearables, such as smartwatch, Apple Watch and Fitbit. According to some media articles, the malware that they attach to these devices will be called headless-worms, and will be able to spread from device to device, which will make it spread very quickly and easily.

Next we have The Cloud. With the growth of businesses around the world, and the service they now offer through The Cloud, malware creators will soon take their sights on creating programs that aim to infect could-based infrastructure, virtual machines used in cloud computing, etc ...

On the other hand we have The Connected Home. In these times, there are no limits for hackers, since everything is connected, and therefore could hack even the houses where we live. The automotion of houses is a fact, and now internet-connected door locks, app-controlled lighting, security, temperature control, etc... are a thing of the present. Hackers will easily find a way to exploit the weaknesses in these technologies. A hacker could control our house from anywhere in the world, only finding a gap in the security of this technology.

Some advice that we are given to be protected from the new threats are, to be always up to date with regard to security, that is to say, know the risks of an infection, and therefore know how to act not to be infected, and in case we are infected also know quickly the steps to follow in order to get rid of this virus.

Another advice is of course to keep the applications of our device always updated, and have the last patch that has been released for this, in this way we ensure that the latest threats that may have been discovered are not a threat for us, since we will not have any breach of security. We will also have to do the same with our operating system, and with the device itself. It is also important that we activate the automatic updates, in this way we make sure that we do not pass any updates to have to do it manually.

And to finish, and as we have mentioned many times in this work, we are also advised to have installed an anti-virus, although we think that we do not need it, and we must scan with the anti-virus our device periodically. In addition, it is also recommended to have another anti-virus installed, in order to have a second opinion when scanning the device to search for infectious malware.

Development

It was in 1948, when Von Neumann began lecturing on the self-production of machines. In 1949 he wrote an article entitled "Theory and Organization of Complicated Automata", which presented evidence of the possibility of developing replicating programs capable of taking control of other programs with similar structure.

In 1959, a well-known mathematician named Lionel S. Penrose decided to give his opinion on the subject of automated reproduction in an article he wrote called "Self-Reproducing Machines" where he affirms that there are programs capable of reproducing, activating and attacking, supporting previous studies. It is in the same year that three programmers of the Bell Computer laboratories, Robert Thomas Morris, Douglas Mcllroy and Victor Vysottsky develop a game called CoreWar, which is inspired by Von Neumann's theory. This game is the precursor of computer viruses, and it is a battle between programs with the aim of occupying all the memory of the machine eliminating in this way the opponent.

It was not until 1972 that the first virus itself came out, which was able to infect the IBM 360 machines through an ARPANET network. This virus was named Creeper, created by Robert Thomas Morris and displayed a periodic message. To eradicate it was created a program called Reaper, which had the function of finding the virus and remove it completely from the system. This was also the origin of the current antivirus.

In 1974 appears another virus called Wabbit (making analogy to the rabbit like animal), that its function was to reproduce itself. It acted as a fork bomb, which is a denial-of-service attack, a process that continually replicates itself to deplete the system resouces, slowing down or crashing the system due to resource starvation.

The following year, in 1975, John Walker inadvertently gives birth to the first trojan in history. This is the name of Animal and it is because the software was a game that had to guess the name of an animal based on the questions asked to the users. The game routine was able to update the copies of Animal in the user's directories, each time it was executed, that's why is a trojan. Due to a programming error, the game made copies of itself in various directories of the machine. The solution to this problem was to create a version of the game that will look for previous updates and eliminate them.

In the late seventies, John Shoch and Jon Hupp, tried to give practical use to the CoreWars, creating it as a program that would handle maintenance tasks and night management, propagating through all systems. Here was created the first worm, since it spread through the network and caused huge problems, so it was decided the complete extermination of this.

Already in the decade of the eighties, the computers gain popularity and began to evolve quickly. More and more people understood computer science and wrote their own programs, which also, of course, caused the first harmful programs to be developed.

In 1981, Richard Skrenta wrote the first widely-replicated virus, the Elk Cloner. This was stored on 360 kb floppy disks and resided in the computer's memory once it was removed. This virus was innocuous for the system, but had a counter of starts and when it reached fifty the following poem was showed:

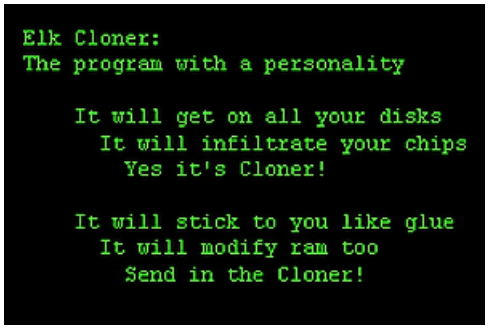

Figure1. Elk Cloner Poem

In 1986, the first epidemic of a virus compatible with IBM PCs was detected. This virus was called Brain, and was able to infect the boot zone, and was also the first stealth virus, since it was able to hide its presence. This virus was already capable of getting personal data from those who was infected. This information was provided by users, since this virus was no more than an anti-piracy experiment and was never meant to be a harmful virus. The only thing the virus did was show a line of text to contact the creators.

*Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...*

Figure2. Line of text, virus Brain.

They realized the magnitude of the epidemic when they received calls from different parts of the world demanding the cleaning of their system of said virus. In December of that year, a convention was held, where the social issue of viruses was first discussed, expressing in this convention "that its creation was mainly due to the poor social position of the programmers", and that "the problem is not viruses, but dependence on technology".

By 1987, Burger wrote a book on computer viruses. This publication gives rise to what today we call variants, since many expert programmers created their own viruses from the publication of Burguer. In this year also appears the virus Lehigh, in the university that gave name to him, being this the first one of the harmful viruses. By then, virus experts were already familiar with the ways in which the virus could not escape the site of its creation, Lehigh University.

Also that year appeared the virus Jerusalem, able to infect files that had extension .EXE and .COM. That year also appears Cascade virus, which was the first virus encrypted to be known, and infected .COM files.

In 1988, Robert Tappan Morris, a student at MIT, created the first mass-reproduction worm, which infected and collapsed 10% of ARPANET, including NASA and MIT for three

days. This program would go down in history as Morris Worm. It used the vulnerability of UNIX operating systems, taking advantage of the holes in the systems. Although some call it catastrophe, it was an alert for the computer community to realize the consequences that could have a massive attack on the network. Finally, Morris was caught and put on trial for fraud and trick, so he was convicted. Even so, the judge said that with the creation of this worm could not be accused as it acted on its own, without Morris doing anything, so the sentence was 3 years of probation, a fine and community services.

Due to the expansion of some viruses, a programmer from the UK, Dr. Alan Solomon, began disassembling them and creating detection and disinfection methods for the control of these viruses. That is why, that same year the antivirus Dr. Solomon's Ant-Virus Toolkit is launched.

In 1989, the "Bulgarian virus factory" was born, headed by Dark Avenger, a writer named Eddie. This was one of the creators of viruses with more original techniques, and its main creation is the virus that bears his name and the first to jointly exploit the stealth and polymorphic techniques that infected .COM and .EXE files. Starting this year and those who are following them were born groups of antivirus companies, who increasingly created more and more antivirus to be able to deal with viruses that could affect worldwide. As early as 1991 came, CARO (Computer Antivirus Research Organization) was created because of the evident amount of antivirus that exists, and this organization is in charge of regulating techniques for naming viruses.

With the launch of Microsoft Windows 95, the Concept virus, which infected thousands of Microsoft Word documents, was the first macro virus written in WordBasic language, affecting the platform on which it was run. The following year, the Laroux virus, was the first virus capable of infecting macros in Microsoft Excel files. Two years later the Staog and Bliss viruses, which are the first viruses for ELF files from the emerging Linux operating system, appear. Also the same year appears for the first time a macro virus capable of sending infected documents by email through MSMail, the virus ShareFun.

In 1998, a prominent virus called CIH (initials of Taiwanese student Chen Ing-Hou) appeared, which was a revenge against the incompetence of antivirus software developers. The mission of the virus was to erase the first 2048 sectors of the hard disk, overwriting some Flash-Bios, and leaving unusable the motherboard of the computer. Chen was accused by the justice and they declared him guilty, fulfilling condemnation by its creation.

In the next year, 1999, two viruses appear that were responsible that the standard of not opening a message from a stranger was kept short, as these viruses were sent by people known and therefore trusted. These viruses are the Happy trojan, which acted as a worm transmitted by MS Outlook, and which displayed a message of "Happy New Year 1999 !!" and fireworks effects. His ability lay in that he was able to send himself to each person that the user would send an email. The other virus we talked about is Melissa, who started emailing an attachment, and was sent by someone well-known. When the user opened the attachment with Word, it was automatically sent to the first 50 contacts in the user's mailing list. This made the propagation string exponential because it was sent with the name of a file that the user had on his system. Because of the capabilities of this virus and the trust of the user who sent the mail, caused it to expand with overwhelming speed and cause great economic losses. The infection by this virus of the power in software, Microsoft, and of the power in hardware, Intel, made that they united

in the fight against the cybernetic crime and that they gave with the author of the virus, David L. Smith, that was sentenced to 20 months of prison, in addition to a fine of $ 5000.

In September of that year, another rule that until then had been irrefutable fell, and was that any malware could not infect a computer by just reading an email. Bubbleboy virus, which was programmed in VBS and took advantage of the vulnerability of the Internet Explorer web browser and the Outlook Express mail client. This starts a new kind of malicious worms that have the ability to propagate via email without the need to open an attachment, and log into the system when the message is opened by the user. This worm was created by the Argentine Zulu taking advantage of the vulnerability hole that the Spanish Juan Carlos García Cuartango discovered. Microsoft solved the problem of vulnerability soon, but this worm continued to spread because users did not update their systems.

In the year 2000, a worm generator, called VBSWG (Visual Basic Script Worm Generator) gain popularity, among its most outstanding creations we can mention the Anna Kournikova virus, which came to infect NASA. Also stand out, with the appearance of the virus transmitted by messages, the love worm called LoveLetter, which arrived by email with an attachment with the subject of the message ILOVEYOU, damages that were calculated on millions of infected systems and millions of dollars lost too.

In 2001, there was the spread of worms that use combinations of vulnerabilities for their purpose. In the following year, 2002, Frethem and Bugbear, give way to packaged malware, which makes their detection by anti-virus very complex. This packaging consisted on the compression and encryption of an executable file, which made its size drastically decreased and its appearance changed. Also this year appears a virus called Benjamín, that was the first worm that reproduces by a network of interchange of files Peer-to-Peer.

Arriving to the year 2003, the Slammer worm uses vulnerabilities in the Microsoft SQL server, achieving unimaginable records of system infection in the shortest possible time. This worm infected 90% of vulnerable computers in the first 10 minutes of its propagation, doubling its propagation area every 8,5 seconds. Another worm that break records that year was Blaster, and with the excessive traffic it generated in search of vulnerable systems to infect, affected the Internet in the days of its expansion, causing a DDoS (Distributed Denial of Service) attack and collapsing it this way. It is this year also when they start to use botnets (robot network), which are multiple computers infected with remote-controlled software that allows hacker to run automated programs on the botnet. According to studies, the size of a botnet is variable, but can reach 50,000 systems controlled by a single group.

In 2004 the first viruses that are spread by mobile technology appear, which some specialists and experts in the matter were already feared. Among them are the Brador, a trojan that affects the Pocket PC devices with Windows operating system, that can communicate with the author of the malware and open a port so that it takes control of the infected device. Also Symbian devices were affected by this new trend, with trojans like Skull and Mosquito.

2005 marks the beginning of malware used as business for money, and in a very profitable way, no longer created by "entertainment". Spywares appear, distributed through spam or using other malwares to steal personal and bank information of the infected user. They act by remaining in the memory and in this way they can follow the user's browsing, so when they access to a website, the spyware can get all the data that the user introduces.

In 2006, the popularization of online games resulted in the birth of malware that was designed to obtain information about players profiles, called phising. In the same way, the first versions of Qhost, a trojan designed to modify the hosts files of any operating system, appear on the scene and it lead the users to a false web page. In 2007 the line of the previous year was continued, the malicious codes created with the aim of stealing personal information of the user to later be able to commit criminal actions against these increased notably, especially the cases of phising. Also the trojan Qhost began to spread with much more force. Also this year the old infection techniques reappear, to highlight the virus Sality, which had the characteristics of a polymorphic worm and infected the executable files that were in the victim computer and allowed access to the system in an unconventional way backdoor and it registered the information that was entered in the system by the keyboard, with capacity also to finish with some processes of the antivirus. We can also highlight the Virut virus, which had the same attack vector as the Sality virus, but also infected binary type files with .SRC and .EXE extension. Last but not least we have the Nuwar polymorphic worm, which not only formed one of the most important and harmful botnet of the year, but also used very innovative methods of tricks to propagate the malware through e-mail, one of the most used communication system. One of the methods that this virus used was to take advantage of social events or news in a way that managed to travel the media worldwide and in this way spread more and more. On the other hand, there were applications designed to install on servers and exploit vulnerabilities in systems, such as Mpack. By installing these applications on web servers, through modifications, users are able to download malware onto their computers every time they visit the affected page. Note that these packages are not malware, but are programs with a certain amount of scripts and exploits installed on the web servers, with which they can exploit the vulnerabilities of the user's systems, and with this that the desired malware is downloaded in the equipment concerned. Finally, this same year, increased the use of instant messaging such as MSN Messenger, AOL Instant Messenger or Yahoo! Messenger among others, was an important focus for increasing the spread of malware.

In 2008, the phenomenon of social networks such as Facebook, Twitter or MySpace, which had more and more users and became more popular, did not go unnoticed, so the first malicious code soon became visible and tried to exploit these social networks. But then they were not only trying to extract information from users, but also tried to reach the most unprepared users with fake profiles and displaying all kinds of advertising, a phenomenon called splog. Also with the widespread increase of the storage devices that were connected through the USB port, as they can be PenDrivers, it creates a channel of attack very exploited by the malware, through an autorun.inf file, that executes automatically when connecting the device to the computer and that is spread throughout this. These types of attacks are called INF / Autorun.

In 2009, it is assumed that the tendency of malware is to use the Internet as the main platform of attack, and also use it to get economic rewards through malicious code. The crimes that were committed were of greater magnitud and proper to the cyber crime. It was called Crimeware to malicious codes that have a financial purpose. Also this year, botnet networks continued to proliferate, with the use of management packs becoming more widespread, and the media also continued to be a very effective strategy for spreading malicious code. Several campaigns of false application installers were initiated, which were carried out using SMS Scam, where the user was charged a text message to install an application, and in many cases were false. Attacks on social networks also continued to grow during this year, the Koobface worm spread through Facebook earlier this year, and later attacked twitter.

The following years until now have continued with the same dynamics, in addition to the growth experienced in the smartphone market, since at the beginning phones only fulfilled

basic functions such as calls and text messages, but now have been turned into mobile computers and their characteristics are increasingly sought after by cyber criminals. This are the reasons of the expansion of crimeware and computer crime today. Also mention the DDoS attacks, which are very frequent lately, and the objective of these is to interrupt a service temporarily or indefinitely, all for reasons of the computer warfare that we suffer today.

Conclusions

In this section of the work we will draw conclusions about what was discussed in the previous point, that is, we will analyze how malwares have evolved over time to the present, focusing on the events that have been most relevant to evolution and how malware has evolved. We will also analyze the operation of these malwares to know better how they work and what is their attack vector in each case.

It all starts with research on the replication of programs that have the ability to take over other programs of the same structure. With this research, it was not expected to create what we now know as malware, but was a way to advance in technology and an area that Von Neumann was interested and tried in his article "Theory and Organization of Complicated Automata" . This article also called the interest of many, who continued with the research to be able to expand this field and that will come to have a utility in the future.

With all this, thanks to Neumann, and the researches also carried out by other experts in the field such as the mathematician Lionel S. Penrose, who also wrote an article entitled "Self-Reproducing Machines", confirming the existence of programs capable of self-reproduced by supporting previous studies, some programmers began to consider reproducing these studies. And so did Robert Thomas Morris, Douglas Mcllroy and Victor Vysottsky, creating a game called CoreWar, which was inspired by Neumann's theory. Without knowing it, they had created what would later become the forerunner of viruses.

CoreWar was based on a game where it was a battle between programs, in order that one of them occupied all the memory of the computer and in this way eliminated its opponent.

As we can see, the history of malware does not begin with bad intentions, but it was following investigations of a theory with the intention to discover more about the technology and to continue advancing with methods that were not known.

It was a few years later, in 1972 when the first virus as such was created, and the name it received was Creeper, its creator was Robert Thomas Morris, and the virus display a message periodically on the screen, which was the following:

Figure3. Creeper Message

This is the first virus that was created for the purpose of infecting a system as such, and was not programmed as a result of unconsciousness of what was being done. Virus itself cannot be called malicious software, due to the fact that it had no impact on the data of the systems it infected, but only displayed on the screen the message mentioned above.

Not many years later, in 1975, appears what we can call the first trojan in history, although it was created in an unintentional way. Jonh Walker, an expert programmer, created a game called Animal, the software of which tried to guess the name of an animal based on the questions that were asked to the users who executed it. By a failure in the program, the program routine updated the copies of the program in the user's directory each time it was run. It is unlikely that Animal ever caused any measurable damage. The program contained no deliberately malicious code and did not even exploit any system vulnerabilities. It even took special care to not affect any of the user's programs.

This is why it is considered the first trojan, since the user thinks that the program is doing a function, which in this case is the entertainment, but behind the program is carrying out other functions, basically, the way to attack of what today we call trojan.

In the late seventies, computer scientists John Schoch and Jon Hupp tried to make use of the CoreWar programming code by modifying and using it so that the software took care of maintenance tasks and carried out the night tasks when no one could be directing it. So they propagated this software throughout the system, creating without knowing it the first computer worm, causing serious damage to the network due to program failures.

This is why it is considered the first worm in history, as it spreads through the network attacking and causing damage in this, sending copies of themselves to other computers in the network, as happened with the software implemented by Schoch and Hupp.

So, with all this, we see that the first variants of malware were created by mistake, both trojans and worms, giving way to an entire world to discover about these software that were able to perform functions that until then they had not even thought about it.

At this time, the popularity of computers and everything that surrounded them made many more people interested in this area, so the number of experts programmers grew exponentially. This means that many more programs will be created, and with this, the first ones began to emerge for harmful purposes, in order to damage or disrupt networks and systems around the world.

It was in 1987, when the first harmful virus emerged, Lehigh, infecting .COM files, and keeping an infection count in its body. After 4 infections, the virus may overwrite the boot sector and file allocation table. Also other viruses, Jerusalem and Cascade came out that besides attacking the .COM files, also attacked the .EXE files. In addition, the Cascade virus was the first to use encryption.

The next year was created the first mass reproduction worm, which managed to infect and collapse 10% of the ARPANET, and was named Morris Worm in honour of its creator Robert Tappan Morris. At the time Morris was caught and placed before the court, but the judge

ruled that the penalty for what he had done could not be as great as he could, because the only thing he had created was a programming code, so he was sentenced to 3 years probation, a fine and community services.

In this same year, due to the number of malware that was emerging, programmer Alan Solomon began to disassemble them and to create methods for their detection and elimination. That is why at the end of the year came the first antivirus to market, called Anti-Virus Toolkit.

We can already see, as we said before, that with the increasing activity of expert programmers, malware is also beginning to be created, and this fact does not go unnoticed, which is why the first steps are also taken to be able to solve the problem that causes a malware in case of being infected, appear the first anti-virus.

Shortly afterwards viruses appear with stealth and polymorphic techniques, so the task of detecting these viruses becomes more complicated. Because of this, the creation of anti-virus designed to combat these new techniques increases a lot, and an association is born that is going to regulate the name of the viruses according to the techniques that they use. The association was called CARO (Computer Antivirus Research Organization).

Years later, the first macro viruses written in WordBasic language, capable of infecting documents of Microsoft Word and Microsoft Excel appear, among them Concept and Laroux. It also gives the first case of transmission of a file infected by a virus via MSMail, the virus ShareFun. Antivirus could not cope with the influx of malware with new techniques that were attacking everyone, and that is why a Taiwanese student named Chen Ing-Hou created a virus that he called CIH by referring to his initials. This virus created by the young student was no more than a criticism of the incompetence of the creators of antivirus software. Cheng was brought to trial and sentenced for his creation, having to serve sentence as punishment.

To all this, added the appearance of malware that were sent via mail, but this time by someone known, so the rule that had been implemented that did not open emails from strangers fell short. Among them is the Happy trojan, which was propagated via MS Outlook, and had the ability to be sent automatically when the user sent a mail to another person. To the person who received it, it appeared that it was a known contact, and when the message was open, it displayed "Happy New Year 1999 !!" and had fireworks effects on the screen. Another malware that highlighted at the time in its mailing was the Melissa virus, which came with an attachment from a known contact, and when this file was opened in Word, it sent himself to the first 50 contacts in the list of the user who had opened it. This made its spread very fast and therefore very dangerous for market giants such as Microsoft and Intel, who decided to join to fight against the cyber crime that was occurring. In the end they found the author of the virus, David L. Smith, who was sentenced to 20 months in prison and a fine of $ 5000. There was not much to wait for the viruses that infected just opening an email without having to open an attachment appeared. They were worms that exploited the vulnerability of holes in the network system.

Gradually malwares were gaining strength, using new techniques to infect systems, and also looking for vulnerabilities in the victim's network to be able to take advantage of any hole through which to enter into it and thus spread the whole network and system . The trend continued, and malware continued to evolve to become more difficult to detect and exterminate.

As early as 2000, it was not overlooked that viruses were a way to attack a network very effective, and that is why in the same year was created the VBSWG (Visual Basic Script Worm Generator) worm generator. It created important viruses that came to infect even NASA.

Years later we have the development of packaged malwares, which made the detection of these by the anti-virus very complex. The packaging consisted of the compression and encryption of the executable file containing the virus.

The appearance of worms in the transmission of files Peer-to-Peer was also an important event, as Peer-to-Peer content was widely used for these dates.

The rate of infection was also a feature that developed during this time. The most notable example of that time was the Slammer worm, which, using the vulnerabilities of the Microsoft SQL server, managed to enter the system and infect 90% of vulnerable computers in the first 10 minutes of its propagation, doubling its propagation area each 8.5 seconds.

In 2003, botnets (robotic network) were started, using computers connected through the internet, which in turn are running one or more bots, and can cause DDoS (Distributed Denial of Service) attacks, steal data, or even send spam, in addition to being able to access and control the connected device.

In the following years, with the growing expansion of mobile devices, it did not take much time until the malware that affected these devices appeared. Among the affected mobile devices we found the ones that had the Windows operating system and the Symbian devices.

As can be seen in the malwares created to date, these had no economic interest, it is from 2005, when it begins to wake up the interest in exploiting these methods in a way that could be beneficial from them. The potential that malwares had to be a very profitable source of income is what triggered a series of cybercrimes for this.

Spywares appear, which were used mostly to have the possibility of access to personal information and bank accounts of infected users. These malwares act by staying in the memory of the device, and in this way when you access the browser and enter the data you are interested in, the creators of the spyware can recover them for their benefit.

Also, with the gain of popularity that obtained the video games online, the programmers began to take advantage and created malwares to be able to obtain information of the profiles of the players, these malwares received the name of phising. Coupled with the growing popularity of online games, there was also instant messaging such as the MSN Messenger platform, and the programmers of malwares also wanted to take advantage of the opportunity to be able to spread malicious code. And on the other hand applications for mobile devices was also used for that purpose.

Soon also with the massive use of the social networks was discovered another way to be able to infect the users of these, obtaining in this way that the range of possibilities to contaminate many users by different methods became wide.

We can see that the use of malware in history has changed over the years, from being failed programming experiments in the first place, to then being used to be able to collapse networks and create chaos in some networks of important companies, up to the present moment, that also continues to be done in protest or panic in the world, but that the most common is to use malwares as a way to earn easy money and also to live on it. Also mention that the sentences and punishments over the years has been increasing, because thanks to the knowledge of the operation of viruses, or the intention of its use, people are more aware of how dangerous it can be a malicious program attack against any type of network or set of systems. It should also be added that at this time the era of technology is being lived, and almost everything we do in our daily lives includes the use of electronic devices that are connected to a network, so if the device we are using is infected we may have serious problems in the day to day tasks. Technology does not stop advancing, and with it, the methods that can be developed to be able to infect it with malware. Also the defence against these methods continues advancing and discovering methods to face the attacks that can be carried out, and one thing is certain, this battle between malwares and anti-virus will never stop to exist by this development that we finish to mention.

References

1. Kopřiva, Jan1986-, **Malware history**, 128 l. : grafy. (2013) DOI: http://hdl.handle.net/10467/16092

2. Sikorski, Michael and Honig, Andrew, **Practical malware analysis : the hands-on guide to dissecting malicious software**, 978-1-59327-290-6 (brožováno) 1-59327-290-1 DOI: 000779558

3. Ken Dunhaml. , **Mobile malware attacks and defense**, xxv, 409 s. : il. DOI: https://aleph.cvut.cz/F?func=direct&doc_number=000726176&local_base=DUPL&format=999

4. Pluskal, Ondřej , **Malware Detection**, Diplomová práce (Ing.)--ČVUT, FEL, katedra kybernetiky, 2013 DOI: http://hdl.handle.net/10467/15989

5. Levin, Richard B., **The Computer Virus Handbook**, 0-07-881647-5 DOI: 000099573

6. Jan Hruska, **Computer Viruses and Anti-Virus Warfare** ., 0-13-036377-4 (1992) DOI: 000099767

7. Kokeš, Josef , **Analysis of cryptovirus**, Diplomová práce (Ing.)--ČVUT, FIT, katedra počítačových systémů, Praha, 2016 DOI: http://hdl.handle.net/10467/62948