V I D Z E M E U N I V E R S I T Y O F A P P L I E D S C I E N C E S

**F A C U L T Y O F E N G I N E E R I N G**

C Y B E R S E C U R I T Y E N G I N E E R I N G

Malware and digital forensics

V A L M I E R A , 2 0 2 2

**C O N T E N T S**

**1 Introduction 4**

**2 Literature search 5**

**3 Main description**

**4 Summary**

**5 References**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document history** | | | |
| Version | Status / Changes | Date | Author |
| 1.0 | The first version | 27.12.2022 | Denys Shabelnyk |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Contacts and responsible person (s)** | | | |
| Name, Surname | Department | Role | Contact information (e-mail) |
| Denys Shabelnyk | IT | Individual Work | Denys[.Shabelnyk@va.lv](mailto:Mefat.shabani@va.lv) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**1 Introduction**

Defense against malware has very important part in cybersecurity nowadays.

More and more commercial and non-commercial organizations face with malware and their effects.

Malware are more complicated and deleterious than before.

It is very important and actual problem in our century. The rapid development of Internet and computer networks makes digital forensics very hard job, because we don’t know for sure where a server located and what type has it ? It can be physical server or virtual. Maybe it is not one node but cluster. Only logs, cooperation with service providers and close work with corporations can help achieve success in digital forensics and catch the criminal.

Big enterprice companies spent more and more money every year to improve their cybersecurity policy and update their software to save business. Nowadays, new detection

methods have been developed and now AI-based methods helps to achive maximum level of cybersecurity defence.

Digital forensics methods are not stay alone. Their are also improved and they are gone step by step followed by malware development. There are two main groups of malware in literature: **host-dependent** and **host-independent**.([Ilker Kara,Express systems with applications](https://db.va.lv:2075/record/display.uri?eid=2-s2.0-85141470133&origin=resultslist&sort=plf-f&src=s&st1=Cybersecurity+analysis&sid=f9cbf4af2de0315e0cfc82eb202d31db&sot=b&sdt=b&sl=27&s=KEY(Cybersecurity+analysis)&relpos=1&citeCnt=0&searchTerm)). Host-dependent are malwares which developed for particular systems and were widespread at the dawn of the computer age and before the Internet era. The main way to spread this type of threats was floppy drives, types and CD-disks. A completely different type of viruses have host-indepented malwares. They are spread within Internet and have so many types. I will cover this in more detail later in my report.

Generally, there are a lot of articles, books and other matherials nowadays in the market. They have descriptions about types of malwares and other threats which can damage corporate or home system and even have descriptions about malwares which attack mobile devices. It is a new type of malware which have different ways of spread.

In my paper work I will try make little research about this problem, find and share statistics and tell more about malware, their types and how to protect corporate networks against them.

**2 Literature search**

Let’s make overview in literature. How this problem is explored nowadays ?   
Malware is any software intentionally designed to cause disruption to a computer, server,client or computer network, leak private information, gain unathorized access to information, or which unknowingly interferes with the user’s computer security and privacy([Wikipedia](https://en.wikipedia.org/wiki/Malware)) gets defenition Wikipedia. Yes, indeed. Very accurate and correct definition. Also, this article lists the main types of them: computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware([Wikipedia](https://en.wikipedia.org/wiki/Malware))  
Pretty complete list.

There are two main type of malware tells us Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges([Ilker Kara,Express systems with applications](https://db.va.lv:2075/record/display.uri?eid=2-s2.0-85141470133&origin=resultslist&sort=plf-f&src=s&st1=Cybersecurity+analysis&sid=f9cbf4af2de0315e0cfc82eb202d31db&sot=b&sdt=b&sl=27&s=KEY(Cybersecurity+analysis)&relpos=1&citeCnt=0&searchTerm)). The special place the author assigns to fileless malwares which spread within the Internet and work and hide using WMI and damage only Windows based systems.

Big development company also take up exploration and research this question. Microsoft on its FAQ article([Learn Microsoft](https://learn.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN)) gets clear and well organized overview about malwares, viruses, cookies and different them. Also, about viruses, worms and how to protect systems against them. Microsoft does not forget tells us about Trojan horses, what they are and how to prevent these attacks. Apple also has the e-library about malwares ([Apple support](https://support.apple.com/guide/mac-help/what-is-malware-on-mac-mh27449/mac)) which tells about what is a malware and how to protect Mac systems againts them. Open-source foundation also works under this question but there are not much viruses which work against Linux-based systems. The Linux malware article([Linux malware article, Wikipedia](https://en.wikipedia.org/wiki/Linux_malware)) include overview about viruses and trojan horses, worms and targeted attacks, web scripts, buffer overruns attacks, cross-platform viruses, social engineering and Go-written malwares.

I would like to separately talk about books which have written by professional experts and gives us deep understanding about subject of my report. The first book which I have found is Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software ([Amazon](https://www.amazon.com/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901)) which has written by Michael Sikorski and Andrew Honig.  
The authors tells us about practical ways to find and analyze malwares and also how to set up a safe virtual environment to analyze malware, quickly extract network signatures and host-based indicators, how to use key analysis tools like IDA Pro, OllyDbg and WinDbg.  
Also tell us about how to overcame malware tricks.   
Another good book is Malware Data Science: Attack Detection and Attribution([Amazon](https://www.amazon.com/Malware-Data-Science-Detection-Attribution/dp/1593278594)) written by Joshua Saxe and Hillary Sanders. The authors describe how to identify, analyze and classify large-scale malware using machine learning and data visualization methods. After reading this book we can know how to analyze malware using static analysis, observe malware behavior using dynamic analysis, identify adversary groups through shared code analysis. The special overview author make for catch 0-day vulnerabilities by building your own machine learning detector, measure malware detector accuracy and identify malware campaigns, trends, and relathionships through data visualisation.

Also, I want to make little overview about tutorials which learn us how to protect our systems against malwares and how to find them and analyse.

The most popular training center in my opinion is Kaspersky training center([Kaspersky](https://xtraining.kaspersky.com/?redef=1&THRU&reseller=gl_xtr-psearch_acq_ona_sem_bra_onl_b2b__textad_smteam______&gclid=CjwKCAiAzKqdBhAnEiwAePEjkqoyknrcejFLGw_ORElgwo5Bwk4b3R9F5Wso3I4nzcmrvqdso0-qhxoCg2IQAvD_BwE)) which provide full practical courses about malwares, analyze and detection methods, also about mobile malware reverse engineering.

Executive-Ed([Executive-Ed](https://executive-ed.xpro.mit.edu/professional-certificate-cybersecurity?utm_source=Google&utm_network=g&utm_medium=c&utm_term=learn cybersecurity&utm_location=9061069&utm_campaign_id=19229814603&utm_adset_id=144920305872&utm_ad_id=641039174608&gclid=CjwKCAiAzKqdBhAnEiwAePEjkpcU24kE3mELhRIbl8wdvZhvq86f9_EjxWg9xP8kEFS3jtkXjNNE-hoC2LcQAvD_BwE)) also provides systematic course about cybersecurity which consist of 24 week of study.

There are a lot of free courses and trainings on the Internet. For example:  
W3School([W3School](https://www.w3schools.com/cybersecurity/)), Simplilearn([Simplilearn](https://www.simplilearn.com/tutorials/cyber-security-tutorial)) and etc.

**3 Main descriptions**

Let’s talk depply about malwares and how to run digital forensics related with tgheir type.

**1) trojan horses** – is a harmful program, host-independent malware, that misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it. A Trojan horse usually carries a hidden destructive function that is activated when the application is started.   
Trojan horses are generally spread by some form of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(security)), porn sites, dating sites nowadays for example, where a user is duped into executing an email attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by [drive-by download](https://en.wikipedia.org/wiki/Drive-by_download). Although their payload can be anything, many modern forms act as a backdoor, contacting a controller (phoning home) which can then have unauthorized access to the affected computer, potentially installing additional software such as a keylogger to steal confidential information, cryptomining software or adware to generate revenue to the operator of the trojan.   
**Forensics signs**: while Trojan horses and backdoors are not easily detectable by themselves, computers may appear to run slower, emit more heat or fan noise due to heavy processor or network usage, as may occur when cryptomining software is installed. Cryptominers may limit resource usage and/or only run during idle times in an attempt to evade detection. First step on this case – plug out network cable and scan all system on safe mode.

2) **rootkits** – is the type of malware, host-dependent or host-independent type of malware, which can damage all system using hidden processes and can for example erase all documents from computer or send its copy to another computers within network.  
**Forensics signs**: so much hidden process in a system on every time of monitoring.  
Some processes aren’t stop. After rebooting these process run again even after full system load.

3) **backdoors** – this type of malware not a virus or any other damage code. Is more a method than the virus. A backdoor is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed in order to allow access in the future, invisibly to the user. There is an idea that software manufacturers company integrate backdoors to their software products for technical support reasons and collect a statistics about software usage.   
**Forensics signs:** divided by two parts: a commercial software or an open-source software. In case commercial softwares which as usually required mandatory registration by customers, the last one can get letters with advertising of products which the company never developed or never provided services. In case open-source softwares you can explore the source code by themselves or compare program functionality with description. On this case a customer can see advertisement while an application is running or the application can request money from customer to open part of functionality.

**4) infectious malware** – it is a group of host-dependent or host-independent malware which consist of **worms** and **viruses.  
Worm -** is a stand-alone malware software that actively transmits itself over a network to infect other computers and can copy itself without infecting files. These definitions lead to the observation that a virus requires the user to run an infected software or operating system for the virus to spread, whereas a worm spreads itself.  
**Forensics signs:** strange peoples and friends complain about spam letters from infected host. It is a main mark about this malware.  
**Viruses -** is software usually hidden within another seemingly innocuous program that can produce copies of itself and insert them into other programs or files, and that usually performs a harmful action (such as destroying data).An example of this is a portable execution infection, a technique, usually used to spread malware, that inserts extra data or executable code into PEfiles A computer virus is software that embeds itself in some other executable software (including the operating system itself) on the target system without the user's knowledge and consent and when it is run, the virus is spread to other executable files.   
**Forensics signs:** viruses – always have malicious code. If you receive an unknown letter or open an unknown web-site and see how another browser’s tabs are being opening or command line interface is being opening that’s the sign of viruses.

**5) ransomware** – it is also a group of host-dependent or host-independent group of malicious code which consists of **screen-locking ransomware** and **encryption-based ransomware.**

**screen-locking ransomware -** lock-screens, or screen lockers is a type of “cyber police” ransomware that blocks screens on Windows or Android devices with a false accusation in harvesting illegal content, trying to scare the victims into paying up a fee.  
**Forensics signs:** if you had strength propositions about follow a link or download a file before screen block - you have caught this type of screen-locking ransomware. As a rule reinstall the operation systems don’t help in this case because the malicious code integrates to the part of system which loades before operational system. Only reinstall BIOS can recover your system.

**encryption-based ransomware -**  is a type of ransomware that encrypts all files on an infected machine. These types of malware then display a pop-up informing the user that their files have been encrypted and that they must pay (usually in Bitcoin) to recover them. Some examples of encryption-based ransomware are CryptoLocker and WannaCry  
**Forensics signs:** all data won’t be decrypted even a victim paid money to bad guys.   
The main sign in this case – after run malicious code a computer always reboots and after you see screen with an ugly message and way to pay a ransom.

6) **grayware** – is a new type of malware. Is a term, coming into use around 2004, that applies to any unwanted application or file that can worsen the performance of computers and may cause security risks but which is not typically considered malware. Greyware are applications that behave in an annoying or undesirable manner, and yet are less serious or troublesome than malware. Grayware encompasses spyware, adware, fraudulent diares, joke programs ("jokeware"), remote access tools and other unwanted programs that may harm the performance of computers or cause inconvenience. For example, at one point, [Sony BMG](https://en.wikipedia.org/wiki/Sony_BMG) compact discs silently installed a rootkit on purchasers' computers with the intention of preventing illicit copying.   
**Forensics signs:** if you see annoyed advertisement while you are working at the computer and you didn’t have interested in such things before – you have got this type of malware. Remove web-browser cash memory or erase browser history and cookies helped as usually on this case.

7) **potentially unwanted programm(PUP) -** are applications or programmes that would be considered unwanted despite being downloaded often by the user, possibly after failing to read a download agreement. PUPs include spyware, adware, and fraudulent dialers. Many security products classify unauthorised key generators as grayware, although they frequently carry true malware in addition to their ostensible purpose. Malwarebytes lists several criteria for classifying a program as a PUP. Some types of adware (using stolen certificates) turn off anti-malware and virus protection; technical remedies are available.

8) **droppers -** are a sub-type of Trojans that solely aim to deliver malware upon the system that they infect with the desire to subvert detection through stealth and a light payload

**4 Summary**

In this small report I tried to make little research about malware and digital forensics.

This topic well learned by students, cybersecurity experts with rich experience in investigations and end-users who faced (include me) with malwares and its impact.  
There are two main of malware: host-dependent which spread by shared devices: types, floppy drives and CD disks and host-independent which spread within Interent.

There are some kind of malware which don’t do any bad activities on victim computer but transports bad code to the victims.  
  
TODO: continue