2 - Malicious Software

2.1 Basic concepts

Malware:

This term comes from '**mal**icious soft**ware**' and is used to define any kind of software which intention is harmful or intrusive. Besides, it can exploit system vulnerabilities to carry on malicious actions. They can take the form of documents, executables files, web pages, etc.

An extra definition states: *"Malware is software designed with malicious purpose. It may be designed to disable your phone or computer, remotely control your device, or steal valuable information like credit card information or passwords"* (The network support company, 2016).

A malware file could be divided into different parts depending on its actions, the most important are: payload, signature and propagation section.

Payload:

The payload part of a virus is that portion of the code not related to propagation or concealment, namely, is in charge of performing the malicious action. From the attacker point of view, this is the part where he takes advantage of the system, for example, adding a new user, controlling a webcam, etc.

Signature:

The signature part of a virus is that portion where the malware identifies whether the machine is infected or not, thus avoid overloading the machine with several instances of the same virus performing actions in parallel. Signature is usually a string with an impossible date or another sequence easy to search. Antiviruses have signatures databases which are used to find malware.

Propagation section:

This part is in charge of replication when the malware attempts to copy itself to other files or systems and sometimes, trying to reach as many infections as possible.

Malware can be classified into a variety of categories, depending on propagation, concealment, or their malicious actions. They are further presented in the following lessons.

2.2 Types of malware: Propagation

The categorization by propagation is divided into two well-known groups virus and worms:

Virus:

A computer virus is a harmful piece of executable code which is used to take advantage of a device without the user's consent, typically by attaching itself to a host document that will generally be an executable file. The propagation is strictly by human-iteration; therefore, it depends on a special action to be executed, for example, by opening a document, clicking on a link, etc.

The most common host for viruses are:

- Executable files (such as the .exe files in Windows).
- Boot sectors of disk partitions.
- Script files for system administration (shell scripts files in Unix).

- Documents (MS Office files, pdfs).
- Every O.S. that allows third-party programs to run can support viruses.

The replication is done by inserting the code in other host documents, however, these copies can be different. These are called mutation virus, which makes more difficult its detection by signature matching.

Worms:
A computer worm is a self-contained malware that spreads copies of itself without needing to inject itself into other programs, and often without human interaction. Typically, they exploit software/systems vulnerabilities and are propagated over the network to infect additional devices.

In most cases, they have a payload which deletes files or installs backdoors. However, worms can cause indirect damage without a payload, for example overloading the network or memory ram.

Hence, the main difference is that a virus requires user-assistance for propagation, and a worm spreads itself.

2.3 Types of malware: Concealment

The categorization by concealment is the following:

Virus:
Viruses are hidden in another file. There are several concealment methods such as Encrypted, Polymorphic, and Metamorphic virus. They are presented in the following lesson.

Trojan:
A Trojan is a program that performs some useful tasks (from a user point of view), but also does something with malicious consequences (e.g., add a new account). Usually, a user or administrator accidentally install trojans, however, they can also be part of another malware.

Trojans are commonly used for phishing since they have the largest potential for infection since a human being is considered the weakest link. Considering a trojan, its maximum potential for infection is by social-engineering, man-in-the-middle or download from insecure websites.

Rootkit:
A Rootkit is a malware that modifies an operating system to hide the existence of itself or another service (e.g. a reverse shell). Thus, it prevents and makes harder the detection for antiviruses. A common rootkit migrates a utility (used by the attacker) to a default service handled by an Operating System (e.g. Explorer.exe in windows).

Backdoor:
A backdoor is a hidden feature or command in a program, that allows a given agent to bypass an authentication method. It could be used by authenticated users or not, usually, they are installed for an admin to easily get access and provide support for users. However, backdoors are exploited by attackers such as Easter Eggs in DVDs and software.

2.4 Other types of malware

There are several extra types of malware, the most popular are:

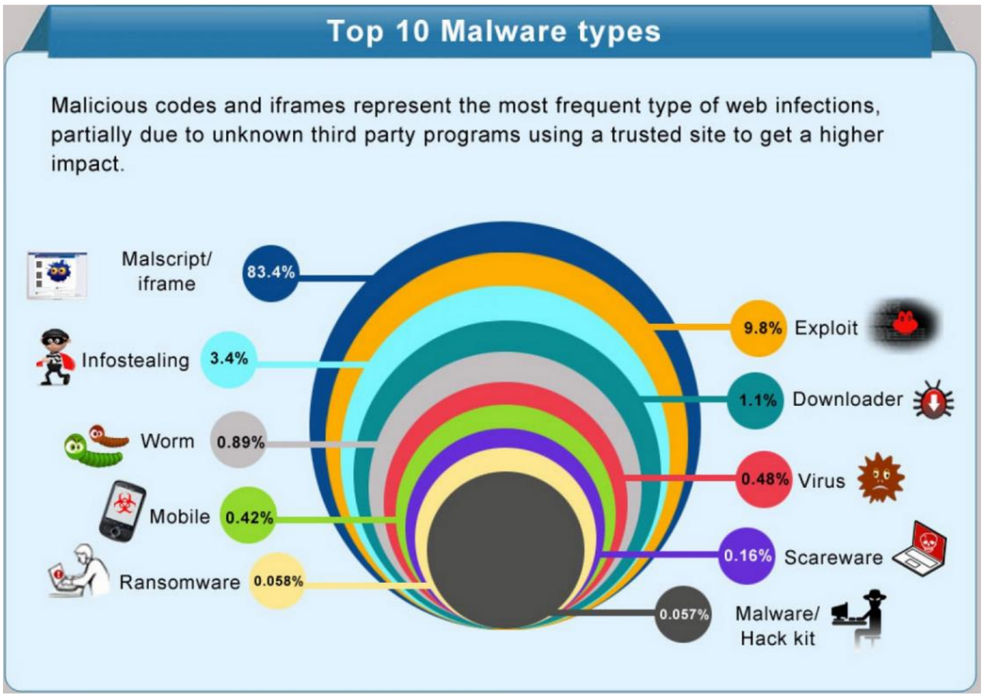
Spyware:
A spyware is a piece of code that gathers information about users without their consent and sends it to a third malicious person. They can be part of a trojan horse, the typical spywares are: keyloggers, accessing to webcam and microphone remotely.

Ransomware:
A ransomware is considered as a type of malware that uses cryptography to harm data from a device. It encrypts the victim's data with a secret key in order to block the access from a legitimate user. Typically, it is used for extortion, the attacker demands a payment for exchanging the secret key and thus decrypting the files. A popular ransomware was spread in May 2017, called Wannacry and attacked 104 countries (Goswami, 2017).

Adware:
The malware identified as adware is any kind of software able to automatically send advertisements. They are usually installed as a trojan and connected to an adware engine which is in charge to deliver the ads. The adware engine's owner profits money for each view or click. They are common in browsers and mobile phones.

Botnet:
A botnet is a collection of bots capable of working together against one target. A bot is an individual machine under control of a bot-master and typically equipped with a larger repertoire of behaviours. The master sends a command received by each bot to perform the action. All bots together are powerful and can be used as distributed denial-of-service attack(DDoS).

Furthermore, on the cyber world, there are several kinds of malware that are not mentioned in this research. The following image illustrates the most common types.



Top 10 Malware types

Malicious codes and iframes represent the most frequent type of web infections, partially due to unknown third party programs using a trusted site to get a higher impact.

Figure 1 https://visual.ly/community/infographic/computers/malware-effect-trusted-site

2.5 Malware obfuscation

Antivirus scanners attempt to stop malware contamination, but malware developers have been working on different techniques to evade them, creating new malware that makes harder understanding its code, its purpose and its impact. The scanners look for signatures in code, but malware obfuscation creates a new different version with equal functionality, resulting in a completely different signature, thus scanners cannot detect it. There are three main methods: encrypted, polymorphic, and metamorphic.

Encrypted malware:

This technique is built with an encryptor/decryptor engine which takes the code and encrypts it in a new version of itself; and, when the infected file is running, this engine decrypts the malware to perform the malicious action. It can generate different keys; therefore, a virus scanner looks for decryption engine instead of a specific signature. Popular methods used are XOR encryption, base64 encoding or a combination of these two.

Polymorphic malware:

This technique consists in the ability to mutate the malware. Their decryptor engine creates new decryptor engines (variations of itself), thus always generating a new one that the antivirus cannot search the engine. However, antivirus has also evolved for detecting polymorphic malware through CPU emulator.

Metamorphic malware:

Metamorphic methods are extremely challenging to be detected and they consist on malware that can transform its body by translating, editing and rewriting into new generations of themselves. The metamorphic body is different in each instance. This is the difference with polymorphic malware that has always the same body. Several techniques can be found, such as permutation of its code/instructions, dead-code insertion or instructions replacement.

References

Christopher Truncer in Informational, T. V. (2017, March 21). *Veil 3.0 Command Line Usage*. Retrieved from Veil – Framework: https://www.veil-framework.com/veil-command-line-usage/

Davis, M. a. (2009). *Hacking Exposed Malware and Rootkits.* McGraw-Hill, Inc.

Fosnock, C. (2005). Computer worms: past, present, and future. *East Carolina University*, 8.

Goswami, D. (2017, 05 14). *Wanna Cry ransomware cyber attack: 104 countries hit, India among worst affected, US NSA attracts criticism.* Retrieved from India Today in.: http://indiatoday.intoday.in/story/wanna-cry-ransomware-attack-104-countries-hit-nsa-criticised/1/953338.html

Lee, J. (2017, May 23). *Metasploit-framework:How a payload works*. Retrieved from Rapid7 Community: https://github.com/rapid7/metasploit-framework/wiki/How-payloads-work

Maynor, D. (2011). *Metasploit toolkit for penetration testing, exploit development, and vulnerability research.* Elsevier.

Microsoft Security TechCenter. (2008, October 23). *Microsoft Security Bulletin MS08-067 - Critical*. Retrieved from https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Porras, P. A. (2009). A Foray into Conficker's Logic and Rendezvous Points. *LEET*.

Rapid 7 Community. (2012, 06 01). *Metasploitable 2 Exploitability Guide.* Retrieved from Metasploit Community: https://community.rapid7.com/docs/DOC-1875

Rapid 7 Community. (2013, 07 05). *How To Set Up A Penetration Testing Lab.* Retrieved from Rapid 7 Community: https://community.rapid7.com/docs/DOC-2196

Rapid 7 Community. (2016, September 14). *Metasploit-framework: msfvenom*. Retrieved from Metasploit-framework: https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

Rapid 7 Community. (2017, 06 06). *Metasploit User Guide.* Retrieved from Penetration testing software for offensive security teams.: https://community.rapid7.com/docs/DOC-1563

Scambray, J. a. (2007). *Hacking Exposed Windows.* Tata McGraw-Hill Education.

Singh, A. (2012). *Metasploit Penetration Testing Cookbook.* Packt Publishing Ltd.

Spafford, E. H. (1989). The Internet worm program: An analysis. *ACM SIGCOMM Computer Communication Review, 19*, 17--57.

The network support company. (2016, 10 06). *What Is Malware? [Infographic].* Retrieved from network-support: https://www.network-support.com/wp-content/uploads/2016/10/What-Is-Malware-Infographic.jpg