POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

Automatic Malware Signature Generation

Relatori
prof. Antonio Lioy
ing. Andrea Atzeni

Michele Crepaldi

Anno accademico 2020-2021

Thanks...

Summary

Summary...

Acknowledgements

Aknowledgments...

Contents

Chapter 1

Introduction

Introduction...

Chapter 2

Background

2.1 Malware

Malware, short for ***malicious software***, is a general term for all types of programs designed to perform harmful or undesirable actions on a system. In fact in the context of IT security the term *malicious software* means:

> *Software which is used with the aim of attempting to breach a computer system's security policy with respect to Confidentiality, Integrity and/or Availability.*

Malware consists of programming artefacts (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware is not (and should not be confused with) defective software - software that has a legitimate purpose but contains harmful bugs (programming errors).

The term ***software*** should here be understood in the broadest sense, as the malicious effect may make use of executable code, interpreted code, scripts, macros etc. The computer system whose security policy is attempted to be breached is usually known as the ***target*** for the malware. We shall use the term "***initiator*** of the malware" to denote the subject who originally launched the malware with the intent of attacking one or more targets. Depending on the type of malware, the set of targets may or may not be explicitly known to the initiator. Note that this definition relates the maliciousness of the software to an attempted breach of the target's ***security policy***. This in turn means that it depends on the privileges of the initiator on the target system. A program P which would be classified as malware if initiated by an user with no special privileges, could easily be quite acceptable (though obviously a potential danger to have lying about) if executed by a system administrator with extensive privileges on the target system.

Different companies, organizations and people describe malware in various ways. For example **Microsoft** defines it in a generic way as:

> *Malware is a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network*

The **National Institute of Standards and Technology** (**NIST**), on the other hand, cites multiple definitions for malware, describing it as "hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose."

In another more specific definition **NIST** affirms that Malware is:

> *A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.*

In other words, software is often identified as malware based on its *intended use*, rather than a particular technique or technology used to build it.

2.1.1 Why Malware is used

Typically, cybercriminals use malicious tools to access sensitive data, extort ransoms, or simply cause as much damage as possible to the affected systems. More generally malware serves a variety of purposes. For example, most commonly cybercriminals use malware:

- **To profit financially (either directly or through the sale of their products or services)**. For example, they may use malware to infect targets' devices to steal account information or cryptocurrency. They may sell their malware to other cybercriminals to use as they see fit or may sell it as a service offering. E.g. DDoS as-a-service and ransomware-as-a-service are more and more common these days.
- **As a means of revenge of to carry out a personal agenda**. For example, Brian Krebs of Krebs on Security was struck by a big DDoS attack a few years ago after having talked about a DDoS attacker on his blog.
- **To carry out a political or social agenda**. Some perfect examples of this would be nation-state actors (like state-run hacker groups in China and North Korea) and hacker groups such as Anonymous.
- **As a way to entertain themselves**. Some cybercriminals find enjoyment in victimizing others.

Obviously there can be also reasons for non-malicious actors to create and/or deploy some types of malware too - for example it can be used to test security.

More practically some examples of cybercriminals' uses of malware are:

- Tricking a victim into providing personal data for identity theft.
- Stealing consumer credit card data or other financial data.
- Assuming control of multiple computers to launch denial-of-service (DOS) attacks against other networks.
- Infecting computers and using them to mine bitcoin or other cryptocurrencies.

and many more.

2.1.2 How does malware spread

In general malware exploits existing network, device, and/or user ***vulnerabilities*** (the latter being frequently underrated), to spread and perform harmful operations.

More specifically malware authors use a variety of physical and virtual means to spread malware that infects devices and networks. For example, malicious programs can be delivered to a system with a USB drive or can spread over the internet through ***drive-by downloads***., which automatically download malicious programs to systems without the user's approval or knowledge. ***Phishing*** attacks are another common type of malware delivery where emails disguised as legitimate messages contain malicious links or attachments that can deliver the malware executable file to unsuspecting users. Sophisticated malware attacks often feature the use of a ***command-and-control*** server that enables threat actors to communicate with the infected systems, exfiltrate sensitive data and even remotely control the compromised device or server.

Moreover malware can hide inside legitimate software applications or files, or its author can disguise it as a seemingly harmless app that users download unknowingly.

2.1.3 Malware types

The classification of malware depends on the execution characteristics or the program. Malware is also classified depending on its payload, how it exploits or makes the system vulnerable and how it propagates.

There are a number of different ways of categorizing malware; the first is by *how* the malicious software spreads. Names like *virus*, *worm* and *trojan* are commonly used interchangeably to indicate malware, but they actually describe three subtly different ways malware can infect target computers:

- ***Virus***. The term "computer virus" is used for a self-replicating malicious program that has infected some executable software (and/or boot sectors) and, when run, causes the virus to spread to other executables. Depending on how complex the virus code is, it may be able to modify the replicated copies. Ultimately the virus is passive and needs to be transferred through files, media files or network files in order to infect other hosts.

  Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus is able to replicate itself and spread through the system. Viruses can also spread through script files, documents, and cross-site vulnerabilities in web apps.

  Viruses may also perform other actions other than just replicating, such as creating a backdoor for later use, damaging files, stealing information, creating botnets, render advertisements or even damaging equipment.

- ***Worm***. On the other hand, a worm is a self-replicating and active malicious program that can transmit itself over the network and spread by exploiting various system vulnerabilities. It uses targeted vulnerabilities in the operating system or installed software. It contains harmful routines but can be used to open communication channels which serve as active carriers. The Worm consumes a lot of bandwidth and processing resources through continuous scanning and makes the host unstable, which can sometimes cause the system to crash. Computer worms can also contain "payloads" that damage host computers. Payloads are composed by pieces of code written to perform actions on the affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files or create bots, that can lead the infected systems to become part of a botnet.

  Worms are usually spread via software vulnerabilities or phishing attacks.

- ***Trojan horse***. In broad terms, a *Trojan Horse*, commonly referred to as "Trojan", is any program that disguises itself as legitimate and invites the user to run it, concealing a harmful or malicious payload. The payload - malicious routines - may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or further installing malicious or undesirable software. Trojan horses known as *droppers* are used to start off a worm outbreak, by "injecting" the worm into users' local networks. Trojans may hide in games, apps, or even software patches, or they may be embedded in attachments included in phishing emails.

  A trojan horse cannot self-replicate and relies on the system operators to activate. It can however give remote access to an attacker who then can perform any malicious activity that is of interest to them. Trojan horse programs have different ways they affect the host depending on the payload attached to them and are usually spread through social engineering.

  One of the most common ways that *spyware* is distributed is a Trojan horse, bundled with a piece of desirable software that the user downloads from the internet. When the user installs the software, the spyware is installed alongside. Spyware authors who attempt to act in a legal fashion may include an end-user licence agreement that states the behaviour of the spyware in loose terms, which the users are unlikely to read or understand.

These definitions lead to the observation that both viruses and trojans require *user intervention* to spread, whereas a worm spreads itself automatically. A virus, however, cannot execute or

reproduce unless the app it has infected is running. This dependence on a host application makes viruses different from trojans, which require users to download them, and worms, which do not use applications to execute.

Malware can also be installed on a computer "manually" by the attacker themselves, either by gaining physical access to the computer or using privilege escalation to gain remote administrator access.

Another way to categorize malware is by what it *does* once it has successfully infected its victim's computers. There are a wide range of potential attack techniques used by malware, here are some of them:

- ***Rootkits***. Originally, a *rootkit* was a program or, more often, a collection of software tools installed by a human attacker on a Unix system, allowing the attacker to gain remote administrator (root) access. Today it is more generally considered as a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet. Rootkit prevention, detection, and removal can be difficult due to their stealthy operation. Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behaviour for irregular activities, system file signature scanning, and storage dump analysis.

  Moreover, some use the term 'rootkit' also for denoting concealment routines in a malicious program. These routines are very advanced and complex programs written to hide within the legitimate processes on the infected computer. Therefore they are very invasive and are difficult to remove. They are designed with the capability of taking full control of the system and gaining the highest privileges possible on the machine among other possible malicious activities.

  Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection and disinfection. The same is true when a human attacker breaks into a computer directly. Techniques known as rootkits allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read.

  In an attempt to keep the user form stopping a malicious process, another is sometimes installed to monitor it. When the process is stopped (killed), another is immediately created. Modern malware starts a number of processes that monitor and restore one another as needed. In the event that a user running Microsoft Windows is infected with such malware (if they wish to manually stop it), they could use Task Manager's 'processes' tab to find the main process (the one that spawned the "resurrector" process(es)"), and use the 'end process tree' function, which would kill not only the main process, but the "resurrector(s)" as well, since they were started by the main process. Some malware programs use other techniques, such as naming the infected file similarly to a legitimate or trustworthy file to avoid detection in the process list.

- ***Backdoors***. A *backdoor*, also called Remote Access Trojan (RAT), is a deliberately hidden vulnerability in the program code that allows privy users to circumvent typical protection mechanisms, such as authentication using login credentials. In other words it is a method of bypassing normal authentication procedures. Once a system has been compromised (by one of the above methods, or in some other way), one or more backdoors may be installed in order to allow easier access in the future without alerting the user or the system's security programs. Backdoors may also be installed prior to malicious software, to allow attackers entry.

  These digital backdoors are also often hidden in programs by intelligence services in order to gain easy access to sensitive information. For example, Cisco network routers, which

process large volumes of global internet traffic, were in the past provided with backdoors for the US Secret Service.

- ***Spyware***. *Spyware* is a type of malicious software that can be installed on computers, and uses functions in an operating system with the intention of spying on the user activity. More specifically it collects small pieces of information about users, like for example credit card details and passwords, without their knowledge. The information gathered is then sent back to the cybercriminal(s) responsible for it. The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer.

  While the term spyware suggests software that secretly monitors the user's computing, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet connection or functionality of other programs. They spread by attaching themselves to legitimate software, Trojan horse or even taking advantage of known software vulnerabilities. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is provided by the term *privacy-invasive software*.

  Classification of code as spyware (or sometimes browser cookies as "tracking" cookies) can be controversial. Often the software is installed by the user knowing that some amount of monitoring will take place (Users generally agree to this activity to get free software and it is often associated with music and video sharing). Some such software allows the user to turn off the monitoring, assuming they are aware of it and can find instructions for disabling it. Anti-spyware is usually part of anti-virus programs.

  Spyware is often used by law enforcement, government agencies and information security organizations to test and monitor communications in a sensitive environment or in an investigation. But spyware is also available to consumers, allowing purchasers to spy on their spouse, children and employees.

- ***Loggers***. Keystroke logging (often called *keylogging*) is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. The collected information is stored and then sent to the attacker who can then use the data to figure out passwords, usernames and payment details, for example. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

  Key logging is often used by law enforcement, parents, and jealous or suspicious spouses. The most common use, however, is in the workplace, where your employer is monitoring your use of the computer.

- ***Adware***. Adware, or "Advertising supported software", is any software package which automatically plays, displays, or downloads advertisements to a computer. Some adware may also re-direct the user's browser to dubious websites. These advertisements can be in the form of a pop-up ads or ad banners that lure the user into making a purchase. The objective of the Adware is to generate revenue for its author. Adware, by itself, is harmless; however, some adware may come with integrated spyware, such as keyloggers, and other privacy-invasive software. This type of malware usually gets onto users' computers from dubious download portals or infected websites. It also may gain access by appearing to be an innocent ad or by attaching itself to another app, gaining access to the system when installing the apparently benevolent program. Once installed, adware can only be removed from the system at great expense, as the tools are deeply embedded in the operating system and web browsers.

  Advertising functions are integrated into or bundled with the software, which is often designed to note what Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. For example, an advertiser might use cookies to track the webpages a user visits to better target advertising. Adware is usually seen by

the developers as a way to recover development costs, and in some cases it may allow the software to be provided to the user free of charge or at a reduced price. The income derived from presenting advertisements to the user may allow to motivate the developer to continue to develop, maintain and upgrade the software product. Conversely the advertisements may be seen by the user as interruptions or annoyances, or as distractions from the task at hand.

Some adware is also shareware, and so the word may be used as a term of distinction to differentiate between types of shareware software. What differentiates adware from other shareware is that it is primarily advertising-supported, like many free smartphone apps. Users may also be given the option to pay for a "registered" or "licensed" copy to do away with the advertisements.

There is a group of software (Alexa toolbar, Google toolbar, Eclipse data usage collector, etc.) that send data to a central server about which pages have been visited or which features of the software have been used. However, differently from "classic" malware, these tools document activities and only send data with the user's approval. The user may opt in to share the data in exchange to the additional features and services, or (in the case of Eclipse) as the form of voluntary support for the project. Some security tools report such loggers as malware while others do not. The status of the group is questionable. Some tools like PDF Creator are more on the boundary than others because opting out has been made more complex than it could be. However, PDF Creator is only sometimes mentioned as malware and is still subject of discussion.

- ***Bots***. Bots are software programs designed to automatically perform specific operations. Bots are derived from 'robots' which were first developed to manage chat channels of IRC - Internet Relay Chat - a text based communication protocol that appeared in 1989. Some bots are used for legitimate and harmless purposes like video programming, video gaming, internet auctions and online contest, among other functions. It is however becoming increasingly common to see bots being used maliciously. Malicious bots can be (and usually are) used to form botnets. A botnet is defined as a network of host computers (zombies/bots) that is controlled by an attacker or bot-master. Botnets are frequently used for DDoS (Distributed Denial of Service) attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. Websites can guard against bots using CAPTCHA tests that verify users as humans.

- ***Ransomware***. Ransomware, also called an encryption or a crypto Trojan, is a program that infects a host or network and holds the system captive while requesting a ransom from the system/network users. In particular it encrypts data on the affected system (or anyway locks down the system so that the users have no access) and only unblocks it when the correct password (decryption key) is entered. The latter is not given to the victims until after they have paid a ransom to the attacker. Without the decryption key, it's mathematically impossible for victims to regain access to their files. Messages informing the system user of the attack and demanding a ransom are usually displayed. Digital currencies such as Bitcoin and Ether are the most common means of payment, making it difficult to track the cybercriminals. Moreover, there is no guarantee that payment will result in the necessary decryption key being handled back or that the decryption key provided will function properly. Ransomware is one of the most profitable, and therefore one of the most popular, and dangerous kinds of malware programs of the past few years. Companies, in particular, have recently received demands to pay millions to unblock critical services. The most well-known ransomware variants include WannaCry and Petya.

- ***Rogue Software***. Rogue software pretends to offer targets help with getting rid of viruses and other kinds of malware. It then coerces them into, inadvertently, installing - and paying for - malware.

- ***Scareware***. Scareware is a generic term for malware that uses social engineering to frighten or shock a user into thinking their system is vulnerable to an attack. The objective is to induce the user to install a specific software. However, in reality no danger has actually been detected - it is a scam. The attacker succeeds when the user purchases unwanted -

and potentially dangerous - software in an attempt to eliminate the "threat". The term is derived from the word "scare". In most cases, the suggested software is additional malware or purportedly protective software that, in reality, has no value whatsoever. Scareware is mainly found on questionable online platforms and is primarily aimed at inexperienced users.

Some versions of scareware act as a sort of shadow version of ransomware; they claim to have taken control of the system and demand a ransom, but actually they are just using tricks like browser redirect loops to make it seem as if they have done more damage than they really have, and unlike ransomware can be relatively easily disabled.

- ***Crypto-miners***. Crypto-miners, also called Cryptojacking, are a novel family of malware. This malware is employed by cybercriminals to mine digital currencies such as Bitcoin and bitcoin-alike currencies in the background. The computing power of the infected system is used for this - without the user's knowledge, of course. Crypto-miners hide themselves, for instance, as scripts on websites, where they are smuggled in by cybercriminals via security vulnerabilities. The mined coins end up in the attackers' digital crypto wallets. In some cases, crypto-miners are also used quite legally, to monetize websites, for example. However, the site operator must clearly inform visitors of the use of such tools.
- ***File-less malware***. File-less malware is a type of memory-resident malware that uses legitimate programs to infect a computer. As the term suggests, it is malware that operates from a victim's computer memory, not from files on the hard drive. File-less malware registry attacks leave no malware files to scan and no malicious processes to detect. Because there are no files to scan, it is harder to detect and remove than traditional malware; this makes them up to ten times more successful than traditional malware attacks. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted.

Other cyber threats which are not strictly malware are, for example:

- ***Malvertising***. Malvertising is the use of legitimate ads or ad networks to covertly deliver malware to unsuspecting users' computers. For example, a cybercriminal might pay to place an ad on a legitimate website. When a user clicks on the ad, code in the ad either redirects them to a malicious website or installs malware on their computer. In some cases, the malware embedded in an ad might execute automatically without any action from the user, a technique referred to as a "drive-by-download".
- ***Spam & Phishing***. While not being really a malware type, Phishing is a type of social engineering attack commonly used to perform cyber attacks. Phishing is successful since the emails sent, text messages and web links created, look like the are from trusted sources. They are sent by criminals to fraudulently acquire personal and financial information.

  Some are highly sophisticated and can fool even the most savvy users. Especially in cases where a known contact's email account has been compromised and it is then used to spread phishing attacks or malware such as worms. Others are less sophisticated and simply spam as many emails as they can with a message about 'checking your bank account details', for example.
- ***Bug***. In the context of software, a bug is a flaw which produces an undesired outcome. These flaws are usually the result of human error and typically exist in the source code or compilers of a program. Minor bugs only slightly affect a program's behaviour and as a result can go for long periods of time before being discovered. More significant bugs can cause crashing or freezing. Security bugs are the most sever type of bugs and can allow attackers to bypass user authentication, override access privileges, or steal data. Bugs can be prevented with developer educatino, quality control, and code analysis tools.

Any specific piece of malware has both a means of infection and a behavioural category. So, for instance, WannaCry is a ransomware worm. Moreover a particular piece of malware might have different forms with different attack vectors: for instance, the Emotet banking malware has been spotted in the wild as both a trojan and a worm. Finally, many instances of malware fit into multiple categories: for example Stuxnet is a worm, a virus and a rootkit.

Real-world examples

- ***Ransomware example***: In year 2019, the city of Baltimore was hit by a type of ransomware named *RobbinHood*, which halted all city activities, including tax collection, property transfers, and government email for weeks. This attack has cost the city more than $18 million. The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million.
- ***File-less Malware example***: *Astaroth* is a file-less malware campaign that spammed users with links to a .LNK shortcut file. When users downloaded the file, a WMIC tool was launched, along with a number of other legitimate Windows tools. These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners. Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server.
- ***Spyware example***: *DarkHotel*, which targeted business and government leaders using hotel Wi-Fi, used several types of malware in order to gain access to the systems belonging to specific powerful people. Once that access was gained, the attackers installed keyloggers to capture their targets passwords and other sensitive information.
- ***Adware example***: adware called *Fireball* infected 250 million computers and devices in 2017, hijacking browsers to change default search engines and track web activity. However, the malware had the potential to become more than a mere nuisance. Three-quarters of it was able to run code remotely and download malicious files.
- ***Trojan example***: *Emotet* is a sophisticated banking trojan that has been around since 2014. It is hard to fight Emotet because it evades signature-based detection, is persistent, and includes spreader modules that help it propagate. The trojan is so widespread that it is the subject of a US Department of Homeland Security alert, which notes that Emotet has costed US state, local, tribal and territorial governments up to $1 million per incident to remediate.
- ***Worm example***: *Stuxnet* was probably developed by the US and Israeli intelligence forces with the intent of setting back Iran's nuclear program. It was introduced into Iran's environment through a flash drive. Because the environment was air-gapped, its creators never thought Stuxnet would escape its target's network - but it did. Once in the wild, Stuxnet spread aggressively but did little damage, since its only function was to interfere with industrial controllers that managed the uranium enrichment process.

Chapter 3

Proposed Tool

Description of the proposed tool..

Chapter 4

Results

Results analysis..

Chapter 5

Conclusions

Qui si inseriscono brevi conclusioni sul lavoro svolto, senza ripetere inutilmente il sommario.

Si possono evidenziare i punti di forza e quelli di debolezza, nonché i possibili sviluppi futuri o attività da svolgere per migliorare i risultati.

Bibliography