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.

By how they spread

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

- ***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.

- ***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. By embedding copies of itself into files (a.k.a. infecting other executables), which by some means or another are transported to the target, the virus spreads from one computer to another. The medium of transport is often known as the *vector* of the virus. Depending on how complex the virus code is, it may be able to modify the replicated copies. The transport of infected files may be initiated by the virus itself (for example, it may send the infected files as an e-mail attachment) or rely on an unsuspecting human user (who for example transports a USB drive containing the infected file). 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 back-door 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.

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.

By what they do

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:

- ***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. Users sometimes unknowingly infect themselves with adware installed by default when they download and install other applications.

  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.

- ***Backdoor***. 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.

  Most device or software manufacturers place backdoors in their products intentionally and for a good reason. If needed, company personnel or law enforcement can use the backdoor to access the system when needed. 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.

- ***Browser Hijacker***. A *Browser Hijacker*, also called "hijackware", noticeably changes the behaviour of the victim's web browser. This change could be sending the user to a new search page, slow-loading, changing the victim's homepage, installing unwanted toolbars, redirecting the user to sites he did not intend to visit, and displaying unwanted ads. Attackers can make money off advertising fees, steal information from users, spy, or redirect users to websites or apps that download more malware.

- ***Bots/Botnet***. 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, but there are other ways that botnets can be useful to cybercriminals:

  - **Brute force & credential stuffing attacks** - Bots can be used to carry out different types of brute force attacks on websites. They'll use a pre-configured list of usernames and passwords combinations on website login pages. The hope is that with enough tries, they'll get lucky and find a winning combination.
  - **Data and content scraping** - Scraping uses botnets as web spiders to comb through websites and databases to cull useful information they can use to undercut their competition. This could be site content, pricing sheets, or other useful information.
  - **Botnet-as-a-service opportunities** - Cybercriminals sometimes rent their botnets to all types of malicious users - including those who are less tech savvy. This service is also sometimes called malware-as-a-service, according to the International Botnet and IoT Security Guide 2020 by the Council to Secure the Digital Economy (CSDE). These bot armies essentially serve as mercenaries-for-hire to take down a target's servers and networks.
  - **Spambot** - A botnet can also be used to act as a spambot and render advertisements on websites.
  - **Malware distributor** - Finally Botnets can even be used for distributing malware disguised as popular search items on download sites.

Websites can guard against bots using CAPTCHA tests that verify users as humans.

- ***Crypto-miner***. Crypto-miners 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.

  Most crypto-mining apps are usually categorized as PUAs - potentially unwanted apps - or, in rarer cases, as trojans. However, there is a more modern method of crypto-mining - crypto-jacking - that also works in browsers.

  Moreover, according to ESET, most crypto-miners focus mostly on *Monero* as target crypto-currency because it offers anonymous transactions and can be mined with regular CPUs and GPUs instead of expensive, specialized hardware.

- ***File-less malware***. File-less malware is a type of memory-resident malware that uses legitimate code that already exists within the target computer or device 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, taking advantage of legitimate tools and software (known as "LOLBins") that exist within the system. 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.

- ***Keylogger***. 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 loggers can be inserted into a system through phishing, social engineering or malicious downloads.

  Key logging have also legitimate uses, in fact it is often used by law enforcement, parents, and jealous or suspicious spouses. The most common use, however, is in the workplace, where employers monitor the employees' use of the company computers.

- ***RAM Scraper***. *RAM scraper* malware, also known as *Point-of-Sale (POS)* malware, harvests data temporarily stored in a system's memory, also known as Random Access Memory (RAM). This type of malware targets POS systems like cash registers or vendor portals where an attacker can access unencrypted credit card numbers. While this sensitive payment data is only available for milliseconds before passing the encrypted numbers to back-end systems, attackers can still access millions of records.

- ***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. Additionally, some forms of ransomware threaten victims to publicize

sensitive information within the encrypted data. 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: Verizon's 2020 Data Breach Investigation Report shares that 27% if all malware-related incidents they tracked in 2019 involved ransomware.. Companies, in particular, have recently received demands to pay millions to unblock critical services. The most well-known ransomware variants include WannaCry and Petya.

The "Five Uneasy E's" of ransomware, according to Tim Femister - vice president of digital infrastructure at ConvergeOne - are:

- **Exfiltrate**: Capture and send data to a remote attacker server for later leverage.
- **Eliminate**: Identify and delete enterprise backups to improve odds of payment.
- **Encrypt**: Use leading encryption protocols to fully encrypt data.
- **Expose**: Provide proof of data and threaten public exposure and a data auction if payment is not made.
- **Extort**: Demand an exorbitant payment paid via cryptocurrency.

- ***Rogue Security Software***. Rogue Security Software is a from of ransomware or scareware. An attacker enabling this method tricks users into thinking their system or device is at risk. The malware program will present itself as a fake security tool to remove the problem at a cost. In actuality, the user pays up and the artificial security software installs more malware onto their system.

- ***Rootkit***. 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, record user activities, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, mount attacks on other systems 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. Rootkits can be injected into applications, kernels, hypervisors, or firmware. They spread through phishing, malicious attachments, malicious downloads, and compromised shared drives.

  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.

Traditionally, rootkits can install themselves in ring zero (kernel level), although some sources say that they can install themselves all the way up to ring three (user level). This means that they can get as much (or as little) access as necessary.

There are different types of rootkits, which are typically categorized by the reach of the system they affect:

- User-level/application level rootkits - This rootkit can alter security settings, allowing the attacker to replace executables and system libraries and modify interface behaviour.
- Kernel-level rootkits - The rootkit alters the very core of the system, the kernel. Resembling device drivers or loadable modules, they operate at the same security level as the OS, giving the appearance of credibility.
- Hardware/firmware rootkits - Firmware is often use by organizations, however, their persistent presence in the router, network card, hard drive, or BIOS makes detecting it difficult if used maliciously.
- Bootkit rootkits - A type of kernel-mode rootkit infecting boot functionality during computer start-up, subverting the kernel upon powering on.
- Virtualization rootkits - Also known as a hypervisor, the rootkit hosts the target OS as a virtual machine (VM). It can forgo modifying the kernel and subvert the OS.

- ***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.

- ***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.

Other cyber-threats

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

- ***Bug***. In the context of software, a bug is a flaw in a segment of code 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. All software has bugs, and most go unnoticed or are mildly impactful to the user. Security bugs, however, 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 education, quality control, and code analysis tools.
- ***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".
- ***Phishing***. While not being really a malware type, Phishing is a type of social engineering attack commonly used to perform cyber attacks. Phishing, and social engineering in general, is a type of email attack that attempts to trick users into divulging passwords (or anyway personal and financial information), downloading a malicious attachment or visiting a website that installs malware on their system. Phishing is successful since the emails sent, text messages and web links created, look like the are from trusted sources.

  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.

  More targeted efforts at specific users or organizations are known as *spear phishing*. Because the goal is to trick the user, attackers will research the victim to maximise trick potential.

  There are different types of Phishing. Here are mentioned some of them:

  - *Deceptive Phishing* - The most common type. It uses an email headline with a sense of urgency from a know contact. This attack blends legitimate links with malicious code, modifies brand logos, and evades detection with minimal content.
  - *Spear Phishing* - As noted, spear phishing targets specific users or organizations by exploring social media, recording out-of-office notifications, compromising API tokens, and housing malicious data in the cloud.
  - *Whaling* - Even more targeted than spear phishing, whaling targets chief officers of an organization by infiltrating the network, exposing the supply chain, and following up the malicious email with a phone call to give legitimacy.
  - *Vishing* - Targeting victims over the phone, vishing is the use of Voice over Internet Protocol (VoIP), technical jargon, and ID spoofing to trick a caller into revealing sensitive information.

  - *Smishing* - Smishing also targets phone users, but this one comes in the form of malicious text messages. Smishing attacks often include triggering the download of a malicious app, link to data-stealing forms, and faux tech support.
  - *Pharming* - Moving away from trying to trick users, pharming leverages cache poisoning against the DNS, using malicious email code to target the server and compromise web users' URL requests.

- ***Spam***. In IT security, spam is unwanted email. Usually, it includes unsolicited advertisements, but it can also have attempted fraud or links or attachments that would install malware on the victim's system. Most spam emails contain one or more of the following:

  - Poor spelling and grammar
  - An unusual sender address
  - Unrealistic claims
  - Links that look mighty risky

  Spyware might be one of the most universally understood forms of malicious attacks. As billions of users enable email for their everyday lives, it makes sense that malicious actors try to sneak into their inbox. Some of the most common types of spam emails include fake responses, PayPal, returned mail, and social media. All of which are disguised as legitimate but contain malware.

General considerations on malware types

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.

Moreover, in recent years, also ***mobile devices-targeted attacks*** have grown popularity more and more. In fact, among the huge amount of available apps, an increasing amount are not desirable; and the problem is even more acute with third-party app stores. While app store vendors try to prevent malicious apps from becoming available, some inevitably slip through. These mobile malware threats are as various as those targeting desktops and include Trojans, Ransomware, Advertising click fraud and more. They are mostly distributed through phishing and malicious downloads and are a particular problem for jail-broken phones, which tend to lack the default protections that were part of those devices' original operating systems.

Real-world examples

- ***Adware*** *example*: While there are hundreds of adware versionms, some ot the most common examples include *Fireball*, *Appearch*, *DollarRevenue*, *Gator* and *DeskAd*. These adware strains often present themselves as a video, banner, full screen, or otherwise pop-up nuisance.

  The 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.

  Adware dominated the consumer threat detection category in 2019. Malwarebytes reports in its 2020 State of Malware Report that there were 54 million adware detections on Windows (24 million) and Apple (30 million) devices. Adware also captured the top business malware detection as well, increasing a incredible 463% from its 2018 detections.

- ***Backdoor*** *example*: Because backdoors are often intentionally built into products, the number of instances they've been used maliciously is numerous. in 2005, Sony BMG delivered millions of CDs with a rootkit that monitored listening habits and unintentionally left a

backdoor to the device for cybercriminals. In 2017, more than 300,000 WordPress websites were affected by a malicious plug-in that allowed an attacker to place embedded hidden link on victim websites.

- ***Browser Hijacker*** *example*: A handful of notable browser hijackers are *Ask Toolbar*, *Conduit*, *CoolWebSearch*, *Coupon Saver*, *GoSave*, and *RockTab*. These browser hijackers typically come in the form of an added toolbar, and because they are often included in other software downloads, users rarely recognize their potential harm.

- ***Bots/Botnet*** *example*: In 2008, the ***Kraken*** botnet with 495,000 bots infected 10% of the Fortune 500 companies. This instance of a botnet attack was also the first where malware went undetected by anti-malware software. In 2016, one of the biggest (and worse) botnets in existence, ***Mirai***, left most of the eastern U.S. with no internet. This massive botnet of compromised IoT devices, with over 600,000 of them, is responsible for some of the biggest DDoS attacks in recent years and exposed just how vulnerable IoT devices could be and led to the "IoT Cybersecurity Improvement Act" of 2020.

  Echobot is a variant of the well-known Mirai. Exhobot attacks a wide range of IoT devices, exploiting over 50 different vulnerabilities, but it also includes exploits for Oracle WebLogic Server and VMWare's SD-Wan networking software. In addition, the malware looks for unpatched legacy systems. Echobot could be used by malicious actors to launch DDoS attacks, interrupt supply chains, steal sensitive supply chain information and conduct corporate sabotage.

- ***Bug*** *example*: Because bugs are often the root vulnerability that enables malware, almost every attack has something to do with a bug-related exposure.

- ***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.

- ***Keylogger*** *example*: a keylogger called ***Olympic Vision*** has been used to target US, Middle Eastern and Asian businessmen for business email compromise (BEC) attacks. Olympic Vision uses spear-phishing and social engineering techniques to infect its targets' systems in order to steal sensitive data and spy on business transactions. The keylogger is not sophisticated, but it is available on the black market for $25 so it is highly accessible to malicious actors.

  A strain of keylogger malware dubbed ***LokiBot*** notably increased in 2020. CISA reported that LokiBot "employs Trojan malware to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials".

- ***Mobile Malware*** *example*: ***Triada*** is a rooting Trojan that was injected into the supply chain when millions of Android devices shipped with the malware pre-installed. Triada gains access to sensitive areas in the operating system and installs spam apps. The spam apps display ads, sometimes replacing legitimate ads. When a user clicks on one of the unauthorized ads, the revenue from that click goes to Triada's developers.

- ***RAM Scraper*** *example*: Since 2008, RAM scraping has been a boon for retailers. A handful of years later, the now infamous spyware dubbed *BlackPOS* led to the compromise of 40 million Target customers and 56 million Home Depot customers. Heading into the 2020s, a few notable RAM scraping malware families are *FrameworkPOS*, *PoSeidon/FindStr*, *FighterPOS*, and *Canabak/Anunak*.

- ***Ransomware*** *example*: With vendors and organizations increasingly moving online, more data is at risk of exposure. Attackers know this and often take advantage of small to mid-sized oranizations with weaker network security, requesting an amount they knoe the organization can afford. Notable examples from the 2010s included *CryptoLocker*, *Locky*, *WannaCry*, *Hermes*, *GrandCrab* and *Ryuk*.

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.

In year 2020, a new ***CryCryptor*** ransomware masquerading as COVID alert - the official COVID-19 contact-tracing app for Canada - was detected. Thankfully, ESET researchers were able to create a decryption tool to help those whose files were encrypted by the ransomware.

- ***Rogue Security Software*** *example*: Sine if the most common rogue security software have come in spam campaigns and adware. however, a different infection vector for this malware is the technique known as *Black Hat SEO*. By following the most popular keywords on the internet through public records like Google Trends, attackers use malicious scripts to generate websites that appear legitimate.

- ***Rootkit*** *example*: ***Zacinlo*** infects systems when users download a fake VPN app. Once installed, Zacinlo conducts a security sweep for competing malware and tries to remove it. Then it opens invisible browsers and interacts with content like a human would - by scrolling, highlighting and clicking. This activity is meant to fool behavioural analysis software. Zacinlo's payload occurs when the malware clicks on ads in the invisible browsers. This advertising click fraud provides malicious actors with a cut of the commission.

- ***Spyware*** *example*: Spyware often comes in the form of adware, trojans, keyloggers, and rootkits. Some of the best-known spyware strains include *CoolWebSearch*, *Gator*, *Internet Optimizer*, *TIBS Dialer*, and *Zlob*. For example, *CoolWebSearch* used Internet Explorer vulnerabilities to direct traffic to advertisements, infect host files, and rewrite search engine results.

  One recent example of spyware is ***DarkHotel***, which targeted business and government leaders using hotel Wi-Fi. It 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.

- ***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.

  Other notable trojan strains include: ***Trickbot***, ***Ryuk***, ***Sodinokibi***, ***Mirai*** and ***SamSam***.

- ***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.

2.1.4 Malware History

The history of malware begins in the 1960s. At that time, hackers created computer viruses mainly for fun, displaying generally harmless messages that then spread to other computers. Malware has evolved from the days when it was an exciting prank/experiment gone wrong or uncontrolled to now when malware is used for commercial gain. There are various documented instances of malware created within a laboratory setting like the 1962 ***Darwing game***, 1971 ***Creeper***, 1974 ***Rabbit Virus*** and 1975 ***Pervading Animal***.

In particular, the malware called ***Creeper*** was designed to infect mainframes on ARPANET. The program did not alter functions, nor it stole or deleted data, but it moved from one mainframe

to another without permission while displaying a Teletype message that read "I'm the creeper: Catch me if you can." This malware was later altered with the addition of the ability to self-replicate and became the first known computer worm.

The concept of malware took root in the technology industry, and examples of viruses and worms began to appear on Apple and IBM personal computers in the early 1980s before becoming popularized following the introduction of the World Wide Web and the commercial internet in the 1990s.

The previously mentioned 1960s and 1970s malware were kept within a laboratory environment and never escaped to the wild. The first virus known to have been able to escape its creation environment was the ***Elk Cloner*** introduced in 1981, six years after the first personal computers. After the success of this prank gone wild, ***Brain***, the first Microsoft PC virus, was seen in the wild in 1986, and like *Elk Cloner*, it was more annoying than harmful. However, it is the first virus known to conceal its existence on the disk thus evading detection. The next malware that changed the propagating properties of malware is the ***Morris*** worm written in 1988 as an experimental, self-propagating, self-replicating program which was released on the internet.

In 1990, Yisreal Radai coined the term **malware**, short for "malicious software", that would thereafter be used to as a generic term for all software with undesired intent within a system. The following decades saw an evolution in malware that is best defined as a two-dynamic evolution; the growth in complexity and malware sample numbers.

The growth in complexity is defined by the different generations of malware seen over the years:

- The first generation (DOS Viruses) of malware mainly replicate with the assistance of human activity
- Second generation malware self-replicate without help and share the functionality characteristics of the first generation. They propagate through files and media.
- Third generation utilise the capabilities of the internet in their propagation vectors leading to big impact viruses.
- Fourth generation are more organization specific and use multiple vectors to attack mainly anti-virus software of systems due to the commercialisation of malware.
- Fifth generation is characterized by the use of malware in cyberwarfare and the now popular malware as-a-service.

Each jump in generation is characterized by an increase in complexity of the malware and more propagation vectors. Tricks of the older generation of malware are always seen to be re-utilised in newer generations of malware and complexities discovered over the years always seem to follow the evolving trends in technology. The commercial value attached to having access to exploited systems or the ability to infiltrate a network has led to the birth of malware samples which are very evasive. Here is an overview of the most famous malware or malware-related events in recent history:

- ***Melissa*** (1999) - This was a mass-mailing macro virus released in 1999. As it was not a stand-alone program, it was not classified as a worm. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic. The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled "list.doc" containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.
- ***ILOVEYOU*** (2000) - Sometimes referred to as *Love Bug* or *Love Letter for you*, spread like wildfire in year 2000. It is a computer worm that infected over ten million Windows

personal computers when it started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". That file extension ('vbs') was most often hidden by default on Windows computers of the time, leading users to think it was a normal text file. Opening the attachment activated the Visual Basic script. The worm inflicted damage on the local machine, overwriting random types of files, and sent a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook. This made it spread much faster than any other previous email worm.

- ***SQL Slammer*** (2003) - This malware, exploiting a buffer overflow bug in Microsoft's SQL Server, caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic within minutes. It spread rapidly, infecting most of its 75,000 victims within ten minutes.

- ***MyDoom*** (2004) - Also known as *W32.MyDoom@mm*, *Novarg*, *Mimail.R* and *Shimgapi*, it is a computer worm affecting Microsoft Windows. It became the fastest-spreading e-mail worm ever, exceeding previous records set by the Sobig worm and ILOVEYOU, a record which as of 2021 has yet to be surpassed. MyDoom appears to have been commissioned by e-mail spammers so as to send junk e-mail through infected computers. The worm contains the text message "andy; I'm just doing my job, nothing personal, sorry," leading many to believe that the worm's creator was paid. The actual author of the worm is unknown.

- ***Storm botnet*** (2007) - Also known as *Storm worm botnet*, *Dorf botnet* and *Ecard malware*, it is a remotely controlled network of "zombie" computers (or "botnet") that have been linked by the Storm Worm, a Trojan horse spread through e-mail spam. At its height in September 2007, the Storm botnet was running on anywhere from 1 million to 50 million computer systems, and accounted for 8% of all malware on Microsoft Windows computers. Finally it infected about 10 million computers in 9 months in 2007.

- ***Koobface*** (2008) - It was a network worm that attacked Microsoft Windows, Mac OS X, and Linux platforms. This worm originally targeted users of networking websites like Facebook, Skype, Yahoo Messenger, and email websites such as GMail and Yahoo Mail. It also targeted other networking websites, such as MySpace, Twitter, and it could infect other devices on the same local network.

- ***Conficker*** (2008) - Also known as *Downup*, *Downadup* and *Kido*, it was a computer worm targeting the Microsoft Windows operating system. It used flaws in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet. The Conficker worm infected over 15 million Windows systems including government, business and home computers in over 190 countries, making it the largest known computer worm infection since the 2003 *Welchia*. Despite its wide propagation, the worm did not do much damage, perhaps because its authors did not dare use it because of the attention it drew.

- ***Zeus*** (2007-2009) - Also known as *ZeuS*, or *Zbot*, it was a Trojan horse malware package that ran on versions of Microsoft Windows. While it could be used to carry out many malicious and criminal tasks, it was often used to steal banking information by man-in-the-browser keystroke logging and form grabbing. It was also used to install the *CryptoLocker* ransomware. Zeus spread mainly through drive-by downloads and phishing scams. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009.

- ***Stuxnet Worm*** (2010) - It was an extremely sophisticated worm that infected computers worldwide but only did real damage in one place: the Iranian nuclear facility at Natanz, where it destroyed uranium-enrichment centrifuges, the mission it was built for by U.S. and Israeli intelligence agencies.

- ***CryptoLocker*** (2013) - It is considered as the first widespread ransomware attack. It targeted computers running Microsoft Windows and it propagated via infected email attachments, and via an existing *Gameover ZeuS* botnet. When activated, the malware encrypted certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers. The malware

then displayed a message which offered to decrypt the data if a payment (through either bitcoin or a pre-paid cash voucher) was made by a stated deadline, and it threatened to delete the private key if the deadline passes. If the deadline was not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in bitcoin. There was no guarantee that payment would release the encrypted content. Its code now keeps getting repurposed in similar malware projects.

- ***Mirai*** (2016) - First malware to scan the Internet of Things (IoT) - such as IP cameras and home routers - vulnerable devices and used them to perform DDoS attacks on various sites. It turned networked devices running Linux into remotely controlled bots that could be used as part of a botnet in large-scale network attacks. The Mirai botnet was first found in August 2016 and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on computer security journalist Brian Krebs' web site. The source code for Mirai was published on Hack Forums as open-source. Since the source code was published, the techniques have been adapted in other malware projects.

- ***Petya*** *and* ***NotPetya*** (2016-2017) - These global malware attacks also spread far and wide, with particularly damaging effects in Ukraine, where the national bank was hit. The Petya family of ransomware resulted in around $10 billion in damages worldwide. *Petya* targeted Microsoft Windows?based systems, infecting the master boot record to execute a payload that encrypted a hard drive's file system table and prevented Windows from booting. It subsequently demanded that the user make a payment in Bitcoin in order to regain access to the system. The *Petya* malware had infected millions of people during its first year of its release. Variants of Petya were first seen in March 2016, which propagated via infected e-mail attachments. In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. The new variant propagated via the EternalBlue exploit, which was generally believed to have been developed by the U.S. National Security Agency (NSA), and was used earlier in the year by the WannaCry ransomware. This new version was called *NotPetya* to distinguish it from the 2016 variants, due to these differences in operation. In addition, although it purports to be ransomware, this variant was modified so that it is unable to actually revert its own changes.

- ***WannaCry*** (2017) - Quickly became the largest ransomware attack in history. It targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked at least a year prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. The attack was halted within a few days of its discovery due to emergency patches released by Microsoft and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. It spread infecting systems at a terrifying rate of 10,000 PCs per hour. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.

- ***Equifax data breach*** (2017) - Hackers pulled off one of the most devastating data breaches in history when they managed to crack Equifax (also in 2017, which was a difficult year for cybersecurity). One of the four major credit reporting bureaus, Equifax keeps highly sensitive data including social security numbers, credit card numbers, load and debt info, bank account details, birthdays, and more. Hackers were able to access the personal data of 143 million people in the hack.

- ***Emotet*** (2018) - This malware, also known as *Heodo*, was first detected in 2014 and deemed one of the most prevalent threats of the decade. First versions of the Emotet malware functioned as a banking trojan aimed at stealing banking credentials from infected hosts. Throughout 2016 and 2017, Emotet operators, updated the trojan and reconfigured it to work primarily as a "loader," a type of malware that gains access to a system, and then

allows its operators to download additional payloads. Second-stage payloads can be any type of executable code, from Emotet's own modules to malware developed by other cybercrime gangs. Initial infection of target systems often proceeds through a macro virus in an email attachment. The infected email is a legitimate-appearing reply to an earlier message that was sent by the victim. It has been widely documented that the Emotet authors have used the malware to create a botnet of infected computers to which they sell access in Malware-as-a-Service. Emotet is known for renting access to infected computers to ransomware operations, such as the Ryuk gang. In 2020, Emotet campaigns were detected globally, infecting its victims with TrickBot and Qbot, which are used to steal banking credentials and spread inside networks. In January 2021, international action coordinated by Europol and Eurojust allowed investigators to take control of and disrupt the Emotet infrastructure. The reported action was accompanied with arrests made in Ukraine.

- ***LockerGoga*** (2019) - This is a new ransomware family that has been detected attacking industrial companies, severely compromising their operations. It has the ability to spawn different processes in order to accelerate the file encryption in the system. The file-encrypting malware's entrance to the scene began when it was allegedly involved in attacking an engineering consulting firm based in France.

- ***Ryuk*** (2019-2020) - This is a type of ransomware known for targeting large, public-entity Microsoft Windows cybersystems. It typically encrypts data on an infected system, rendering the data inaccessible until a ransom is paid in untraceable bitcoin. Ryuk is believed to be used by two or more criminal groups, most likely Russian, who target organizations rather than individual consumers.

- ***COVID-19 related scams*** (2020) - In 2020, as the COVID-19 pandemic rocked the global landscape, affecting nearly every person and every industry in the world - hackers took notice. Many cybercriminals took advantage of the people's fear of the novel coronavirus to peddle COVID-19 related phishing scams. From spoofing the World Heath Organization to offering fake remote jobs, hackers used fake communications to deploy malware and hijack sensitive personal data to use for identity theft and other purposes. Another example is that of a malicious Android app called *CovidLock*, which claims to be a real-time coronavirus outbreak tracker but instead is a ransomware that attempts to trick the user into providing administrative access on their device and then locks it requesting a ransom.

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