BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES
ÚSTAV JAZYKŮ

MALWARE: BEHAVIOUR, DETECTION AND PREVENTION
MALWARE: CHOVÁNÍ, DETEKCE A PREVENCE

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR **Jakub Langer**
AUTOR PRÁCE

SUPERVISOR **Mgr. Ing. Eva Ellederová, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Angličtina v elektrotechnice a informatice**
obor Angličtina v elektrotechnice a informatice
Ústav jazyků

Student: Jakub Langer ***ID:*** 220916

Ročník: 3 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Malware: chování, detekce a prevence

POKYNY PRO VYPRACOVÁNÍ:

Vymezte koncepci malwaru, vysvětlete, jak se různé druhy malwaru chovají a navrhněte, jak se dají detekovat a jak jim předcházet.

DOPORUČENÁ LITERATURA:

1) Aycock, J. (2006). Computer viruses and malware. Berlin: Springer.
2) Bettany, A., & Halsey, M. (2017). Windows virus and malware troubleshooting. New York: Apress.
3) Koret, J., & Bachaalany, E. (2015). The Antivirus hacker's handbook. Indianapolis: Wiley.
4) Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). Malware analyst's cookbook and DVD. Tools and techniques for fighting malicious code. Hoboken: Willey Publishing, Inc.
5) Sikorski, M., & Honig, A. (2012). Practical malware analysis: The hands-on guide to dissecting malicious software. San Francisco: No Star Press.
6) Szor, P. (2005). The art of computer virus research and defense. Boston: Addison-Wesley.

Termín zadání: 9. 2. 2023 ***Termín odevzdání:*** 30. 5. 2023

Vedoucí práce: Mgr. Ing. Eva Ellederová, Ph.D.

doc. PhDr. Milena Krhutová, Ph.D.
předseda oborové rady

Abstract

This bachelor's thesis deals with a form of cybercrime that takes advantage of malicious software, also called malware. It outlines the basics of computer security threats, explaining relevant terms and concepts. Next, the thesis progresses through the most common and dangerous types of malware, describing each of them while also incorporating information such as how the particular type of malware has affected the world. Then, it focuses on the fundamentals of malware detection and outlines how users can protect themselves through prevention techniques. The thesis aims to create a manual that ordinary computer users could use to protect themselves from different types of malware.

Key words

Malware, Internet, computers, cybercrime, computer security, IT, detection, prevention

Abstrakt

Tato bakalářská práce pojednává o formě počítačové kriminality, která využívá škodlivý software zvaný malware. Nastiňuje základy počítačových bezpečnostních hrozeb a vysvětluje relevantní pojmy a koncepty. Poté práce postupuje přes nejběžnější a nejnebezpečnější typy malwaru, přičemž každý z nich popisuje a zároveň začleňuje informace o tom, jak konkrétní druh malwaru ovlivnil svět. Práce se dále zabývá základy detekce malwaru a popisuje, jak se uživatelé mohou chránit pomocí preventivních technik. Cílem práce je vytvořit manuál, který by mohli použít běžní uživatelé počítačů ke své vlastní ochraně před malwarem.

Klíčová slova

malware, internet, počítače, kyberkriminalita, počítačová bezpečnost, IT, detekce, prevence

Rozšířený abstrakt

V dnešní době jsou internet, mobilní telefony a chytrá zařízení nezbytnou součástí našich životů. Uživatelé však často zapomínají na to, že závislost na technologiích otevírá dveře dalšímu nebezpečí zvanému malware. Nebezpečí, která většinou začínají řešit příliš pozdě. Tato bakalářská práce na téma *Malware: chování, detekce a prevence* (*Malware: behaviour, detection and prevention*), pojednává o škodlivých programech známých jako malware – z anglického malicious software, tedy škodlivý software.

Práce má charakter teoretické studie, která využívá různé zdroje jako například odborné knihy a časopisy, výzkumné zprávy, blogy, ale také dokumenty a manuály firem, které vydávají anti-malwareové programy a publikují novinky z oblasti kyberbezpečnosti. Formou bakalářské práce je literární rešerše, která tyto zdroje kriticky vyhodnocuje, porovnává a zjišťuje, jak kvalitně je téma malwaru zpracováno, popřípadě kde by bylo vhodné pokračovat s výzkumem. Celá práce je zpracovaná tak, aby ji mohli využít jak odborníci z oblasti informačních technologií, tak i méně zkušení uživatelé.

Úvodem práce vymezuje koncept malwaru a zmiňuje hrozby spojené s používáním počítačů a jiných zařízení. V první kapitole je uveden popis několika nejznámějších druhů malwaru a rozdíly mezi nimi se zohledněním historie daného malwaru a příkladem již provedených útoků. Kapitola představuje teoretický základ důležitý pro druhou kapitolu zaměřenou na detekci malwaru.

Druhá kapitola popisuje, jak se anti-malwareové programy snaží malware najít, identifikovat a zneškodnit. Vzhledem k neustálému vývoji a obecné komplexnosti tohoto tématu jsou v této kapitole vysvětleny převážně základy fungování detekce. Cílem této kapitoly je přiblížit uživatelům, jak funguje ochrana před malwarem.

Třetí kapitola se zabývá prevencí malwaru, kterou by měli jak uživatelé, tak i firmy aplikovat v každodenním životě. Tato kapitola například teorie tvorby hesel, správné zálohování dat, ale také zmiňuje nejčastější chyby, které uživatelé dělají. Tyto informace mohou být užitečné pro uživatele při aplikaci preventivních opatření proti malwaru a mohou být sdíleny s dalšími lidmi, kteří jsou náchylní stát se obětí malwaru.

Práce je zakončena stručnými doporučeními pro bezpečnost uživatelů v online světě. Závěrečná podkapitola „Malware Prevention Tips“ shrnuje všechny informace získané

během rešerše literatury a představuje alternativu pro ty, kteří nechtějí číst celou práci, ale chtějí rychlý přehled o tom, čeho je třeba se vyvarovat, a co naopak dodržovat.

Cílem předložené bakalářské práce bylo zpracovat text, ve kterém se čtenáři dozví základy fungování malwaru. Kromě popisu jeho druhů a rozdílů, čtenáři získají základní informace o detekci a prevenci útoků. Kombinace těchto znalostí by měla sloužit pro pochopení této problematiky, a následné edukaci ostatních. Na téma malware, a obecněji kyberbezpečnost lze objevit nespočet informací, od informací z devadesátých let až po informace z tohoto roku. Díky neustálému vývoji malwaru a technologií to není překvapivé, ale stále se mohou vyskytnout chyby, jako například zaměňování slov virus a malware, kdy virus je pouze jeden z různých druhů malwaru. Tuto stejnou chybu lze nalézt i u popisu anti-malware programů, kdy mnohem zaběhlejší (a nesprávný) termín je anti-virus, tedy program, který by se snažil detekovat a zneškodňovat pouze a jen virusy. Většina publikací se zabývá malwarem z technického hlediska a popisují, jak funguje jeho kód, jak vzniká a jak ho odhalit. I když je to velmi důležité pro pokrok v detekci a obraně, takový proces může být pro běžné uživatele dlouhý, složitý a nezajímavý. Pokud je cílem vzdělávat uživatele globálně, je nutné začít popisovat malware i ve zjednodušené formě, která bude pochopitelná i pro ty, kteří nejsou technicky zdatní.

Malware z našeho světa nezmizí. Dokud existují počítače, chytré telefony a další technologie, budou existovat i lidé, kteří se budou snažit je nekale využít. Jako uživatelé se s tímto musíme naučit žít a stejně jako se lidé učí dodržovat dopravní předpisy, je důležité, abychom se také naučili bránit se proti malwaru. Digitální svět je dnes pro mnoho z nás nedílnou součástí života, a proto je nutné, abychom se naučili chránit svá data a svou digitální identitu.

Langer, J. (2023). *Malware: Behaviour, Detection and Prevention*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. 44 s.
Vedoucí bakalářské práce: Mgr. Ing. Eva Ellederová, Ph.D.

Prohlášení

Prohlašuji, že bakalářskou práci na téma *Malware: chování, detekce a prevence* jsem vypracoval samostatně pod vedením vedoucí bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne 30. 5. 2023 .....

Jakub Langer

Acknowledgements

I want to thank my supervisor Mgr. Ing. Eva Ellederová, Ph.D., for her guidance, assistance and great interest in helping me with my work.

Table of Contents

Introduction

Computers, the World Wide Web, and the Internet of Things (IoT) are nowadays an integral part of humanity. They are used everywhere, by individuals, companies, and even in various industries, for example in healthcare, education, engineering, transport, agriculture, commerce and finance. The use cases involve not only communication between individuals but also the storage of enormous quantities of data, ranging from databases to vital infrastructure in every country. Nowadays, it is quite unthinkable to live without electronic communication for days, let alone weeks. If humanity ended up in some extreme scenario, where all devices used to connect to the Internet stopped working for a week, a global pandemic would occur. Besides the essential survival needs such as housing, food and water, humanity has become dependent on access to computers and the Internet, and it is not able to function without it again

However, besides considerable benefits, the Internet and computers bring serious disadvantages, such as cybercrime – criminal activity used by and on devices that can connect to a network. It is particularly important to note that cybercrime can affect *anyone*, not only ordinary computer users but also highly educated computer-literate individuals.

The goal of this bachelor's thesis is to deal with a form of cybercrime that utilizes malicious software or malware. Although malware was examined quite extensively, there can be found some inconsistencies in concepts by different authors. Furthermore, understanding scholarly articles and books requires considerable information technology (IT) expertise, hence making it an unreachable resource to many ordinary users.

I have decided to discuss the topic of malware because of the benefits and opportunities that computers and digital world around us provide, but I am conscious of the risks involved. For this reason, my aim is to make a simple, yet comprehensive guide to the dangers that malware causes to computer users and to clarify some misconceptions as well. The thesis begins with some fundamental concepts and information that serve as a foundation for understanding the following chapter which describes different types of malware. A particular type of malware is always framed, followed by the description of its behaviour, possible dangers and real-world examples. Understanding how malware operates is crucial, therefore this thesis should serve as a comprehensive manual for all computer users.

1 The Concept of Malware

Malware is a serious threat to computer security, as it can cause a wide range of problems, from stealing sensitive information to disrupting the normal functioning of a computer. There are many types of malware, each with its own unique characteristics and methods of operation. Each type of malware has its own specific characteristics that can cause different types of damage. It can be spread in several ways, including through email attachments, downloads from the Internet, and even through removable media such as USB drives.

As malware becomes increasingly sophisticated, individuals and organizations need to take steps to protect themselves. By understanding the threats posed by malware and implementing appropriate precautions, they can help reduce the risk of successful attacks.

This chapter will provide a brief introduction to computer security threats and an explanation of the term *malware*. Furthermore, it will discuss different types of malware, their behaviour, potential harm and various methods to spread and infect systems.

1.1 Introduction to Computer Security Threats

According to Aycock (2006), computer threats can be divided into four major groups: spam, bugs, denial-of-service attacks, and lastly, malware. In order to understand the basic concept of malware, this chapter will focus on these four groups.

The first one is *spam*. It is a term that is now commonly known among Internet users. Spam is defined as an "unwanted email, usually advertisements" ("Spam", n.d.) which is true, but also it is not a complete definition. Spam itself is not only bound to be an email, but any type of unsolicited message being sent to a large number of receivers. The intentions can indeed be advertisements, but they can be also used for fraudulent purposes. One of them can be phishing, which is trying to get privileged information from users. This can be done by gaining their trust (pretending they are someone that they know), impersonation of a known entity (pretending to be a bank they use) or even trying to scare them. Most of the time, the end goal is to get a user to click on a link, let them type their password, or make them download something such as malware, which will be covered later on (Aycock, 2006).

Bugs are errors in the source code of programs. They result in programs behaving as not intended – think of a "settings" button that does not register when it is being clicked on. That

is an example of quite a harmless bug. Bugs can be considered as vulnerabilities. Sometimes, there can be instances of bugs that cause security weaknesses that can be exploited – exposing users to data leaks or ransom. Since most of cybersecurity is a cat-and-mouse game, where criminals find and abuse vulnerabilities while the other side is trying to fix them, companies are making "bug bounties". That is when company X offers price Y to anyone who finds major bugs. This acts as an incentive for skilled people to find and report them, instead of abusing them or selling them to nefarious parties (Aycock, 2006).

A *denial-of-service attack* (DoS) makes access to site resources impossible for the user. It overwhelms the host services of the attacked network, making the desired site slow or unusable. This disruption can end with overloading and crashing the site or completely shutting the services down. For example, if someone goes to order food at an empty restaurant, they get it almost immediately since there is no traffic. If they go there later on when there are 50,000 people, not only will they never get their order or food, but the entire restaurant might collapse (Aycock, 2006).

Finally, there is malicious software or malware. *Malware* is an umbrella term that covers types of it such as viruses, trojans and spyware. Other related threats will be covered in greater detail in the upcoming chapters. What is important is that malware is used with malicious intentions, often using various means to be distributed or deployed. It can be distributed via spam, deployed when a perpetrator discovers bugs leading to security breaches and, by taking advantage of them, they can carry out DoS attacks (Aycock, 2006).

1.2 Types of Malware

The proliferation of malware has been a major concern for individuals and organizations alike, as it can have serious consequences, such as financial losses, reputational damage, and even national security threats. In recent years, malware has become increasingly sophisticated and difficult to detect and defend against, making it a constant and evolving threat to both personal and business computers.

This chapter will examine the behaviour, historical impact and current state of different types of malware and discuss the methods and tactics employed by cybercriminals to infect the devices, spread, and evade detection and mitigation.

1.2.1 Viruses

The virus is a type of malware that acts similarly to the term virus used in biology. The latter injects its code into a host cell, effectively turning the cell into a factory that keeps replicating and creating more viruses that try to find new host cells, and the whole process repeats. Computer viruses work similarly. They are smaller strings of code that wait for a specific trigger. They are not executable files by themselves. Instead of being standalone programs, they are typically integrated into another program. Once opened, the virus code spreads to other executable files, evolving and replicating (Aycock, 2006; Schneider, 1989).

What Aycock (2006) fails to address is the potential harm that can come out of viruses. The damage that they can cause ranges from deleting programs to reformatting hard drives – resulting in deleting all the data.

The slight differences between its new generations make the virus difficult to eliminate. Even if a specific malicious code is detected, new generations of viruses might have already spread and need to be located. Schneider (1989) points out that the virus in its *incubation phase* is virtually impossible to detect. There are two more phases. The second one is the *infection phase* which is when the virus attempts to spread and replicate. The final phase is the *destroy phase* when the virus starts harming devices by deleting or modifying files. Viruses spread within a single computer. In order to infect others, it needs a human that takes it via a flash drive, SSD, or any other media storage that has files infected with viruses. By plugging it into another computer, the virus spreads once again.

1.2.2 Spyware

Spyware is a type of malware that, as the name indicates, spies on computer users. Bettany and Halsey (2007) explain that it gathers private data about the users from both the online and physical worlds. The collected data can be what the users buy, what they like, what their interests and even their locations are.

Bettany and Halsey (2007) seem to oversimplify and fail to fully express the risks of spyware. Aycock (2006), however, offers a more in-depth look at what spyware gathers. The first and foremost are *usernames and passwords* that can be subsequently used by anyone to log in to the user's numerous accounts and have complete control over them. Similarly, it can steal their credit card numbers, software license keys (with the purposes of software

pirating) and email addresses. Email addresses are especially valuable for phishing attacks. Alkhalil et al. (2021, March 9) confirm that by using email, phishers try to redirect users to malicious websites. A *phisher* is an individual who seeks to deceive someone by phishing ("Phisher", n.d.) They use social engineering to get people to click on links, distributed via emails. Some of this can be done by using software called *keylogger*. Keyloggers function by recording and stealing consecutive keystrokes that the user enters on a device (Aycock, 2006; Bettany & Halsey, 2007; Malwarebytes, n.d.).

Aycock (2006) emphasizes that it is also necessary to note that worms and viruses can act similarly to spyware. They can collect data about their victims but there is a distinction, spyware cannot reproduce by itself. However, it can be a part of another program the users install, or it can exploit some technical flaws in web browsers.

1.2.3 Trojans

A *Trojan horse* (*Trojan*) is a type of malware that pretends to be an application the users want, while secretly retaining another malicious payload. To be more precise, it can pretend to be a web browser plug-in, pirated video game or installer for an operating system such as new Windows 11 (Bagnall, Broomes & Russell, 2000).

The name is based on Greek mythology. According to a legend, the Greeks built a gigantic wooden horse in which they hid soldiers. They later presented this horse to the Trojans as a victory trophy. This clever tactic allegedly worked, and the Trojans brought the present inside the city. That night, the soldiers left the horse and opened the gates for the rest of the Greek army, creating chaos and thus ending the war.

The functioning of Trojans can be understood by giving an example of a pirated video game. While the user is distracted enjoying their new application, the Trojan can set up in the background while being overlooked by the user. Aycock (2006) describes this malicious attack as follows:

> A classic example is a password-grabbing login program which prints authentic-looking "username" and "password" prompts, and waits for a user to type in the information. When this happens, the password grabber stashes the information away for its creator, then prints out an "invalid password" message before running the real

> login program. The unsuspecting user thinks they made a typing mistake and re- enters the information, none the wiser. (p. 27)

As claimed by Syngress (2000), users can observe alternative potential payloads that can wipe out files, format the hard drive or launch a real working application, like the pirated operating system, with the intent of defeating security.

The term *Trojan* was first used in *Unix Programmer's Manual* by Thompson and Ritchie (1971). Interestingly, the manual already assumed the users know the term Trojan Horses and what can it accomplish. Thompson and Ritchie (1971) note that "one may not change the owner of a file with the set-user-ID[1] bit on, otherwise one could create Trojan Horses able to misuse other's files". Another reference to Trojan is made in the US Air Force report concerned with vulnerabilities in the Multics operating system (Karger & Schell, 1974).

1.2.4 Ransomware

Ransomware is one of the most dangerous types of malware whose goal is to extort victims into paying a ransom. It does this by encrypting documents and data that are important to users. If users want to use their computers and have their files back, they need a decryption key which will be handed over to them, assuming they will pay the initial ransom. Cybercriminals typically demand ransom in the form of cryptocurrency, digital money that is unregulated by any authority or bank (Reshmi, 2021; Bettany & Halsey, 2017). Cybercriminals find it highly convenient since they can choose the cryptocurrency that cannot be tracked back to them, hence making it a tempting option. Figure 1 displays what a ransomware message can look like.

[1] Set-user-ID on execution is a special type of file permission in Unix and Unix-like operating systems such as Linux and BSD. It is a security tool that permits users to run certain programs with escalated privileges. (*Computer Hope Dictionary*, 2020, August 2)

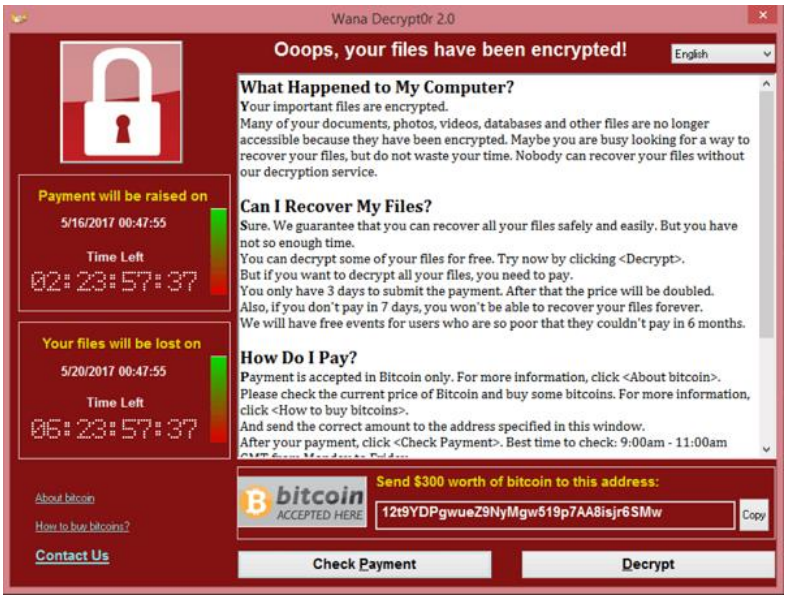

Figure 1. Example of ransomware message.
Reprinted from https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/

Reshmi (2021) focuses on how ransomware is specifically dangerous for big corporations and in digital infrastructures, such as the energy sector, financial services sector, emergency services sector and, naturally, the information technology sector. Bettany and Halsey (2017) further indicate that when some of these massive companies or sectors become infected by ransomware, they lose money or, in cases such as hospitals, even lives. Since every minute can mean a serious loss, they prefer paying a "fair" ransom rather than facing and dealing with unplanned downtime and losing sensitive data and files. Many people and companies pay ransom every year because cybercriminals are conscious of the fact that they cannot make the ransom too high, otherwise no one would pay them.

Regarding a "fair" price, according to the report by Kaspersky Lab (n.d.), global cybersecurity and anti-virus provider, the ransomware attack called WannaCry demanded initially $300 and later on $600 for the decryption key. This attack hit around 230 000 computers in 150 countries and led to $4 billion in losses. It is important to note that businesses lose not only money from the ransom itself but also from the downtime they face.

In order to better understand how serious the threat of ransomware is, Osterman Research, (2016) conducted a survey with 540 companies from Canada, Germany, the United Kingdom and the United States and found out that 39 percent of the companies dealt with ransomware.

Another fascinating takeaway was that globally, approximately 40 percent of the victims paid the ransom, and the most targeted industries were healthcare and financial services. Lastly, over 50 percent of companies deemed ransomware to be a “concern” or “extreme concern”.

1.2.5 Bots

Bots are more complicated since they are not inherently evil by themselves. The way in which they are utilized determines whether they are used for good or bad intentions. Malwarebytes (n.d.), an anti-malware software provider, define a bot as

> an automated piece of software that performs predefined assignments, usually over a network. We use bots for the same reason we use machines in factories: efficiency. A bot can perform monotonous responsibilities quicker and better than a human being over a long period. They are so useful that some estimates indicate that over 50% of web traffic is just bots doing tasks.

Chatbots used by online stores and business websites can be considered harmless and useful bots. In these environments, the bots are applied to deal with customer inquiries, e.g. frequently asked questions (FAQ). Therefore, corporations do not need to employ humans to manually respond to everyone, but they predefine answers to the most frequent questions. Zeifman (2017, January 24) examined 16.7 billion visits to 100,000 randomly selected domains as part of their extensive research on bot traffic in 2016. He found out that 48.2 percent of Internet traffic was done by humans, while the remaining 51.8 percent was achieved by bots out of which 28.9 percent were perceived as harmful. Zeifman’s results confirm the above-mentioned statement by Malwarebytes (n.d.), but the question arises of how harmful malicious bots can be.

Malicious bots have a wide range of capabilities, but their most common use is to launch DoS attacks (Banday & Qadri, 2009; Bettany & Halsey, 2017). To launch a DoS attack, the cybercriminals require a considerable number of bots and thus they need to set up software called *botnet* (Geer, 2005). Botnets can be understood as an army of bots that can swarm simultaneously on a given site to make its service unavailable. The coordinated attack overwhelms the target’s network, rendering it useless. It is necessary to note that at this point, a distinction between a DoS attack and a Distributed Denial of Services (DDoS) attack,

where the latter is a situation where the attack utilizes different compromised systems (Banday & Qadri, 2009; Bettany & Halsey, 2017; Geer, 2005). Aycock (2016) also uses an important term called *zombies* to characterize computers that were compromised and can be operated by cybercriminals. According to Geer (2005), "botnets can also be used for mass spam mailings, installing key-logging software that can steal victims' passwords and data, and compromising computers to prepare them for infection by future viruses" (p. 1).

1.2.6 Worms

Bettany and Halsey (2007) explain that both viruses and worms are the most known types of malware. Interestingly, they are both named after the means of their distribution in the system. As mentioned before, viruses can spread from one medium to another only with the help of humans, e.g. a person plugging infected flash drives into a new machine. Worms, on the other hand, can propagate to other devices by "burrowing", just like earthworms, through networks. Another distinction between worms and viruses is that the worms are standalone.

Shah et al. (2017) classify worms into five major categories: *email worms* that distribute through emails and spread when their victim, for example, opens attachments**;** *instant messaging worms* (IM worms) that use messaging applications such as Viber or Facebook Messenger; *Internet worms* that move through the network, relying on their speed of propagation; *worms propagating via Internet Relay Chats*[2] that work on the same principle as email worms only using a different medium; and lastly, *file-sharing network worms* that spread through a peer-to-peer (P2P) network.

Worms can have malicious payload attached to them, but even the ones without any can cause harm. The harm is caused when they keep constantly replicating, which results in losing a space on the hard drive or slowly but steadily overloading networks (Shah et al., 2017).

The most infamously known worm is the Morris worm also referred to as the Internet worm. It was designed by a Cornell University student, Robert Tappan Morris, and published on November 2, 1988. Allegedly, the intention behind this worm was to map out the Internet at that time, and it was made solely for educational purposes (Jajoo, 2021, December 15). Due

[2] Internet Relay Chat (IRC) is a text-based chat system for instant messaging. IRC is designed for group communication in discussion forums, called channels (Oikarinen & Reed, 1993).

to its nature, the Moris worm spread to ten percent of all computers (circa 60 000 computers). Each additional infection on the same machine slowed it down until the point where computers started crashing. FBI (2018, November 2) says that "the exact damages were difficult to quantify, but estimates started at $100,000 and soared into the millions". Morris was tried and convicted of violating Title 18 of the United States Code. After appeals, they sentenced him to three years' probation, four hundred hours of community service, and a fine equivalent to $20,000 in 2021 (Markoff, 1990, May 5).

1.2.7 Adware

Adware stands for advertising-supported software. The most common way to experience this is through advertisements displayed while browsing the web. The advertisements are delivered as web banners or pop-up ads (Australian Institute of Criminology, 2016).

Stafford and Urbaczewski (2004) point out how adware not only delivers ads to users, but also how it tries to tailor the advertisements for them. It does so by tracking the user activity and then bringing relevant advertisements, for instance, while searching for a new pair of running shoes, they may begin to receive pop-ups for websites that sell similar shoes shortly after, which indicates that the purpose of adware is primarily commercial. This behaviour of adware is observed by Aycock (2006) and the Australian Institute of Criminology (2016) who also add that adware not only monitors the activity of users but also their habits and computer usage. They then acknowledge that the information collected about users may be further passed on to other parties for marketing purposes without the knowledge of users.

Assuming the breach of privacy is ignored, adware is relatively harmless compared to other types of malware discussed previously, but it is particularly annoying for users to deal with. There are some instances where adware promotes pornographic materials, be it websites, videos or pictures, which users can find offensive and inappropriate (Australian Institute of Criminology, 2016; Bettany & Halsey, 2017). Regarding its classification, it is sometimes difficult to decide where adware actually belongs. For example, Bettany and Halsey (2017) classify adware as its own class of malware. Similarly, Aycock (2006) echoes this approach, but he also mentions that there are some resemblances with spyware. However, Stafford and Urbaczewski (2004) contradict this and deal with adware as a subcategory of spyware. They observe that spyware has the potential to be incorporated into adware. As already acknowledged in this chapter, in some cases it can gather and monitor data about the users.

Sriramachandramurthy, Balasubramanian and Hodis (2009) discuss how adware can include keyloggers to further obtain information such as emails, passwords and bank details. This is confirmed by the Australian Institute of Criminology (2016) and Sriramachandramurthy et al. (2009). They further delve into how this opens up an opportunity for potential identity theft.

1.2.8 Logic Bombs

The malware attacks dealt with in the previous chapters have one thing in common: they originate from the outside, i.e. when a cybercriminal is located somewhere else than at the victims' homes, which may be in a different country or even in a different continent. But some attacks are launched from the inside, such as using logic bombs. Since an insider attack requires a certain level of system access, these attacks can be even more dangerous (Dusane, 2020).

Botacin and Grégio (2021) define *logic bombs* as malware that is triggered only under predefined specific conditions. They mention that this kind of malware is one of the hardest to stop since it is frequently embedded in legitimate software. While they neglect how a logic bomb is designed in relation to coding, Aycock (2006) states that the code contains two parts, the first one is the *payload*, which is the action that the code performs. The second part is called a *trigger*. The trigger is a condition under which the payload gets executed. What is interesting is that the trigger is not restricted to anything, it can be based on the date, time, and the number of database entries as well as the absence of something, e.g. when a user does not log in on a particular day (Aycock 2006; Bist, 2014; Dusane, 2020). Logic bombs that only activate under specific time conditions are referred to as *time bombs*.

Bist (2014) further discusses how the logic bomb must be unwanted and also unknown to the user. Users regularly come across free time-limited trials for software which allow them to use the program for a set amount of time, such as thirty days, after which the program stops working and prompts them to purchase the full version. Although there are resemblances to the logic bomb, users might realize that this is simply a sample version that cannot be interpreted as unwanted, malicious or unknown.

A contract employee for Siemens Corporation was found guilty in 2019 by the federal court and given punishment in the form of a $7,500 fine, a six-month jail term, and two years of

supervised release when he was discharged from prison. From 2014 through 2016, the convicted, David Tinley, embedded logic bombs into software created for Siemens Corporation, which resulted in software corruption. Siemens was unaware of the cause of the malfunctions and asked Tinley to fix them, which allowed him to profit from both the creation of the program and the patching of flaws that he purposefully caused (United States Department of Justice, 2019, December 17).

1.2.9 Fileless Malware

Malware can be divided into two classes: fileless malware and malware that requires a host to function. Thus, fileless malware does not require a host file to run, which is important since this allows it to be harder to trace, hence making it troublesome to detect and protect attacked users (Kara, 2022). Mansfield-Devine (2017) agrees with this but also adds that "when a computer is compromised, one of the first things a security specialist will look for is software that shouldn't be there" (p. 7). Sudhakar and Kumar (2020) claim that this was one of the reasons why fileless malware was developed. It works by utilizing the system's main memory, making very few changes in the files and hence leaving fewer traces of its existence. Since all antivirus software back in 2002 could not identify this sort of malware, it developed into a threat.

Johansen (n.d.) divides fileless malware into four types based on how they can infiltrate computers. The first type uses phishing emails, which contain links that look legitimate on the surface. When users click on the link, it loads into the computer's memory, allowing the perpetrator to utilize scripts to collect and subsequently share users' data. The second type uses already installed applications, for example, Microsoft Word or JavaScript in which the malicious code can be injected. The third type uses highly trusted applications e.g. Microsoft PowerShell or Windows Management Instrumentation. Lastly, there can be websites arranged to look like legitimate ones. These are set up by cybercriminals with the purpose to deceive users into believing they are on the correct website. The website searches for opportunities to exploit when users get there. One of these may be a flaw in the Flash plugin, which would make it possible for malicious code to run in the browser memory.

1.3 Summary of Chapter 1

In this chapter, an introduction to computer security threats including spam, bugs, DoS, and most notably malware, was presented to provide readers with a solid foundation for the following chapters of this thesis. The subsequent sections explored different forms of malware, outlining their functionalities, applications, and associated hazards. Understanding this chapter is crucial for readers to gain important insight into the detection of malware, which is the primary focus of the next chapter.

2 Malware Detection

As malware threats grow in the modern digital environment, it is necessary to develop efficient approaches for finding malware, which is currently a critical aspect of computer security. Malware detection refers to the identification and removal of harmful code or activity within a system or network. However, detecting malware is challenging because cybercriminals are improving their methods to avoid detection. Effective malware detection is essential for protecting computer systems and networks from cyberattacks, data theft, and other malicious activities. For this reason, this chapter aims to examine and explain fundamental methods of malware detection and their advantages and drawbacks in an easy-to-understand manner.

2.1 Anti-malware Detection Techniques

Many anti-malware detection techniques have been utilized throughout history and are currently in use to detect and prevent malware. The topic of anti-malware detection plays a significant role in malware prevention. As such, this chapter will focus on the main malware detection techniques and their description.

2.1.1 The Process of Detection

According to Aycock (2016), anti-malware software performs three primary tasks: detection, identification and disinfection.

Detection involves determining whether a piece of code is infected with a malware or not. This process produces a Boolean result, indicating whether the code is infected (yes) or not (no). However, to put it simply, detection is an unwinnable game. Cybercriminals can create malware that initially goes undetected by anti-malware software. In response, anti-malware software must be updated regularly to keep pace with these evolving threats. The cyclical nature of malware detection and evasion perpetuates the challenge of effectively mitigating malware attacks, posing a significant threat to computer security. The ongoing cycle of malware detection and evasion makes it challenging to effectively prevent malware attacks, which creates a grave threat to computer security.

Identification is used for sorting the actual type of malware. In other words, after detecting malware, it identifies what type of malware has been detected.

Disinfection is cleaning or removing detected malware. To conduct disinfection, the malware must first be accurately identified.

Aycock (2016) notes that the malware analysis methods can be divided into two categories, *static* and *dynamic*, and while Souri and Hosseini (2018) acknowledge this, they also stress that the main detection approaches *are* behaviour-based and signature-based. It is crucial to investigate both types of methods of identifying and analysing malware, as they are important detection techniques.

Souri and Hosseini (2018) explain that *signature-based detection* is the most generally utilized procedure in anti-malware software. Signature-based malware detection is a way for anti-malware software to find and stop malware by comparing the code of a file to a list of known malware signatures. This method looks for specific patterns in the code that match known malware. However, this method requires constant updates to the list of known malware and may be ineffective at detecting new or quickly changing malware. The advantage is that it is very thorough and can analyse all conceivable execution paths of a given file.

In comparison, *behaviour-based detection* is a way of identifying and stopping harmful computer programs by observing how they behave. This method involves running the program in a protected environment and monitoring what it does while it is running. The actions of the program are recorded and analysed to determine if it behaves like a normal, harmless program or if it acts suspiciously or maliciously. This approach is helpful because it allows researchers to understand how malware behaves and how it is implemented (Souri & Hosseini, 2018). Behaviour-based malware detection can be compared to a security guard monitoring a crowded shopping mall. Just as the security guard is trained to detect suspicious behaviour among the shoppers, the behaviour-based malware detection system monitors the actions of a program running in a protected environment. Both the security guard and the detection system aim to prevent harm by identifying and stopping suspicious activity.

Aycock (2016) distinguishes the other two major categories, static and dynamic. In *static detection*, anti-malware software attempts to identify malware without running any code, while in *dynamic detection*, the software runs the code and observes how the software behaves. Rani and Reeja (2019) add that studying malware provides a thorough

understanding of its functioning and enables one to determine effective measures to eliminate the associated threats.

2.1.2 File Integrity Monitoring

File integrity monitoring (FIM) is a security tool that helps to ensure the integrity of files on a computer or network and is often used to optimize file security. These tools are designed to detect any changes or modifications to files, which can indicate the presence of malware or unauthorized access. File integrity tools compare the current hash value of monitored files to their original value to detect any changes in the file content. If it finds any, it notifies the user (Udzir & Samsudin, 2011).

This detection technique can be useful when detecting new malware that is not known yet. By looking for changes in files, rather than for the malware itself, it can detect that something is wrong even without knowing the exact type of malware with it deals with.

2.1.3 Scanners

To detect malware, anti-malware applications scan users' files and while doing so, utilize a database of malware definitions or *signatures* that describe the behaviour and identification of malicious software. Upon scanning a file, the application compares its characteristics against the database and marks it as potentially harmful if it corresponds to a known malware definition. Despite the effectiveness of this method in detecting known threats, the database requires frequent updates to detect alternative forms of malware (Zamora, 2015). These scanners can be either run *on-demand* or *on-access*. Aycock (2016) states that on-demand scanners are run explicitly by the user and are particularly useful when there is a suspicion of infection or if a questionable file has been downloaded. In contrast, an on-access scanner operates continuously, examining every file whenever it is accessed. However, due to this continuous operation, the scanner uses computer resources and may adversely affect system performance.

Ligh et al. (2010) suggest that by using online public antivirus scanners, such as www.virustotal.com, users can go to a single website, submit a file, and have it quickly scanned by over sixty (at the time of writing this thesis) anti-malware software. They additionally point out that there are potential hazards involved. It is common for newly

released malware to remain unnoticed for several weeks. Therefore, even if all sixty anti-malware tools indicate that the file is secure, it may not necessarily be so. Moreover, people who use these online services cannot ascertain whether their files will be distributed among other third-party entities, even if the website claims it will not.

2.1.4 Heuristics

Zamora (2015) points out that anti-malware software uses heuristics to detect malware. Unlike database scanning, the heuristic analysis identifies malware based on its behaviour and characteristics rather than comparing it to a list of known malware. This allows the software to detect new threats that were previously unknown. For example, if an application tries to remove important system files, the anti-malware software may flag it as malware. However, this approach may sometimes produce false positives where legitimate programs are mistaken for malware.

It works by gathering data and analysing them. Aycock (2016) highlights that, when scanning the data, the anti-malware software looks for suspicious code called *boosters*. The probability of the analysed code being infected with malware is higher when a booster is present. Boosters, such as self-modifying code, junk code, decryption loops, or the use of terms like "virus," are examples that may indicate the presence of a harmful code during analysis.

2.1.5 Emulation

Emulation is a technique that analyses the malware in a controlled environment. Since opening and starting potentially malicious files on users' computers would cause harm, the anti-malware opens it in an emulated environment with the aim of detecting any malware that may be present. By conducting this analysis in the emulated environment, any malware discovered would not be able to cause damage to the actual computer system Aycock (2016).

Sun et al. (2011) add that there are some techniques employed by malware creators to prevent the collection, analysis, and reverse engineering of their malicious programs. In other words, cybercriminals that develop malware are aware of emulation, and they use tactics to conceal their malware when it is it is subjected to emulation.

2.2 Summary of Chapter 2

The main topic of Chapter 2 was to investigate the mechanisms involved in malware detection. The chapter presented readers with an overview of the detection process, which involves detecting whether a file is infected through anti-malware software, identifying the specific type of malware, and finally, disinfecting, where software ensures the threat is no longer there. The chapter also explained the two primary techniques used for malware detection: signature-based detection, which examines the malware code, and behaviour-based detection, which analyses the behaviour of the malware. Additionally, various anti-malware detection techniques were listed. This chapter serves as an introductory guide to malware detection and is necessary for understanding concepts discussed in the subsequent chapter focused on malware prevention.

3 Malware Prevention

The previous chapters dealt with various types of malware, the risks they pose to digital society and how they can be detected. While understanding how malware behaves and gets detected is important, it is necessary to stop this threat before it starts to negatively affect people's lives. For this reason, this chapter will focus on prevention measures.

This chapter will draw attention to the common mistakes that computer users make to highlight potential risks and then recommend how to prevent them. Then, it will discuss the password theory, describe how long it takes to break particular kinds of passwords and introduce the best practices for creating strong passwords. Regarding the statistics, examples of how particular groups, such as older people, are more susceptible to malware attacks will be given. This is closely related to the concept of social engineering, the act of manipulating people into disclosing confidential information without realizing it, which will be framed in this chapter as well.

The second part of this chapter will emphasize the importance of educating the public since prevention is not only easier but also more effective than dealing with the aftermath of a malware attack. The chapter will also describe the tools used as a Plan B, for example, data backups and a prepared emergency response plan that can significantly lower the chances of irreversible damage. Besides, the security issues encountered by large organizations well as the education of their employees will be discussed here.

The chapter will conclude with a short guide on the most crucial computer safety precautions. This way, even individuals who choose not to read the entire article may use this section to make their computer usage safer and even pass it along to those who could be at risk, including their close family or friends. Overall, this chapter informs readers that knowledge will lead to prevention, and in today's digital age, installing anti-malware software is simply not good enough anymore.

3.1 Common Mistakes

This chapter will deal with the common mistakes that individuals and organizations make when preventing malware infections. Even though the majority knows that there is a threat, many individuals and companies end up getting infected. This could be because of a lack of

understanding about how malware works, but also due to failure to implement basic security measures. In order for people and organizations to take the appropriate precautions, I want to highlight certain common errors and, by doing so, increase awareness of them. By understanding and avoiding these mistakes, it is possible to significantly reduce the risk of a malware infection and protect sensitive information and systems. These mistakes are not in any particular order, and it is best to avoid all of them.

1) *Failing to keep software and systems up-to-date.* Rajivan, Aharonov-Majar, and Gonzalez (2020) state that installing software updates is a simple yet essential step that people may take to improve the security of their devices and data. This rule applies not only to anti-malware software but also to all software, including everything from the Microsoft Suite to operating system updates. It is advisable to avoid postponing updates whenever possible.
2) *Not using strong passwords.* Passwords are a barrier between users and their data. The stronger this barrier is, the harder it is for someone unauthorized to get into our accounts. It is important to showcase how to make a strong password, but according to Yıldırım and Mackie (2019), users need to be motivated and persuaded to act. This can be achieved by pointing out the potential consequences of malware attacks and their aftermath.
3) *Downloading attachments from unknown, untrusted, or suspicious sources.* Although it can be tempting, by clicking on random links or even worse, by opening unknown attachments, malware can infect the system. It might result in data loss, illegal access, system failures, and other severe security problems, including infecting other devices and networks.
4) *Not using anti-malware software.* Although using anti-malware software cannot provide an absolute guarantee against malware infections, it can considerably decrease the likelihood of being infected. Lévesque et al. (2006) presented that anti-virus effectiveness is 91.81% in real-life scenarios. Over the course of 4 months, they evaluated about twenty-seven million different systems for their study.
5) *Not backing up important data.* Data backup is an important and occasionally overlooked topic. Regular data backup is crucial because it ensures that valuable data can be recovered from other, uninfected device. Later in my thesis, I will discuss this topic subject in greater detail.

3.1.1 Password Theory

Password security is a key aspect of modern-day digital life, as passwords serve as a defensive barrier to protecting users' files, sensitive information, and data. It is essential to learn how to create a password, since the more secure it is, the less likely someone else will be able to gain access to users' accounts.

It is advisable for computer users to utilize the site made by Kaspersky Lab (Kaspersky: Secure Password Check, n.d.). Typing passwords in any location is generally considered to be unsafe. Therefore, instead of typing real passwords, it is recommended to create something that is structurally similar. For instance, instead of typing a real password such as "Volvo2003", "Skoda2023" should be used as a structurally similar alternative. Using an approach called *brute force*, the website will provide information on the amount of time it would take to crack the password. Brute force is a simple type of attack, where the malicious party uses tools that try to guess the user's password repeatedly (Imperva, 2022). The basic concept behind brute force is to keep guessing the password until either the user or the software successfully finds it. However, when used with a combination of outside logic and variables, it becomes a serious threat. Guessing passwords with no variables is time-consuming, so the cybercriminals use databases of previously breached passwords, the most common password, trying to add 123 at the end, using capital letters only at the start and so on. By doing this, they narrow the range of outcomes and test only a million combinations as opposed to billions. The more information is available about the user, the more educated guess can be made about which variables to include in the password.

When making a strong password, the users need to consider length, or more precisely, the number of characters. To demonstrate, a password that uses six random numbers has 1 000 000 combinations. If the users use twelve numbers, they end up with close to 9 000 000 000 combinations. However, they have only ten numbers, whereas the alphabet has 26 letters – 26 options for each character. Additionally, if they include a letter case, they end up with double the characters. The more variables the users add, for example @&#, the stronger and harder to crack the password will be. So instead of having a password 83517202, they can use 6@oě!#6Z. Most of the people will not care enough to remember this, however adding variables, be it only some of them, will improve their chances of not being hacked.

Another way to improve password security is using multi-factor authentication (MFA). Ibrokhimov et al. (2019) present that MFA works by using more than one authentication method for securing our accounts. For example, users need to enter the password, then they need to scan their fingerprint, and lastly, a code is sent to their email that they have to type in. Other methods include receiving a code through text message, using third-party applications like Google Authenticator, or using biometrics like facial scanning. It becomes more difficult for someone to access our accounts the more stages we have.

3.1.2 Social Engineering

Another technique used by cybercriminals is social engineering. Its main goal is to push humans into performing an act, that they would otherwise not do. Rosencrance (2021) states that

> the objective is to influence, manipulate or trick users into releasing sensitive information or access within an organization. Many social engineering exploits rely on people's willingness to be helpful or fear of punishment. For example, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources.

While this is true, Applegate (2009) adds that the most common example of social engineering is phishing, which is defined as an attempt to trick someone into giving information over the Internet ("Phishing", n.d.) and Trojan email. These emails are carefully crafted so they can lure victims into opening attachments, downloading files or clicking on links. Attackers may attempt to pose as the user's bank, someone they know, or even exploit their greed, as in the case of "If you click here and register, we will pay you $100!"

The defence against social engineering can get tricky since it abuses human psychology and plays with fear, trust or authority (Applegate, 2009). It is most important to know about this and realize that anyone can pretend to be someone else. It is recommended that the user should never open unknown emails and trust anyone asking for their username or password. Besides, they should always verify the unknown caller's identity, in particular, if the call is supposed to be from the user's bank. When in doubt, it is advisable to hang up the phone and contact the bank directly from their official website. This is a simple yet effective way to avoid falling prey to phone-based scams in which fraudsters impersonate banks and try to

steal sensitive information. Abass (2018) adds that education of both the users and companies is a vital part of a defence against this threat.

3.1.3 Updating Devices

Keeping software updated is a critical aspect of preventing malware infections. When software developers identify a vulnerability in software, they release an update to fix it. Not only can the issue be minor such as a non-functional button in an Internet banking mobile app, but it can also be something exploitable by cybercriminals, for example, a way for them to access people's accounts. By updating all software as soon as possible, users can have the latest security patches applied.

It is important to note that the aforementioned information applies to more things, such as the following:

1) *Operating system updates.* These commonly include security patches that fix newly found vulnerabilities. It is essential to ensure that our operating system is always up to date as a compromised operating system can potentially lead to the compromise of all the data and applications within it. After a certain period, software support will end. This is the case of Microsoft Windows 7, which does not receive any new security patches. By using outdated software users are in extreme danger, therefore they should get a new operating system as soon as possible (Zunesis, n.d.).
2) *Firmware updates.* According to Lutkevich (2022), "firmware is installed directly onto a piece of hardware during manufacturing. It is used to run user programs on the device and can be thought of as the software that enables the hardware to run." This means that updating the firmware is just as important as updating other types of software because it must work as intended, without any security issues.
3) *Anti-malware application updates*. Anti-malware software developers most of the time catch up with the newest malware. This "wait-and-see" attitude means that after new malware is created, anti-malware software gets updated – to detect it. By not updating anti-malware software regularly, users' devices become vulnerable (University of Strathclyde, n.d.).

Updating devices such as mobile phones, tablets, and smart things is just as important as updating computers. Many of these devices are connected to the Internet and can be

vulnerable to malware attacks if they are not kept up to date with the latest security patches and firmware updates.

In addition to updating the device's operating system and firmware, it is also recommended to allow applications to update automatically whenever possible. This can help ensure that the latest security features and bug fixes are installed as soon as they become available, thus reducing the risk of malware infections and other security issues. However, many people may be reluctant to update their devices, either because it is inconvenient or because they believe that updating something that works well may make it worse. This can be a dangerous attitude, as outdated software and firmware can create security vulnerabilities that cybercriminals can exploit.

3.2 Types of Malware Prevention

3.2.1 Cybersecurity Training for the Internet Users

One of the effective strategies for preventing malware is education. Educating people about malware prevention can increase awareness of potential risks, provide knowledge and skills to protect devices and networks, change behaviour to be more security-conscious, and ultimately reduce costs associated with malware attacks, be it monetary ones or non-monetary ones such as damage to reputation, loss of trust, and disruption of operations.

Luo and Liao (2007) state that the presence of ransomware endangers the involvement of people in e-commerce, defined as the business of buying and selling goods and services on the Internet ("E-commerce, n.d.). To address this issue, the computer, banking, and retail sectors must launch a significant effort to educate both existing and potential customers on how to remain safe and secure while using the Internet. However, companies and their employees must adopt similar measures as well. Luo and Liao (2007) emphasize that it is important to demonstrate the direct impact of ransomware on the company and its employees, e.g., that the company could shut down, lose stock value or important customers.

Similarly, Alharbi and Tassaddiq (2021) investigated and evaluated the degree of cybersecurity awareness and user compliance with security protocols among undergraduate students enrolled at Majmaah University. A total of 576 students completed a questionnaire comprising questions related to various aspects of cybersecurity, including phishing awareness, cybersecurity knowledge, Internet usage and browser security. This study

concluded that the university courses should include a cybersecurity awareness and training initiative for students, which must be strongly endorsed by top executives and managers. Alharbi and Tassaddiq (2021) also point out that using passive awareness methods such as newsletters, emails, and oral presentations is not effective enough for educating Internet users. They propose taking proactive measures, like interviews and training, or, even better, a combination of both passive and active learning. Lastly, they noted that educating individuals on security awareness from a young age is vital to establish sustainable cybersecurity behaviour among them.

3.2.2 Data Backup

Data backup is an essential aspect of computer security. In light of the continuously increasing danger posed by malicious software, it has become crucial for both individuals and organizations to implement resilient data backup protocols. Users risk losing their files, sensitive information, and personal information. The loss of critical data can have significant implications for organizations, such as financial losses, reputational damage, and legal repercussions. For this reason, a comprehensive and reliable backup strategy is crucial to ensure that data can be restored quickly and efficiently in case of an attack. The United States Computer Emergency Readiness Team (US-CERT) published a paper including backup strategies. The objective behind the establishment of US-CERT in 2003 was to protect the nation's Internet infrastructure against potential cyber threats and vulnerabilities (Homeland Security, n.d.).

Krogh (2009, as cited in Ruggiero & Heckathorn, 2012, p. 1) claims that to increase chances of recovering lost or corrupted data the 3-2-1 Rule (Krogh & Peter, 2009) should be followed:

3) Keep *3 copies* of any important file: 1 primary and 2 backups,
2) Keep the files on *2 different media types* to protect against different types of hazards,
1) Store *1 copy offsite* (For instance, in areas outside of one's home or business facility).

When it comes to data backup, users have the following three options, as suggested by Ruggiero and Heckathorn (2012).

Cloud Storage (remote backup) is a service that utilizes a network of external servers maintained by a cloud storage provider, which means that users can access or back up their

data anytime they access the Internet. People can use this way of backing up for its convenience, whether they need a small or big storage capacity, and it protects them from natural disasters and failures on local devices. However, there are some downsides. Cloud service consumers typically have limited information regarding the cloud infrastructure and reliability of their service provider, resulting in reduced transparency. This also applies to the security of a given cloud. Although the service provider may claim that they encrypt their data, clients may never be certain of whether they actually do so, how successfully they do it, or what their actual procedures are.

Internal Hard Disk Drives. The majority of desktop and laptop computers rely on their internal hard drives to store crucial system files necessary for operation, along with the user's files. Hard drives come in a variety of capacities and are reasonably priced. They are therefore the ideal option to quickly back up data while maintaining total control over it. The disadvantages of this method are that if users get infected with malware, their hard drive becomes compromised as well. Not only can it be stolen if someone gets access to it, but it can also be damaged and it can malfunction and corrupt their data. By implementing encryption measures, physically securing their computer, and adhering to standard anti-malware practices, they can enhance the security of using hard drives.

Removable Storage Media. are types of storage that can be connected and disconnected from the computer, such as external hard drives and USB flash drives. The biggest advantage is that they can be unplugged from the computer, which ensures that even if it becomes infected, all information will be protected unless the external hard drive is plugged in. This physical separation also helps in more extreme scenarios, e.g. in case of house fire. This portability means that the device can be lost, stolen and if it gets infected, malware can be spread to other computers connected it to. Similar to internal hard drives, external hard drives must be physically secured, removed from computers when not in use, and subjected to standard anti-malware procedures.

In the end, the decision depends on the type of user and the value they place on their data. Besides the different back up options, the 3-2-1 rule should be used as a general guideline. It is important to note that any backup is better than none, and although users may feel like nothing bad can happen to them, it always can.

3.3 Malware Prevention Tips

The current state of malware behaviour, prevention and detection has been reviewed in this thesis. This was accomplished by literature research of many media, ranging from books to cybersecurity news.

While there is no one-size-fits-all answer when it comes to protecting against malware, there are steps that individuals and organizations can take to reduce their risk of infection. In this chapter, I will provide a list of prevention tips using the key ideas and useful strategies learned from the literature review. This guide is meant to serve as a practical resource for anyone wishing to enhance their cybersecurity, whether they are a home user, a small business owner, or a cybersecurity specialist. Unlike the rest of this thesis, this part will be my personal list and thus, biased to some degree.

This list provides readers with advice and recommendations that will help them defend against malware threats and minimize the potential impact of any attacks that do occur. While no approach can guarantee complete protection against all potential threats, taking these basics measure will help. The list does not follow any particular sequence, as every measure is considered equally valuable.

- *Use a strong password* in combination with *multi-factor authentication*. By using a strong password followed by additional steps such as a fingerprint or face scan, you add an extra layer of security that cybercriminals would have to bypass.
- *Use anti-malware software*. Although lower-end computers may experience a slight performance hit, the added security outweighs this. Both Windows and macOS have good built-in anti-malware, so make sure it is not disabled.
- *Keep all software updated*, especially your operating system and anti-malware software. Many malware attacks exploit outdated software, so updating it regularly ensures you have the latest security patches. Although some people may not like changes and believe that software updates are worse than the previous version, it is important to keep your software up to date.
- *Do not download any attachments from unknown, untrusted, or suspicious sources*.
- *Use common sense* – trust but verify. Social engineering is a serious threat where cybercriminals try to exploit you, rather than your computer. They may pretend to be your bank account manager and try to extract valuable information from you, such

as your date of birth or passwords. If you are ever unsure, hang up and call the company directly from their official website.

- If you download an attachment but have second thoughts about its content, you can use online anti-malware software that crosschecks the given file with over 60 anti-malware scanners.
- *Back up your data***.** A good way to do this is by using the 3-2-1 rule: keep three copies of any important files, store the files on two different media types (e.g., one on a hard drive and one online), and keep one copy offsite (e.g., outside your workplace). Investing in an external hard drive or subscribing to an online service where you can back up your data may feel unnecessary, but the moment you lose something important, it will be too late to fix it.
- *Share this knowledge* with your family and friends. While for some, these measures may seem obvious to take, many people may come from different circles and have no idea how dangerous the internet and the technology surrounding it can be. Education is key to raising awareness and promoting safe online practices.

3.4 Summary of Chapter 3

In this chapter, readers were provided with information on how they can protect themselves from malware. The chapter began by outlining the most common mistakes made by users, such as failing to update their devices or not using strong passwords. This was followed by a discussion on the password theory, which demonstrated how to create stronger passwords and, more importantly, introduced the concept of two-factor authentication. The chapter then highlighted the importance of regularly updating various devices and introduced the topic of social engineering, where cybercriminals attempt to exploit not just devices but also users themselves. For example, by impersonating a user's bank officer to obtain valuable information. The chapter also emphasized the significance of education as a critical component of anti-malware discourse. As a result, the final chapter of this thesis provided a brief yet comprehensive tips for preventing malware. Chapter 3.3 serves as a short version of the prevention part of thesis and can be utilized to educate various users simply and efficiently.

Conclusion

The main objective of this bachelor's thesis was to present an overview of malware that could be used by users with the intention of protecting themselves from cybercrime. A thorough literature review of currently available scholarly books and theoretical and empirical studies was conducted, followed by a comprehensive survey of malware suitable for ordinary computer users. This was accomplished by comparing, cross-checking, and searching for discrepancies.

The first chapter of the thesis should acquaint the reader with the fundamental concepts related to the computer security threats, such as spam, DoS and bugs. While an in-depth analysis requiring considerable IT expertise is unquestionably necessary, there should also be some kind of medium ground that works well without being overly simple or complex.

Chapter 2 provided an exploration of the methods used in detecting malware. This chapter covered the detection process, which included recognizing whether a file is infected, classifying the type of malware, and performing disinfection procedures. The chapter also introduced two principal techniques for detecting malware, namely signature-based and behaviour-based detection. The former involved cross-referencing malware with a list of previously identified malware, while the latter analysed the actions of the scanned file. Furthermore, the chapter outlined various anti-malware detection techniques. These concepts were crucial for comprehending the subsequent chapter's discussion on malware prevention, including the aspects of malware usually overlooked by average users.

The last chapter thoroughly examined the measures to be taken by individuals and organizations to protect themselves from the dangers of malware. The chapter started by outlining the common mistakes made by users, such as failing to update their devices and using weak passwords. It then introduced the password theory and the concept of two-factor authentication as a more secure way of protecting accounts. Additionally, the text underlined the importance of keeping devices up-to-date and being vigilant against social engineering tactics employed by cybercriminals to manipulate users while also emphasizing the critical role of education within the anti-malware discussion.

At the end of Chapter 3, a concise list of measures and recommendations was presented to help readers defend themselves against malware threats and minimize the potential impact of any attacks. These points serve as a valuable resource for individuals and organizations

seeking to secure their digital environments and safeguard their sensitive data from malicious actors. It is crucial to implement a comprehensive security strategy comprising both preventive and responsive measures to ensure the most efficient defence against malware threats.

Unfortunately, malware will keep evolving, and there is no doubt that the issues discussed in this thesis will eventually become outdated. However, the research revealed that studies conducted as early as the 1990s are still important and relevant in the present context. Despite the evolving nature of malware, the fundamental concepts and techniques remain largely unchanged, with newer strains simply being variations of previously existing ones. There is a common issue in the field of malware education where existing papers are highly technical and not targeted towards average users. This complexity can make it difficult for individuals without technical expertise to understand and apply the information to their daily computing practices. As a result, more user-friendly resources are needed to educate non-technical users and empower them to protect themselves against malware.

The prevailing view is that knowledge and awareness of malware's inner workings provide the strongest defence against it. Given the widespread use of computers today, this knowledge is essential. Cybercriminals are usually one step ahead while the rest of the world is trying to catch up with them. This thesis is expected to help bridge this gap, at least to some extent.

List of Figures

List of References

Abass, I. a. M. (2018). Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, *09*(04), 257–264. Retrieved from https://www.scirp.org/journal/paperinformation.aspx?paperid=87360

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(23), 1–15.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 1–23.

Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective*, *18*(1), 40–46. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/19393550802623214

Australian Institute of Criminology. (2016). More malware – adware, spyware, spam and spim. *High Tech Crime Brief*, 11, 1–2. Retrieved from https://www.aic.gov.au/sites/default/files/2020-05/htcb011.pdf

Aycock, J. (2006). *Computer viruses and malware.* Berlin: Springer.

Bagnall, B., Broomes, C. O., & Russell, R. (2000). *E-mail virus protection handbook: Protect your e-mail from Trojan horses, viruses, and mobile code attacks*. Rockland: Syngress.

Banday, M. T., & Qadri, J. (2009). Study of botnets and their threats to internet security. *Sprouts*, *9*(24). 1-12

Bettany, A., & Halsey, M. (2017). *Windows virus and malware troubleshooting*. New York: Apress.

Bist, A. S. (2014). Detection of logic bombs. *International Journal of Engineering Sciences & Research Technology*, *3*(2), 777–779. Retrieved from https://www.academia.edu/6329597/Detection_of_Logic_Bombs

Botacin, M., & Grégio, A. (2021). Malware multiVerse: from automatic logic bomb identification to automatic patching and tracing. Retrieved from https://arxiv.org/abs/2109.06127

Dusane, P. S. (2020). Logic bomb: An insider attack. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3662–3665.

E-commerce. (n.d.) In *dictionary.cambridge.org* Retrieved from https://dictionary.cambridge.org/dictionary/english/e-commerce

FBI. (2018, November 2). The Morris worm. 30 Years since first major attack on the internet. Retrieved from https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Geer, D. (2005). Malicious bots threaten network security. *Computer*, *38*(1), 18–20.

Homeland Security. (n.d.). US-CERT - United States Computer Emergency Readiness team. Retrieved from https://www.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

Ibrokhimov, S., Hui, K. L., Abdulhakim Al-Absi, A., Lee, H. J., & Sain, M. (2019). Multi-factor authentication in cyber physical system: A state of art survey. *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 279–284.

Jajoo, A. (2021, December 15). A study on the Morris Worm. Retrieved from https://www.researchgate.net/publication/357046348_A_study_on_the_Morris_Worm#read

Johansen, A. G. (n.d.). What is fileless malware and how does it work? Retrieved from https://us.norton.com/blog/malware/what-is-fileless-malware

Kara, I. (2022). Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. *Expert Systems with Applications*, *214*, 1–10.

Karger, P., & Schell, R. (1974). Multics security evaluation: vulnerability analysis. *18th Annual Computer Security Applications Conference, 2002. Proceedings*, 127–146.

Kaspersky Lab. (n.d.). What is WannaCry ransomware? Retrieved from https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry

Kaspersky Password Checker. (n.d.). Check your password. Retrieved from https://password.kaspersky.com/

Lévesque, F. L., Fernandez, J. M., Young, G., & Batchelder, D. (2006, October 5). Virus Bulletin: Are They Real? Real-Life Comparative Tests of Anti-Virus Products. Retrieved from https://www.virusbulletin.com/conference/vb2016/abstracts/are-they-real-real-life-comparative-tests-anti-virus-products

Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). *Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code*. Indianapolis: Wiley Publishing, Inc.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security*, *16*(4), 195–202.

Lutkevich, B. (2022, June). What is firmware? Retrieved from https://www.techtarget.com/whatis/definition/firmware

Malwarebytes. (n.d.). What is a bot? Retrieved from https://www.malwarebytes.com/bot

Malwarebytes. (n.d.). What is a keylogger. Retrieved from https://www.malwarebytes.com/keylogger

Mansfield-Devine, S. (2017). Fileless attacks: compromising targets without malware. *Network Security*, *2017*(4), 7–11.

Markoff, J. (1990, May 5). Computer intruder is put on probation and fined $10,000. Retrieved from https://www.nytimes.com/1990/05/05/us/computer-intruder-is-put-on-probation-and-fined-10000.html

Oikarinen, J., & Reed, D. (1993). Internet Relay Chat protocol. Retrieved from https://datatracker.ietf.org/doc/html/rfc1459

Osterman Research (2016). Understanding the depth of the global ransomware problem. An Osterman research survey report. Retrieved from https://www.malwarebytes.com/pdf/whitepapers/understandingthedepthofransomwareintheus.pdf

Phisher. (n.d.) In *dictionary.cambridge.org*. Retrieved from https://dictionary.cambridge.org/dictionary/english/phisher

Phishing. (n.d.) In *dictionary.cambridge.org* Retrieved from https://dictionary.cambridge.org/dictionary/english/phishing

Rajivan, P., Aharonov-Majar, E., & Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *Journal of Cybersecurity*, *6*(1), 1–12. Retrieved from https://academic.oup.com/cybersecurity/article/6/1/tyaa002/5788613

Rani, S. S., & Reeja, S. (2019). A survey on different approaches for malware detection using machine learning techniques. In P. Karrupusamy, J. Chen, & Y.Shi (Eds.), *Sustainable communication networks and application* (pp. 389–398). Cham: Springer.

Reshmi, T. (2021). Information security breaches due to ransomware attacks – a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.

Rosencrance, L. (2021, June 3). *social engineering*. TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/social-engineering

Ruggiero, P., & Heckathorn, M. A. (2012). Data backup options. Retrieved from https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf?fbclid=IwAR2txy6SAxAf-FtMubsPmzdAWqIgGfU--i90jNAXT_iz8glj4Njn3Lfw6UI

Schneider, W. (1989). Computer viruses: What they are, how they work, how they might get you, and how to control them in academic institutions. *Behavior Research Methods, Instruments, & Amp; Computers*, *21*(2), 334–340.

Set-user-ID. (2020, August 2). In *Computer Hope Dictionary*. Retrieved from https://www.computerhope.com/jargon/s/setuid.htm

Shah, D., Shah, V., Shah, H., & Kanani, P. (2017). Survey on computer worms. *International Journal on Recent and Innovation Trends in Computing and Communication*, *5*(8), 20–24.

Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-centric Computing and Information Sciences*, *8*(1), 3–6.

Spam. (n.d.). In *dictionary.cambridge.org*. Retrieved from https://dictionary.cambridge.org/dictionary/english/spam

Sriramachandramurthy, R., Balasubramanian, S. K., & Hodis, M. A. (2009). Spyware and adware: how do internet users defend themselves? *American Journal of Business*, *24*(2), 41–52.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: the ghost in the machine. *Communications of the Association for Information Systems*, *14*(1), 291–306.

Sudhakar, & Kumar, S. (2020). An emerging threat Fileless malware: a survey and research challenges. *Cybersecurity*, *3*(1). 1–12.

Sun, M., Lin, M., Chang, M. C., Laih, C., & Lin, H. (2011). Malware virtualization-resistant behavior detection. *International Conference on Parallel and Distributed Systems*. Retrieved from https://ieeexplore.ieee.org/document/6121379

Thompson, K., & Ritchie, D. M. (1971). *Unix programmer's manual*, Holmdel: Bell Telephone Laboratories, Inc. Retrieved from https://www.bell-labs.com/usr/dmr/www/1stEdman.html

Udzir, N., & Samsudin, K. (2011). Towards a dynamic file integrity monitor through a security classification. *International Journal of New Computer Architectures and Their Applications*, *1*(3), 789–802. Retrieved from https://www.researchgate.net/publication/230771292_Towards_a_Dynamic_File_Integrity_Monitor_through_a_Security_Classification

United States Department of Justice. (2019, December 17). Siemens contract employee gets jail time for intentionally damaging computers. Retrieved from https://www.justice.gov/usao-wdpa/pr/siemens-contract-employee-gets-jail-time-intentionally-damaging-computers

University of Strathclyde (n.d.). Updates and anti-virus. Retrieved from https://www.strath.ac.uk/professionalservices/is/cybersecurity/updatesandanti-virus/

Imperva. (2022). Brute force attack. Retrieved from https://www.imperva.com/learn/application-security/brute-force-attack/

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18(6), 741–759. Retrieved from https://link.springer.com/article/10.1007/s10207-019-00429-y

Zamora. (2015, December 11). How does anti-malware work? Retrieved from https://www.malwarebytes.com/blog/news/2015/12/how-does-anti-malware-work

Zeifman, I. (2017, January 24). Bot Traffic Report 2016. Retrieved from https://www.imperva.com/blog/bot-traffic-report-2016/

Zunesis. (n.d.). Why it's important to install Windows updates and patches. Retrieved from https://www.zunesis.com/why-install-windows-updates/