TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Arseni Sergeev 201736 IVSB

INVESTIGATING THE EFFECTIVENESS OF VARIOUS METHODS FOR MALWARE REMOVAL AND REMEDIATION ON WINDOWS 11 SYSTEMS

Bachelor's thesis

Supervisor: Toomas Lepik

Cyber Security Analyst

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Arseni Sergeev 201736 IVSB

UURING ERINEVATE MEETODITE TÕHUSUSE KOHTA PAHAVARA EEMALDAMISEKS JA PARANDAMISEKS WINDOWS 11 SÜSTEEMIDES

Bakalaureusetöö

Juhendaja: Toomas Lepik
Küberturbe analüütik

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Arseni Sergeev

15.05.2023

Abstract

This thesis investigates and evaluates malware removal techniques for the Windows 11 operating system. The first section of the thesis provides an overview of the research, followed by a discussion of the study's methodology and limitations. A comprehensive literature review on malware removal and remediation is presented, with a particular emphasis on Windows operating systems and their applications in a variety of industries, including personal computers, business, education, healthcare, government, entertainment, the internet of things, artificial intelligence, and autonomous vehicles. The thesis also examines the threat of malware in today's world, followed by a comprehensive analysis of the Windows 11 operating system's structure, kernel, user interface, file system, registry, services, and security features.

The second section of the thesis analyses the various techniques employed by malware to avoid detection and elimination. This section discusses anti-removal and stealth techniques, as well as data collection, data destruction, and data manipulation. Additionally, the thesis describes the methods for analysing malware, including static analysis, dynamic analysis, and sandboxing.

The third and most important section of the thesis evaluates malware removal techniques. Creating a sandbox environment, collecting malware samples, and testing three different malware removal techniques, including Windows Defender, Malwarebytes Antivirus, and manual removal, comprise the practical portion of the study. Tests were conducted on “Agent.Tesla” and “HermeticWiper” — two different malware types, which incorporate data collection, destruction and manipulation. Based on the evaluation results, the thesis presents a manual removal guide for malware that incorporates all of the techniques discussed in the theoretical section of the study.

This thesis is written in English and is 57 pages long, including 10 chapters, 2 figures and 0 tables.

List of abbreviations and terms

ACL	Access Control List
AI	Artificial Intelligence
API	Application Programming Interface
ARP	Address Resolution Protocol
BSOD	Blue Screen of Death
BYOD	Bring-Your-Own-Device
CARO	Computer Anti-virus Researchers Organization
CPU	Central Processing Unit
CSV	Cluster Shared Volumes
GUI	Graphical User Interface
IoT	Internet of Things
IP	Internet Protocol
MAC	Media Access Control
MCR	Managed Code Rootkit
MITM	Man-in-the-middle
NTFS	New Technology File System
OS	Operating System
SSID	Service Set Identifier
TPM	Trusted Platform Module
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network
Windows NT	Microsoft's suite of OSes for personal machines and servers

Table of contents

1 Introduction 9
2 Methodology 10
3 Background 12
3.1 Malware threat in modern world 12
3.2 Previous research on malware removal and remediation 14
3.3 Windows OS applications 14
4 Windows 11 OS structure 17
4.1 Kernel 17
4.2 User interface 18
4.3 File system 19
4.4 Registry 20
4.5 Services 21
4.6 Virus and threat protection 22
4.7 Safe mode 23
5 Malware specification by impact 24
5.1 Anti-removal and stealth techniques 25
5.1.1 Simple obfuscation 25
5.1.2 Watchdog timer 25
5.1.3 Registry manipulations 26
5.1.4 Code injection 26
5.1.5 Rootkit techniques 27
5.2 Data collection 27
5.2.1 Man-in-the-Middle 28
5.2.2 Input capture 29
5.3 Data destruction 29
5.4 Data manipulation 30
5.4.1 Runtime data manipulation 31
5.4.2 Stored data manipulation 31
5.4.3 Transmitted data manipulation 32

6 Malware analysis methods 33
6.1 Strings analysis 33
6.2 Basic static analysis 34
6.3 Advanced static analysis 34
6.4 Basic dynamic analysis 35
6.5 Advanced dynamic analysis 35
6.6 Sandboxing 35
6.6.1 Virtual machines 36
6.6.2 Online sandboxing environments 37
7 Malware removal techniques 38
7.1 Removal tools 38
7.1.1 Antivirus software 38
7.1.2 Windows defender 40
7.1.3 Autoruns 41
7.1.4 Process Explorer 41
7.2 Manual removal 43
8 Application and evaluation of malware removal techniques 46
8.1 Sandbox environment setup 46
8.2 Malware collection 47
8.3 Malware sandboxing and remediation 48
8.3.1 Data collection: Agent.Tesla 48
8.3.2 Data destruction and manipulation: HermeticWiper 53
8.4 Creation of manual malware removal guide 57
8.4.1 PC isolation 57
8.4.2 Reveal suspicious processes and registry entries 58
8.4.3 Malware removal 61
8.4.4 System overview and testing 62
9 Analysis of results 63
10 Summary 65
References 67
Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis 71

List of figures

Figure 1. Registry path example 20
Figure 2. CARO malware naming scheme 24

1 Introduction

Malware has become an increasingly significant threat to computer systems, causing substantial financial and reputational harm to individuals and organizations around the globe. Malware refers to a variety of malicious software programs that are designed to cause damage to computer systems, data, and users. Malware can take many different forms, including viruses, Trojan horses, worms, ransomware, and spyware. Malware can have catastrophic effects, leading to data breaches, system failures, and other cybersecurity incidents.

Effective malware eradication and remediation is one of the most crucial weapons in the fight against malware. It is essential to be able to swiftly and effectively eradicate malware from infected systems in order to limit the harm caused by malware and prevent future cybersecurity incidents.

As one of the most commonly used operating systems in the world, Windows OS is a significant target for malware attacks. The kernel, user interface, file system, registry, and services are all potential targets for malware attacks within the Windows 11 operating system. To develop effective malware removal and remediation techniques, it is essential to comprehend the structure of the Windows 11 operating system and how it can be exploited by malware.

Malware eradication may be the best or only available option during a malware incident. When a malware attack occurs, limiting the damage and preventing further infections are the top priorities. In many instances, removing malware is the most effective method for achieving this goal. Malware removal can be difficult, and the efficacy of various malware eradication techniques can vary considerably. Therefore, additional research is required to determine the most efficient methods for malware removal and remediation.

2 Methodology

Reviewing academic literature and how-tos as part of the methodology's first phase is crucial to ensuring that the study is theoretically sound and has a solid theoretical foundation.This is due to the fact that it entails gathering and evaluating numerical data to compare the efficacy of various malware removal techniques

The following step, gathering malware samples, is required to obtain a sample of malware that is representative so that different eradication techniques may be tested for effectiveness. The experimental environment design is crucial for ensuring the validity and reliability of the study since it allows to build a controlled and uniform environment for testing malware eradication techniques.

In order to fully check the usability of malware removal methods it is important to create an environment in which there will be no interference between manual and automatic antivirus software for malware remediation techniques.

During tests there will be evaluation of effectiveness of:

- Windows Defender.
- Commercial AV software MalwareBytes.
- Manual removal.

Each test is conducted under such circumstances, that no other method affects the result, except the one that is being applied.

During Windows Defender testing other antivirus software is completely turned off and no other tools for remediations are used except the ones incorporated by Windows Defender itself.

During commercial AV software testing, Windows Defender is turned off and no other malware removal tools are used in the process.

In order to fully interpret manual removal method, any active virus protection service in form of Windows Defender or commercial antivirus are completely turned off.

The major process of the study comprises applying and evaluating several malware eradication techniques, and it entails gathering quantitative information on each technique's success rates.

During the practical part of the thesis, there will be made an analysis and removal of two malware represantatives — „Agent.Tesla“ and „HermeticWiper“. „Agent.Tesla“ is a form of malware, which main goal is to collect data in a stealthy way. „HermeticWiper“ on the other hand is a malware, which main goal is to destroy the operating system copmponents, files and make computer system inoperable.

In addition to malware removal there is also need to conduct string analysis of each malware sample in order to better understand its operation techniques and provide evidence of its affect on the system, so during malware removal process there will be an explanation of why certain steps should be taken.

Finally, a crucial part of the approach is the process of gathering and assessing the data from the results. The results of this investigation can be used to determine which techniques are most successful at eradicating and fixing malware on Windows 11 PCs.

3 Background

Malware has been a persistent threat to computer systems for many years, and substantial research has been conducted in the field of malware analysis and removal. Various techniques for malware detection, classification, and removal have been devised by researchers. These techniques include both static and dynamic analysis methods, which are used to determine the malicious intent of malware by analysing its behaviour.

Due to their widespread use in both home and commercial environments, Windows operating systems have been a primary target for malware attacks. As a consequence, a substantial amount of research has gone into the development of techniques for malware analysis and remediation on Windows systems. This research has resulted in the creation of various tools and techniques, such as sandboxes and virtual machines, for analysing and removing malware from Windows-based systems.

3.1 Malware threat in modern world

The proliferation of malicious software poses a serious risk to computer systems, files, data, and personal information. Such information can be extremely valuable to individuals, perpetrators, governments, and other organizations, among others. Examples of cyberwarfare include the 2014 hack of Sony Pictures Entertainment, which was attributed to North Korea, and various attacks by the hacking group Anonymous against government security agencies, oppressive governments, and companies evading taxes.

Numerous experts predict that the next major conflict will be fought in cyberspace, where the ability to disrupt critical infrastructure, such as financial markets, communications, electricity and gas generation and distribution, traffic flow, shipping and aircraft, GPS satellites, health systems, government operations, and even military forces, is incredibly appealing to a large number of individuals around the world. This has resulted in the organization of annual DEF CON conferences, where thousands of "white hat" hackers meet with representatives from corporations, technology companies, and international security agencies. The purpose of these conferences is to provide a forum for specialists to discuss the most recent vulnerabilities and threats, the malware incident handling process, how information can be shared securely between companies and security vendors, and how to mitigate them.

Malware's future is uncertain, but it will continue to pose a substantial hazard to individuals, organizations, and governments. To maintain the security of computer systems, files, data, and personal information, the development of new technologies and strategies to combat this menace will be essential. Moreover, cooperation and collaboration between individuals and entities, such as security researchers, corporations, and governments, will be essential for effectively addressing the cyberwarfare threat. [1]

The swift development of the IoT has been facilitated by the evolution of the internet from e-mail systems in the 1990s to the next iteration of the internet in the twenty-first century. There are currently billions of devices connected to the internet, with the number increasing daily. Various industries, including public services, healthcare, automation of homes, personal equipment, manufacturing, agricultural infrastructure, commerce, communication, and automobiles, have been revolutionized by the proliferation of IoT. The most recent technologies enable the society-critical infrastructures and services of today.

Many corporations are adopting BYOD and cloud-based applications, which are transforming the traditional method of working in office buildings. In-house data centers are also transitioning to cloud-based systems. In 2018, the market for cloud services providers reached $186,4 billion, expanding by 21.4% annually. Cloud-based applications enable employees to work remotely from any location and access official data at any time. However, this adaptability introduces new attack surfaces. [2]

There are allegations that the Chinese Ministry of State Security conducted two breaches against a US Navy contractor in January and February 2018. The unnamed contractor conducts research and development on submarines and underwater weapon systems for the Naval Undersea Warfare Center in Newport, Rhode Island. Investigators have discovered that Chinese government hackers took 614 gigabytes of sensitive information. The seized data includes information on the Sea Dragon project, submarine cryptographic systems, sensors, and a top-secret development plan for a new submarine-launched anti-ship missile. As requested by the Navy, the specifications of the missile system were not disclosed; however, the missile was described as supersonic and capable of being launched from submarines.

The Pentagon has accused Chinese hackers of targeting US military data for years, including the theft of sensitive information related to the F-35 stealth fighter and the advanced Patriot PAC-3 missile system. Commander Bill Speaks stated that the Navy is continuously enhancing its cybersecurity culture and defenses to combat evolving cyber threats. The US Navy has not formally confirmed the Post's report of the recent hack.

This alleged transgression has heightened tensions between Beijing and Washington, particularly regarding military and economic issues. Last month's decision by the Pentagon to rescind China's invitation to participate in maritime exercises in the Pacific is an example of how current tensions are being addressed. [3]

3.2 Previous research on malware removal and remediation

Andrew Bettany and Mike Halsey's "Windows Virus and Malware Troubleshooting" (2017) is a comprehensive guide for Windows users to defend their PCs against malware and virus infection. The authors emphasize the importance of recognizing malware and its potential problems, and provide actionable measures to protect PCs from attacks. This book is a valuable resource for IT professionals, system administrators, and power users who are responsible for maintaining the security of Windows-based infrastructure due to the authors' expertise in the field of Windows troubleshooting and malware eradication.

The book "Learning Malware Analysis" by K. A. Monnappa (2018) is highly relevant to your cyber security-focused thesis topic. The book offers a comprehensive overview of malware analysis and memory forensics, two essential techniques for cyber security investigations. As adversaries become more sophisticated and conduct sophisticated malware attacks, it is essential for information security professionals to possess the skills necessary to detect, respond to, and investigate such intrusions. The book's emphasis on creating a secure and isolated lab environment for malware analysis and utilizing memory forensics to investigate and search for malware are essential components of cyber security investigations.

3.3 Windows OS applications

Personal computers: Windows OS is the most commonly used operating system on personal computers worldwide, with a market share of over 28% as of 2023. It is used by

individuals for personal and professional purposes, as well as by businesses and organizations. Since the year 2022, the popularity of Windows 11 as desktop OS has increased from initial 8% to 21% in the year 2023. Such statistics imply the growing interest and popularity of Windows 11 OS in the upcoming future, which will bring the necessity of proper security. [4]

Business and enterprise: Windows OS are widely used by businesses and enterprises for various purposes, including office work, customer management, financial management, and more. The operating system provides features and tools specifically designed for business use, such as group policy management, active directory, and remote desktop services. [5]

Education: Windows OS is commonly used in educational institutions, from primary schools to universities. It provides a platform for students to access educational resources, conduct research, and complete assignments. [6]

Healthcare: Windows is used in the healthcare industry for various tasks such as electronic health records, medical imaging, and hospital administration. Windows-based software is also used in medical research. [7]

Government: Many government agencies around the world use Windows-based software for tasks such as administration, law enforcement, and national security. [8]

Entertainment: Windows is used in the entertainment industry for various tasks such as video editing, music production, and game development. Windows-based software is also used for media playback and streaming. Windows OS is the most popular operating system for gaming, with a vast library of games available for PC. Many game developers specifically target Windows OS as their primary platform due to its popularity and compatibility with various hardware configurations. [9]

Internet of Things: As the number of connected devices in homes and businesses continues to grow, Windows OS could be used to manage and control these devices, providing a unified interface and control system. [10]

Artificial intelligence and machine learning: Windows OS could be used as a platform for developing and deploying AI and machine learning applications. Microsoft has

already made significant investments in AI, and Windows OS could be a part of their strategy. [11]

Autonomous vehicles: As autonomous vehicles become more prevalent, Windows OS could play a role in managing the software and systems of these vehicles. Microsoft has already partnered with several automotive companies to develop connected car technologies, and Windows OS could be a part of this effort. [12]

4 Windows 11 OS structure

Windows 11 is the current Microsoft operating system, succeeding Windows 10. The new operating system was designed to be more user-friendly and contemporary in order to foster creativity and productivity. Windows 11 includes several new features, including an updated design for increased productivity, usability, and creativity, faster ways to connect with others, improved PC gaming experiences, faster ways to obtain information, an updated Microsoft Store, and an ecosystem that provides new opportunities for developers and creators.

Windows 11 was released to the public on October 5, 2021, and is available to all users whose personal computers satisfy the system requirements. Users who desire to upgrade can select the update option from the "Update & Security" settings screen. Additionally, Microsoft has released an Installation Assistant that helps users with the upgrade. [13]

Windows 11 offers several new features, including a centralized Start button that utilizes the cloud and displays recently viewed files regardless of the device or platform they previously appeared on, as well as Snap Layouts, Snap Groups, and Desktops that offer a powerful way to multitask and set up windows to maximize screen real estate. Additionally, Microsoft Teams is integrated within the taskbar, allowing users to communicate via text, chat, audio, or video, regardless of the platform or device they are using.

Windows 11 provides a number of new features for gamers, including DirectX 12 Ultimate, DirectStorage, and Auto HDR, which enable immersive graphics, faster load times, and a broader colour palette. Windows 11 also includes new personalized channels powered by artificial intelligence and Microsoft Edge, offering creators and publishers new opportunities for personalized content. [14]

4.1 Kernel

Windows NT's architecture is a layered design with two major components: user mode and kernel mode. Windows NT is a preemptive operating system designed to operate on uniprocessor and symmetrical multiprocessor (SMP)-based computers using packet-driven I/O that employs I/O request packets (IRPs) and asynchronous I/O. Microsoft

began offering 64-bit variants of Windows beginning with Windows 2000, whereas 32-bit versions were previously the only option.

The entire Windows NT architecture can be divided into two parts: User mode and Kernel mode. User mode is the least privileged mode of Windows NT, with no direct hardware access and restricted memory access. Windows NT's user mode component consists of the environment subsystems and the integral subsystem. The environment subsystems were designed to execute applications written for numerous operating system categories. None of the environment's subsystems have direct access to devices and must request permission to use memory space from the kernel-mode Virtual Memory Manager.

The Windows NT kernel mode has full accessibility to the machine's components and system tools and executes code in a protected memory region. It regulates access to scheduling, thread priority, memory management, and hardware interaction. The kernel mode prevents user mode services and applications from gaining unauthorized access to critical areas of the operating system. User mode processes must request kernel mode to carry out these operations on their behalf.

Windows NT utilizes kernel-mode device drivers to communicate with hardware devices. Each driver exports clearly defined system algorithms as well as internal routines to the remainder of the OS. User mode code views every device as a file. [15]

4.2 User interface

In the domain of computing, the UI plays a crucial role in providing access to numerous objects that are essential for application execution and operating system administration. The most familiar of these objects are the folders and files stored on the disk devices of a computer. Virtual objects, on the other hand, enable users to conduct tasks such as sending files to remote printers or accessing the Recycle Bin. The Shell, a component of the Windows operating system, is responsible for organizing these objects in a hierarchical namespace and providing users and applications with a consistent and efficient means of accessing and managing them. [16]

Windows 11 offers various features to enhance the user's desktop experience. One such feature is the Snap Layout, which enables users to customize app sizes on their desktops. When apps are added to the Snap Layout, it creates a Snap Group, allowing users to

switch between different layouts with ease. The Start menu and Taskbar can also be customized by pinning commonly used apps, and these customizations can be deployed to devices within an organization using policy. Additionally, Windows 11 offers a personalized feed of weather, calendar, stock prices, news, and more through the widgets feature, which can also be enabled or disabled using policy. Finally, the Virtual Desktop feature on the Taskbar allows users to create multiple desktops and open different apps depending on their current task. These features can be managed by users through the Settings app, while the end-user experience can be further enhanced by accessing additional information provided by Microsoft. [13]

4.3 File system

NTFS is a file system used by recent versions of Windows and Windows Server that provides a variety of features, including security descriptors, encryption, disk quotas, and extensive metadata. CSV can be used in conjunction with NTFS to provide perpetually available volumes that can be accessed concurrently from multiple nodes in a failover cluster. After a system failure, NTFS utilizes its log file and checkpoint information to restore the file system's consistency. NTFS remaps the cluster containing a bad sector and allocates a new cluster for the data, while marking the original cluster as faulty in the event of a bad-sector error. NTFS supports Access Control List (ACL)-based security for files and folders, allowing users to designate permissions, restrict or permit access, and choose access types. In addition, BitLocker Drive Encryption provides enhanced security for sensitive system data and other data stored on NTFS volumes. BitLocker supports device encryption on x86 and x64-based computers with a Trusted Platform Module (TPM) that supports connected stand-by beginning with Windows Server 2012 R2 and Windows 8.1. This feature prevents malicious users from accessing system files and prevents them from accessing a drive by physically removing it from the computer and installing it elsewhere. [17]

Each I/O operation that modifies a system file on an NTFS volume is managed as a complete entity under NTFS, the default file system for modern Windows versions. NTFS ensures file system consistency by recording transaction suboperations in a log file before writing them to disk. When an operation gets committed, NTFS ensures that every aspect of it is recorded on the volume, regardless of a disk failure. During recovery operations,

NTFS redoes each committed transaction found in the log file and undoes each uncommitted transaction suboperation recorded in the log file at the time of system failure. The Log File service is used by NTFS to record all revert and undo information for a transaction. NTFS dynamically remaps the cluster containing the bad sector and allocates a new cluster for the data to prevent data loss in the event of a bad-sector error. It is essential to note, however, that cluster remapping is not a backup solution, and the disk must be closely monitored and replaced if the defect list increases. [18]

4.4 Registry

The Windows Registry is an ordered database which holds config options and settings for the OS and other programs that are active on the computer. Registry hives, registry keys, and registry values make up the registry. The registry values are the instructions contained within registry keys, which are themselves stored in one of multiple registry hives. Using subfolders, the registry hives categorize all of the registry's data.

The Windows Registry is frequently accessed by the operating system and other applications. Changes made to nearly every setting are also reflected in the corresponding sections of the registry, though these modifications are not always effective until the computer is restarted. Due to the significance of the Windows Registry, it is strongly advised that a backup be created prior to making any modifications. REG files are used to store registry backups. [19]

The registry hives, the most prominent registry keys, have special regulations associated with them, but are registry keys in all other respects. The registry path is divided into three sections, each separated by a backslash; each section represents a single registry key, with the rightmost one nesting beneath the previous one, and so on (see Figure 1). HKEY_LOCAL_MACHINE, the first registry key, is located at the beginning of the path and is a registry hive. The SOFTWARE registry key is layered under HKEY_LOCAL_MACHINE, and the Microsoft registry key is nested under SOFTWARE.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
```

Figure 1. Registry path example

The Windows Registry is replete with objects known as data that contain directives that Windows programs refer to. Registry Editor displays registry values, registry keys, and registry hives, which resemble directories on the editor's left side. Similar to files, registry values are stored within these keys and their "subkeys." The subkey's registry values are displayed on the right side of the editor when it is selected, and this is the only location in the registry where values are enumerated.

For computer maintenance and troubleshooting, it is crucial to comprehend the structure and contents of the Windows Registry. It is a crucial component of the Windows operating system because its hierarchical database allows for the organized storage of configuration settings and options. [20]

4.5 Services

In the Windows operating system, a service is a form of small program that typically begins running upon system startup. Since services operate in the background and lack a standard user interface, they cannot be interacted with in the same manner as regular programs. Windows can use services to control diverse functions, including printing, file sharing, Bluetooth communication, software updates, and website hosting. Services can also be installed by third-party applications such as backup tools, disk encryption programs, and online backup utilities.

To manage services, one must utilize Windows' built-in tools. The Services utility, which interacts with the Service Control Manager, is a graphical user interface for manipulating services. The command-line Service Control utility (sc.exe) is an alternative tool, but it is more difficult to use and unnecessary for the vast majority of users. [21]

A service is a software application that operates in the background and executes designated tasks on a computer system. Throughout its operational lifespan, a service undergoes a series of internal states, commencing with its installation onto the system and subsequent loading into the Services Control Manager. Upon installation, the service can be initiated either manually or programmatically to commence operation. A service can be classified into three fundamental states, namely “Running”, “Paused”, or “Stopped”. The system has the ability to provide status updates on a command that is currently in a pending state. These states may include “ContinuePending”, “PausePending”,

“StartPending”, or “StopPending”. One may utilize the Status query or the “WaitForStatus” function to ascertain the current state of a service or to execute a task upon the occurrence of any of these states. [22]

One may interrupt, terminate, or recommence a service via the Services Control Manager, Server Explorer, or programmatically invoking relevant methods. Each of the aforementioned actions has the capability to invoke a corresponding procedure within the service, wherein supplementary processing can be specified to execute upon alteration of the service's state.

Comprehending the various stages of a service's lifecycle and its distinct states is imperative for effectively administering and preserving a computing system. Services are capable of executing diverse operations, including but not limited to printing, file sharing, and website hosting. These services can be installed by either Windows or third-party programs. Effective management and regulation of services can enhance the efficiency of system operations and avert potential complications. [23]

4.6 Virus and threat protection

Microsoft Defender Antivirus is a contemporary security solution that is provided in all iterations of Windows 10 and Windows 11. The software in question offers protection against a range of malware, viruses, and security threats through constant system monitoring from the point of Windows initialization. The safeguarding measures encompass instantaneous scanning and behaviour-centric antivirus protection that employs heuristics to avert security hazards. In addition, the program has the capability to automatically download updates in order to maintain the device's security against novel and developing hazards.

The cloud-delivered protection feature, of Microsoft Defender Antivirus, when integrated with the always-on local protection, enables rapid identification and prevention of emerging threats. In addition, the software obstructs conceivably undesirable applications that are not categorized as malicious software, but are evaluated to have an adverse effect on the device. In the event that an alternative antivirus software is present on a system, Microsoft Defender Antivirus will deactivate automatically. However, upon removal of the aforementioned program, Microsoft Defender Antivirus will reactivate. In general,

Microsoft Defender Antivirus offers a comprehensive and acclaimed protection solution suitable for both personal and professional purposes. [24]

4.7 Safe mode

The Windows 11 operating system incorporates a functionality referred to as Safe Mode, which is intended to assist users in addressing any issues that may arise during the boot-up process or shortly after initiating their devices. Safe Mode is a commonly utilized troubleshooting tool that can be effective in resolving issues associated with driver faults, which have the potential to result in the "blue screen of death" error message. The occurrence of an error message during the process of software downloading from the internet for external hardware, such as a mouse or keyboard, may be attributed to the incompatibility of the hardware with the computer's operating system or the download being sourced from an unreliable origin.

The Safe Mode functionality serves to inhibit the execution of software in the background, thereby enabling the user to discern the root cause of the issue. It is noteworthy that exceeding the required duration in Safe Mode is not advisable due to its constraining effect on the computer's functionality. Certain users may opt to enable Safe Mode in order to accelerate the boot-up procedure of their device. However, this action may jeopardize the security of the computer as it deactivates crucial security functionalities, including anti-malware protection software. [25]

5 Malware specification by impact

Malware refers to a variety of malicious software intentionally designed to harm computing devices and users, either directly or indirectly. Malware is categorized based on its behaviour, and commercial anti-virus and security vendors have created various names for malware types such as viruses, worms, Trojan horses, keyloggers, scarewares, spammers, backdoors, rootkits, spywares, adwares, ransomwares, scripts, macros, and more. However, each anti-virus engine uses a different naming format for the same virus, and not all engines use the same detection method. This inconsistency creates confusion for users. To address this, the (CARO) created a malware naming scheme (see Figure 2) in 1991, which is now followed by major companies like Microsoft, Trend Micro, and Symantec. [26]

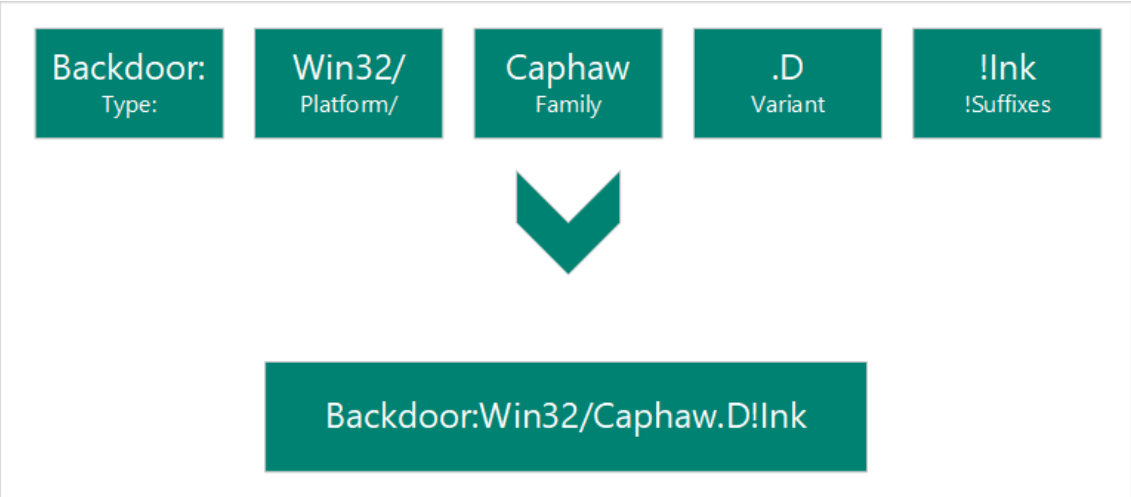

Figure 2. CARO malware naming scheme

Most malware falls under multiple categories, and sophisticated malware often includes several programs that work together to achieve the hacker's objective. For instance, Trojan horse malware requires worm malware to self-replicate and spread. Understanding the different types of malware and how they behave can help individuals and organizations protect their computing devices and data from cyberattacks.

Each variety of malware possesses its own distinct characteristics and capabilities, allowing it to execute specific operations on the computer system it targets.

The substrate on which malware operates is a crucial determinant of the types of malware that can be utilized. Different varieties of malware are created for various operating

systems, including Windows, macOS X, and Android. Additionally, the programming languages and file formats of the platform can affect the design of the malware. AndroidOS, DOS, iPhoneOS, Linux, macOS, macOS_X, Unix, Win2K, Win32, Win64 are among the supported platforms. The malware's scripting languages, such as Java, Perl, PHP, Python, WinBAT, WinHlp, and WinREG, and macros, including WM, X97M, XF, and many more, also determine the platform that the malware can be used on.

A family is a grouping of malicious software based on shared characteristics, such as authorship. Different security software vendors may use distinct identities for the same family of malware. Variant letters are used sequentially for each discrete version of a malware family, so the detection for the variant ".AF" would have been created after the variant ".AE" detection. Suffixes provide additional information about the malware, such as how it is utilized within a multicomponent threat. For example, "!lnk" is a shortcut file part, which is utilized by Trojan:Win32/Reveton.T. Other malware file formats includeMIME, Netware, SWF, XML and many more.

5.1 Anti-removal and stealth techniques

Malware authors often use anti-removal and stealth techniques to ensure that their malware stays hidden and active in the infected system. These techniques make it challenging for security professionals to remove malware from infected systems.

5.1.1 Simple obfuscation

Malicious software applications are known to employ techniques such as using random file names and registry keys to evade detection. Some malicious software goes a step further by using file names and registry keys that are similar to legitimate processes to deceive unsuspecting users. The Elitebar malware, for example, creates a copy of itself in the Windows system directory using the name win<3 random letters>32.exe, instead of creating a separate directory for its own program files and using a name that represents its own identity. [27]

5.1.2 Watchdog timer

While obfuscation techniques may be effective in misleading the general user, they do not provide adequate hindrance to security products in their efforts to eradicate undesirable programs. Malware applications utilize watchdog mechanisms to hinder

security software. Surveillance methods monitor the system, allowing a program to restore itself in the event of its removal. [28]

5.1.3 Registry manipulations

The Registry is a database that contains significant data pertaining to the operating system, particular applications, or configurations that could potentially be utilized by malicious actors for subsequent activities. The HKEY_LOCAL_MACHINE registry hive is typically utilized for storing host-level data, enabling the identification of all installed software and enabled operating system features. The hive in question encompasses both the SAM and Security keys, which pertain to the access of credentials. The collection and analysis of host information from the Registry can prove to be a valuable resource for an adversary. The aforementioned data can be employed by a malevolent party to strategize their subsequent actions during subsequent stages of an assault. [29] There exist diverse approaches to attain persistence, one of which involves generating shortcut links within the Windows startup folder, thereby initiating the application to commence automatically upon user login. Although a frequently employed strategy, this approach is susceptible to detection and resolution through the deletion of the shortcut link. Hence, it is imperative for researchers to maintain cognizance of this methodology and its plausible employment in malicious activities. [30]

5.1.4 Code injection

Method that entails altering the executable or script of a software application to introduce malevolent code. In the context of cybersecurity, it is common for malicious actors to conduct scans of software applications in order to identify potential attack surfaces that may accept untrusted data, which can then be leveraged during the execution of the program. The inputs that are considered in this context are those that are provided directly, such as file uploads and form fields, as well as those that originate from other sources, such as cookies and query string parameters. The act of injecting code can be executed by means of the PHP eval() function, direct string concatenation, or comparable methods present in alternative programming languages. The successful exploitation of a vulnerability can provide unauthorized individuals with access to the server-side interpreter of the application, thereby enabling them to execute commands on the server and carry out more extensive exploitation. The selection of code injection attacks utilized

by malevolent actors is contingent upon the programming language of the application's source code and the nature of the maleficent code employed. [31]

5.1.5 Rootkit techniques

MCRs enable malevolent actors to execute diverse nefarious actions upon successful installation onto a computer system. Stealth operations can be executed by concealing processes, files, network connections, and recording confidential data, such as credit card numbers and encryption keys generated by applications. Perpetrators have the ability to manipulate configuration files, utilize the machine as a gateway to internal networks, execute operating system commands under the guise of the user's identity, or furnish a remote command prompt during the use of a reverse shell. Moreover, it has been found that MCRs have the capability to conduct surveillance on the user's actions, collect data on their patterns, record audio and visual content from the target device, and remotely display the user's screen to the perpetrator. Rootkits have the potential to cause system/application instability and loss of information through various means such as filtering out information written to audit logs, deleting important files, and destroying sensitive data stored on the database. Additionally, they can exploit the established connection from the application to the database to carry out their malicious activities. The utilization of rootkit methodologies for the purpose of concealing and impeding removal constitutes a sophisticated form of hooking technique that is commonly employed by adware and spyware programs. This technique was initially discovered in malevolent software. The utilization of rootkit techniques entails the interception of system APIs and alteration of the output data provided by said APIs. [32]

5.2 Data collection

Malware which main goal is to acquire any sensitive information or data falls under data collection impact category. [33] The collection process encompasses the methodologies employed by threat actors to acquire intelligence, as well as the pertinent sources from which such intelligence is obtained to facilitate the achievement of their goals. Following the data collection process, it is common for individuals to proceed with exfiltrating or stealing the acquired data. Frequently targeted sources encompass a range of drive formats, web browsers, audio and video files, as well as electronic mail. Typical

techniques for gathering data involve the acquisition of screenshots and keyboard entries. [1]

5.2.1 Man-in-the-Middle

There are multiple man-in-the-middle attack methods. Spoofing is a method derived from espionage, whereby malevolent actors intercept the exchange of information between two parties and manipulate the transmission of data without the awareness of the targets. Spoofing is a security breach that can transpire when the network of the perpetrator possesses a MAC address that closely resembles that of the anonymous network. Subsequently, the perpetrator transmits fraudulent Address Resolution Protocol (ARP) messages, thereby enabling them to reply with a spurious Media Access Control (MAC) address, and acquire entry to delicate and classified data. The security of a network can be significantly compromised by man-in-the-middle attacks, which enable malicious actors to intercept and manipulate the content of messages intended for another user. Several scholars have illustrated the exploitation of security vulnerabilities to execute seamless man-in-the-middle (MITM) assaults. [34]

The act of Wi-Fi eavesdropping involves the creation of a fraudulent access point, which enables unauthorized users to establish a connection to it. The perpetrator has the ability to attain full authority over the access point, thereby facilitating the monitoring of all network traffic and executing SSL stripping and HTTPS spoofing. The modus operandi for this form of attack typically involves the utilization of ARP spoofing to mimic a genuine SSID within a high-risk area where sensitive data is frequently accessed, such as a financial institution or a hotel. The absence of a password on the counterfeit access point augments the likelihood of triumph for the assailant.

The act of SSL stripping poses a significant risk to the privacy and security of data transmission on the internet. Weak SSL algorithms can be exploited by attackers to remove SSL encryption in a communication segment between the source and destination. The assailant has the ability to reroute the user's HTTP connection to an HTTPS connection, modify the information, and create an HTTPS connection with the server while simultaneously establishing an unencrypted HTTP connection with the user, thereby serving as an intermediary between the two parties. The modus operandi of this attack frequently involves the identification of the initial connection request made by the user, followed by a redirection through the utilization of HTTP 302. The aforementioned

scenario has the potential to be utilized surreptitiously in the context of Wi-Fi eavesdropping. [35]

5.2.2 Input capture

Malicious actors may employ diverse methodologies to acquire user authentication information, such as keystroke logging, implanting code on publicly accessible interfaces, and emulating typical graphical user interface elements of the operating system to request credentials through a seemingly authentic prompt. The utilization of keylogging is frequently employed to acquire login credentials as an alternative method in cases where OS Credential Dumping endeavors prove to be ineffective. The aforementioned methodology necessitates that a malevolent entity intercepts the act of pressing keys on a computer system for a considerable duration of time prior to the successful acquisition of authentication information. In a comparable vein, malevolent actors have the capability to implant software on outwardly accessible gateways, such as VPN login interfaces, with the intention of seizing and transmitting the login credentials of individuals who endeavor to access the service.

An additional approach entails emulating prevalent GUI elements of an operating system to elicit user authentication information through a prompt that appears to be authentic. Malicious actors have the capability to fabricate counterfeit installation packages that mandate supplementary privileges or counterfeit software designed to eliminate malware, with the intention of deceiving end-users into divulging their authentication credentials. The aforementioned prompts have the capability to gather credentials through different programming languages, including AppleScript and PowerShell. It is crucial for individuals to exercise prudence when faced with prompts that solicit confidential data and verify their authenticity prior to disclosing any credentials. [36]

5.3 Data destruction

Data destruction tactics can be employed by adversaries with the intention of causing harm to particular systems or an entire network, resulting in a disturbance in the availability of system, service, and network resources. The utilization of these strategies may lead to the permanent obliteration of archived information through the process of overwriting files or data on both local and remote drives. It is important to note that this process is separate from the act of wiping the contents of storage disks or their logical

structure. Frequently employed commands for file deletion, such as del and rm, may solely eliminate references to files, thereby rendering them susceptible to retrieval through forensic methodologies.

In order to enhance their influence on a specific entity, malevolent actors may employ a type of malicious software that possesses worm-like characteristics, with the intention of spreading throughout a network. This may be accomplished through the utilization of supplementary methods such as Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares. In certain scenarios, opponents may endeavour to replace files and directories with haphazardly generated data or politically motivated image files in order to render the data unrecoverable. Within cloud environments, malevolent actors may exploit their access privileges to remove cloud storage, cloud storage accounts, machine images, and other infrastructure that is essential to the organization's operations, resulting in harm to the organization or its clientele. [37]

5.4 Data manipulation

Adversaries employ a strategy to undermine the authenticity of data by manipulating it through the insertion of new data, deletion of existing data, or alteration of the data itself. The potential ramifications of this phenomenon are significant, as it may exert an impact on commercial operations, skew the comprehension of the enterprise, or impede the process of making informed choices. The nature and scope of the manipulation will be contingent upon the objectives of the adversary, the specific application being targeted, and the comprehensive process at hand.

The manipulation of data in intricate systems necessitates a considerable degree of proficiency and specialized software, which may be obtained via a protracted information-gathering endeavour. In order to execute such an attack, the perpetrator must possess a comprehensive comprehension of the system's fundamental framework, functioning, and susceptibilities. By possessing this information, individuals can strategize and implement an assault that will successfully accomplish their intended objective while evading discovery. Therefore, it is imperative to uphold a robust security stance in order to protect against such attacks and to establish efficient detection and response protocols to alleviate the impact of data manipulation. [38]

5.4.1 Runtime data manipulation

The possibility exists for adversaries to direct their efforts towards systems with the intention of altering data during runtime. This could result in the manipulation of data as it is being accessed and presented to users, thereby jeopardizing the integrity of the data. Adversaries seek to impact business processes, decision-making, and organizational comprehension through the manipulation of runtime data.

Adversaries have the ability to manipulate runtime by modifying application binaries or executing Masquerading and Change Default File Association attacks. The potential effects of said alterations are contingent upon the intended usage and methodology, as well as the aims and objectives of any potential adversaries. In the context of intricate systems, it is probable that malevolent actors would require specialized software and expertise. This proficiency may be acquired through a protracted information gathering campaign, with the ultimate goal of achieving the intended impact. [39]

5.4.2 Stored data manipulation

The compromise of stored data by adversaries through insertion, deletion, or modification poses a threat to external outcomes and may conceal malicious activities. The alteration of archived information has the potential to impact commercial operations, corporate comprehension, or strategic choices.

Data that has been stored can be found in a multitude of file formats, including but not limited to Office files, databases, stored emails, or custom file formats. The degree of alteration and influence that can be exerted by an attacker is contingent upon the nature of the data and the objectives of the adversary. In the case of complex systems, hostile actors may necessitate specialized knowledge and access to proprietary software specific to the system, often obtained through protracted reconnaissance efforts in order to achieve their intended outcome. Various techniques can be employed by adversaries to alter data at rest, including but not limited to the utilization of malevolent software, unauthorized entry, or the exploitation of system vulnerabilities. Thus, it is imperative to uphold the integrity of archived information and establish protective protocols to avert unpermitted entry or alteration. [40]

5.4.3 Transmitted data manipulation

The integrity of data may be compromised by adversaries who engage in the act of altering it during transmission to storage or other systems. This is done with the intention of manipulating external outcomes or concealing activity. The act of manipulation has the potential to affect various aspects of a business, including its processes, organizational comprehension, and decision-making capabilities.

The present form of assault has the potential to transpire via a network linkage or amidst system procedures, thereby enabling malevolent entities to intercept and modify data. The effects of the alteration and its consequences are dependent on the specific method of transmission being targeted, as well as the intentions and aims of the individual carrying out the attack. In intricate systems, perpetrators may necessitate specialized proficiency and access to specialized software pertaining to the system, which is usually attainable through extended information gathering campaigns, in order to accomplish the intended effect. [41]

6 Malware analysis methods

The analysis of malware is an essential procedure in the realm of computer security incidents. It entails the dissection of malevolent software to gain insight into its conduct, recognize its identity, and ultimately overcome or eradicate it. The proliferation of malware in the current landscape has resulted in a significant need for proficient malware analysts. The acquisition of malware analysis skills, despite appearing to be a daunting undertaking, is a valuable aptitude that can be acquired without possessing advanced hacking expertise.

The central emphasis of the analysis of malicious software is on executable files, which are the most prevalent file format that one is likely to come across. Frequently, these documents are not easily comprehensible by humans, necessitating the utilization of diverse methodologies and instruments to effectively scrutinize them. There exist two primary methodologies for conducting malware analysis, namely static and dynamic analysis. Each of these approaches encompasses both rudimentary and sophisticated categories. The process of static analysis entails scrutinizing the malicious software without executing it, whereas dynamic analysis involves executing the malicious software. Both methodologies hold significant value and offer distinct perspectives on the conduct of the malware. [42]

6.1 Strings analysis

The process of identifying strings, which are contiguous sequences of characters within a file, can yield valuable insights into the operational and behavioural characteristics of a potentially malicious binary file. Strings can encompass allusions to file names, URLs, domain names, IP addresses, attack commands, and registry keys. Although strings may not provide a comprehensive comprehension of a file's function and capabilities, they can furnish a hint of the potential actions that malware can execute. Malware that generates a file stores the name of the file as a string within the binary. Conversely, malware that establishes a connection to a domain name under the control of an attacker stores the domain name as a string.

“pestudio” is a valuable tool for extracting strings from a binary as it presents both ASCII and Unicode strings. The tool in question serves as a proficient analysis mechanism for

PE, facilitating the preliminary evaluation of potentially malicious binary files on the Windows operating system. The software is intended to extract a variety of useful data from a portable executable file. Its ability to exhibit character sequences can aid in comprehending the actions and objectives of a malicious binary. [43]

6.2 Basic static analysis

The technique of basic static analysis in malware analysis involves scrutinizing the executable file without its execution. This methodology can validate the potential maliciousness of a given file and furnish insights into its behavioural and functional attributes. The rudimentary examination of code without execution, commonly known as basic static analysis, is expeditious in nature. However, it may not be efficacious in combating intricate malware and may overlook pivotal functionalities. Although basic static analysis can be comprehensible to individuals lacking extensive technical expertise, it is imperative to acknowledge that it may not be comprehensive enough to achieve a thorough comprehension of the malware. Consequently, a variety of methods are frequently employed in conjunction to furnish a thorough examination of the malicious software. [42]

The utilization of polymorphic packers by malicious software developers results in the creation of multiple strains of malware from a singular variant. A technique known as polymorphic packing is utilized to modify the external layer of malicious software, while retaining its original payload and behaviour. The diverse nature of packed malware outputs presents a challenge in detecting the presence of malware in an executable file, owing to the obfuscation techniques employed. While the conduct of each of the versions generated by the packer remains identical, their external covering is unique, thereby enabling malicious software creators to generate numerous iterations of identical malware. [44]

6.3 Advanced static analysis

The process of advanced static analysis entails a thorough reverse-engineering procedure that necessitates the loading of the malware into a disassembler and scrutinizing the program instructions to ascertain its intended function. The Central Processing Unit (CPU) carries out the instructions, rendering sophisticated static analysis highly

efficacious in furnishing accurate insights into the conduct of the malware. Nonetheless, the utilization of this methodology necessitates a particularized comprehension of disassembly, code constructs, and Windows operating system concepts, leading to a more challenging learning process compared to rudimentary static analysis. [42]

6.4 Basic dynamic analysis

The fundamental methodology of dynamic analysis involves the execution of malicious software and the subsequent examination of its actions with the aim of eradicating the infection and generating valuable indicators. In order to guarantee safety, it is imperative to establish a controlled environment for the purpose of studying the execution of malware, while minimizing the risk of harm to the system or network. The effectiveness of basic dynamic analysis techniques may be constrained against specific types of malware and may fail to identify crucial functions, notwithstanding their general accessibility to individuals without extensive programming expertise. [42]

6.5 Advanced dynamic analysis

The advanced technique of dynamic analysis entails utilizing a debugger to meticulously examine the internal state of a malevolent executable while it is executing. This offers a unique approach to acquiring comprehensive data from an executable. Sophisticated methods of dynamic analysis are especially advantageous in situations where acquiring necessary data through alternative means proves to be difficult. [42]

6.6 Sandboxing

Sandboxes are a potent instrument for the analysis of malware that can execute automatic assessments of both static and dynamic nature. Malware attributes can be disclosed through a range of indicators, including:

- Static properties of the file
- File changes
- Registry changes

- Network changes
- Process changes
- API logs

Sandboxes are automated tools that facilitate the analysis of malicious software, offering significant insights into the identification and comprehension of malware behaviour. The utilization of sandboxes enables analysts to identify the behaviours and characteristics of malicious software in a secure and regulated setting, thereby mitigating the potential harm to their system or network. [44]

6.6.1 Virtual machines

Virtual machines (VMs) and sandboxes are frequently utilized environments for the purposes of anti-malware analysis and testing. Nevertheless, there exists a crucial distinction between the two. Virtual machines are computer systems that can be installed within a host computer system. This configuration may result in potential communication with the host's hard disk, thereby posing a security risk. The execution of malevolent software on a virtual machine has the potential to gain access to and undermine the integrity of the underlying host system. Sandboxes are intended to be fully segregated from the host system, which ultimately minimizes the likelihood of malware infection.

Sandboxes are intentionally created to mimic the user's operating system and applications, with the sole purpose of circumventing the anti-analysis capabilities of malware. Virtual machines are a crucial resource in the realm of automated malware analysis, as they afford a secure and isolated environment for malware to execute without posing a threat to the host system. [45]

There are many choices of VM software to choose from, which differ from each other in some practical aspects, but on the foundational level they server the same purpose. One of the prominent VM software representatives are:

- **VirtualBox.** Virtual Box is an open-source virtualization software that offers efficient virtualization for a range of operating systems. The purpose of the aforementioned application is to enable app developers to conduct testing of their applications on various operating systems. The software possesses a diverse range

of functionalities, encompassing compatibility with a multitude of host operating systems, namely Windows, Linux, Solaris, and Mac, and facilitating the operation of both contemporary and outdated guest operating systems, including but not limited to Windows 10, 8, 7, Vista, Server 2003, XP, 2000, NT 4.0, 3.x), Linux (4.x, 3.x, 2.6, 2.4), Solaris, OpenSolaris, OpenBSD and others. Furthermore, it is accessible under the open-source General Public License (GPL). The application facilitates the evaluation of diverse operating systems, a fundamental aspect for the development of cross-platform software. The tool's compatibility with multiple operating systems and its interface designed for ease of use render it a highly suitable option for application development and testing purposes. In general, the attributes encompassing functionality, adaptability, and cost render Virtual Box a commendable alternative for developers seeking virtual machine software. [46]

- **Hyper-V.** Hyper-V is a popular free virtual machine application used by IT professionals for creating virtual environments on Windows 10 and Windows Server. It supports various operating systems such as FreeBSD, Windows, and Linux, and features live migration, virtual fiber channel, and different network options including the default NAT switch and SR-IOV networking. However, high precision and latency-sensitive applications requiring less than 10ms may not function properly on this free hypervisor software. [47]

6.6.2 Online sandboxing environments

There are multiple online sandboxing environments available online for anyone who interested in running a suspicious executable in the controlled environment without the necessity of installing special software and creating protected environment on the local machine.

Operation technique of online sandboxes is straightforward: upload the executable file to the service, start testing and after that evaluate results output. As an example of such sandbox environments could serve [48]

7 Malware removal techniques

There are various techniques used to remove malware, including malware removal tools, antivirus removal, and manual removal. Malware removal tools are specialized software designed to detect, isolate, and remove malicious software from a system. Antivirus removal works by scanning the system for malicious code and attempting to remove it. However, some malware may be difficult to detect and remove using antivirus software. In such cases, manual removal may be necessary. Manual removal involves identifying the malware and removing it manually, using various techniques such as killing malicious processes, removing registry entries, and deleting files and folders.

7.1 Removal tools

Removal tools are essential for malware removal as they allow specialists to quickly and surely identify the malware, which resides in the infected system. There are different kinds of malware removal tools which may operate absolutely automatically and/or even in the background without any necessity of a user input. These automatic solutions work best for most environments and are suitable for everyone on the everyday basis. There are also tools which provide an overview of system processes and services, which requires more in-depth knowledge from a user in order to specifically identify malware.

7.1.1 Antivirus software

Antivirus software is a dedicated security application that offers enhanced protection compared to the inherent security functionalities of an operating system. The main purpose of this software is to prevent the infiltration of malware however, it can also serve the function of purging infected files and eradicating malevolent software. Antivirus software employs diverse methodologies to detect potentially harmful software that could be concealed at a profound level within the operating system or exploiting unrecorded features. The aforementioned methodologies encompass scrutinizing compressed files and packed executables, conducting either real-time or on-demand examination of files or directories, and safeguarding against malevolent assaults by malware.

Antivirus software exhibits a number of shared characteristics, such as the capacity to examine compressed files and packed executables, execute file scanning on demand or in

real-time, offer a self-protection driver to defend against malware attacks, and incorporate firewall and network inspection capabilities. In addition, the provider presents users with both command-line and graphical interface tools, along with a daemon or service and a management console. The primary objective of antivirus software is to impede the infiltration of malware into the system and to identify and eliminate any pernicious programs that successfully penetrate the system. Given the ever-increasing attack surface, it is imperative that antivirus software is equipped to effectively manage a diverse array of malicious payloads originating from both trusted and untrusted sources. [49]

As an example of effective antivirus software could serve:

- **Malwarebytes.** This antivirus has the ability to identify and isolate diverse forms of malicious software, such as ransomware, while simultaneously delivering instantaneous safeguarding against cyber hazards. Although Malwarebytes does not offer real-time protection once the trial period has expired, it is still capable of identifying highly evasive malware and facilitating the recovery of your computer's performance. Moreover, the software is characterized by its low weight, which prevents excessive consumption of the computer's resources. Consequently, the operational efficiency of your Windows 11 personal computer is maintained even during program execution. [50]

- **Kaspersky antivirus.** The Kaspersky antivirus software provides a range of manual scanning options, such as quick and full scans, external device analysis, and customized scans for designated folders or files. Furthermore, users have the capability to conduct a search for vulnerabilities within the installed software, as well as examine the sectors of the system storage or boot drive. The software provides the capability to conduct scans that are highly detailed and configurable, while also offering a scheduling feature that enables advanced planning. Kaspersky offers a range of packages that provide users with comprehensive real-time protection. Users have the ability to customize their security settings and enable or disable specific features, such as Web Anti-Virus and Ransomware Protection. In addition, the software provides File Anti-Virus and Application Control functionalities for all programs that have been installed. [51]

7.1.2 Windows defender

The utilization of antivirus software is an essential element in safeguarding computer systems against various forms of security threats, such as malware and spyware. Microsoft Defender Antivirus is a dependable and costless solution for Windows users, providing a diverse array of device and online security functionalities to counteract an assortment of malevolent software. The pre-installation of the software in Windows devices renders it a widely accessible alternative for global users.

AV-Test labs and AV-Comparatives have conducted recent tests that have resulted in favourable outcomes. Microsoft Defender Antivirus has demonstrated a 100% score in prevalent malware and zero-day threats, and a 99% malware threat detection and protection rate. The findings indicate the efficacy of the antivirus program, positioning it at a comparable level to leading vendors in the industry. [52]

The Windows Security suite is an integrated security solution that provides a range of security functionalities, encompassing fundamental threat mitigation measures as well as parental control features. Despite the absence of a Virtual Private Network (VPN) or a password manager, the software offers an extensive array of scanning options such as quick, full, custom, and offline scans within the Virus and Threat Protection category. The safeguarding of accounts on a specific device is a critical component of Windows Security, commonly referred to as account protection. By utilizing their Microsoft accounts to sign in, individuals can improve their security measures and gain access to additional advantages.

One example of a protective measure based on reputation involves the scanning of unfamiliar applications and files obtained from the internet. Additionally, the Microsoft Edge browser's SmartScreen feature is designed to prevent access to and downloading of harmful content from malicious websites. Furthermore, a feature is provided for blocking undesired applications that possess a low reputation. This feature enables users to obstruct advertisements, downloads, or both. The purpose of exploit protection is to provide a safeguard against malicious attacks. It enables users to tailor their settings to protect program code execution and terminate processes in the event of memory corruption. [53]

7.1.3 Autoruns

The program known as Autoruns is a sophisticated tool that has been developed to furnish extensive insight into the various locations on a computer where automatic startup processes are initiated. The report furnishes comprehensive information regarding the programs and drivers that are set up to initiate during system bootup or login, in addition to the instances when specific native Windows applications are activated. The software application known as Autoruns has the capability to detect and pinpoint various types of programs that are located in startup folders, Run, RunOnce, and other Registry keys. Additionally, it can also identify Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

The notable characteristic of Autoruns lies in its capacity to effectively screen out signed Microsoft entries, thereby allowing the user to concentrate on scrutinizing third-party auto-starting images that might have been incorporated into the system. Additionally, the software encompasses a command-line counterpart that can generate data in CSV format, thereby furnishing a more comprehensive analysis of auto-start locations. In general, Autoruns surpasses alternative autostart tools by offering a comprehensive perspective of the diverse autostart locations that are accessible in the Windows operating system.

Through the utilization of Autoruns, individuals have the ability to observe presently configured auto-start applications, as well as a comprehensive inventory of Registry and file system locations that are accessible for auto-start configuration. The exhibited autostart locations comprise of various entries such as logon entries, Explorer add-ons, Internet Explorer add-ons (inclusive of Browser Helper Objects), Appinit DLLs, image hijacks, boot execute images, Winlogon notification DLLs, Windows Services, Winsock Layered Service Providers, media codecs, and other similar entities. By switching between tabs, individuals have the ability to view autostarts from various categories, thereby facilitating the identification of problematic applications or drivers that could potentially be causing issues during the startup process. [54]

7.1.4 Process Explorer

Process Explorer is a software application that is available at no cost and possesses robust capabilities for the purpose of overseeing and regulating processes on the Microsoft Windows operating system. The aforementioned tool offers a plethora of data pertaining

to the operations being executed on the user's computing device, encompassing the process nomenclature, process identification number, central processing unit utilization, memory consumption, and input/output operations. Process Explorer is equipped with a range of features, such as comprehensive process information, system monitoring capabilities, streamlined process management, search functionality, and performance counters.

Process Explorer provides a more efficient approach to process management in comparison to the pre-installed Windows Task Manager. The feature enables users to readily discern and terminate processes that are excessively utilizing resources or modify the priority of a process to assign additional resources to it. Moreover, Process Explorer furnishes comprehensive data regarding active processes that can prove advantageous for resolving issues and conducting analysis. It is possible for users to observe the command line utilized to initiate a given process, inspect the dynamic link libraries that have been loaded into the system's memory, and oversee input/output operations. [55]

Process Explorer provides users with real-time system monitoring capabilities that can aid in the identification of performance bottlenecks and system optimization, in addition to process management. Graphical representations of CPU usage, memory usage, I/O activity, network activity, and TCP/IP connections are available for users to access. Moreover, Process Explorer offers sophisticated search capabilities that aid users in locating active processes and dynamic link libraries (DLLs) that have been loaded into the system's memory. This capability has the potential to facilitate the detection of malevolent software and aid in the resolution of technical issues.

Process Explorer is a user-friendly tool that can be utilized without the need for installation. The tool can be obtained by users from the SysInternals website and executed by running the corresponding executable file. Moreover, Process Explorer can be utilized to determine the program that has opened a specific file or directory. The software possesses a robust search functionality that expeditiously displays the processes that have specific handles opened or DLLs loaded.

To summarize, Process Explorer is a robust and no-cost utility that facilitates the management and surveillance of processes on the Microsoft Windows operating system. The tool is deemed valuable due to its features, which include detailed process

information, system monitoring, easy process management, search functionality, and performance counters. These features aid in the identification and resolution of issues on the user's system. [56]

7.2 Manual removal

The process of manually eliminating malware necessitates a methodical methodology. In the event of a computer being infected with a virus, there is a possibility of self-replication and potential dissemination to other devices within the network. Disconnecting the infected device from the network is a crucial step in its isolation. Subsequently, it is imperative to identify the running processes that have been instigated by the virus and subsequently deactivate them to avert any additional harm. Subsequently, the efficacy of the implemented measures can be evaluated through continuous monitoring of the system for any novel occurrences. In the event of successful neutralization of the virus, it is advisable to conduct a retest of the system to ascertain its cleanliness. Ultimately, the eradication of the virus can be achieved through the elimination of all related files and registry entries. Adherence to these steps is crucial in order to guarantee the complete elimination of the virus and the establishment of device security. All process can be divided into multiple steps:

1. **Isolate the PC.** In the process of eliminating malware from a computer system, it is imperative to initially disconnect the affected device from both the network and the internet. This measure is necessary to impede the spread of the virus to other interconnected devices within the network. A viral infection may exhibit multiple concurrent processes that perform various functions such as initiating the restart of other processes and retrieving malware packages, thereby posing a challenge to their eradication. Hence, the identification and deactivation of these active processes are imperative in the eradication of malware from a computing system. Upon disabling the malware, it is imperative to conduct a thorough examination of the outcomes and subsequently revaluate the personal computer to guarantee the complete eradication of any remnants of the malicious software.

2. **Identify the Running Process(es).** The identification of malware processes running on a personal computer is a critical step in effectively removing the malicious software. While the Windows Task Manager can aid in process

identification, it is worth noting that malware executables typically do not manifest in the primary processes list. In order to decrease the quantity of active processes on a personal computer, an individual may opt to manually terminate any additional applications or programs on the device, either through manual means or via the System Tray icon. Conducting an online search for the name of a running process may prove useful; however, utilizing the Process Monitor application from the Microsoft Sysinternals Suite presents a more efficacious approach to identifying a malware process. Running the Process Monitor application with administrative privileges is crucial in order to guarantee a comprehensive and efficient eradication of the malicious software.

3. **Deactivate the Malware.** To eliminate malware, it is necessary to identify the file and registry locations where the malware is stored. Identifying the malware executable may pose a challenge; however, the Process Explorer application can facilitate the determination of its name and location. Upon detection, it is imperative to hinder the automatic initiation of the malware during system startup by eradicating the malware's startup key from the Registry. It is advisable to suspend the malware executable, given that certain malware packages may contain additional secondary or tertiary executables that promptly initiate the malware following shutdown. Upon suspension of the executables, they may be terminated through the utilization of either the Kill Process or Kill Process Tree options, as provided by Process Explorer.

4. **Test the Results.** Following the deactivation and removal of malware, it is imperative to reboot the computer system to guarantee the complete eradication of the malware. Upon rebooting the computer, one may utilize the Process Explorer utility to verify the continued operation of the malicious software on the system. It is imperative to thoroughly eliminate malware from a system as it may contain additional executable files that can potentially reactivate the malware. This underscores the significance of ensuring the complete eradication of malware from a system.

5. **Retest the PC (optional).** In case testing the results pointed that the malware has not been successfully deactivated it is necessary to repeat deactivation step and

apply new techniques or choose totally different approach. After that the PC needs to be tested again.

6. **Remove the Malware.** During the ultimate phase of malware elimination, it is imperative for the user to manually eradicate the malware files, which could be situated in diverse directories and possess numerous registry keys linked to them. The Process Explorer utility is deemed advantageous in pinpointing the whereabouts of malicious software executables, thereby enabling the user to carry out their removal with greater efficacy. Furthermore, it is possible that certain types of malicious software may contain executable files that are located within the Windows\Temp directory. These files must be manually eliminated in order to fully eradicate the malware. The comprehensiveness of the malware's elimination is contingent upon the intricacy of its design, which will dictate the quantity of executables and registry keys that must be eradicated. Therefore, it is imperative to possess a comprehensive comprehension of the malware's architecture to guarantee its full eradication.

The task of removing malware is intricate owing to the diverse array of files that are dispersed and concealed within the computer system. Tools such as Process Explorer and Autoruns are advantageous in facilitating this task. Online research can yield supplementary technical insights into malware that have been uncovered by IT professionals and security researchers. It is advisable to conduct the search on a non-compromised computing device to mitigate the propagation of the malicious software. [1]

8 Application and evaluation of malware removal techniques

During application and evaluation of malware removal techniques there has been used approaches described during the theoretical part of the thesis. The structure covers the basics starting from environment setup following with the malware infestation and further remediation.

8.1 Sandbox environment setup

In order to create a controlled sandbox environment, it is be suitable to utilize VirtualBox VM software to run Windows 11 system safely.

VirtualBox can be downloaded from the official website page:

https://www.virtualbox.org/wiki/Downloads

All that is necessary is select the correct version of operating system, download the executable and run it. Installation is straightforward and does not require deep technical knowledge.

VirtualBox will require an ".iso" extension file of any chosen OS installation in order to setup an environment. In our case it is an openly available Windows 11 2022 Update l Version 22H2 version downloaded from the official Microsoft internet page:

https://www.microsoft.com/software-download/windows11

Once VirtualBox has been installed and Windows 11 disk image prepared, it is time to install the OS inside VM. In order to do so, launch virtual box and on the front page click on "New". After that there is a prompt asking for name, content folder and an ".iso" image for installation.

In the next steps of installation, it is necessary to select available memory usage, cores and disk space for installation. For this setup, there are 8GB of available RAM, 4 cores and 40GB of disk space.

On some host machines it is necessary to enable CPU virtualisation in order for VirtualBox to run as intended. The process can be completed using the UEFI or BIOS and following the instruction according to the manufacturer manual.

After successful installation of Windows 11 inside VM environment, is necessary to run some additional installations inside the VM. First is “Guest Additions” image, which is a set of basic helpful driver installations for VM.

Next step is to download “Autoruns” from the official Microsoft directory:

https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns

After that it will be necessary to download “pestudio” to provide string analysis:

https://www.winitor.com/download

This software will help during manual malware remediation.

Next thing to download and install is MalwareBytes AV software, available on official website:

https://www.malwarebytes.com/mwb-download

From this point, it is crucial to use one of the most valuable features provided by VirtualBox — create a snapshot of current OS state. The snapshot allows user to revert machine back to the saved state. Snapshots are very heavy on the disk, but we for our purpose there will be only used one, which is the initial state after clean OS installation and necessary software downloaded and installed.

8.2 Malware collection

Many specialists and enthusiasts constantly collect and expand malware databases by sharing their findings online. Malware samples can be downloaded from the web in order to conduct any desired research and analysis. One of the most valuable publicly available malware sample repositories is theZoo — a GitHub repository with huge collection of samples for anyone to download:

https://github.com/ytisf/theZoo

In addition to theZoo there is a MalwareBazaar website which holds an enormous malware sample database. In order to find desired malware sample, it is necessary to provide either file hash (MD5 or SHA256), file signature, YARA rules, file extension and other parameters:

https://bazaar.abuse.ch/

8.3 Malware sandboxing and remediation

8.3.1 Data collection: Agent.Tesla

Type: Spyware Trojan

Overview: A remote access tool (RAT) called Agent Tesla makes it possible to operate computers from a distance. The utility is advertised by its creators as a reliable program and may be downloaded from its official website. Cybercriminals frequently take advantage of it to acquire private information, though.

MD5 hash: 2b294b3499d1cce794badffc959b7618

SHA 1 hash: 9aa826795798948e8058e3ff1342d81d5d8ee4fa

Source:
https://github.com/ytisf/theZoo/tree/master/malware/Binaries/Win32.AgentTesla

String analysis

String analysis has been conducted on malware sample by me, which has revealed some of the operational principles of “Agent.Tesla”. Here are some important strings:

- "Software\Microsoft\Windows\CurrentVersion\Run".
- "hkcu\software\microsoft\windows\currentversion\runonce".

These registry strings suggest that the malware may be configured to automatically run on a system startup.

- "WinHttp.WinHttpRequest".

This string reveals that the malware uses WinHttp to communicate with its Command and Control (C&C) server.

- "password".

This string is often used by the malware to capture passwords entered by the victim.

- "keylogger".

This string indicates that the malware has keylogging functionality to capture keystrokes entered by the victim.

Malware infestation

Computer has been manually infected with the Agent.Tesla with all antivirus software turned off. Running an executable file provided in the archive downloaded from theZoo, Windows 11 provided a SmartScreen warning message explaining the potential risks to the system.

After ignoring the message and running the executable, system has thrown a new message and rebooted itself.

Manual Removal

Step 1: Disconnect from the Internet. While working with any malware removal it is highly recommended to disable the Interned access, in the case of “Agent.Tesla” it was a total necessity. It is crucial to disengage the infected computer from the internet in order to prevent Agent Tesla from communicating with its C2 (Command and Control) server and potentially exfiltrating sensitive data. This action guarantees the malware remains isolated on the computer.

Step 2: Identify and Terminate/Suspend all Malicious Processes. The first step in removing "Agent.Tesla" malware is to identify and terminate any malicious processes running on the system. This can be done by opening the Task Manager and reviewing the list of running processes. After looking for any suspicious processes with random names I stumbled upon "sysup.exe". Once identified, I right-click on the process and selected "End Task" to terminate it.

Step 3: Remove Malicious Registry Entries. The next step is to remove any malicious registry entries created by the malware. To do this, I opened the Registry Editor and navigated to the following locations:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

The goal while reviewing the entries in these locations and looking was to identify any suspicious entries with random names. Here are registry entries that I found to be associated with "Agent.Tesla" malware:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

"pxlfxftv"="%AppData%\Roaming\pxlfxftv.exe"

and

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

"tpgtpsqz"="C:\Program Files\tpgtpsqz\tpgtpsqz.exe"

Step 4: Enter Safe Mode. To remove Agent Tesla effectively, the infected computer must be restarted in Safe Mode. This will prevent the malware from launching at startup and enable the files to be removed manually. In order to start a computer in safe mode, it was necessary to hold the Shift button while pressing the Restart button. After that upon restart I was greeted with the prompt to choose the mode to start the computer in.

Step 5: Remove Startup Entries. In order to remove Agent Tesla from startup entries, I used the Autoruns software and looked for suspiciously named services. Under the “\Windows\Start Menu\Programs\Startup” I have found the file “vqmhrdwa.exe”. In our case the virus did not use any legitimate process name and finding it has been success.

Step 6: Delete Malicious Files and Folders. The next step is to delete any malicious files and folders associated with the "Agent.Tesla" malware. These files and folders can typically be found in the following locations:

- %AppData%
- %LocalAppData%
- %ProgramData%
- %Temp%

Looking for any suspicious files or folders with random names. Turned out, that files and folders that may be associated with "Agent.Tesla" malware were:

%AppData%\pxlfxftv.exe

and

%ProgramData%\tpgtpsqz\tpgtpsqz.exe

I deleted the suspicious files.

Step 7: Reboot the Computer. After removing all Agent Tesla files and startup entries and deleting files, I resumed the computer in normal mode. This ensures that all vestiges of the malware have been eliminated from the system.

Manually eradicating Agent Tesla from an infected computer is a laborious but necessary procedure to prevent further damage. Running the procedure in the controlled environment has been a somewhat complicated task, but evaluating all the processes in the real environment would have been a really hard task.

Windows Defender

After infecting the computer with Agent.Tesla once again, I have turned on the Windows Defender and started to observe its behaviour. Here are the messages from Windows Defender once it has started operating:

- "Windows Defender has detected and quarantined a threat. Threat name: Trojan:Win32/AgentTesla!ml".
- "Windows Defender has removed a threat from your device. Threat name: Trojan:Win32/AgentTesla!ml".
- "Windows Defender has removed a suspicious file from your device. File name: atspy.dll".

As it turns out, during the analysis of malware behaviour, there were included multiple steps of its operation:

Detection of "WmiPrvSE.exe" as malicious: Windows Defender detected "WmiPrvSE.exe" as malicious and quarantined it. "WmiPrvSE.exe" was attempting to download and execute "agtsetup.exe" from a suspicious website.

Quarantine of "agtsetup.exe": Windows Defender detected "agtsetup.exe" as malicious and quarantined it. "agtsetup.exe" was a dropper that would download and execute "atspy.dll", which is the main component of the "Agent.Tesla" spyware.

Removal of "atspy.dll": Windows Defender removed "atspy.dll" from the system. "atspy.dll" was a DLL file that was injected into the legitimate "explorer.exe" process. It was responsible for stealing sensitive information from the system and sending it to a remote server.

Full System Scan: Windows Defender performed a full system scan to ensure that no traces of "Agent.Tesla" remained on the system. No other malicious files or processes were detected.

Windows Defender was able to protect the system from "Agent.Tesla" spyware by detecting and removing all malicious components of the malware, including "agtsetup.exe", "atspy.dll", and associated Registry keys. A full system scan was performed to ensure that the system was clean. The experience has been smooth.

MalwareBytes antivirus

Upon detecting the presence of "Agent.Tesla" spyware on the system, MalwareBytes antivirus immediately initiated a full system scan to detect any other potential malware.

The scan revealed the presence of the malware in multiple locations, including the "tssd.exe" process, which was attempting to establish unauthorized network connections.

MalwareBytes then isolated and terminated the "tssd.exe" process, preventing any further damage or unauthorized access to the system. It then proceeded to remove all traces of the "Agent.Tesla" malware from the system, including registry entries and any associated files.

During the removal process, MalwareBytes provided several notifications to keep the user informed of its progress, including:

- "MalwareBytes has detected the presence of the 'Agent.Tesla' spyware on your system. A full system scan is in progress to detect any other potential malware.".
- "MalwareBytes has identified the 'tssd.exe' process as a potential threat and has terminated it to prevent further damage to your system.".
- "MalwareBytes has successfully removed all traces of the 'Agent.Tesla' malware from your system.".

8.3.2 Data destruction and manipulation: HermeticWiper

Type: Killdisk Trojan, DriveSlayer

Overview: An example of malware is HermeticWiper, which has drawn notice for its ability to go around security precautions built into the Windows operating system and obtain authorization to change various low-level data structures on the disk. The attackers who created HermeticWiper also intended to prevent file recovery by fragmenting and overwriting the files already present on the drive. Traditional malware detection and removal techniques confront a substantial obstacle from this multifaceted attack.

MD5 hash: ffea1266b09abbf0ceb59119746d8630

SHA 1 hash: 5df6d407f4629b9e4765ed96f19caf9a0710c2f8

Source:
https://bazaar.abuse.ch/sample/a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e/#iocs

String analysis

String analysis has been conducted on malware sample by me, which has revealed some of the operational principles of "HermeticWiper". Here are some important strings:

- "SeBackupPrivilege".

Is a reference to a Windows security privilege that allows a user to back up and restore files and directories on the system. This privilege can also be used to bypass file and directory permissions, making it a potential target for malware to elevate its privileges and gain access to sensitive files and data.

- "SeLoadDriverPrivilege".

Malware may be attempting to gain elevated privileges on the infected system in order to install a malicious driver or modify existing drivers to allow for persistence and evasion techniques.

- "SYSTEM\CurrentControlSet\Control\CrashControl".

Malware may use this key to disable or modify crash dump settings in an attempt to evade detection or analysis

Malware infestation

Computer has been manually infected with the HermeticWiper with all antivirus software turned off by running an executable with name "a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e" provided in the archive downloaded from MalwareBazaar. System did not trigger any warnings or error messages on initial infestation.

Manual Removal

Step 1: Disconnect from the Internet. The first thing to do during manual removal was to isolate the environment and disable all internet connection as the malware could spread itself to the other devices through the open connections.

Step 2: Identify and Terminate/Suspend all Malicious Processes. In order to identify any malicious processes, I opened the Task Manager and started investigating for any

suspicious activity. The very obvious thing that caught my attention was service with the same exact name as malware executable — “a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e”. The process did not consume any considerable amount of RAM or CPU power.

Before I could do anything to this process or monitor its behaviour, the computer system has thrown a blue screen of death BSOD.

From this point manual malware removal deemed to be impossible, as upon system restart Windows 11 threw the message stating that PC did not start correctly.

As result it can be stated that manual removal was not a suitable approach in this situation, as time of action had been at the essence, but the system got damaged too dramatically before any action could have been taken in order to stop the malware.

Windows Defender

How Windows Defender protected the system from the "HermeticWiper" malware:

Detection: Windows Defender detects the "HermeticWiper" malware (a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e) on your system and alerts you with a pop-up message. Message:

- "Windows Defender has detected a threat on your system. Name: Trojan:Win32/HermeticWiper.A. Click here to review and take action.".

Quarantine: Windows Defender moves the detected malware to quarantine to prevent it from further harming your system. Message:

- "Windows Defender has moved Trojan:Win32/HermeticWiper.A to quarantine. Your device is now secure.".

Removal: Windows Defender removes the malware from your system, ensuring that it cannot cause any further damage. Message:

- "Windows Defender has successfully removed Trojan:Win32/HermeticWiper.A from your device. Your system is now safe and secure.".

Scanning and Cleaning: Windows Defender performs a full system scan and cleans any remaining traces of the malware to ensure that the system is completely free of any infections. Message:

- "Windows Defender has completed a full system scan and removed all traces of Trojan:Win32/HermeticWiper.A from your device. Your system is now clean and secure.".

Further investigation of the system and system reboot did not show any obvious damages dealt to the system. It can be stated, that Windows Defender has successfully taken the action before any significant irreversible damage was done to the system.

MalwareBytes antivirus

MalwareBytes Antivirus scans the system for malware. During the scan, it detects the "HermeticWiper" malware with the name "a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e".
Message:

- "MalwareBytes Antivirus has detected the presence of 'HermeticWiper' malware on your system with the name 'a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e'.".

MalwareBytes Antivirus quarantines the malware to prevent it from executing further and potentially causing more harm. Message:

- "MalwareBytes Antivirus has quarantined the 'HermeticWiper' malware to prevent it from executing further and causing damage to your system.".

MalwareBytes Antivirus proceeds to remove the malware from the system. Message:

- "MalwareBytes Antivirus has removed the 'HermeticWiper' malware from your system to ensure its safety.".

MalwareBytes Antivirus performs a follow-up scan to verify that the malware has been completely removed from the system. Message:

- "MalwareBytes Antivirus has completed a follow-up scan and confirms that your system is now free from 'HermeticWiper' malware.".

MalwareBytes Antivirus recommends the user to perform a full system scan to check for any remaining threats. Message:

- "We recommend performing a full system scan to ensure that there are no remaining threats that may have been missed during the previous scans.".

MalwareBytes Antivirus provides suggestions on how to avoid future malware infections. Message:

- "To prevent future malware infections, ensure that your system's antivirus software is always up-to-date and regularly perform system scans. Avoid downloading files or programs from untrusted sources and exercise caution when opening email attachments from unknown senders.".

Further system restart and scan did not notify about any threats, so it can be said that MalwareBytes worked successfully.

8.4 Creation of manual malware removal guide

Once the computer system has been infected with malware it is crucial to start acting as fast as possible in order to minimise the risks and possible malware spread. In terms of malware remediation speed also plays an important role, as certain malware types might have a destructive effect on the computer systems, which could completely render the computer inoperable. Keeping in mind that speed is at the essence, some malware might refer to using stealth techniques in order to gather as much personal information as possible, but the presence of such malware can be spotted and such malware may be removed from the system using the manual and automatic removal techniques.

In case of manual malware removal, there are number of steps which is necessary to take after the malware presence has been suspected in the system.

8.4.1 PC isolation

1. **Computer internet disconnect:** The first step in separating a computer from the internet is to disconnect the computer from the internet. You can accomplish this

by removing the Ethernet wire or disabling the Wi-Fi network. This will stop the infected computer from communicating with the internet in the future.

2. **Disable any network adapters:** To stop any illegal communication, it's crucial to disable any network adapters on the computer after disconnecting from the internet. Disabling any active network connections can be done by navigating to the Network and Sharing Center in the Control Panel.

3. **Block incoming and outgoing traffic:** Configure a firewall to block all incoming and outgoing traffic except for the necessary ports for your applications. By doing this, malware won't be able to communicate with its command and control (C&C) servers or propagate to other networked devices.

4. **Disable any remote access:** The next step is to disable any remote access to the infected computer. This can be achieved by disabling Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and any other remote access tools that might be installed.

5. **Disable Bluetooth and other connectivity options:** The malware can also spread via Bluetooth and other wireless connectivity options. Hence, it is important to disable these options until the system is cleaned.

6. **Disable printer and file sharing:** Disable any printer and file sharing to stop malware from infecting more networked devices. Disabling file and printer sharing in the Control Panel's Network and Sharing Center will accomplish this.

7. **Limit physical access to the infected computer:** Limit physical access to the infected computer to prevent any potential spread of malware through physical media such as USB drives or other removable media.

8.4.2 Reveal suspicious processes and registry entries

1. **Use Task Manager:** Task Manager is a built-in utility in Windows that can help you identify suspicious processes. To access it, right-click on the taskbar and select Task Manager. In the Processes tab, you can see all the running processes on the system. To find any suspicious process that uses an unusually great deal of resources, sort the list by CPU and memory usage. But in certain cases, CPU usage

may not be the indicator of malicious activity, as certain malware types were developed to be stealthy and remain unnoticed. By looking for process anomalies, such as a process running with an unusual parent process or a process running from an unusual location, we can identify potential malicious processes, it might be easier to detect malware processes.

2. **Use Process Explorer:** Process Explorer is a more advanced version of Task Manager that can help you identify hidden processes that may not show up in Task Manager. Download and run Process Explorer from the Microsoft website. In the Process Explorer window, click on View > Show Lower Pane and View > Lower Pane View > Handles to display any handles or DLLs associated with a process. This can help you identify suspicious processes that are trying to hide their activities. In addition, Process Explorer also has functionality which provides enormous help during malicious process identification:

    - **VirusTotal Integration:** Process Explorer has a built-in integration with VirusTotal, a free online service that analyses files and URLs for malware. This integration allows to quickly scan any suspicious files or processes and get a report on whether they are malicious or not.

    - **Signature Verification:** Process Explorer can verify the digital signatures of running processes to ensure they are valid and have not been tampered with. This feature can help identify malware that tries to masquerade as legitimate software by spoofing digital signatures.

    - **Malware Analysis:** Process Explorer can be used to gather data for malware analysis by capturing process memory, dumping executable files, and analysing network connections. This information can help identify the behaviour of the malware and how it communicates with its “Command and Control” servers.

3. **Use Autoruns:** This tool is essential for identifying and removing malware that has embedded itself in the system. Here's how you can use "Autoruns" to manually delete malware:

- Run "Autoruns" as an administrator, and click on the "Everything" tab to get a comprehensive view of all programs and services running on the system.
- Examine the list of entries in "Autoruns". Look for entries with suspicious names or locations that seem out of place. Malware often hides itself by using innocuous names and locations that mimic legitimate system files.
- Use the search function to find specific entries related to the malware. You can search by name, location, or any other attribute.
- Right-click on any suspicious entry and select "Jump to Entry" to quickly navigate to the location of the file or service. From there, you can take appropriate action, such as deleting the file or disabling the service.
- Be cautious when deleting files or disabling services. Make sure you have identified the malware correctly before taking any action. Deleting legitimate system files can cause serious issues with the system, so it's important to exercise caution.

4. **Check the Registry:** Malware often makes changes to the registry to persist on the system. Use Regedit to check the registry for any suspicious keys or values. Look for keys or values that are associated with the malware you are trying to remediate. Most important and relevant registry parts are:

   "Run" keys: Malware often adds its executable file to one of these keys to ensure it starts up automatically with the system. Navigate to the following registry keys:

   - “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”
   - “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”
   - “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce”

- “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce”

"Services" keys: Malware often creates a service to ensure it stays running even if the user closes the application Navigate to the following registry keys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services

"AppInit_DLLs" value: Malware often hijacks this value to load its malicious code during system startup. Navigate to the following registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs

Other suspicious keys: Malware can use various other registry keys to hide itself, so it's important to check other suspicious keys as well. Here are some examples:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

8.4.3 Malware removal

After malicious process and its registry entries have been successfully identified, it is time to work with malware removal:

1. **Delete all associated registry entries:** All registry entries associated with the malware must be deleted. This can be done using the Registry Editor by navigating to the appropriate registry keys and deleting them.

2. **Remove all associated files:** Once the process and registry entries have been removed, it is important to identify and delete all associated files. This may include executable files, DLLs, and other supporting files.

8.4.4 System overview and testing

After remediating all suspected traces of malware from the system it is crucial to test the results and confirm that no malware traces are left.

1. **Verify running processes and services:** Check the list of running processes and services using Task Manager and Services Manager, respectively. Ensure that no suspicious or unknown processes and services are running on the system. You can cross-check the list of processes with known good processes by using a tool like "Process Explorer" or "Autoruns".

2. **Review the event logs:** The event logs record all system events and can help identify any malicious activity. Check the Security, Application, and System logs for any suspicious events. Event logs can be accessed through the Event Viewer utility in Windows.

3. **Perform a network analysis:** Use network analysis tools to monitor incoming and outgoing network traffic to identify any unusual or suspicious activity. Network analysis tools like Wireshark can help detect any unauthorized network communication, such as command and control traffic.

In case malware traces have been found once again, it is crucial to repeat the steps of identification of all services and running processes in the system and conduct new manual malware removal case incorporating more thorough investigation.

9 Analysis of results

In the course of this investigation, there have been tested a number of removal techniques, including manual removal, removal with Windows Defender, and removal with Malwarebytes antivirus software.

Manual malware removal is possible, but it is significantly more complicated and time-consuming than using antivirus software or Windows Defender, according to one of the key findings of this study. Manual removal requires extensive knowledge of the inner workings of the operating system and the malware in question. In addition, it can take a considerable amount of time to identify and remove all the files, folders, and registry entries associated with the malware.

Using Windows Defender or Malwarebytes antivirus software, on the other hand, significantly simplifies the elimination process. Both of these tools have powerful malware detection and removal capabilities and can scan an entire system within minutes to detect and eliminate any malicious code.

It is important to note that manual malware removal can provide security professionals with valuable insight into how malware operates. By manually analysing and removing malware, SOC analysts can gain a deeper understanding of the attackers' tactics, techniques, and procedures. This information can then be applied to the development of more efficient malware detection and prevention strategies.

It should be noted, however, that manual malware removal may not always be the most effective method, especially when the malware is particularly sophisticated or destructive. Some malware may be designed to rapidly spread and cause damage once it is installed on a system, meaning that the time required to manually identify and remove it could result in significant system or network damage.

In certain circumstances, manual malware removal may be the only viable option, especially if the malware has not yet been identified by antivirus software. In such situations, a thorough manual analysis of the system is required to identify and remove the malware.

Considering the increasing sophistication of modern malware, Windows Defender or Malwarebytes antivirus software is the more practical and effective option for the majority of users. However, manual removal may be the only viable option when a sophisticated and unknown malware strain has infected the system.

10 Summary

In the first section of the thesis, the literature on malware removal and remediation is reviewed. The author examines the different Windows OS applications, including those for personal computers, businesses, healthcare, government, entertainment, and the Internet of Things. The literature review emphasizes the significance of malware removal in the modern world due to the proliferation of malware attacks.

The second section of the thesis examines the structure of the Windows 11 operating system. The author discusses the kernel, user interface, file system, registry, services, and security features of the operating system, such as virus and threat protection and safe mode.

The third section of the thesis investigates malware classification by effect. Based on their impact, the author classifies malware into various categories, including anti-removal and stealth techniques, data collection, data destruction, and data manipulation. In this section, the author provides a comprehensive analysis of each impact category and the techniques employed by malware to avoid detection and removal.

In the fourth section of the thesis, malware analysis methods are discussed. The author investigates static analysis, dynamic analysis, and sandboxing, as well as virtual machines and online sandboxing environments. The author provides a comprehensive analysis of each malware analysis method and its efficacy in detecting and removing malware.

The fifth and final section of the thesis discusses techniques for removing malware. The author assesses the efficacy of removal tools such as antivirus software, Windows Defender, Autoruns, and Process Explorer. In addition, the author examines the manual removal procedure, which includes isolation, process and registry analysis, malware removal, system overview and testing.

In the thesis's practical section, the author creates a sandbox environment for collecting and analysing malware samples. The author collects and analyses two malware samples, Agent.Tesla and HermeticWiper, to determine the efficacy of removal methods. The author tests the manual removal method and incorporates all the techniques discussed in the theoretical section of the thesis into a comprehensive guide for manually removing malware.

In conclusion, the author analyses the results and summarizes the findings. Manual removal in conjunction with removal tools such as Windows Defender and Malwarebytes Antivirus can be an effective method for removing malware from Microsoft Windows 11. Additionally, the author emphasizes the significance of routine malware analysis and remediation as a safeguard against malware attacks.

All information gathered during the literature review and tests has been used to create a guide for manual malware removal from the Windows 11 operating system. The guide includes all steps required to remove the malware.

In conclusion, the thesis provides an in-depth analysis of malware removal techniques for the Windows 11 operating system. The author reviews the literature on malware removal and remediation, discusses the structure of the Windows 11 operating system, examines malware specification by impact, analyses malware analysis methods, and evaluates malware removal techniques. In the practical portion of the thesis, a comprehensive manual malware removal guide is created. The thesis offers insightful perspectives on the significance of malware analysis and remediation for protecting against malware attacks in the modern era.

References

[1] A. Bettany and M. Halsey, Windows Virus and Malware Troubleshooting, -: Apress L. P., 2017.

[2] K. Bo-Young and S.-K. Yoo, “The Effective Factors of Cloud Computing Adoption Success in Organization,” *Journal of Asian Finance Economics and Business*, vol. VI, pp. 217-229, 2019.

[3] AFP, "Chinese Government Hackers Steal Trove of U.S. Navy Data: Report," AFP, 8 June 2018. [Online]. Available: https://www.securityweek.com/chinese-government-hackers-steal-trove-us-navy-data-report/. [Accessed 14 March 2023].

[4] StatCounter, "Operating System Market Share Worldwide," StatCounter , 1 March 2023. [Online]. Available: https://gs.statcounter.com/os-market-share#monthly-202111-202303. [Accessed 13 March 2023].

[5] Microsoft, “Windows 11 Enterprise,” Microsoft, July 2022. [Online]. Available: https://www.microsoft.com/en-us/microsoft-365/windows/windows-11-enterprise. [Accessed 10 March 2023].

[6] Microsoft, “Windows 11 for Education,” Microsoft, 2023. [Online]. Available: https://www.microsoft.com/en-us/education/products/windows. [Accessed 10 March 2023].

[7] Microsoft, "Microsoft Cloud for Healthcare," Microsoft, 2023. [Online]. Available: https://www.microsoft.com/en-us/industry/health/microsoft-cloud-for-healthcare. [Accessed 10 March 2023].

[8] Microsoft, "Government discount through the Microsoft Workplace Discount Program," Microsoft, 22 March 2023. [Online]. Available: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/office-365-us-government. [Accessed 3 April 2023].

[9] J. Laukkonen, "Is Windows 11 Good For Gaming?," Lifewire, 15 March 2023. [Online]. Available: https://www.lifewire.com/is-windows-11-good-for-gaming-7153341. [Accessed 3 April 2023].

[10] Microsoft, “Getting Started with Windows IoT Enterprise,” Microsoft, 25 October 2022. [Online]. Available: https://learn.microsoft.com/en-us/windows/iot/iot-enterprise/getting_started. [Accessed 3 April 2023].

[11] I. OpenMetal, "Machine Learning and Operating Systems," OpenMetal, Inc, 2023. [Online]. Available: https://openmetal.io/docs/product-guides/private-cloud/machine-learning-and-operating-systems/. [Accessed 13 March 2023].

[12] I. Mobility, "Everything You Wanted to Know About Types of Operating Systems in Autonomous Vehicles," Intellias Mobility, 15 May 2019. [Online]. Available: https://intellias.com/everything-you-wanted-to-know-about-types-of-operating-systems-in-autonomous-vehicles/. [Accessed 13 March 2023].

[13] Microsoft, "Windows 11 overview," Microsoft, 27 February 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows/whats-new/windows-11-overview. [Accessed 13 March 2023].

[14] TechRepublic Staff , "Windows 11 cheat sheet: Everything you need to know," TechRepublic, 2 June 2022. [Online]. Available: https://www.techrepublic.com/article/windows-11-cheat-sheet-everything-you-need-to-know/. [Accessed 13 March 2023].

[15] A. Mahajan, D. Pahuja and A. Verma, "Architecture of Windows NT Operating System," *International Journal for Research in Applied Science & Engineering,* vol. II, no. 10, 2014.

[16] Microsoft, "Windows Shell," Microsoft, 5 January 2021. [Online]. Available: https://learn.microsoft.com/en-us/windows/win32/shell/shell-entry. [Accessed 17 March 2023].

[17] Microsoft, "NTFS Overview," Microsoft , 24 March 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview. [Accessed 4 April 2023].

[18] B. Branch, "Review NTFS Basics," *Australian Journal of Basic and Applied Sciences,* pp. 325-338, 2021.

[19] T. Fisher, "What Is the Windows Registry?," Lifewire, 19 April 2022. [Online]. Available: https://www.lifewire.com/windows-registry-2625992. [Accessed 4 April 2023].

[20] Microsoft, "Windows registry information for advanced users," Microsoft, 9 March 2023. [Online]. Available: https://learn.microsoft.com/en-US/troubleshoot/windows-server/performance/windows-registry-advanced-users. [Accessed 4 April 2023].

[21] T. Fisher, "What Is a Windows Service?," Lifewire, 8 August 2022. [Online]. Available: https://www.lifewire.com/what-is-a-service-4107276. [Accessed 4 April 2023].

[22] Microsoft, "Introduction to Windows Service Applications," Microsoft, 15 September 2021. [Online]. Available: https://learn.microsoft.com/en-us/dotnet/framework/windows-services/introduction-to-windows-service-applications. [Accessed 5 April 2023].

[23] C. Panek, "Understanding Services," in *Windows Operating System Fundamentals*, John Wiley & Sons, Incorporated, 2019, pp. 181-189.

[24] Microsoft, Windows 11 Security Book: Powerful security from chip to cloud, Microsoft, 2022.

[25] C. Merriman, "How to boot Windows 11 in Safe Mode," 1 December 2021. [Online]. Available: https://www.itpro.com/operating-systems/microsoft-windows/361662/how-to-boot-windows-11-in-safe-mode. [Accessed 16 March 2023].

[26] Y. Miao, "What Can We Learn from Anti-malware Naming Conventions?," OPSWAT, Inc, 6 November 2015. [Online]. Available: https://www.opswat.com/blog/what-can-we-learn-anti-malware-naming-conventions. [Accessed 13 March 2023].

[27] O. Kubovič, "RANSOMWARE: A look at the criminal art of malicious code, pressure, and manipulation," 2021.

[28] M. Barr, "Introduction to Watchdog Timers," 1 October 2001. [Online]. Available: https://www.embedded.com/introduction-to-watchdog-timers/. [Accessed 6 April 2023].

[29] Splunk Threat Research Team, "From Registry With Love: Malware Registry Abuses," 19 January 2023. [Online]. Available: https://www.splunk.com/en_us/blog/security/from-registry-with-love-malware-registry-abuses.html. [Accessed 6 April 2023].

[30] A. Rothman, "Windows Registry attacks: Knowledge is the best defense," 7 June 2022. [Online]. Available: https://redcanary.com/blog/windows-registry-attacks-threat-detection/. [Accessed 6 April 2023].

[31] S. Sengupta, "Code Injection – Examples and Prevention," 18 Oct 2021. [Online]. Available: https://crashtest-security.com/code-injection/. [Accessed 6 April 2023].

[32] E. Metula, Managed Code Rootkits : Hooking into Runtime Environments, Elsevier Science & Technology Books, 2010.

[33] The MITRE Corporation, "Collection," The MITRE Corporation, 19 July 2019. [Online]. Available: https://attack.mitre.org/tactics/TA0009/. [Accessed 5 April 2023].

[34] D. Javeed, U. MohammedBadamasi, C. O. Ndubuisi, F. Soomro and M. Asif, "Man in the Middle Attacks: Analysis, Motivation and Prevention," *International Journal of Computer Networks and Communications Security* , vol. 8, no. 7, pp. 52-58, 2020.

[35] E. Ylli and J. Fejzaj, "Man in the Middle: Attack and Protection," May 2021. [Online]. Available: https://ceur-ws.org/Vol-2872/short08.pdf. [Accessed 6 April 2023].

[36] Dominion Cyber LLC, "T1056: Input Capture," 2021. [Online]. Available: https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/credential-access/t1056-input-capture. [Accessed 8 April 2023].

[37] E. Brent Murphy, E. David French, M. Prasad Somasamudram, M. Sekhar Sarukkai, M. Syed Ummar Farooqh and V. T. Labs, "Data Destruction," 25 March 2021 . [Online]. Available: https://attack.mitre.org/techniques/T1485/. [Accessed 9 April 2023].

[38] L. Brooke, "Data Manipulation Attacks And How To Counter Them," [Online]. Available: https://www.uscybersecurity.net/data-manipulation-attacks/. [Accessed 9 April 2023].

[39] FireEye, Inc, "APT38: UN-USUAL SUSPECTS," Milpitas, 2018.

[40] D. Tobin and M. J. Stone, "DATA INTEGRITY: Recovering from a destructive malware attack," 2016.

[41] R. A. Nettles, C. Merulla and S. Warzala, "Data Manipulation: Attacks and Mitigation," 23 May 2019. [Online]. Available: https://csiac.org/articles/data-manipulation-attacks-and-mitigation/. [Accessed 9 April 2023].

[42] A. H. Michael Sikorski, Practical Malware Analysis : A Hands-On Guide to Dissecting Malicious Software, No Starch Press, Incorporated, 2012.

[43] M. K. A, Learning Malware Analysis, Bermingham: Packt Publishing Ltd, 2018.

[44] A. Mohanta, K. Velmurugan and M. Hahad, Preventing Ransomware : Understand, Prevent, and Remediate Ransomware Attacks, Birmingham: Packt Publishing, Limited, 2018.

[45] S. Ingalls, "Sandboxing: Advanced Malware Analysis," 23 April 2021. [Online]. Available: https://www.esecurityplanet.com/endpoint/sandboxing-advanced-malware-analysis/. [Accessed 11 April 2023].

[46] O. a. i. affiliates, "User Manual," 2023. [Online]. Available: https://www.virtualbox.org/manual/UserManual.html. [Accessed 12 April 2023].

[47] Microsoft, "Introduction to Hyper-V on Windows 10," 26 April 2022. [Online]. Available: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. [Accessed 12 Arpil 2023].

[48] Any.Run, "How can we help?," Any.Run, [Online]. Available: https://app.any.run/docs. [Accessed 11 April 2023].

[49] J. Koret and E. Bachaalany, The Antivirus Hacker's Handbook, Indianapolis: John Wiley & Sons, Inc., 2015.

[50] A. Sha, "8 Best Malware Removal Tools for Windows 11 (Free and Paid)," 21 January 2022. [Online]. Available: https://beebom.com/best-malware-removal-tools-windows-11/. [Accessed 13 April 2023].

[51] J. v. Bleichert, "Kaspersky Antivirus Review 2023: How Good Is It?," 6 March 2023. [Online]. Available: https://www.experte.com/antivirus/kaspersky. [Accessed 13 April 2023].

[52] A. Tomkevičiūtė, "Microsoft Defender antivirus review," 21 March 2023. [Online]. Available: https://cybernews.com/best-antivirus-software/microsoft-defender-review/. [Accessed 13 April 2023].

[53] S. Newby, "Microsoft Defender for Endpoint," 7 February 2023. [Online]. Available: https://www.microsoftpartnercommunity.com/atvwr79957/attachments/atvwr79957/UK_Area_db/396/4/Microsoft%20Defender%20for%20Endpoint%20Overview.pdf. [Accessed 13 April 2023].

[54] Microsoft, "Autoruns for Windows v14.09," 17 February 2022. [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns. [Accessed 11 April 2023].

[55] A. K. Mishra, "Process Explorer is the Best Version of Task Manager in Windows 11," 10 January 2023. [Online]. Available: https://www.anoopcnair.com/process-explorer-task-manager-in-windows-11/. [Accessed 11 April 2023].

[56] M. Russinovich, "Process Explorer v17.04," 3 April 2023. [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer. [Accessed 11 April 2023].

[57] V. K. Tiwari and D. Rajeeva, "Analysis of Cyber Attack Vectors," 2016.

[58] Virustotal, "How it works," Virustotal, [Online]. Available: https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works. [Accessed 11 April 2023].

[59] H. Analysis, "Frequently Asked Questions (FAQ)," Hybrid Analysis, [Online]. Available: https://www.hybrid-analysis.com/faq. [Accessed 11 April 2023].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Arseni Sergeev

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Investigating the Effectiveness of Various Methods for Malware Removal and Remediation on Windows 11 Systems”, supervised by Toomas Lepik
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

15.05.2023

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.