Aleksanteri Numminen

WINDOWS TECHNICAL HARDENING AGAINST THE MOST PREVALENT THREATS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

ABSTRACT

Numminen, Aleksanteri
Windows technical hardening against the most prevalent threats
Jyväskylä: University of Jyväskylä, 2023, 61 pp.
Cyber Security, Master's Thesis
Supervisor(s): Hämäläinen, Timo

This thesis identified the most essential hardening measures in Windows to combat the current most prevalent threats. The goal was set to identify the tactics used by the current most prevalent threats and to identify the suitable security controls in Windows to answer these threats. The research questions were set to "What are the tactics used by the current most prevalent threats?" and "What are the most important security controls that should be hardened in Windows to be protected against the most prevalent threats?"

The research method in this thesis is constructive, where the identified problem is that organizations do not know on which Windows security features to focus their resources. The outcome of the research is to figure out a list of the most important security mechanisms in Windows that an organization should focus on to be protected against the most prevalent threats. A widely known and used framework MITRE ATT&CK Enterprise matrix was used for the research. The framework contains the techniques used by known threat actors and tactics, which are the categories for the techniques. MITRE ATT&CK was examined closer in its own chapter.

Three current threat landscape reports were chosen for the analysis of tactics used by the current most prevalent threats. The MITRE ATT&CK tactics were identified from those reports. Six of the tactics, Initial Access, Execution, Credential Access, Lateral Movement, Command and Control, and Impact, were selected for further analysis as they were referenced by all the reports. Windows technical hardening was also examined in its own chapter to form an understanding of the available Windows security features.

The six most used tactics most used by threat actors were examined closer in the actual content chapter, where each technique within those tactics were examined. The attempt was to find suitable security features in Windows to mitigate each of the techniques. As an outcome, five security features were identified that covered the largest number of MITRE ATT&CK techniques. They were Windows Firewall, Windows Defender antivirus, application allowlisting using AppLocker or Windows Defender Application Control, access control and user rights, and Attack Surface Reduction rules.

Keywords: most prevalent cyber threats, Windows, hardening, security features

TIIVISTELMÄ

Numminen, Aleksanteri
Windowsin tekninen koventaminen kaikkein yleisimpiä uhkia vastaan
Jyväskylä: Jyväskylän yliopisto, 2023, 61 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Hämäläinen, Timo

Tutkielmassa selvitettiin tärkeimpiä Windowsin suojausmenetelmiä kaikkein yleisimpiä kyberuhkia vastaan. Tavoitteena oli tunnistaa tämän hetken tärkeimmät ja yleisimmät kyberuhat ja löytää sopivat Windowsin tietoturvakontrollit vastaamaan näihin uhkiin. Tutkimuskysymyksiksi asetettiin "Mitä ovat tämän hetken yleisimmät kyberuhkien käyttämät taktiikat?" ja "Mitä ovat tärkeimmät tietoturvakontrollit Windowsissa yleisimpiä uhkia vastaan suojautuessa?".

Tutkimus toteutettiin konstruktiivisena tutkimuksena. Tutkimuksen ongelma on se, että organisaatiot eivät tiedä, mihin Windowsin suojausmekanismeihin tulisi keskittää resurssit. Lopputuloksena konstruktiivisella tutkimuksella on kehittää lista suojausmekanismeista, joihin resurssit tulisi keskittää suojautuakseen yleisimmiltä kyberuhilta. Viitekehyksenä tutkielmassa käytettiin laajalti käytettyä ja tunnettua MITRE ATT&CK Enterprise matriisia, joka sisältää kattavan listan kyberuhkatoimijoiden käyttämistä tekniikoista ja tekniikoiden yläkategorioista eli taktiikoista. MITRE ATT&CK viitekehys käytiin läpi syvällisemmin omassa teorialuvussaan.

Tämän hetken yleisempien uhkien analyysissä valittiin kolme tunnettua viime aikoina laadittua raporttia tämän hetken kyberuhkakuvista. Raporteista pystyttiin tunnistamaan yleisimmin käytetyt MITRE ATT&CK taktiikat, joista yhteensä kuuteen kaikki raportit viittasivat: Initial Access, Execution, Credential Access, Lateral Movement, Command and Control ja Impact. Nämä kuusi valittiin jatkoanalyysiin. Myös Windowsin tekninen tietoturva käytiin läpi omana lukunaan, jonka perusteella pystyttiin valita sopivia tietoturvakontrolleja.

Kuutta yleisimmin käytettyä taktiikkaa käytiin läpi tekniikoidensa puolesta sisältöluvussa. Jokaiselle tekniikalle pyrittiin löytämään sopiva tietoturvakontrolli Windowsissa. Tutkimuksen lopputuloksena tärkeimmät tietoturvaominaisuudet, jotka kattavat mahdollisimman monta tekniikkaa valituista taktiikoista, ovat Windowsin palomuuri, Windows Defender virustorjunta, sovellusten suorituksen rajoittaminen AppLocker tai Windows Defender Application Control -ominaisuuksilla, käyttöoikeuksien rajaaminen ja Attack Surface Reduction -säännöstö.

Asiasanat: yleisimmät kyberuhat, Windows, koventaminen, tietoturvaominaisuudet

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Windows is a mature operating system that has evolved over the years since its infancy in 1985. The latest iterations of the operating system, Windows 10, and Windows 11 are very complex in nature. Consisting of countless features and millions of lines of code, the operating system has a large potential attack surface (Cusumano, 2006).

Cyber threat actors take advantage of the operating system's attack surface. They use many techniques to achieve their goals in the victim's network. This includes using a lot of the features and the vulnerable nature of the Windows operating system (OS): its design philosophy is to be as compatible as possible to ensure software designed for other versions of Windows work on it too (Joh, 2019). Mitre Corporation's (2023a) Common Vulnerabilities and Exposures (CVE) Glossary defines vulnerability as "a flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components". Confidentiality, integrity, and availability (CIA) is a basic concept of information security (Samonas & Coss, 2014). Together those three aspects form the CIA triad, a basis for information security.

To prevent negative impact to one of the components of CIA triad, it is essential for an organization such as companies, banks or states to implement security controls and mechanisms on their Windows endpoints. The process has a known term in the field of cyber security: hardening. Hardening as a term in this context refers to changing the configuration of a system to be more secure. However, as many organizations do not have the resources to delve deep into Windows hardening themselves, they may not implement the best protection against the most common current threats in their efforts to secure their own network.

There are a lot of different threats and a lot of different options to consider regarding the available Windows security mechanisms. This thesis aims to identify the most important mechanisms or hardening mechanisms that an organization should focus on. To do such ranking, this thesis examines what are most prevalent threats in the current threat landscape. After exploring the current threats, the available Windows technical hardening measures are examined. The comparison of the two subjects, the most prevalent threats and the available Windows security hardening measures, is made in the content chapter, where the applicable security measures are identified. The goal is to create a list of the most important security controls that an organization should focus on when securing their Windows environment. Only investigating what are the most important controls or settings to implement, an organization can put its efforts in protecting itself at least from the most prevalent threats.

There is limited academic research available regarding what are the main security controls of the Windows operating system that can or should be implemented. Kim K. et al (2008) have written about a tool called PCChecker that performed checks on the security configuration of Windows. The authors highlighted the importance of Windows security configuration in addition to patching, antivirus, and anti-spyware products. Oosthoek & Doerr (2019) also reference what MITRE ATT&CK techniques and trends are there in Windows malware. The research is focused only on malicious software running on the operating system and does not include other threats. There is also research about how security configuration guides such as Microsoft Security Baseline can be automatically applied (Stöckle et al., 2021). Outside academic research, there are books like ”Mastering Windows Security and Hardening” written by Mark Dunkerley and Matt Tumbarello in 2020. Some researchers have focused on hardening specific features and measuring how the successfulness of an attack vector is affected by the change (Durve & Bouridane, 2017). There are also many published guides about how an organization should focus on improving their security in general such as the ISO 27001 standard and NIST Special Publications like SP800-53 (NIST, 2020). None of the explored research considers the protections in Windows against the current, most common threats.

This research paper has been divided to seven different chapters. First, this introductory chapter introduces the motivation and background for the subject, the research questions and methods. The second chapter introduces the main framework for this thesis: the MITRE ATT&CK. The third and the fourth chapter present the theoretical background for this research: the most prevalent threats and Windows hardening as a subject. Both subjects are studied so that the Windows hardening methods could be mapped properly against the identified threats in the current threat landscape. The fourth chapter includes the main concept of this research paper: how the most prevalent threats can be mitigated with Windows security features. The chapter uses the MITRE ATT&CK as a framework to find out the most relevant hardening measures against the known tactics, techniques, and procedures (TTPs) used by the identified most relevant threats. After the main research chapter that includes the results as well, there is a chapter for discussion. The chapter discusses the potential gravity of the findings and introduces ideas that can be used for additional research on the matter. The conclusion chapter is the final chapter, which has a summary of this research.

1.1 Research questions

The main objective of this research is to identify the main security controls that can be configured in the Windows operating system to combat the most prevalent threats. The importance of the security controls is determined by their relevance in the current cyber security threat landscape. The research questions were formed based on the main objective. First, the most current prevalent threats against Windows are determined. Using the knowledge from the threats, the most important security controls can be identified that can help in preventing those threats. The research questions are as follows.

- What are the tactics used by the current most prevalent threats?
- What are the most important security controls that should be hardened in Windows to be protected against the most prevalent threats?

1.2 Research methods and scoping

The research method for the thesis is constructive because this thesis aims to solve a real-life problem by developing something new like a model or framework. Kasanen et al. (1993) discuss that the method is often used in technical sciences, mathematics, clinical medicine and originally in management accounting research. Kasanen et al. (1993) divide the process of constructive research into the following seven activities:

1. Find a relevant problem that has potential theoretical contribution.
2. Find if long term research collaboration is possible with the target organization.
3. Get a deep understanding of the research area both theoretically and practically.
4. Innovate a solution and develop a construct that could also have theoretical contribution.
5. Implement a solution and test that it is valid.
6. Consider where the solution could be applied.

The first activity in constructive research is finding the relevant problem (Kasanen et al., 1993). The problem in this thesis is that organizations do not know what security mechanisms they should prioritize when they are in the process of hardening Windows. The second activity, defined by Kasanen (1993), in constructive research is the research made in this master's thesis. The third activity, a deep understanding of the research area, is explored in chapters 2, 3 and 4. In those chapters, both the theoretical background and the framework for the study is being introduced. As the fourth activity, the solution to the problem is being innovated by trying to identify the most important security mechanisms against the most prevalent threats in the chapter 5. Activity five, implementing and testing are not part of this research, but activity six is because the application of the solution is discussed in the discussion chapter of this research.

This thesis focuses on Windows, as it has a market share of about 70 % on the desktop operating systems (StatCounter, 2023a). On Windows, the focus is on the most relevant and used operating systems, Windows 10 and Windows 11. They represent the majority of the market share of Windows operating systems: they have a market share of about 95 % representation combined (73,46 % + 20,95 %) (StatCounter, 2023b).

The focus of the thesis is only on the use of Windows in the business as home users' operating systems are limited in the configuration point of view due to licensing. This is because Microsoft (2023a) publishes different versions of Windows aimed for different purposes. For example, Windows 10 Home, which is offered for consumers, does not have features such as Group Policy Management or AppLocker that are offered in the business versions Pro, Education and Enterprise. Windows Home version is missing many configuration options and capabilities that are assumed to be available in this research (Microsoft, 2023a).

Second factor in limiting the scope to only business users is that home users' threat landscape is relatively different compared to the business one (Xavier & Pati, 2012). This thesis focuses only on native Windows operating system with its built-in tools without the use of third-party tooling. With this limitation, the research outcome can be applied without dependencies to a third-party software such as an antivirus vendor. Only the local computer policies and protections are part of the scope, not the entire Windows domain network. This thesis does not include every single Windows hardening setting. Therefore, only the foundation of Windows security and the main security features are included as opposed to every single setting. An example of a single setting that is not included in the research is selecting the specific encryption types that the computer uses to communicate to other computers.

The effectiveness of the identified security controls is not tested in this thesis. The research is carried out by comparing different attack methods against a known framework, MITRE ATT&CK. It was chosen as a framework for this thesis to prioritize organization's defenses against the tactics used by the most relevant cyber threats as the framework is widely used in the cyber industry.

Sources for the literature review are collected from known libraries and related international journals such as IEEE Xplore and ACM Digital Library. To search for related research, Google Scholar, and University of Jyväskylä's JYK-DOK library are used. In addition, internet sources are searched using Google Search. One of the most important sources of information has been Microsoft documentation as it is the vendor of the Windows operating system.

Multiple different terms were used to search for previous research on the matter. The terms that were use included "Windows technical hardening", "Windows security mechanisms", "MITRE ATT&CK", "MITRE ATT&CK technical hardening Windows", "the most [current/relevant/important] threats" and "threat landscape reports". In addition, similar search terms were used to delve deeper into certain subjects.

2 MITRE ATT&CK FRAMEWORK

To better understand cyber adversary behavior, a framework introduced by Mitre Corporation (2022a) called MITRE ATT&CK was chosen to help with understanding and matching different adversary behavior and mitigations related to the identified behavior. MITRE ATT&CK Framework is a widely used collection of different tactics, techniques, and procedures (TTP) used by known threat actors. The framework was developed by Mitre Corporation in 2013 to represent the different stages of a cyber-attack lifecycle used by known threat actors (Mitre Corporation, 2022a).

Mitre Corporation (2023b), the developer behind MITRE ATT&CK, the introduces itself as a non-profit organization that was founded originally by the United States Air Force. Today, Mitre Corporation operates federally funded research and development centers and has been involved in multiple important globally recognized projects like the SATIN that aimed to develop a unified system for managing the U.S. airspace.

MITRE ATT&CK has large knowledge base of different techniques. The framework organizes the techniques into tactics (categories), that provide the "why" as a context to a technique. The technique itself is "how" an actor tries to achieve the objective (tactic). An example of a tactic category is "Execution", and an example of a technique is executing commands using PowerShell (technique T1059). In addition to the organized approach, the ATT&CK framework provides information about threat actors that have reportedly used the technique and information about mitigation and detection methods related to that technique.

Today MITRE ATT&CK is widely used in the information security industry as the basis of categorizing alerts and identifying activity. The framework is an alternative to the widely known Cyber Kill Chain that was developed by Lockheed Martin (Lockheed Martin, 2023). It is notable that another model, the Unified Kill Chain has been developed based on MITRE ATT&CK and Cyber Kill Chain that extends the Cyber Kill Chain with the elements of MITRE ATT&CK and aims to include the objectives of a thread actor as part of the model (Pols, 2017).

Mitre Corporation (2022a) has published multiple different matrices of MITRE ATT&CK. In this thesis, the MITRE ATT&CK Matrix for Enterprise is used. In addition to the Enterprise matrix, other matrices are Cloud, Mobile and ICS. In the Enterprise matrix, only the tactics and techniques relevant for Windows is taken into consideration due to the nature of this thesis.

The latest version of the MITRE ATT&CK Framework published by Mitre Corporation (2023c) is version 13. Compared to the previous versions, the version 13 brings numerous changes. Released April 25, 2023, it introduced revised versions of many of the techniques and updates to threat actors, malicious software, and mitigations. The latest version consists of a total of 14 tactics, 196 techniques, 411 sub-techniques, 388 groups, 22 campaigns and 740 different pieces of software (Mitre Corporation, 2023c).

Mitre Corporation's (2022e) ATT&CK Enterprise Matrix consists of fourteen tactics that work as a category for the action that a threat actor is aiming to do. The techniques themselves refer to the actual technical action that the threat actor is attempting to do. For example, "Execution" tactic has a technique T1059 "Command and Scripting Interpreter" which includes a sub-technique T1059.001 "PowerShell". As an example, one could say related to an incident that a threat actor attempted to execute some sort of malicious payload using PowerShell as the Windows native command interpreter. All current fourteen tactics and their explanations according to the MITRE Corporation have been described in Table 1.

Table 1 MITRE ATT&CK Framework's all fourteen tactics with descriptions (Mitre Corporation, 2022b)

Name	**Description**
Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
Resource Development	The adversary is trying to establish resources they can use to support operations.
Initial Access	The adversary is trying to get into your network.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Defense Evasion	The adversary is trying to avoid being detected.
Credential Access	The adversary is trying to steal account names and passwords.
Discovery	The adversary is trying to figure out your environment.
Lateral Movement	The adversary is trying to move through your environment.

Collection	The adversary is trying to gather data of interest to their goal.
Command and Control	The adversary is trying to communicate with compromised systems to control them.
Exfiltration	The adversary is trying to steal data.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

3 THE MOST PREVALENT THREATS

According to ENISA (2022), cybersecurity actors can be divided into four differently motivated groups: state-sponsored actors, cybercrime actors, hacker-for-hire actors and hacktivists. As the interest of all the groups change, so do the trends in the current threat landscape. The threats that were relevant five to ten years ago, may not be relevant anymore.

Threat landscape reports are used to understand the most current threats. Threat landscape reports are an organization's view on the past year's observed threats. There many both public and private organizations that release the threat landscape reports. The reports often also predict what is to come soon.

Three reports are chosen for further inspection. The threat landscape reports from different organizations have similar analysis of the current cyber threats, which is why it wouldn't be too beneficial to go through all of them. This research will include the results from reports made by the European Union Agency for Cybersecurity (ENISA), Cisco Systems Incorporated and Red Canary.

The European Union Agency for Cybersecurity, ENISA (2022) releases a report called ENISA Threat Landscape (ETL). The 2022 version of the report identifies top threats, current trends, threat actors and the attack techniques that they used. In addition, the report includes motivation and impact analysis. The latest ENISA (2022) annual threat landscape report released in November 2022 lists the following eight items as the top current threats.

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: denial of service
6. Threats against availability: internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

In addition to the general list, the report also includes a summary of the tactics used categorized by MITRE ATT&CK framework. The tactics are listed in table 2 with the number of techniques that were found related to those respective tactics. The attachment 1 includes the original ENISA threat landscape reports observations of the relevant Windows techniques.

Table 2 The tactics mentioned in the ENISA (2022) threat landscape report.

Tactic	Count
Initial Access	16
Execution	5
Persistence	5
Privilege Escalation	3
Defense Evasion	13
Credential Access	2
Discovery	12
Lateral Movement	2
Collection	11
Command and Control	6
Exfiltration	9
Impact	16

Cisco Systems Incorporated (2021) lists the most common security threats in its own threat landscape report called "Cyber security threat trends". According to Cisco (2021), the most current threats are cryptocurrency mining, phishing, trojans and ransomware. Other threats include droppers, botnet, adware, RAT (Remote Access Trojan), APT (Advanced Persistent Threat), browser hijacking, spam, information stealing, exploit kits, loaders, potentially unwanted applications, scareware and malvertising (malicious advertising) (Cisco Systems Incorporated, 2021).

Unfortunately, Cisco Systems Incorporated report does not include a summary of the identified MITRE ATT&CK tactics or techniques. However, based on the nature of the techniques used in the threats, the relevant MITRE ATT&CK tactics can be identified. The first identified tactic, Initial Access, is needed to get the first initial foothold through phishing or using vulnerabilities. Then, Cisco (2021) report mentioned different executables like droppers that are closely connected to Execution. To conduct information stealing or to deploy ransomware, stealing credentials is a technique that is related to those threats. It belongs in the Credential Access tactic. The Lateral Movement, Exfiltration and Impact tactics are present in those threats as well. In addition, Command and Control is an important tactic in threats such as botnet and RAT. The identified tactics are presented in table 3.

Table 3 The tactics that were identified in Cisco's (2021) threat report.

Tactic
Initial Access

Execution
Credential Access
Lateral Movement
Command and Control
Exfiltration
Impact

Red Canary Incorporated (2023) has published their recent Threat Detection Report in 2023. It shows that the current most prevalent cyber threats include ransomware, different initial access vectors, command and control (C2) frameworks, email threats, information stealers, identity attacks and adversary emulation and testing. The report also manages to name the most prevalent MITRE ATT&CK techniques according to their data. The techniques are displayed in table 4. In addition to the ones listed in the table, Red Canary names multiple additional observed techniques from Defense Evasion, Lateral Movement and Credential Access tactics. Impact and Initial Access are also identified because they are closely related to the different initial access vectors and ransomware (Red Canary, 2023).

Table 4 Red Canary (2023) report's most prevalent techniques and tactics

Rank	**Technique**	**Tactic**
1	T1059.003 Windows Command Shell	Execution
2	T1059.001 PowerShell	Execution
3	T1047 Windows Management Instrumentation	Execution
4	T1028 Obfuscated Files or Information	Defense Evasion
5	T1218.011 Rundll32	Defense Evasion
6	T1105 Ingress Tool Transfer	Command and Control
7	T1055 Process Injection	Defense Evasion
8	T1569.002 Service Execution	Execution
9	T1036.003 Rename System Utilities	Defense Evasion
10	T1003.001 LSASS Memory	Credential Access

A lot of similarities are found in the threat reports. All of them list ransomware, execution of malicious software and phishing threats. Lateral Movement, Command and Control and some sort of Impact were present in the reports at least in the form of ransomware. Most of the techniques presented in all three reports are focused on the cyber adversary gaining the first foothold on the target (Initial Access) and running malicious payloads (Execution). The MITRE ATT&CK tactics mentioned in the threat reports can be seen in Figure 1.

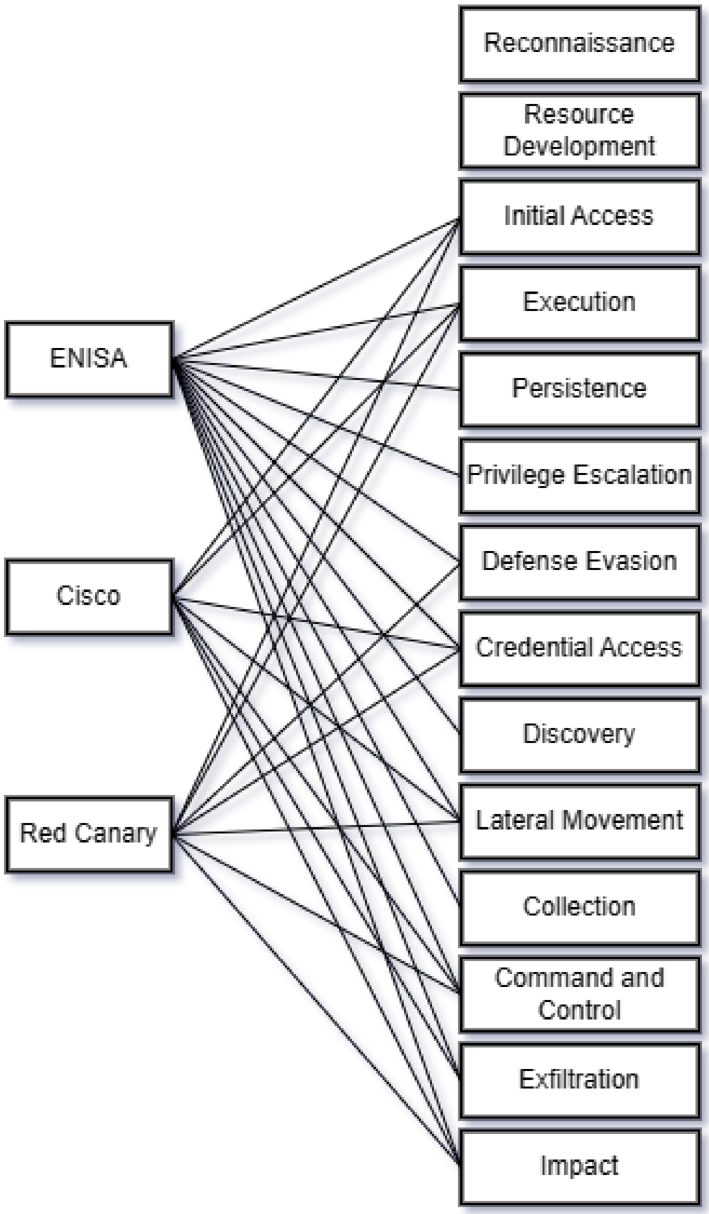

Figure 1 The MITRE ATT&CK tactics found in the three threat reports.

As seen in the figure 1, all the reports mentioned some of the tactics. Those tactics can be identified as the most important tactics for this research. In summary, the tactics in the following list are found to be the most prevalent ones based on the three chosen threat reports.

- Initial Access
- Execution
- Credential Access
- Lateral Movement
- Command and Control
- Impact

4 WINDOWS TECHNICAL HARDENING MEASURES

The many hardening measures of the Windows operating system have evolved as the product has matured (Berghel, 2017). The latest iteration of the operating system, Windows 10 and Windows 11 have advanced security with many different features. Despite the fact Windows security has been developed to be secure by default in recent years (Lipner & Howard, 2023), the operating system still needs configuration to make it more secure to use. There are a lot of methods for configuring Windows, including but not limited to Group Policy, Intune, registry, scripts and other command-line tools. However, the way of configuring is not in the scope of this research.

The following chapter introduces the foundation of security in Windows, its modern security model, how it was developed to be secure in the first place and how important aspect high privileges are in the operating system. The next two chapters explain how the security has advanced in both latest versions of the operating system, Windows 10 and Windows 11. Then, security baselines, the security configuration templates provided by multiple vendors are introduced in their own chapter. Finally, the various security features and capabilities of Windows are explored in the many different security levels of the operating system.

Windows operating system's security mechanisms have been divided into the following categories for this research. There is limited categorization available for the features. The chosen categorization model has been used by Microsoft in their documentation (Microsoft, 2023b).

- Hardware security
- Authentication and access control
- Operating system security
- Malware protection
- Application security

4.1 Windows security foundation

Ramasamy et al. (2019) present that Windows security, like other types of security, works in layers. For the operating system and the applications on top of it to be secure, the more down-level layers are to be secured as well. Everything starts from the hardware level, where technologies such as UEFI Secure Boot make the boot process secure, and BitLocker ensures that the integrity of the operating system has not been compromised. Only then, when the hardware and the bootup process can be trusted, the operating system will be initialized. The kernel and the core operating system functions have their own security features that base the foundation for the next layer, the application layer.

According to Weston (2019), the Xbox is also based on Windows nowadays. Newest Xbox implements many of the advanced security features of Windows by default, but it differs from its security model as Xbox does not need to protect itself only against external threats, but physically from the user itself also to prevent installing modifications. A lot of the same features that are available as hardening measures on Windows are enabled on the Xbox and therefore used by millions of users, proving that the security measures can work in a larger scale (Weston, 2019).

4.1.1 Zero trust, the modern Windows security model

The modern Windows security model is based on the principle of zero trust. The modern security model is designed for the cloud era, where the traditional network boundaries do not apply anymore. Zero trust as a concept is defined in NIST (2020) SP 800-207 as follows.

> Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). (NIST, 2020)

NIST (2020) states that the "Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource." To enable such advanced protection, the security capabilities of Microsoft's (2022e) Zero trust model are enabled through cloud technologies. Microsoft Cloud allows the use of technologies such as Azure AD Conditional Access and device health attestation capabilities using telemetry. The telemetry in a working Zero trust attestation is collected both from the operating system and its security capabilities such as Defender for Endpoint EDR. Microsoft (2022e) Zero trust principles consist of the following three principles.

- Assume breach
- Use least-privileged access
- Verify explicitly

Due to its nature, the security capabilities of Zero trust architecture are responsive. There are security settings to set in Windows to activate the capabilities but the actual analysis and response to the gathered telemetry is done in Microsoft's Azure AD (Microsoft, 2022c).

4.1.2 Windows development security

An important aspect of Windows security is how it was built and developed. According to Microsoft's (2022c) own statement, they are committed to building highly secure-by-design software and addressing security compliance requirements. To consider security in many levels of the development process, Microsoft has developed a well-known framework, the Microsoft Security Development Lifecycle (SDL) (Lipner & Howard, 2023).

Lipner & Howard (2023) discuss how the Security Development Lifecycle was developed because of the Windows security push that happened in 2002 at Microsoft as the corporation dedicated a team to fix and design the security of Windows as a whole. It has been named the Trustworthy Computing initiative. The SDL is an approach that aims to embed security to the product in all the main stages of its lifecycle. It relies on three core concepts: education, continuous process improvement and accountability. The use of the SDL has been a mandatory internal policy at Microsoft since 2004. Nowadays the latest version of SDL is 5.2 which was released in 2012 (Microsoft, 2023h).

In addition to Microsoft, many other companies use the SDL framework in their own software development processes (Geer, 2010). Despite of SDL, Windows is still vulnerable in its default configuration. Research have found out that the most recent version of Windows 10 is vulnerable to unauthorized exploitation by third parties (Softić & Vejzović, 2022).

4.1.3 Securing privileged access

Microsoft (1993) has established long time ago in their Windows NT 3.1 User's Guide that running Windows as administrator is not considered to be secure. Despite this, the privileged accounts are misused (Motiee et al., 2010). Securing privileged access is a concept from Microsoft (2023e) related to securing privileged account rights, like administrator level access, properly. It was developed to guide organizations to secure their privileged accounts especially in domain environments. Today, the concept of Securing privileged access has developed to "Enterprise access model" which should be adopted by following "Rapid Modernization Plan" or "RaMP". The protection of privileges is closely related to securing the identity of the user and are also a key part of Zero trust concept (Microsoft, 2023e).

Securing privileged access introduces concepts such as Privileged access accounts and Privileged access devices. Privileged access accounts are accounts that usually have higher privileges in the target environment, such as Domain Admin or other administrator privileges. These accounts, with high privileges in the network, should be well protected, as depicted by the Microsoft guidance (Microsoft, 2023e).

4.2 Windows 10 security

Microsoft (2023l) explains that Windows 10 was released originally in 2015. It improved the security over the years with its many updates. The operating system originally received a major update twice a year but that has been reduced to once a year. The operating system has received 14 major updates after its release in 2015 and the latest stable update, named 22H2, was released in October 2022 (Microsoft, 2023l).

Microsoft (2023m) introduced one of the main security features of modern Windows, the virtualization-based security (VBS), with Windows 10. It includes multiple technologies: for example, protection for the sensitive kernel areas of the operating system's memory and Credential Guard. Using Credential Guard meant that the sensitive parts of the operating system like the LSASS process are launched in their own container on top of Hyper-V hypervisor. Local Security Authority Subsystem (LSASS) process is the component in Windows which stores the secrets such as the user's password. There is no memory access from user mode to the sensitive data when using Credential Guard. Instead, the data is accessible only through validated and supported protocols natively provided by Windows API. The functionality of this feature can be seen in the Figure 2. Using Credential Guard makes it substantially harder for an attacker to steal user's credentials from the Windows host operating system (Microsoft, 2023m).

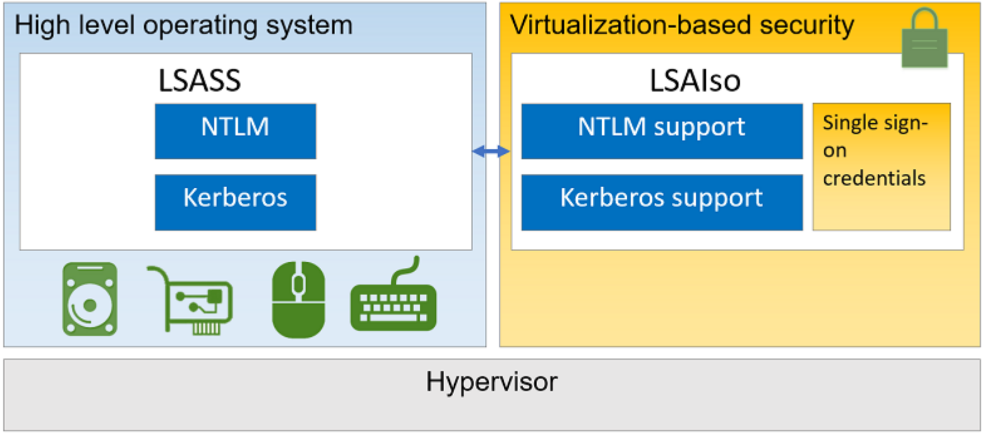
High level operating system
LSASS
NTLM
Kerberos
Virtualization-based security
LSAIso
NTLM support
Kerberos support
Single sign-on credentials
Hypervisor

Figure 2 High-level overview how the LSASS process is protected by Credential Guard. (Microsoft, 2021a)

Microsoft (2021d) states that Windows Defender evolved with Windows 10. It is currently one of best endpoint security products with its EDR functionality Defender for Endpoint (Gartner, 2021). A lot of the Windows security features are renamed Defender X, where the X presents the name of the feature such as Windows Defender Application Control. Other Defender features include for example Attack Surface Reduction, Network protection and Controller folder access. (Microsoft, 2021d) Attack Surface Reduction rules for example, can block known adversary behavior like executing child processes from Outlook email client (in the case of phishing). In addition to advancements in Windows Defender and virtualization-based security, Windows 10 introduced a new allowlisting solution Windows Defender Application Control and Windows Hello, a feature for more secure biometric authentication.

4.3 Windows 11 security

Microsoft (2023n) released Windows 11 on 4th of October 2021. It shares many similarities and most of the features of the Windows 10 and even shares the same operating system version. The operating system has received one update after its release named 22H2 in September 2022.

Microsoft (2023b) describes that the system requirements for Windows changed with Windows 11. The new Windows requires UEFI firmware with Secure Boot support, support for virtualization technologies and a TPM security chip. TPM is found in most systems since 2017 according to Microsoft. With TPM, the secrets of the operating system are stored more securely by using the hardware. The other technologies like virtualization based technologies are required to enable certain security settings.

According to Weston (2023), Windows 11 is designed to be more secure operating system by-default. Out of the box, Windows 11 enforces use of hardware security components, virtualization-based security, memory protections and other security capabilities such as Secure Boot and BitLocker. This is for all the versions of operating systems, including consumer versions of the OS. In addition, the new OS version introduces features such as support for TLS 1.3 and DNS over HTTPS (DoH).

4.4 Security baselines

Moskowitz (2019) explains that hardening Windows could be a labor-intensive operation. It often includes considering any specific needs of the target environment: a single approach does not cover them all. It might be impossible for a single organization to make a specific Windows system secure. However, there are general hardening guidance provided by many different organizations, including Microsoft themselves. These hardening instructions is often referred to as security baselines, a concept first introduced by Parker (1981).

Security baseline is defined by NIST (2023) as "the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection". Parker (1981), defines that the idea of a security baseline is to provide an adequate level of security against common threats that could be applied for a wider audience, therefore leaving behind the need for customizing the configuration for each target system. Still, the security baselines often still need thorough testing to ensure that they do not interfere with the business practices by breaking something (Moskowitz, 2019). There are multiple different hardening guides available on the public domain, including but not limited to the following.

- Microsoft Security Baselines
- CIS (Center for Internet Security)
- NIST/US Department of Defense/DISA STIG (Security Technical Implementation Guides)
- ACSC (Australian Cyber Security Centre)
- NSA (US National Security Authority)
- NCSC (UK's National Cyber Security Centre)
- OpenSCAP security policies
- FIRST Best Practice Guide Library

The security baselines provide baseline protection for the target system. However, they may not properly answer to the threats encountered by the target organization: for example, the security baseline might harden the network configuration and privileges of the system but do not have any mitigations against phishing which is the primary source of malware for an organization. Therefore, the security baselines work great as a foundation, but still require testing and customization to reach the target security state of a particular system.

4.5 Hardware security

According to Microsoft (2023h), the hardware security area relies on the security features provided by hardware. The operating system then utilizes these features with many features such as virtualization-based security, protecting sensitive memory areas from potential threats. Hardware has a large role in the securing the startup process of Windows. With technologies such as Secure Boot and Trusted Boot, malware and corrupted components are prevented from loading and BitLocker, the drive encryption feature of Windows, makes sure that the operating system's drives are not tampered with, ensuring their integrity.

Microsoft (2023h) has advocated for a concept that includes key technology to ensure integrity of the operating system, the "Hardware root of trust" and a concept closely related to that called "Secured-core PCs". The Secured-core PCs incorporate the security features of Windows hardware root of trust by default. The following list includes technologies that are part of the hardware root of trust concept (Microsoft, 2023f).

- Trusted Platform Module (TPM) 2.0
- BitLocker Drive Encryption
- UEFI Secure Boot
- Drivers and Firmware Distributed through Windows Update
- Virtualization and HVCI Enabled
- Drivers and Apps HVCI-Ready
- Windows Hello
- DMA I/O Protection
- System Guard
- Modern Standby

Microsoft (2023t) states that the Trusted Platform Module holds the secrets as the main cryptographic processor on the computer. It allows to store and handle cryptographic keys, ensure the integrity of the hardware with its unique key and helps securing the boot process (Microsoft, 2023o; Perez et al., 2006). A new security processor, Microsoft Pluton, has been developed as a TPM working from within the CPU chip (Microsoft, 2023n).

Microsoft (2022b) explains that the multiple different features complement each other. System Guard and Secure Launch ensure that the system's firmware and hardware are trustworthy by validating the integrity of the system. Hypervisor-protected code integrity (HVCI) protects the system by running operating system's kernel memory integrity checks and by enforcing restrictions. To fully work, the hardware must be certified to work with the feature and updated to ensure their security and compatibility. Kernel Direct Memory Access (DMA) protection restricts the access of external peripherals such as PCIe devices to kernel memory, preventing physical attacks. Finally, Modern Standby allows the device to enforce all the necessary security features while providing a performant sleep mode (Microsoft, 2022a).

4.6 Authentication and access control

The category of authentication involves technologies related to making the user's authentication process secure. Microsoft (2022c) introduces the category as identity protection in their documentation. Weak passwords, password spraying, and phishing are some of main attack vectors for a threat actor. Authentication also includes other related areas such as strong password policies and the concept of multi-factor authentication (MFA). Authentication category includes at least the following security capabilities (Microsoft, 2022b).

- Windows Hello

- Windows Defender Credential Guard and Windows Defender Remote Credential Guard
- FIDO security keys for authentication
- Smart Cards
- Microsoft Authenticator

Haddad et al. (2023) explain that Windows Hello (or Windows Hello for Business) is a biometric authentication framework that became part of the security products in Windows 10. It allows user to use a biometric proof like fingerprint or face to login to Windows. It vastly improves the security compared to passwords, which are a huge issue still in 2020s.

As explored earlier in the Windows 10 chapter, the Credential Guard protects sensitive credentials in memory. Remote Credential Guard also protects credentials. It prevents sending them to the target computer when initiating a Remote Desktop connection (Microsoft, 2023d).

FIDO security keys and smart cards are both used for providing multi-factor authentication. According to Lal et al. (2016), user provides something he has by inserting the smart card or a security key to the computer. This works as the first factor. Smart cards are commonly used with a PIN to unlock it. The PIN works as the second factor, providing multi-factor authentication. (Lal et al., 2016) Microsoft Authenticator is an application for iOS and Android that provides multi-factor authentication and passwordless authentication (Microsoft, 2023k).

Microsoft (2023f) states that access control is the process of controlling access to resources, such as files, folders, and network shares. Windows provides several access control mechanisms, including file system permissions, user rights, and group policy settings. Locally, in Windows, the main factors in access control are the users, groups, and their permissions. Access Control is also closely related to the concept of securing privileged access as well.

One of the main areas of access control is its relation to administrator or other high privileges. It is one of the most important controls in Windows to run it as a normal, non-privileged user, but very few actually do it or even know how to implement proper user account control practices (Motiee et al., 2010). Running Windows as administrator has been considered insecure and against the security architecture of Windows since Windows NT 3.1: the user manual of NT 3.1 explains that the use of local admin rights undermines the built in security of the operating system (Microsoft, 1993).

In authentication and access control, the general guidelines regarding user security apply as well. For example, Ur et al. (2016) and Vu et al. (2007) explain that the password of the user should be unique, complex, and long enough to be secure. In addition, the user should not reuse passwords to prevent the risk of reusing credentials.

4.7 Operating system security

Operating system security includes the core features of the operating system and the protections that are designed to make those features secure. The following features are part of the operating system security (Microsoft, 2021b). The list does not include features already discussed in other chapters.

- Virtualization-based security
- EMET, nowadays Exploit Guard
- Windows Update
- Microsoft Defender SmartScreen
- User Account Control
- Windows Defender Firewall
- IPsec
- Data protection

Microsoft (2022c) explains that Exploit Guard was introduced in Windows 10. It was a replacement for older Microsoft add-on for Windows 7 and 8 called Enhanced Mitigation Experience Toolkit (EMET). Exploit Guard, like EMET, changes the way how Windows handles low-level execution by applying different protections to the system. The protections in Exploit Guard includes things like Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Structured Exception Handling Overwrite Protection (SEHOP) and many others. The protections prevent attackers from exploiting low-level vulnerabilities and execution bypasses in Windows, like a buffer overflow vulnerability (DeMott, 2015).

Wash et al. (2014) explain that Windows Update is considered a security feature as well as it patches vulnerabilities from the system. It is one of the most important parts of keeping a computer secure as it will protect the user from the most common security exploits. The authors also mention that the majority of systems are compromised using known vulnerabilities that have fixes available, but they have not been applied, raising the importance of updating (Wash et al., 2014).

Microsoft's (2023q) Defender SmartScreen is a reputation check feature that has been checking the reputation of a file or an application since Windows 8. In its default setting, an administrator's privileges are required to run a program that does not have a good reputation. It is a very effective mechanism against phishing threats.

Microsoft (2023v) has built protection of network resources from unauthorized access and other network-based attacks to Windows. The main protection feature is Windows Firewall (with Advanced Security) is the built-in firewall solution in Windows. It is a stateful firewall solutions that both inspects and filters all packets for IPv4 and IPv6 traffic. It also incorporates Internet Protocol Security (IPsec) in its configuration. IPsec allows authentication of network traffic to safeguard sensitive data (Microsoft, 2023p).

An important aspect of operating system security is data protection: the protection of sensitive data stored on a system. Microsoft (2022a) has developed security features such as BitLocker and Windows Information Protection in Windows. BitLocker provides full-disk encryption and ensures the integrity of the operating system. Windows Information Protection helps prevent data leakage by classifying and encrypting important data.

4.8 Windows Defender and malware protection

Microsoft (2023j) states that Windows includes protection of the system from viruses, spyware, and other types of malicious software by having a built-in antivirus solution. The Windows Defender Antivirus provides real-time protection against malware. There are many configurable features of the Defender Antivirus (and Defender for Endpoint), including Anti tampering, Controlled Folder Access, Network protection and Attack surface reduction rules. Anti tampering monitors and prevents tampering with the antivirus product itself. Controlled Folder Access limits access to the pre-defined locations to only trusted programs, thus limiting the effectiveness of threats such as ransomware that tries to destroy data widely on the computer. Network protection attempts to block known threats by monitoring local network traffic from the host. Attack Surface Reduction blocks certain techniques commonly used by threat actors based on pre-defined rules. There are 16 different rules available such as “Block Office apps from creating child processes”. All the available rules present in Microsoft’s documentation can be seen in table 5.

Table 5 Attack Surface Reduction rules

Rule name
Block abuse of exploited vulnerable signed drivers
Block Adobe Reader from creating child processes
Block all Office applications from creating child processes
Block credential stealing from the Windows local security authority subsystem (lsass.exe)
Block executable content from email client and webmail
Block executable files from running unless they meet a prevalence, age, or trusted list criterion
Block execution of potentially obfuscated scripts
Block JavaScript or VBScript from launching downloaded executable content
Block Office applications from creating executable content
Block Office applications from injecting code into other processes
Block Office communication application from creating child processes
Block persistence through WMI event subscription
Block process creations originating from PSExec and WMI commands
Block untrusted and unsigned processes that run from USB

Block Win32 API calls from Office macros
Use advanced protection against ransomware

The antivirus product also has cloud-based capabilities such as automated sandbox service, behavior monitoring, cloud-based protection, machine learning and URL protection (Microsoft, 2023j). Microsoft Defender has performed comparably against other known antivirus products from third party evaluations such at MITRE Engenuity ATT&CK Evaluations (Mitre Engenuity, 2022).

In addition to the antivirus, Microsoft (2023d) has included a built-in EDR (endpoint detection and response) product to Windows which requires additional licensing to activate it. EDR records key events from Windows and processes and sends them to the cloud and makes detections based on possible suspicious behavior or other activity. It also provides tools to respond to the threat (Microsoft, 2023c).

4.9 Application security

Microsoft (2023j) explains that Application security is the security level where the protections attempt to mitigate adversaries' capability to affect applications. The adversaries may attempt to run their own malicious code, compromising the confidentiality or integrity of the data. The following features are introduced as part of the application security category (Microsoft, 2023i).

- Windows Defender Application Control
- AppLocker
- Windows Defender Application Guard
- Windows Sandbox
- Email security
- Windows Defender SmartScreen

To prevent execution of malicious payloads, an allowlisting solutions is an effective tool is to determine what can and what cannot run on the system. The allowlisting term is used instead of the old term "whitelist" because the new term is more neutral in nature and has been adopted by many major cyber security organizations (NCSC, 2020). Microsoft (2023p) explains that Windows has had a few iterations of these application allowlisting tools. First Software Restriction Policies were introduced to Windows. After Windows 7 in 2008, AppLocker emerged as a primary tool to be used for allowlisting. In Windows 10, Windows Defender Application Control (WDAC) saw its infancy.

According to Durve & Bouridane (2017), Windows Defender Application Control (WDAC), formerly known as Device Guard Code Integrity Policies, provides a more refined way to allowlist executables on a Windows system. WDAC allows for a more granular approach to the configuration instead of AppLocker. Today, AppLocker and Windows Defender Application Control are the most current versions of application allowlisting and still actively updated by Microsoft. Microsoft also made a change recently to AppLocker, allowing its use in the Windows 10 Pro instead of only Enterprise (Moskowitz, 2019).

Microsoft (2023n) introduced virtualization-based features in Windows 10 such as Windows Sandbox, Edge Application Guard and Office 365 Application Guard on the foundation of virtualization-based security. Application Guard is based on Windows Sandbox. By sandboxing the application that is running, malware that has infected the application can be prevented from infecting the system altogether. For example, if user opens a malicious attachment containing an Office file, the system will not be affected, and the application container sandbox will be destroyed after user closes the program.

Microsoft (2023m) explains that email security is a feature in Windows, allowing a user to sign or encrypt outgoing email messages using S/MIME (Secure/Multipurporse Internet Mail Extensions). The feature provides the recipients a way to verify the integrity of the message and ensures the sender.

5 HARDENING MEASURES AGAINST THE MOST PREVALENT THREATS

As explored earlier in the most prevalent threats chapter, the most prevalent threats include techniques in the MITRE ATT&CK Framework related to mainly to the following tactics:

- Initial Access
- Execution
- Credential Access
- Lateral Movement
- Command and Control
- Impact

The tactics themselves are broad in scope. Only Windows techniques are taken into consideration because of the nature of this thesis. The meaning of each technique is not fully explained in this chapter as they are well documented in the MITRE ATT&CK Enterprise matrix (Mitre Corporation, 2022b). The reference material for each technique in the following chapters is the Enterprise matrix, including the definition of the tactic and possible prevention methods. Each technique in the identified tactics is compared against available Windows security features from the prevention point of view to identify suitable ones.

The following chapters focus on the identified tactics and the techniques found within those tactics. The chapters try to identify suitable security mechanisms in the Windows operating system to mitigate the identified MITRE ATT&CK tactics' techniques. After the techniques and their suitable hardening measures have been introduced, a summarizing chapter "Identifying the key hardening measures" will follow where the most important hardening measures are identified from the chapters.

5.1 Initial Access

Mitre Corporation (2019d) explains that in Initial Access tactic category there are techniques that are used to gain an initial foothold within a target network. In total, there are nine different techniques in the Initial Access tactic category of MITRE ATT&CK framework. In addition, there are 10 sub-techniques. The techniques and the sub-techniques of Initial Access can be seen in table 6.

In Drive-by Compromise technique, an adversary tries to gain access to a system by compromising a website that the victim is browsing to and typically trying to exploit the victim's browser (Mitre Corporation, 2019d). The focus on protecting against malicious sites should be to restrict web-based content. That can be achieved by utilizing Windows Defender antivirus, Attack Surface Reduction Rules, and exploit protection like Exploit Guard. Still, one should also try to protect the browser from exploits by updating browser software and by running the browser in a sandbox like Edge Sandbox in addition to the built-in browser sandbox (Reis et al., 2009).

Mitre Corporation (2019d) defines Exploit Public-Facing Application technique as an adversary trying to exploit a published application like a web server or a database service by taking advantage of a misconfiguration or vulnerability. To mitigate such behavior, the gravity of trying to compromise such application should be limited by implementing features such as Exploit Guard, Windows Firewall, access control and application isolation. The application should be also kept up to date and its vulnerabilities should be discovered by scanning it regularly.

External Remote Services technique Mitre Corporation (2019d) defines as an adversary taking an advantage of an external remote service such as VPN service to get access to the target victim network. Unnecessary features like VPN service, Windows Remote Management or RDP can be disabled or access to them can be limited using network security means such as Windows Firewall.

In Hardware Additions, typically an adversary tries to connect a nefarious device to gain access to the target system (Mitre Corporation, 2019d). To protect against such attacks, Windows 10 and Windows 11 have implemented many hardware and operating system memory protections including Device Guard (with DMA protections) (Yao et al., 2017). Additionally, malicious hardware additions can also be blocked by limiting installation of devices.

Mitre Corporation (2019d) divides phishing technique to three sub-techniques: phishing via attachment, link, or a service. In phishing, the adversary tries to lure the victim to do something malicious: typically to execute some sort of payload on the system. To block phishing, antivirus solution such as Windows Defender that can detect malicious executables or sites can be used. In addition, Attack Surface Reduction rules block some of the used phishing vectors. To limit the effectiveness of phishing, proper user rights assignment can be enforced to limit the privileges of the victim and therefore, the attacker.

According to Mitre Corporation (2019d), Replication Through Removable Media means that an adversary may try to infect a system by introducing malware hosted on a removable media. They then use the Windows built-in feature Autorun to execute the malicious payload on the system. In the recent versions of Windows, attaching an USB drive does not automatically execute the specified file anymore (Anderson & Anderson, 2010). The technique is especially famous from infecting Iran's nuclear enriching centrifuges in 2010 (Chen & Abu-Nimeh, 2011; Langner, 2011). As a mitigation, an application allowlisting solution can prevent running malicious or unwanted software, such as malware from an USB drive.

Table 6 The techniques of the Initial Access tactic category

ID	Name
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service
T1091	Replication Through Removable Media
T1195	Supply Chain Compromise
T1195.001	Compromise Software Dependencies and Development Tools
T1195.002	Compromise Software Supply Chain
T1195.003	Compromise Hardware Supply Chain
T1199	Trusted Relationship
T1078	Valid Accounts
T1078.001	Default Accounts
T1078.002	Domain Accounts
T1078.003	Local Accounts
T1078.004	Cloud Accounts

In addition to the explored techniques, there are the supply chain and relationship related techniques Supply Chain Compromise and Trusted Relationship and their sub-techniques that are hard to combat by hardening Windows in technical manner. Rather, they are related to the trustworthy sourcing of the computer software and hardware and to the co-operation between partners of the organization. The techniques are closely related to the concept of Hardware root of trust by Microsoft (2023f) that aims to ensure the integrity of the operating system is not compromised by implementing multiple different security measures that take advantage of the security features of the hardware. The concept includes features such as UEFI Secure Boot, TPM, System Guard, BitLocker and Device Guard (Microsoft, 2023f).

In the Mitre Corporation's (2019d) Valid Accounts technique, an adversary uses an existing account to gain access to the target system. The technique has four sub-techniques, Default Accounts, Domain Accounts, Local Accounts and Cloud Accounts. In mitigation perspective, the authentication and access control measures are the most relevant security mechanisms. Other security mechanisms to combat the use of the technique include strong password policies, requiring the use of multi-factor authentication and using stronger authentication mechanisms that cannot be used if stolen such as FIDO security keys (Das et al., 2018). Limiting the usefulness of the compromise account to the adversary is possible by enforcing proper access control, including the concept of Securing privileged access.

5.2 Execution

Mitre Corporation (2019c) introduces 14 different techniques in the Execution tactic category of MITRE ATT&CK framework. In addition, there are 22 sub-techniques. The techniques belonging to Execution tactic can be seen in table 7. The techniques T1651, T1059.002, T1059.004, T1059.008, T1059.009, T1609, T1610, T1559.003, T1053.003, T1053.006, T1053.007, T1648 and T1569.001 are not reviewed in this chapter because they do not concern the Windows operating system.

Mitre Corporation (2019c) defines Command and Scripting Interpreter technique, with its five relevant sub-techniques, a way for adversaries to execute commands, binaries, or scripts. In Windows, the main two command shells are the Windows Command Shell (cmd.exe) and PowerShell. Windows has multiple features to mitigate the use of malicious scripts or running arbitrary commands, with the main feature being application allowlisting like AppLocker or WDAC. Based on its configuration, it blocks unwanted software from executing. Also by deploying AppLocker or WDAC, Microsoft (2017) states that PowerShell is automatically put into Constrained Language Mode. In that mode, many of the features of PowerShell are disabled and only the core features are available. In this mode, for example downloading and importing malicious payloads into memory are not possible.

In Exploitation for Client Execution technique, a cyber adversary attempts to exploit vulnerability in the software of a client application to execute their own code (Mitre Corporation, 2019c). Application allowlisting can prevent execution of adversary's own code. Exploit Guard can limit the success rate of such behavior and known malicious payloads can be blocked with an antivirus like Windows Defender. Also, keeping the software up to date is an important measure to mitigate this technique, unless a zero-day vulnerability is used, where a fix isn't available (Bilge & Dumitras, 2012).

Mitre Corporation (2019c) explains that Inter-Process Communication is both name of the technique and a feature in Windows that is used to communicate between processes, for example to share data. The functionality can be used by an adversary to execute arbitrary commands. The technique includes two relevant sub-techniques for Windows: Component Object Model (COM) and Dynamic Data Exchange (DDE). There are Attack Surface Reduction rules that can prevent the technique and sandboxing Office application, where the functionality is used, can prevent such behavior. An antivirus with its behavior monitoring could also prevent the execution.

Native API is explained by Mitre Corporation (2019c) as a way for an adversary to interact with the operating system's application programming interface (API) directly. For example, an adversary can load malicious payloads into memory of a process or create new ones. To block malicious use of Native API, Attack Surface Reduction rule can be used, or the execution can be prevented by using an application control solution like WDAC or AppLocker.

Scheduled Task or a Job technique can be used to schedule the execution of certain commands (Mitre Corporation, 2019c). The technique contains two sub-techniques that are relevant for Windows OS. There are no obvious Windows features that could block malicious use of this functionality.

Mitre Corporation (2019c) explains that an adversary can run malicious payloads by loading dynamic link libraries (DLL). The technique to do this is called Shared Modules. An application whitelisting solution like AppLocker or WDAC can prevent malicious or unwanted payloads from executing.

Software Deployment Tools are tools that allow an administrator to deploy or update software installed on a Windows PC (Mitre Corporation, 2019c). In a typical enterprise network, Microsoft Configuration Manager (SCCM) is used but there are also third-party options available. To mitigate the misuse of Software Deployment Tools, an organization should focus on the access control of that software. Also, a strict configuration of WDAC can prevent unwanted executables from loading.

System Services are a feature in Windows operating systems that allow for execution of tasks in the background (Mitre Corporation, 2019c). There is one relevant sub-technique, Service Execution. There are no obvious Windows features that could block malicious use of this system functionality.

Mitre Corporation's (2019c) User Execution is a technique where the user itself does some actions that lead to execution. Typically, this is related to phishing, where the user is lured to do something. The technique has two relevant sub-techniques for Windows: Malicious Link and Malicious File. Execution of malicious files or links can be blocked or restricted by antivirus, application allowlisting solution or Attack Surface Reduction rules. In addition, if malicious links direct the user to a malicious site, Windows Firewall, SmartScreen or Defender's Network Protection can block it. If the links try to exploit the browser, (Edge) Application Guard can be used to isolate the malicious attempt.

According to Microsoft (2023g), Windows Management Instrumentation is a feature of Windows OS that allows user to execute arbitrary scripts, commands, and payloads. There are Attack Surface Reduction rules to block malicious behavior. Execution of malicious WMI commands can be also limited with WDAC or AppLocker. The privileges given to the account that runs the commands and the access control on the system also define what can be done with WMI.

Table 7 The techniques of the Execution tactic category

ID	Name
T1651	Cloud Administration Command
T1059	Command and Scripting Interpreter
T1059.001	PowerShell
T1059.002	AppleScript
T1059.003	Windows Command Shell
T1059.004	Unix Shell
T1059.005	Visual Basic
T1059.006	Python
T1059.007	JavaScript
T1059.008	Network Device CLI
T1059.009	Cloud API
T1609	Container Administration Command
T1610	Deploy Container
T1203	Exploitation for Client Execution
T1559	Inter-Process Communication
T1559.001	Component Object Model
T1559.002	Dynamic Data Exchange
T1559.003	XPC Services
T1106	Native API
T1053	Scheduled Task/Job
T1053.002	At
T1053.003	Cron
T1053.005	Scheduled Task
T1053.006	Systemd Timers
T1053.007	Container Orchestration Job
T1648	Serverless Execution
T1129	Shared Modules
T1072	Software Deployment Tools
T1569	System Services
T1569.001	Launchctl
T1569.002	Service Execution
T1204	User Execution
T1204.001	Malicious Link
T1204.002	Malicious File
T1204.003	Malicious Image
T1047	Windows Management Instrumentation

5.3 Credential Access

Mitre Corporation (2019b) introduces 17 different techniques in the Credential Access tactic category of MITRE ATT&CK framework. There are also 46 sub-techniques related to those techniques. One of the techniques, Steal Application Access Token, is not relevant for Windows and will not be examined closer. All the techniques of Credential Access category can be found in table 8.

Mitre Corporation (2019b) explains that Adversary-in-the-Middle is the name of the technique and a situation, where adversaries try to intercept traffic between two network devices. The techniques have 3 sub-techniques: LLMNR/NBT-NS Poisoning and SMB Relay, ARP Cache Poisoning and DHCP Spoofing. They all reference a protocol that can be used for the similar purpose: to manipulate the traffic to route to the attacker. As the attack is happening on the network, network protection features can prevent it. One can use Windows Firewall, IPsec to encrypt and authenticate connections to prevent Adversary-in-the-Middle scenarios.

Brute Force is a technique defined by Mitre Corporation (2019b) where an adversary tries to gain access to something by guessing. For example, an attacker can figure out a cleartext password by guessing systematically different combinations of characters. Brute force can happen either against a service or "offline" where the target is usually a stolen password hash. The technique has 4 sub-techniques. By enforcing strong password policies, authentication, and access control, brute force can be prevented. Also, in the case of online brute forcing, the system should be secured with the necessary network protection mechanisms like Windows Firewall or IPsec to prevent such behavior.

In Exploitation for Credential Access, an adversary tries to exploit some software vulnerability to gain access to credentials (Mitre Corporation, 2019b). To mitigate exploiting vulnerabilities, Exploit Protection and application isolation or sandboxing can be used to prevent it. Also, running anything other than approved software can be blocked using application allowlisting software like AppLocker or WDAC. Keeping software up to date and protected from known vulnerabilities by utilizing Windows Update or similar update mechanism can also get rid of the vulnerabilities to prevent the use of this technique.

Forced Authentication is a technique often linked to phishing, where the adversary attempts to lure the victim to authenticate to a service, capturing the victim's credentials (Mitre Corporation, 2019b). Strong password policies can make these captured credentials hard to brute force and blocking the use of these network services using Windows Firewall can prevent the connection to the malicious service and thus preventing the technique.

Mitre Corporation (2019b) defines Forge Web Credentials technique as adversaries attempting to forge credentials that could be used to access web-based applications. It has two sub-techniques. As the technique is about forging, it happens on the adversary's end and cannot be mitigated using technical measures in Windows.

Adversary may try to capture user provided input to obtain credentials: this technique is called Input Capture (Mitre Corporation, 2019b). The technique has 4 sub-techniques: Keylogging, GUI Input capture, Web Portal Capture and Credential API Hooking. There are no apparent security mechanisms that could help in preventing the use of this technique.

Modify Authentication Process is technique where the adversary modifies the authentication mechanism to access credentials (Mitre Corporation, 2019b). It has a total of 8 sub-techniques of which Password Filter DLL, Reversible Encryption, Multi-factor authentication and Network Provider DLL are relevant for a local Windows installation. To prevent modifying authentication processes, the integrity of the operating system can be ensured with tools such UEFI Secure Boot and BitLocker. The loading of malicious software to the authentication process can be prevented by using application whitelisting solution like AppLocker or WDAC. Also, to prevent modifying the authentication provider LSASS, Credential Guard or LSA Protection can be used.

Mitre Corporation (2019b) introduces Multi-factor Authentication Interception and Multi-factor Authentication Request Generation techniques that are both related to each other as they both discuss about the use of multi-factor authentication. The first one is about gaining access to credentials by intercepting the input from multi-factor authentication provider such as smart card. The latter is about sending multi-factor authentication request to the actual user to approve. If sent enough times, the user might approve the login attempt. Both techniques can be blocked by enforcing strong authentication measures such as FIDO security keys or smart cards.

Network Sniffing is a technique used by adversaries to capture important information from network traffic such as authentication information (Mitre Corporation, 2019b). The technique is closely related to Adversary-in-the-Middle technique. Due to their similarity, the same mitigations apply to this technique. Reuse of the captured credentials can be mitigated by using multi-factor authentication.

Mitre Corporation (2019b) explains that OS Credential Dumping is a technique that adversaries use to obtain sensitive materials such as account login information or credentials from the operating systems memory. The technique has 8 sub-techniques. Delpy & Le Toux (2014) have introduced a tool called Mimikatz that is widely used for the OS Credential Dumping technique and its sub-techniques. The tool is widely used in the industry and by several adversaries. To block tools like Mimikatz, Microsoft has introduced Credential Guard and LSA Protection that both aim to protect the credentials in memory so that programs wouldn’t have direct access to it. Similar techniques that have the same protection methods are Unsecured Credentials and Credentials from Password Stores. To prevent stealing sensitive information using techniques Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets or Steal Web Session Cookie, encryption of secrets must be enforced. Forging the authentication material is attacker controlled and cannot be mitigated using available security mechanisms in Windows.

Table 8 The techniques of the Credential Access tactic category

ID	Name
T1557	Adversary-in-the-Middle
T1557.002	LLMNR/NBT-NS Poisoning and SMB Relay
T1557.002	ARP Cache Poisoning
T1557.003	DHCP Spoofing
T1110	Brute Force
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing
T1555	Credentials from Password Stores
T1555.001	Keychain
T1555.002	Securityd Memory
T1555.003	Credentials from Web Browsers
T1555.004	Windows Credential Manager
T1555.005	Password Managers
T1212	Exploitation for Credential Access
T1187	Forced Authentication
T1606	Forge Web Credentials
T1606.001	Web Cookies
T1606.002	SAML Tokens
T1056	Input Capture
T1056.001	Keylogging
T1056.002	GUI Input Capture
T1056.003	Web Portal Capture
T1056.004	Credential API Hooking
T1556	Modify Authentication Process
T1556.001	Domain Controller Authentication
T1556.002	Password Filter DLL
T1556.003	Pluggable Authentication Modules
T1556.004	Network Device Authentication
T1556.005	Reversible Encryption
T1556.006	Multi-Factor Authentication
T1556.007	Hybrid Identity
T1556.008	Network Provider DLL
T1111	Multi-Factor Authentication Interception
T1621	Multi-Factor Authentication Request Generation
T1040	Network Sniffing
T1003	OS Credential Dumping
T1003.001	LSASS Memory
T1003.002	Security Account Manager
T1003.003	NTDS

T1003.004	LSA Secrets
T1003.005	Cached Domain Credentials
T1003.006	DCSync
T1003.007	Proc Filesystem
T1003.008	/etc/passwd and /etc/shadow
T1528	Steal Application Access Token
T1649	Steal or Forge Authentication Certificates
T1558	Steal or Forge Kerberos Tickets
T1558.001	Golden Ticket
T1558.002	Silver Ticket
T1558.003	Kerberoasting
T1558.004	AS-REP Roasting
T1539	Steal Web Session Cookie
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1552.002	Credentials in Registry
T1552.003	Bash History
T1552.004	Private Keys
T1552.005	Cloud Instance Metadata API
T1552.006	Group Policy Preferences
T1552.007	Container API
T1552.008	Chat Messages

5.4 Lateral Movement

Mitre Corporation's (2019e) Lateral Movement tactic contains 9 different techniques. In addition, there are 13 sub-techniques for this category. All the techniques are listed in table 9. For Windows, the SSH hijacking, SSH, Cloud Services, Application Access Token and Web Session Cookie techniques are not relevant. In addition, the Replication Through Removable Media and Software Deployment Tools techniques were already discussed in other tactic categories Initial Access and Execution respectively. The same hardening measures identified for them apply in this tactic as well.

Exploitation of Remote Services is a technique in which the adversary attempts to exploit the available service like SMB or RDP (Mitre Corporation, 2019e). The technique is very similar to the Initial Access techniques Exploit Public-Facing Application and External Remote Services. Therefore, the same mitigations mechanisms apply: Exploit protection through Exploit Guard, application isolation or sandboxing, disabling unnecessary features, firewalling with Windows Firewall, minimizing the impact of potential compromise with proper access control and securing privileged access measures and finally, by updating the service using Windows Update.

Internal Spearphishing is the same technique as Phishing in Initial Access category. The difference is that the activity is being conducted internally within the same organization (Mitre Corporation, 2019e). Thus, the same security mechanisms apply as in Initial Access.

The adversary transfers their tools or files between different systems in a technique called Lateral Tool Transfer (Mitre Corporation, 2019e). To prevent such behavior, the network traffic can be filtered using Windows Firewall. Network Protection features of Windows Defender can also spot known malicious traffic.

Remote Service Session Hijacking and Remote Services are both related to using an account to log in to a published service such as Remote Desktop Protocol (RDP) (Mitre Corporation, 2019e). The technique can be blocked with Windows Firewall by limiting the availability of remote services and multi-factor authentication like a smart card as it forces to validate the authenticity of the user.

Mitre Corporation (2019e) explains that an adversary can deliver malicious payloads by modifying or adding content an existing shared storage location like a network drive. The technique is called Taint Shared Content. The execution of infected content can be prevented with application control solution like AppLocker or WDAC. Windows Defender antivirus can also prevent known malicious executables. To prevent the malicious content being created in the first place, proper access control must be in place.

Mitre Corporation (2019e) associates technique called Use Alternate Authentication Material to the way how an adversary uses other authentication material like Kerberos tickets, password hashes or web session cookies for the authentication. The technique has four sub-techniques but only two of them, Pass the Hash and Pass the Ticket, are relevant for Windows operating system. The technique itself is related to authentication that is a feature. The usefulness of the technique can be limited with access control and securing privileged access.

Table 9 The techniques of the Lateral Movement tactic category

ID	Name
T1210	Exploitation of Remote Services
T1534	Internal Spearphishing
T1570	Lateral Tool Transfer
T1563	Remote Service Session Hijacking
T1563.001	SSH Hijacking
T1563.002	RDP Hijacking
T1021	Remote Services
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1021.003	Distributed Component Object Model
T1021.004	SSH
T1021.005	VNC
T1021.006	Windows Remote Management

T1021.007	Cloud Services
T1091	Replication Through Removable Media
T1072	Software Deployment Tools
T1080	Taint Shared Content
T1550	Use Alternate Authentication Material
T1550.001	Application Access Token
T1550.002	Pass the Hash
T1550.003	Pass the Ticket
T1550.004	Web Session Cookie

5.5 Command and Control

According to Mitre Corporation (2019a), "Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection." In total, there are 16 different techniques in the Command and Control tactic category of MITRE ATT&CK framework. In addition, there are 23 sub-techniques in the tactic category. The techniques belonging to the tactic can be seen in table 10.

There are several security features that could help to combat the different techniques of Command and Control. The main feature is antivirus like Windows Defender antivirus. It can detect and prevent suspicious known connections in techniques like Application Layer Protocol, where an adversary communicates through known application controls such as HTTP.

Communication Through Removable Media is a very similar technique to Replication Through Removable Media. Also, Ingress Tool Transfer is a very similar technique to the Lateral Tool Transfer technique. Both techniques were previously reviewed in this thesis. Thus, they are not reviewed here as the same security measures apply to these techniques.

There are also techniques in the Command and Control category that are hard to detect as malicious unless the exact way that they are used are known to be malicious. Such techniques include Data Encoding, Data Obfuscation and Dynamic Resolution. They could be detected by an antivirus or another security feature that monitors network traffic. The same applies for Encrypted Channel, Fallback Channels, Multi-Stage Channels, Protocol Tunneling, Proxy techniques as they all try to avoid getting detected and try to blend in the normal traffic (Mitre Corporation, 2019a). Non-Application Layer Protocol, Non-Standard Port and Traffic Signaling are all techniques that differ by using abnormal protocol or a port or uses a sequence of packets that can be sent to trigger a response (Mitre Corporation, 2019a). They can all be prevented by deploying strict rulesets to Windows Firewall.

In Remote Access Software, an adversary uses a remote access software such as TeamViewer or AnyDesk to connect to target systems (Mitre Corporation, 2019a). The technique can be prevented by deploying an application allowlisting solution like AppLocker or WDAC that prevents the execution of unwanted software. Windows Firewall can also prevent such connections from being made.

Web Service is a technique in which an adversary uses a legitimate existing external Web service to relay data (Mitre Corporation, 2019a). Threat actors such as Ember Bear has used Discord to deliver malware (Unit 42, 2022). To prevent it, web content should be filtered using features such as Windows Defender antivirus and Network protection. They can prevent connections that are detected as malicious.

Table 10 The techniques of the Command and Control tactic category

ID	Name
T1071	Application Layer Protocol
T1071.001	Web Protocols
T1071.002	File Transfer Protocols
T1071.003	Mail Protocols
T1071.004	DNS
T1092	Communication Through Removable Media
T1132	Data Encoding
T1132.001	Standard Encoding
T1132.002	Non-Standard Encoding
T1001	Data Obfuscation
T1001.001	Junk Data
T1001.002	Steganography
T1001.003	Protocol Impersonation
T1568	Dynamic Resolution
T1568.001	Fast Flux DNS
T1568.002	Domain Generation Algorithms
T1568.003	DNS Calculation
T1573	Encrypted Channel
T1573.001	Symmetric Cryptography
T1573.002	Asymmetric Cryptography
T1008	Fallback Channels
T1105	Ingress Tool Transfer
T1104	Multi-Stage Channels
T1095	Non-Application Layer Protocol
T1571	Non-Standard Port
T1572	Protocol Tunneling
T1090	Proxy
T1090.001	Internal Proxy
T1090.002	External Proxy
T1090.003	Multi-hop Proxy
T1090.004	Domain Fronting
T1219	Remote Access Software

T1205	Traffic Signaling
T1205.001	Port Knocking
T1205.002	Socket Filters
T1102	Web Service
T1102.001	Dead Drop Resolver
T1102.002	Bidirectional Communication
T1102.003	One-Way Communication

5.6 Impact

Mitre Corporation (2019e) introduces 13 different techniques in the Impact tactic category of MITRE ATT&CK framework. In addition, there are 13 sub-techniques. All the techniques can be seen in table 11. In such a late stage of the cyber kill chain, the prevention mechanisms have mostly failed as the adversary is about to achieve their goal. Instead of the prevention mechanisms, the focus is mainly on limiting the damages.

The destructive behavior depicted by tools like ransomware can be prevented with many means. Techniques belonging to the destructive behavior include Data Destruction, Data Encrypted for Impact, Data Manipulation, Disk Wipe and Firmware Corruption (Mitre Corporation, 2019f). The destructive behavior can be limited with Microsoft Defender antivirus, Controlled Folder Access, Attack Surface Reduction rules, UEFI Secure Boot and other boot integrity means. Backup as a security measure is also a very important aspect of recovering from such techniques. Backup is also suitable for recovering from technique Inhibit System Recovery, where an adversary removes built-in data to prevent the recovery of the operating system.

Denial of Service attacks can be limited by reducing the attack surface where such an attack can be performed against. Techniques related to Denial of Service include Defacement, Endpoint Denial of Service and Network Denial of Service. Limitation of those techniques can be done with Windows Firewall (Naik & Jenkins, 2016).

Resource Hijacking such as mining cryptocurrency, as one of the most prevalent threat categories listed, may not be prevented at this point as execution itself has already happened. In the execution stage, Windows Defender antivirus with its behavior monitoring can block the technique. Techniques Account Access Removal, Service Stop and System Shutdown/Reboot are features and therefore hard to pinpoint as malicious.

Table 11 The techniques of the Impact tactic category

ID	**Name**
T1531	Account Access Removal
T1485	Data Destruction
T1486	Data Encrypted for Impact

T1565	Data Manipulation
T1565.001	Stored Data Manipulation
T1565.002	Transmitted Data Manipulation
T1565.003	Runtime Data Manipulation
T1491	Defacement
T1491.001	Internal Defacement
T1491.002	External Defacement
T1561	Disk Wipe
T1561.001	Disk Content Wipe
T1561.002	Disk Structure Wipe
T1499	Endpoint Denial of Service
T1499.001	OS Exhaustion Flood
T1499.002	Service Exhaustion Flood
T1499.003	Application Exhaustion Flood
T1499.004	Application or System Exploitation
T1495	Firmware Corruption
T1490	Inhibit System Recovery
T1498	Network Denial of Service
T1498.001	Direct Network Flood
T1498.002	Reflection Amplification
T1496	Resource Hijacking
T1489	Service Stop
T1529	System Shutdown/Reboot

5.7 Identifying the key hardening measures

The identified features spanned from the bottom of the Windows security stack, hardware security, all the way to the application security level. Table 12 summarizes the number of techniques each security mechanism was able to counter in each MITRE ATT&CK tactic category. It should be noted that in the table Defender antivirus included all its features such as Network protection instead of just the basic features of behavior monitoring and definition-based approach, where the detection is based on characteristics of known threats.

Table 12 Security mechanisms and the number of techniques they were able to counter in each MITRE ATT&CK tactic category.

Hardening measure	**Initial Access**	**Execution**	**Credential Access**	**Lateral Movement**	**Command and Control**	**Impact**	**Total Count**
Windows Firewall (incl. IPsec)	2		4	3	3	1	13

Windows Defender antivirus	2	3		3	2	2	12
Application allowlisting (AppLocker/WDAC)	1	6	2	2	1		12
Access control and limiting user rights	3	2		4			9
Attack Surface Reduction rules	2	3		1		1	7
Exploit Guard	2	1	1				4
Windows Update	1	1	1	1			4
UEFI Secure Boot	1		1			1	3
Windows Sandbox (Edge/Office 365)	1	2					3
FIDO security keys/smart cards	1		1	1			3
BitLocker	1		1				2
Device Guard (DMA)	2						2
Credential Guard			2				2
Controlled Folder Access						1	1
Application isolation	1						1
SmartScreen		1					1

As table 12 shows, Windows Firewall, Windows Defender and application allowlisting solution AppLocker or WDAC were able to counter the greatest number of techniques throughout the identified tactics. They were able to cover at least 12 techniques each. The identified security mechanisms were able to cover at least a minimum of seven techniques (Attack Surface Reduction rules). To summarize, the top five hardening measures against the most prevalent tactics used by current threat actors are the following ones:

- Windows Firewall
- Windows Defender antivirus
- Application allowlisting solution with AppLocker or Windows Defender Application Control (WDAC)
- Proper access control and limiting user rights
- Attack Surface Reduction rules

It is noteworthy that the protection methods seem to mainly prevent the Initial Access and Execution tactic categories: an antivirus can block malicious files or executions, allowlisting solution blocks execution of unwanted software and Attack Surface Reduction rules blocks known unwanted, potentially malicious behavior often associated with those tactics as well. Windows Firewall is utilized to block malicious network traffic or to secure it from unwanted use with IPsec, effectively blocking techniques such as exploit attempts in Initial Access, Lateral Movement and Command and Control. The proper access control and user rights limit the effectiveness of an attack in many stages of the cyber kill chain including Initial Access, Execution, Credential Access and Lateral

Movement. Limiting the privileges and therefore the gravity of an attack can prevents the adversary from achieving their end goal in the Impact tactic category.

6 RESULTS AND DISCUSSION

This research was able to answer both research questions. The most prevalent threats were identified based on three threat landscape reports and by selecting only MITRE ATT&CK tactics that all of them referenced: Initial Access, Execution, Credential Access, Lateral Movement, Command and Control and Impact. The identified tactics and techniques within those tactics were then used as a framework to identify the most important Windows security features. Security features that stood out, covering the largest number of MITRE ATT&CK techniques, were Windows Firewall, Windows Defender antivirus, application allowlisting using AppLocker or Windows Defender Application Control, access control and user rights, and Attack Surface Reduction rules.

The identified protection methods are something an organization can practically focus on to combat against the techniques likely used by a cyber adversary in the current threat landscape. The identification of these security features can help an organization in what they should put their resources to. For example, based on the results of this thesis, the organization is more protected against current threats if they would put their resources in implementing Attack Surface Reduction rules or Windows Firewall instead of other features like Controlled Folder Access or BitLocker. The results of this thesis can also help other academic researchers to both understand the most relevant threats in the current landscape and where the focus of hardening Windows should be.

The results may have been even more clear if no sampling was present: The top MITRE ATT&CK tactics were identified in this thesis as all three of the examined threat reports referenced those. The rest of the tactics that were referenced by the reports but were not included in closer examination also have their own prevention methods that were not part of the identification process. Still, at least the top five security features had many mentions, making them likely hold their importance as top features even with a wider sample.

As there is limited research about the matter, proper comparison with other academic articles cannot be conducted. A comparison could be made in future research where the goal is to examine whether the existing security guidance or baselines from organizations like CIS or Microsoft align with the results of this thesis. They are, after all, designed to protect the system from the most common attacks (Moskowitz, 2019). Another idea, related to the security baselines, is to test whether those security baselines provide adequate protection against the most common threats.

The actual effectiveness of the security hardening measures was not tested in this research. Instead, this thesis based on the strong technical background of the threat landscape reports. The reports were derived from actual cases, thus making the results of this research likely applicable to those cases as well. Still, testing the effectiveness of focusing on the most important security features against the most prevalent threats is something that could give additional insight into the matter. It would also fulfill the constructive research methods fifth method: testing if the model works (Kasanen et al., 1993).

The research only works for the current threat landscape. The threat landscape might shift to a different direction, as stated by ENISA (2022) that "[Used techniques] can change over time as groups evolve and use new techniques." Therefore, the results of this research may not apply in a few years' time. Because of this, it would be worthwhile to revisit this subject as threat landscape evolves.

It should be noted that the prevention of attacks is not always possible, which makes detection and response an important part of the security as well. Detection is important, because according to Al-Shaer et al. (2020) about 68 % of attacks are not discovered at all. And even if they are detected, at least three quarters of those attacks are not remediated within hours or days (Al-Shaer et al., 2020). The importance of detection and response is highlighted from the recent shift of the protection paradigm. The protection has shifted from focusing on prevention methods towards "assume breach" mindset where the assumption is made that the attacker is already inside the network. In an "assume breach" scenario, later stages of the cyber kill chain are the focus for both the adversary and the defender (as opposed to every tactic until Initial Access/Execution). In such a late stage of an attack, detection methods are a key security measure that need configuring from the default settings to be effective. For example, it has been shown that there is need for optimizing the security logging and enhancing the detection capabilities from the default configuration to detect malicious behavior (Baráth, 2017). Detection and response are not part of this research and are thus a possible topic for future research.

Further research could also include the aspect of Active Directory domain network, where the hardening aspect could be different due to domain's dependencies such as encryption types in authentication protocols. Still, that research would focus only on the traditional on-premises protection model. To fully understand the scope of the modern protection mechanisms built into Windows that also Microsoft advocates, cloud-enabled features such as Azure AD Conditional Access and endpoint attestation through telemetry should be taken into consideration as well. Additionally, features like EDR and its dynamical capabilities might play a larger role in the protection of the Windows operating system, where they also try to detect and respond to threats instead of just focusing on prevention. The operating system's local key hardening measures found in this thesis could be different from ones of a cloud connected workstation that tries to comply with the Microsoft modern Windows security concept that adheres to Zero trust.

It would be interesting to understand what security mechanisms the most important ones for Windows Servers are as this research focused only on the endpoint operating system version of Windows. The threats and the suitable security mechanisms in a server operating system could be different despite sharing many of the same features. Additionally, as this research focused only on Windows, the same could be applied for other operating systems, such as Linux and macOS. They might have a very different list of the most important security mechanisms as the MITRE ATT&CK techniques that apply to them are also different.

7 CONCLUSION

In conclusion, this thesis found that there are import security measures in Windows that can help in protecting against common threats. Some measures stood out based on the number of techniques they were able to prevent. Those measures are host firewalling, antivirus, application allowlisting, limiting user account privileges and rights and Attack Surface Reduction – a feature designed to block common techniques used by adversaries.

This thesis was also able to identify the six most used tactics by cyber adversaries from the current threat landscape. In the current threat landscape, ransomware continues to be the one of the most common threats with various malware, different initial access vectors, command and control (C2) frameworks and phishing attacks. The tactics, defined by widely used framework MITRE ATT&CK, are Initial Access, Execution, Credential Access, Lateral Movement, Command and Control and Impact.

Identifying of the most prevalent threats and the tactics that they used were carried out by analyzing three known threat reports from ENISA, Cisco and Red Canary. The reports referenced 12 of the 14 tactics present in the MITRE ATT&CK Enterprise matrix that was used as a framework for this thesis. Identifying the tactics used by known threat actors allowed the thesis to find the best ways to respond to those threats. Of the mentioned tactics, only six were referenced by all the chosen reports and were chosen for further examination. They were also identified as the tactics likely used by threat actors in the current threat landscape.

This thesis was also able to provide an overview of the security in Windows operating system. Windows security mechanisms were examined. The chapter included an overview of the foundation of Windows' security, the latest improvements and an overview of the mechanisms in different levels of the operating system. The overview provided an understanding of the available security mechanisms that can be used to prevent different sorts of cyber adversary behavior.

The thesis found that the identified security features can prevent the largest number of techniques used by current threat actors. Using this knowledge, an organization like a company or a government agency can optimize their efforts in securing Windows by focusing on the most effective hardening measures. By focusing the security efforts, the organization can best protect itself from the most prevalent threats.

BIBLIOGRAPHY

Al-Shaer, R., Spring, J. M., & Christou, E. (2020). *Learning the associations of mitre att & ck adversarial techniques*. 1–9.

Anderson, B., & Anderson, B. (2010). *Seven deadliest USB attacks*. Syngress. https://doi.org/10.1016/C2009-0-61909-7

Baráth, J. (2017). *Optimizing windows 10 logging to detect network security threats*. 1–4. https://doi.org/10.23919/KIT.2017.8109438

Berghel, H. (2017). A Quick Take on Windows Security Evolution. *Computer*, *50*(5), 120–124. https://doi.org/10.1109/MC.2017.136

Bilge, L., & Dumitras, T. (2012, October 16). *Before we knew it | Proceedings of the 2012 ACM conference on Computer and communications security*. https://doi.org/10.1145/2382196.2382284

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*(4), 91–93. https://doi.org/10.1109/MC.2011.115

Cisco Systems Incorporated. (2021). *2021 Cyber security threat trends- phishing, crypto top the list*. Cisco Umbrella. https://learn-cloudsecurity.cisco.com/umbrella-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Cusumano, M. A. (2006). What road ahead for Microsoft and Windows? *Communications of the ACM*, *49*(7), 21–23.

Das, S., Dingman, A., & L. Jean, C. (2018). *Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key | SpringerLink*. https://link.springer.com/chapter/10.1007/978-3-662-58387-6_9

Delpy, B., & Le Toux, V. (2014). Mimikatz. *Mimikatz*.

ENISA. (2022, November 3). *ENISA Threat Landscape 2022* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Geer, D. (2010). Are Companies Actually Using Secure Development Life Cycles? *Computer*, *43*(6), 12–16. https://doi.org/10.1109/MC.2010.159

Haddad, J., Pitropakis, N., Chrysoulas, C., Lemoudden, M., & Buchanan, W. J. (2023). Attacking Windows Hello for Business: Is It What We Were Promised? *Cryptography*, *7*(1), Article 1. https://doi.org/10.3390/cryptography7010009

Joh, H. (2019). Software risk assessment for windows operating systems with respect to CVSS. *European Journal of Engineering and Technology Research*, *4*(11), 41–45. https://doi.org/10.24018/ejeng.2019.4.11.1610

Kasanen, E., Lukka, K., & Siitonen, A. (1993). The constructive approach in management accounting research. *Journal of Management Accounting Research*, *5*(1), 243–264.

Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. *Vol*, *5*, 246–249.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Lipner, S., & Howard, M. (2023). Inside the Windows Security Push: A Twenty-Year Retrospective. *IEEE Security & Privacy*, *21*(2), 24–31. https://doi.org/10.1109/MSEC.2022.3228098

Lockheed Martin. (2023, February 6). *Cyber Kill Chain*®. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Microsoft. (1993). *Microsoft Windows 3.1 User's Guide*. Microsoft Corporation.

Microsoft. (2021a, March 12). *How Windows Defender Credential Guard works—Windows security*. https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-it-works

Microsoft. (2021b, April 10). *Windows operating system security—Windows security*. https://docs.microsoft.com/en-us/windows/security/operating-system

Microsoft. (2022a, December 10). *Windows hardware security*. https://learn.microsoft.com/en-us/windows/security/hardware

Microsoft. (2022b, December 10). *Windows identity and user security*. https://learn.microsoft.com/en-us/windows/security/identity

Microsoft. (2022c, December 22). *Zero Trust and Windows device health*. https://learn.microsoft.com/en-us/windows/security/zero-trust-windows-device-health

Microsoft. (2023a). *Compare Windows 10 Home vs Pro | Microsoft Windows*. Windows. https://www.microsoft.com/en-us/windows/compare-windows-10-home-vs-pro

Microsoft. (2023b). *Windows security*. https://learn.microsoft.com/en-us/windows/security/

Microsoft. (2023c, February 7). *Microsoft Defender for Endpoint*. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint

Microsoft. (2023d, February 17). *Protect Remote Desktop credentials with Windows Defender Remote Credential Guard (Windows 10)*. https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard

Microsoft. (2023e, March 3). *Securing privileged access overview*. https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview

Microsoft. (2023f, March 3). *Why are privileged access devices important*. https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices

Microsoft. (2023g, March 8). *Windows Management Instrumentation—Win32 apps*. https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Microsoft. (2023h, March 9). *Microsoft Security Development Lifecycle*. https://learn.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle

Microsoft. (2023i, March 9). *Windows application security*. https://learn.microsoft.com/en-us/windows/security/apps

Microsoft. (2023j, March 9). *Windows threat protection*. https://learn.microsoft.com/en-us/windows/security/threat-protection/

Microsoft. (2023k, March 10). *Plan a passwordless authentication deployment in Azure Active Directory—Microsoft Entra*. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-deployment

Microsoft. (2023l, March 14). *Windows 10—Release information*. https://learn.microsoft.com/en-us/windows/release-health/release-information

Microsoft. (2023m, March 20). *Virtualization-based Security (VBS)*. https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs

Microsoft. (2023n, May 11). *Microsoft Pluton security processor*. https://learn.microsoft.com/en-us/windows/security/information-protection/pluton/microsoft-pluton-security-processor

Microsoft. (2023o, May 11). *Trusted Platform Module Technology Overview*. https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

Microsoft. (2023p, May 11). *Windows Defender Firewall with Advanced Security (Windows)*. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security

Mitre Corporation. (2019a, July 19). *Command and Control, Tactic TA0011—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/TA0011/

Mitre Corporation. (2019b, July 19). *Credential Access, Tactic TA0006—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/TA0006/

Mitre Corporation. (2019c, July 19). *Execution, Tactic TA0002—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/TA0002/

Mitre Corporation. (2019d, July 19). *Initial Access, Tactic TA0001—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/TA0001/

Mitre Corporation. (2019e, July 19). *Lateral Movement, Tactic TA0008—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/TA0008/

Mitre Corporation. (2019f, July 25). *Impact, Tactic TA0040—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/TA0040/

Mitre Corporation. (2022a). *MITRE ATT&CK®*. https://attack.mitre.org/

Mitre Corporation. (2022b, October 25). *Tactics—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/tactics/enterprise/

Mitre Corporation. (2023a). *Glossary | CVE*. https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryVulnerability

Mitre Corporation. (2023b). *Our Story*. MITRE. https://www.mitre.org/who-we-are/our-story

Mitre Corporation. (2023c, April 25). *Updates—Updates—April 2023 | MITRE ATT&CK®*. https://attack.mitre.org/resources/updates/updates-april-2023/

Mitre Engenuity. (2022). *ATT&CK® Evaluations*. https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-sandworm/

Moskowitz, J. (2019). Security with Baselines, BitLocker, AppLocker, and Conditional Access. In *MDM: Fundamentals, Security, and the Modern Desktop: Using Intune, Autopilot, and Azure to Manage, Deploy, and Secure Windows 10* (pp. 395–437). Wiley. https://doi.org/10.1002/9781119564362.ch10

Motiee, S., Hawkey, K., & Beznosov, K. (2010). Do windows users follow the principle of least privilege? Investigating user account control practices. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 1–13. https://doi.org/10.1145/1837110.1837112

Naik, N., & Jenkins, P. (2016). *Fuzzy reasoning based windows firewall for preventing denial of service attack*. 759–766. https://doi.org/10.1109/FUZZ-IEEE.2016.7737764

NCSC. (2020, April 30). *Terminology: It's not black and white*. https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Oosthoek, K., & Doerr, C. (2019). *Sok: Att&ck techniques and trends in windows malware*. 406–425. https://doi.org/10.1007/978-3-030-37228-6_20

Perez, R., Sailer, R., & van Doorn, L. (2006). *VTPM: virtualizing the trusted platform module*. 305–320. https://www.researchgate.net/publication/228701767_VTPM_Virtualizing_the_trusted_platform_module

Pols, P. (2017). *The Unified Kill Chain*. https://www.unifiedkillchain.com

Ramasamy, K., Thakur, S., & Baskaran, V. K. (2019). *Security in Windows 10*. https://doi.org/10.13140/RG.2.2.18410.75208

Red Canary. (2023). *Welcome to the Red Canary 2023 Threat Detection Report*. Red Canary. https://redcanary.com/threat-detection-report/

Reis, C., Barth, A., & Pizano, C. (2009). Browser Security: Lessons from Google Chrome: Google Chrome developers focused on three key problems to shield the browser from attacks. *Queue*, *7*(5), 3–8. https://doi.org/10.1145/1551644.1556050

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3). https://www.researchgate.net/publication/317011931_The_CIA_strikes_back_Redefining_confidentiality_integrity_and_availability_in_security

Softić, J., & Vejzović, Z. (2022). Windows 10 Operating System: Vulnerability Assessment and Exploitation. *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1–5. https://doi.org/10.1109/INFOTEH53737.2022.9751274

StatCounter. (2023a, March). *Desktop Operating System Market Share Worldwide*. StatCounter Global Stats. https://gs.statcounter.com/os-market-share/desktop/worldwide

StatCounter. (2023b, March). *Desktop Windows Version Market Share Worldwide*. StatCounter Global Stats. https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

Unit 42. (2022, February 26). Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot. *Unit 42*. https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

Wash, R., Rader, E., Vaniea, K., & Rizor, M. (2014). *Out of the loop: How automated software updates cause unintended security consequences*. 89–104. https://dl.acm.org/doi/abs/10.5555/3235838.3235846

Weston, D. (Director). (2019, October 24). *Advancing Windows Security—David Weston, Microsoft—Platform Security Summit 2019*. https://www.youtube.com/watch?v=FJnGA4XRaq4

Xavier, U. H. R., & Pati, B. P. (2012). *Study of internet security threats among home users*. 217–221. https://doi.org/10.1109/CASoN.2012.6412405

Yao, J., Zimmer, V. J., & Zeng, S. (2017). A tour beyond BIOS: Using IOMMU for DMA protection in UEFI firmware. *Intel Corporation*.

ATTACHMENT 1 ENISA THREAT REPORT SUMMARY OF TECHNIQUES

The following threat categories were listed in the report. Within each category there is a list of each of the MITRE ATT&CK techniques observed related to it and the respective tactic that it belongs to.

Ransomware	
T1190 Exploit Public Facing Application	Initial Access
T1133 External Remote Services	Initial Access
T1566 Phishing	Initial Access
T1199 Trusted Relationship	Initial Access
T1106 Native API	Execution
T1047 Windows Management Instrumentation	Execution
T1197 BITS Jobs	Persistence
T1554 Compromise Client Software Binary	Persistence
T1136 Create Account	Persistence
T1133 External Remote Services	Persistence
T1134 Access Token Manipulation	Privilege Escalation
T1068 Exploitation for Privilege Escalation	Privilege Escalation
T1055 Process Injection	Privilege Escalation
T1134 Access Token Manipulation	Defense Evasion
T1197 BITS Jobs	Defense Evasion
T1140 Deobfuscate/Decode Files or Information	Defense Evasion
T1480 Execution Guardrails	Defense Evasion
T1036 Masquerading	Defense Evasion
T1112 Modify Registry	Defense Evasion
T1027 Obfuscated Files or Information	Defense Evasion
T1055 Process Injection	Defense Evasion
T1620 Reflective Code Loading	Defense Evasion
T1497 Virtualization/Sandbox Evasion	Defense Evasion
T1555 Credentials from Password Stores	Credential Access
T1539 Steal Web Session Cookie	Credential Access
T1087 Account Discovery	Discovery
T1217 Browser Bookmark Discovery	Discovery
T1135 Network Share Discovery	Discovery
T1069 Permissions Groups Discovery	Discovery
T1057 Process Discovery	Discovery
T1012 Query Registry	Discovery
T1518 Software Discovery	Discovery
T1614 System Location Discovery	Discovery
T1033 System Owner/User Discovery	Discovery
T1124 System Time Discovery	Discovery

T1497 Virtualisation/Sandbox Evasion	Discovery
T1210 Exploitation of Remote Services	Lateral Movement
T1080 Taint Shared Content	Lateral Movement
T1560 Archive Collected Data	Collection
T1530 Data from Cloud Storage Object	Collection
T1213 Data from Information Repositories	Collection
T1039 Data from Network Shared Drive	Collection
T1113 Screen Capture	Collection
T1568 Dynamic Resolution	Command and Control
T1095 Non-Application Layer Protocol	Command and Control
T1071 Non-Standard Port	Command and Control
T1072 Protocol Tunneling	Command and Control
T1090 Proxy	Command and Control
T1102 Web Service	Command and Control
T1041 Exfiltration over C2 Channel	Exfiltration
T1485 Data Destruction	Impact
T1499 Endpoint Denial of Service	Impact
T1489 Service Stop	Impact
Social Engineering	
T1133: External Remote Services	Initial Access
T1566: Phishing	Initial Access
T1199: Trusted Relationship	Initial Access
T1078: Valid Accounts	Initial Access
T1204: User Execution	Execution
Threats against data	
T1197: BITS Jobs	Persistence
T1197: BITS Jobs	Defense Evasion
T1560: Archive Collected Data	Collection
T1005: Data from Local System	Collection
T1039: Data from Network Shared Drive	Collection
T1025: Data from Removable Media	Collection
T1074: Data Staged	Collection
T1020: Automated Exfiltration	Exfiltration
T1048: Exfiltration Over Alternative Protocol	Exfiltration
T1041: Exfiltration Over C2 Channel	Exfiltration
T1011: Exfiltration Over Other Network Medium	Exfiltration
T1052: Exfiltration Over Physical Medium	Exfiltration
T1567: Exfiltration Over Web Service	Exfiltration
T1029: Scheduled Transfer	Exfiltration
T1537: Transfer Data to Cloud Account	Exfiltration
Threats Against Availability (DDOS)	
T1553: Subvert Trust Controls	Defense Evasion
T1553.003: SIP and Trust Provider Hijacking	Defense Evasion

T1485: Data Destruction	Impact
T1489: Service Stop	Impact
T1499: Endpoint Denial of Service	Impact
T1499.001: OS Exhaustion Flood	Impact
T1499.002: Service Exhaustion Flood	Impact
T1499.003: Application Exhaustion Flood	Impact
T1499.004: Application or System Exploitation	Impact
T1498: Network Denial of Service	Impact
T1498.001: Direct Network Flood	Impact
T1498.002: Reflection Amplification	Impact
Threats Against Availability (internet threats)	
T1189: Drive-by Compromise	Initial Access
T1046: Network Service Scanning	Discovery
T1557: Adversary in the Middle	Collection
T1498: Network Denial of Service	Impact
Disinformation - misinformation	
T1566: Phishing	Initial Access
T1203: Exploitation for Client Execution	Execution
T1204: User Execution	Execution
T1565: Data Manipulation	Impact
T1491: Defacement	Impact
Supply Chain Attacks	
T1195: Supply Chain Compromise	Initial Access
T1195.001: Compromise Software Dependencies and Development Tools	Initial Access
T1195.002: Compromise Software Supply Chain	Initial Access
T1195.003: Compromise Hardware Supply Chain	Initial Access
T1200: Hardware Additions	Initial Access
T1199: Trusted Relationship	Initial Access