CENTRE FOR
CYBER SECURITY

INVESTIGATION REPORT

THE ANATOMY OF TARGETED RANSOMWARE ATTACKS

Targeted ransomware attacks and how to defeat them

Contents

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
E-mail: cfcs@cfcs.dk

First edition, October 2020.

Purpose
This investigation report describes each stage in a typical targeted ransomware attack and presents recommendations to public authorities and private companies on how to further improve their defence against them. Although the report is written in generalised terms, the presented information is based on empirical evidence from attacks in the real world. This report is primarily intended for IT executives and IT technicians.

Summary

- Over the past few years, several Danish private companies have fallen victim of targeted ransomware attacks. The financial impact of these attacks has been significant, in some cases resulting in financial losses of several hundred million DKK.
- Everyone can become a victim of ransomware attacks, but some hackers specifically target large or critical private companies and public authorities because they expect them to be both willing and able to pay large ransoms.
- This report maps how these particularly targeted ransomware attacks unfolds and present specific recommendations on how to improve cyber security.
- Hackers often leverage phishing attacks, use compromised external remote services or exploit vulnerabilities in Internet-facing devices to gain initial access. However, hackers may also gain initial access via drive-by compromise, supply chain compromise or, potentially, also by delivery of infected removable media.
- Once hackers have access to an organization, they will typically begin their attack by staging their malicious tools, conduct network reconnaissance, spread laterally across the network and establish persistence. Subsequently, they will try to elevate their privileges to domain administrator, destroy backups and, in some cases, exfiltrate sensitive data, before deactivating security systems and deploying ransomware.
- Knowledge of the actions hackers typically conduct during targeted ransomware attacks enables public authorities and private companies to better detect and stop targeted ransomware attacks before hackers succeeds in encrypting their systems. The report presents the specific defensive initiatives that counter the impact of the most common attack techniques used by hackers during targeted ransomware attacks.

Introduction

Danish public authorities and private companies are subject to a persistent threat of targeted ransomware attacks. While stealth is the key virtue in cyber espionage, targeted ransomware attacks are designed to be loud and visible as vital systems suddenly become encrypted and a ransom note is displayed.

Everyone can become a victim of ransomware attacks, however, some hackers specifically select their targets based on their expected ability to pay large ransoms, making large or critical public authorities or private companies prime targets.

While some types of ransomware spread automatically and indiscriminately, targeted ransomware attacks require manual execution and significant efforts on the part of the hackers on their victims' internal networks. The Centre for Cyber

Security (CFCS) under the Danish Defence Intelligence Service defines these types of ransomware attacks as ”targeted ransomware attacks”, where hackers invest significant time and manual effort to encrypt vital parts of the IT-infrastructure in large or critical public authorities and private companies for extortion purposes. ”Targeted” does not necessarily denotes that the hackers select and actively target specific organizations. Rather, it means that hackers focus their time and effort to the organizations they expect are willing to pay large ransoms within their larger pool of victims from broader and more opportunistic initial compromises. Targeted ransomware attacks have been particularly on the rise in the past few years, and thus are the focus of this report.

However, targeted ransomware attacks are often not easy to pull off. Consequently, targeted ransomware attacks may take anywhere from days to weeks or even months from the initial compromise to the actual network encryption. This gives organizations a window of opportunity to detect and stop an ongoing attack before the final encryption is conducted.

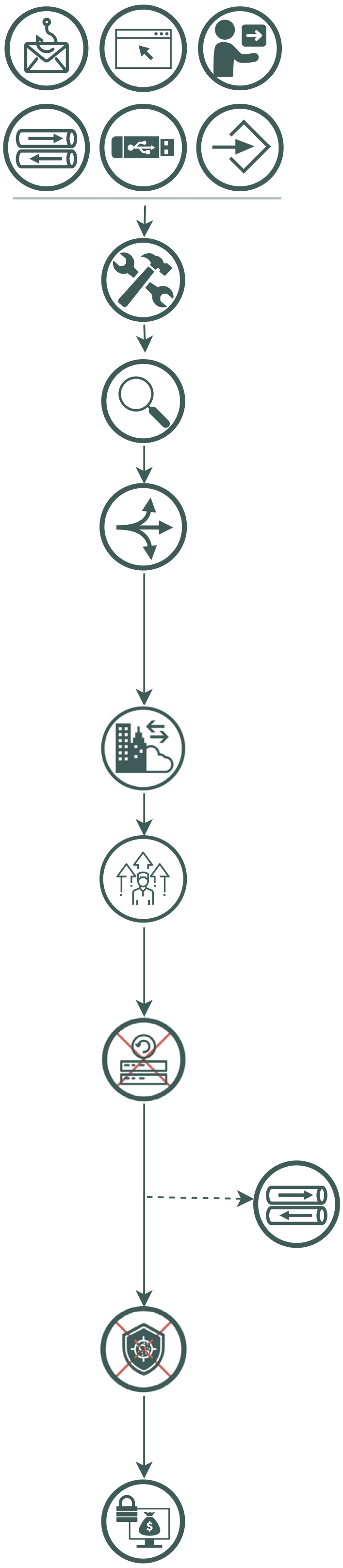
This report maps how a typical targeted ransomware attack plays out and presents specific recommendations for protective measures for public authorities and private companies to follow. Although the report is written in generalised terms, the presented information is based on empirical evidence from real attacks against Danish organizations supplemented with reports from industrial partners and a few open sources.

The report is divided into two major sections. In the first section, each stage in a typical targeted ransomware attack is described. The second section presents a number of specific defensive measures to improve cyber security. More specifically, each attack technique used by hackers is matched with the specific defensive initiatives that limit the effects of each attack technique.

A typical targeted ransomware attack

This section outlines how a typical targeted ransomware attack plays out. The attack is broken down into a number of individual phases, which combined make up the entire attack process. This division is called a “Cyber Kill Chain”, which maps out a sequence of chronologically required stages an attacker must complete to be successful. Accordingly, an attack could potentially be prevented if the hackers are stopped during merely one of the stages. The report makes references to specific ID numbers from MITRE’s ATT&CK® terminology of attack and defence techniques. MITRE is a non-profit organization engaged in cyber security, who has developed an analysis framework called ATT&CK®. The references serve as a shared frame of reference, and organizations can find additional information on each attack and defence technique on MITRE’s website. Figure 1 illustrates how a typical targeted ransomware attack plays out supplemented with ID numbers of the attack techniques most commonly used by hackers within each attack stage.

TARGETED RANSOMWARE ATTACK - STEP-BY-STEP



1

Initial access

- Phishing
- Drive-by Compromise
- Supply Chain Compromise
- External Remote Services
- Removable Media
- Vulnerability

2

Stage capabilities

- Existing malware on the system
- New malware or pen-testing tools
- Legitimate programs on the victim's computer

3

Network reconnaissance

- Scans network

4

Lateral movement

- Steals credentials
- Guesses insecure passwords
- Moves laterally with RDP among other

5

Persistence

- Legitimate remote access tools
- Malware Remote Access Tools (RATs)
- Pen-test Remote Access Tools (RATs)

6

Privilege escalation to domain administrator

- Steals credentials
- Guesses password

7

Destruction of backups

- Shadow copies
- Centralized backup solutions

8

Possible exfiltration of sensitive data

- Finds sensitive data
- Exfiltrates data

9

Deactivation of security systems

- Stops endpoint security solutions
- Interupts other systems that might hinder encryption

10

Ransomware deployment and extortion

- Encrypts systems with ransomware
- Extorts victim for ransom for decryption
- Possibly threatens to publish sensitive data online

MITRE ATT&CK®

TA0001 I Initial Access

T1566 I Phishing
T1189 I Drive-by Compromise
T1199 I Trusted Relationship
T1133 I External Remote Services
T1091 I Replication Through Removable Media
T1190 I Exploit Public-Facing Application
T1078 I Valid Accounts

TA0026 I Stage Capabilities

T1362 I Upload, install, and configure software/tools

TA0007 I Discovery

T1046 I Network Service Scanning
T1135 I Network Share Discovery

TA0006 I Credential Access

T1003 I OS Credential Dumping
T1552 I Unsecured Credentials
T1110 I Brute Force

TA0008 I Lateral Movement

T1021 I Remote Services
T1070 I Lateral Tool Transfer

TA0003 I Persistence

T1033 I External Remote Services
T1505 I Server Software Component
T1053 I Scheduled Task/Job
T1197 I BITS Jobs

TA0006 I Credential Access

T1003 I OS Credential Dumping
T1552 I Unsecured Credentials

TA0004 I Privilege Escalation

T1078 I Valid Accounts

TA0040 I Impact

T1490 I Inhibit System Recovery
T1485 I Data Destruction
T1486 I Data Encrypted for Impact

TA0010 I Exfiltration

T1041 I Exfiltration Over C2 Channel
T1048 I Exfiltration Over Alternative Protocol

TA0005 I Defense Evasion

T1562 I Impair Defenses

TA0002 I Execution

T1059 I Command and Scripting Interpreter
T1053 I Scheduled Task/Job
T1072 I Software Deployment Tools
T1047 I Windows Management Instrumentation

TA0040 I Impact

T1486 I Data Encrypted for Impact

Figure 1: The ten steps in a typical targeted ransomware attack. Each step represents a section in the report.

The hackers' first objective is to defeat their victims' external defences and establish an access into the internal network. To do so they employ an array of techniques described in more detail below. As these initial attack vectors are not exclusively used in targeted ransomware attacks, their description is relevant in understanding and countering other types of cyber-attacks as well.

> **Cybercrime is an industry**
> The initial compromise may be conducted by different actors than those carrying out the remainder of the ransomware attack. A criminal underground market exists where criminals sells accesses to each other or in other ways support each other's criminal activities. In other words, it is rarely a single actor but rather a network of specialized hackers who is behind a targeted ransomware attack.

Once the hackers have access to the internal network of an organisation, they will usually conduct an array of characteristic actions before deploying ransomware to extort their victim. Even though the tools used by the hackers during these attacks vary and are continuously developed, most targeted ransomware attacks follow the same general sequence.

Each of the ten steps in a typical targeted ransomware attack is described in more detail in the following.

1 Initial access

The hacker's first main objective is to gain initial access to their victim. The most common techniques used to gain initial access include phishing attacks, drive-by compromises, compromised external remote services, exploitation of vulnerabilities in Internet-facing systems, supply chain compromise or, potentially, delivery of infected removable media. Some of these techniques provide direct access to a victim's systems, for example via stolen login credentials, while others presuppose the deployment of malware on victim systems serving as the initial entry point. Hackers will either use the initial access themselves or sell them to other criminals. Figure 2 illustrates the most common ways hackers gain initial access to their victims in targeted ransomware attacks.

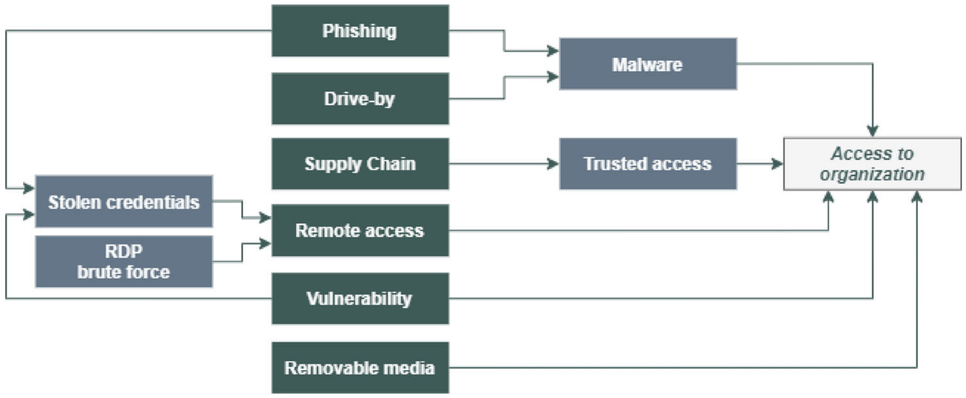


Figure 2: Typical initial access techniques.

Phishing

Phishing attacks are attempts by hackers to manipulate an individual into disclosing personal information, opening infected files or clicking on links to false websites. Sending emails to thousands of recipients is one of the most common phishing techniques, but SMS, social media or other communication platforms can also be used.

Phishing targeted at specific individuals or organizations is called spear-phishing. Here the sender has gone to great lengths to tailor a message to a specific recipient.

If unsuspecting users were to click on a link, they will often either download malware or be redirected to false websites that will attempt to trick them into disclosing personal information such as login credentials. These login credentials can then be used to access the end victim's internal network via external remote services, which is described in more detail below.

If, on the other hand, unsuspected users were to open infected attachments, they will typically download malware directly on to their computer, thereby granting the hackers access to their computer. Many of these attachments, however, require permission to allow macros to run, for instance, or the existence of vulnerabilities in the system.

While IT systems or vigilant employees usually catch the most common phishing attempts, hackers have started to use more sophisticated techniques such as ”email thread hijacking” to trick their victims. In this technique, hackers take over the email account of a business partner and responds to ongoing email conversations. The infected emails thus appear to come from a credible sender within a in continuation of existing conversations. In other words, the hackers exploit the credibility of ongoing email conversations sent from a legitimate business partner to increase the chances of victims opening the malicious attachment or clicking a link to false websites.

Hackers have used email thread hijacking to compromise several Danish victims of targeted ransomware attacks. In one incident, seven employees of a Danish organization received an email from a compromised business partner containing a malicious attachment hidden in a response to an ongoing chain of correspondence. One employee clicked on the link and downloaded a malicious file. The employee accepted the use of macros and opened the file, inadvertently starting a PowerShell script that downloaded a known banking trojan called QBot. The malware gave the hackers access to the employee's computer and served as a gateway to the rest of the network.

The April 2020 the ransomware attack on agricultural company Danish Agro also started with email thread hijacking. In an interview with Agriwatch, Danish Agro CEO Henning Haahr stated that "*the hackers took over the supplier's IT system and sent a phishing email directly from the supplier's account in response to a specific ongoing email correspondence with us. From this they gained access to our system and managed to install hacker software*".

Banking trojans exploited in targeted ransomware attacks

Banking trojans are often deployed ahead of targeted ransomware attacks. A banking trojan is malware originally designed to steal banking credentials. However, the access the malware provides is increasingly used by hackers to launch targeted ransomware attacks instead. Banking trojans have been around for many years, and criminals have established extensive networks of compromised machines. However, the attackers have learned that they can profit from selling these accesses to infected machines to other hackers, who then use them to launch targeted ransomware attacks among other.

Emotet is an example of this type of malware. Originally developed as a banking trojan, Emotet now functions as a global distribution network where selected criminal groups can gain access to infected organizations by having their own malware delivered to the victims' systems. Several cyber-criminal groups have used Emotet access to deliver their own malware, including the operators behind TrickBot and Qbot, which have subsequently deployed Ryuk and DoppelPaymer ransomware.

One of the targeted ransomware attacks against a Danish organization started exactly with the delivery of TrickBot, which gave hackers access to the victim. It is unclear exactly how the malware was delivered, but TrickBot has previously been deployed via phishing, drive-by compromises or been downloaded via the Emotet malware as mentioned. The attack resulted in encryption of large parts of the organization's vital systems with Ryuk ransomware.

Drive-by Compromise

A drive-by compromise refers to the unintentional download of malware in connection with ordinary web surfing activity. In this type of attack, hackers usually hide code on websites that can exploit vulnerabilities in the user's web browser or infect particular content on a website with malicious links. If the visitors click on the infected content, malware is downloaded.

Hackers often target popular legitimate websites or websites visited by specific groups. A targeted drive-by compromise on a chosen website is also called strategic web compromise or watering hole attack.

In regular drive-by compromises, hackers usually start by identifying one or more vulnerable websites whose visitors constitute attractive targets for the hackers. The hackers may use freely available search tools such as Shodan or similar services to scan the Internet for vulnerable web servers hosting websites. In more targeted compromises, hackers will start by identifying which websites their targets probably visit and subsequently look for vulnerabilities in the specific web servers. Alternatively, hackers sometimes build their own legitimate-looking websites to lure visitors to these websites.

If the victims download malware, hackers will gain access into their systems. Drive-by compromises have been used to distribute Dridex and similar banking trojans.

Supply Chain Compromise

A supply chain compromise is characterized by compromise via a supplier or trusted business partners. Outsourcing of services and infrastructure to third party suppliers enables organizations to focus their resources on their core activities. However, this also makes them reliant on their suppliers' cyber security measures as the suppliers typically need access to the organization's internal networks in order to deliver its services. If a supplier is compromised, the access into the organization gained by the hackers will be equal to that of the supplier. If adequate security measures are not in place, the organization's security level will thus be reduced to the lowest level among its suppliers.

Supply chain compromises may be indiscriminate in the sense that the attackers affect all of a supplier's customers or highly focused operations with predetermined targets of interest among the supplier's customers.

In a supply chain compromise, hackers will start by identifying suppliers or partners who can provide access to a lot of targets or targets of particular interest. In order to strengthen their brand, some companies boast about their customers on their websites. Hackers can use this information to direct attacks on these companies and thus their customers.

Managed Service Providers (MSPs), hosting companies and cloud service providers are attractive targets for hackers in relation to supply chain compromises. These organizations typically have direct and unfettered access to their customers' networks and are, in some cases, under less strict security precautions than are alternative accesses into an organization. For instance, the hackers behind Sodinokibi/REvil are known for targeting service providers among other.

Once hackers have identified a supplier, they will often compromise the supplier or its partners using one of the techniques described in this report.

Hackers exploit compromised business partners to launch email thread hijacking against interesting organizations which the partners communicate with via email. If, however, a supplier has direct, trusted access, hackers may look for remote administration solutions and accounts that are used by the supplier to access customer networks. Through such accesses, hackers can access customer networks with the same privileges as the supplier.

In the May 2020 targeted ransomware attacks against GlobalConnect, a supplier of fibre-based data communications and data centres, hackers not only compromised GlobalConnect itself but also several of its customers via trusted access, including the Danish pharmaceuticals procurement company Amgros.

External Remote Services

Hackers also exploit the enhanced possibilities of accessing an organization's internal network via external remote services such as Remote Desktop Protocol (RDP) or Virtual Private Network (VPN). Generally, hackers exploit external remote services in three different ways.

The first two involve stolen login credentials. Disguised as a legitimate employee, hackers use stolen credentials to access their victim's network via remote access solutions.

In the first technique, hackers launch phishing campaigns to trick victims into disclosing login credentials, which the hackers can then exploit to gain access into victim networks.

The second technique involves exploitation of vulnerabilities in the external remote services themselves to obtain login credentials from the target's employees. In 2019, a vulnerability in the VPN solution Pulse Secure Connect was detected (CVE-2019-11510). This particular vulnerability allowed hackers to download usernames and passwords in plaintext directly of the organization's VPN server.

In a targeted ransomware attack on a Danish organization, hackers exploited this particular vulnerability to steal VPN login credentials from several of the organization's employees, enabling them to access the organization's internal network disguised as a legitimate user.

In the third and final technique, hackers exploit vulnerable RDP solutions. Hackers exploit the fact that some RDP connections do not use an RDP Gateway or a VPN connection. Port 3389 is left directly open to the Internet, which in practice means that not only the organization's employees but everyone with Internet connection can try to log in to the target computers. However, this technique presupposes that the attacker knows the IP address of the device with an open port.

Hackers often start this final type of attack by scanning the Internet for open 3389 ports. This is easily done with tools such as Masscan.exe that can scan the entire Internet for open 3389 ports in less than six minutes. Hackers also use open databases such as Shodan, where this kind of information is readily available. The result of the scans provides a list of potential victims.

In the absence of extra security measures, a single password is typically all that holds the hackers at bay. Hackers can make a computer try to guess the password until it finds the right one – a technique known as brute force. If the password length and complexity are not sufficient, a computer may be able to guess a password very quickly. Alternatively, hackers may launch so-called 'password spraying' attacks in which they attempt to guess fewer but particularly popular passwords against a large number of accesses. The latter approach may be used if an organization has set up an account lockout threshold. Once the right password has been cracked, hackers can connect directly to the organization's internal network.

Because RDP accesses are relatively easy to compromise, they are among the most inexpensive and widely available accesses sold on the cybercriminal market. The CFCS has repeatedly warned against the use of RDP. As of September 2020, there are still more than 4,500 potentially vulnerable units with open 3389 ports to the internet in Denmark alone and more than four million worldwide.

Removable Media

External remote media such as USB devices are useful when it comes to transferring files from one machine to another. However, hackers may also distribute infected USB devices that deliver malware if plugged into the computer.

The CFCS is not aware of any targeted ransomware incidents in which USB devices have been used to create the initial compromise. However, infected USB devices are regularly used making it relevant to pay attention to this technique, including the in-house USB policies.

Vulnerability

The final technique, which is often used to gain initial access to organizations, involves the exploitation of vulnerabilities in Internet-facing systems. Though exploitation of vulnerabilities is a sub element in other techniques, it also represents an independent attack vector to gain initial access.

For example, drive-by compromises sometimes require hackers exploiting vulnerabilities in the visitors' web browsers. As described, hackers may also find vulnerabilities in the external remote services themselves, potentially providing them with access to internal networks via VPN solutions. However, other vulnerabilities function independently of the other techniques describes above and thus constitute an independent compromise path.

In 2019, a vulnerability in the Citrix network equipment was identified (CVE-2019-19781) that allowed hackers to deliver malware to organizations directly over the Internet. It did not take long from the vulnerability was disclosed till numerous hacking attempts on Citrix equipment were observed.

Hackers continuously look for vulnerabilities that can be used to compromise organizations. Vulnerabilities are usually published on online forums or on supplier websites, for instance in connection with security patches. Patching of vulnerabilities is thus a double-edged sword as publication of the patch is necessary in order for cyber security personnel to update their systems. However, this also makes hackers aware of the vulnerabilities, which they can try to locate and exploit. Until a patch becomes available, it is thus a race between hackers trying to locate and exploit the vulnerabilities on the one side and security personnel deploying a patch to fix them on the other. Hackers have been known to exploit vulnerabilities only days following their disclosure. Unfortunately, CFCS experiences that security updates are often ignored or not prioritized. Many organizations are thus compromised via known vulnerabilities, some of which have been around for years and could be patched with existing security updates.

In the investigation report ”Hackers remember the vulnerabilities we forget” an in-depth description can be found of how a Danish organization was compromised five times in two years by hackers exploiting an old known vulnerability. The report is available on CFCS' website.

With access to an organization, some hackers choose to sell it to other hackers who use it for their own criminal purposes. Regardless of whether the original hackers or new hackers launch the rest of the targeted ransomware attack, they will typically start by downloading or configuring the tools they expect to use during their deeper attack on the organization's internal networks.

2 Stage capabilities

Even though the hacker's toolkit is ever-changing, we may generally divide them into the following three types of tools typically employed during targeted ransomware attacks:

- **a.** Existing malware on the system.
- **b.** New malware or pen-testing tools.
- **c.** Existing legitimate programmes on the victim's computer.

a. If hackers have cooperated with other criminals to have their own malware delivered via their malware, hackers can exploit the functions offered by their initial malware right from the start. Emotet, for example, has delivered TrickBot, which consists of a number of independent modules with a wide array of functions that the hackers can use. Even though hackers have access to functions in such already existing malware, they will often supplement these with additional malware or other tools.

b. If hackers do not have access to the organization via existing malware, they must download all the tools themselves. This may be the case where hackers have gained access via stolen login credentials to valid accounts with RDP or VPN.

Download and execution of new malware or pen-testing tools sometimes require local administrator privileges. If hackers only have user rights, they will try to escalate their privileges, allowing them to download and put together their own toolkit. This usually further enables them to spread in the network at a later stage. Much of the malware deployed to provide initial access have built-in functions to escalate privileges, allowing hackers to download additional tools. If hackers do not have access to such capabilities, they will typically try to exploit vulnerabilities instead or use other techniques capable of bypassing such restrictions, ultimately allowing them to download additional tools anyway. Hackers typically choose to download the following tools as supplements to existing malware:

- Additional banking trojans.
- Reconnaissance tools.
- Credential stealers.

In many targeted ransomware attacks, hackers have chosen to download several of the types of banking trojans, which have regularly been improved with extra features over the years. The actors behind the BitPaymer ransomware, for example, have used Emotet as a payload delivery service to deliver their own banking Trojan, Dridex, which they have subsequently used to launch ransomware attacks. These supplementary banking trojans or other types of malware typically have different built-in credential-stealing or persistence capabilities that the hackers can use and are continuously updated.

Reconnaissance tools are another type of tools often downloaded by hackers. Once hackers gain access to an organization, they often do not know exactly in which section of the network they have entered or what they have access to. Consequently, they need network scanning tools. Network scanners or related tools also enable hackers to find ways to move laterally in the network and identify the highly privileged accounts that hold the keys to compromise the entire network. Network scanners include legitimate network scanners but also pen-testing tools like Nmap, Process Hacker or BloodHound as evidenced in a number of recent ransomware attacks.

The third and last type of tool, which is almost always downloaded by hackers is a credential stealer, unless they already have access to one such tool built into existing malware. If hackers hope to launch a successful targeted ransomware attack, they need the capability to spread in the network and take over privileged accounts. Credential stealers are often the preferred means to this end. Along with network scanners, credential stealers are thus usually used to locate and steal login information. Mimikatz is a particularly popular credential stealer currently used in numerous targeted ransomware attacks. Other popular credential stealers and techniques include LaZagne and ProcDump.

c. Many of the tools used by hackers are dependent on legitimate programmes already on the computer. More specifically, hackers exploit the fact that computers are increasingly “born” with sophisticated programmes, which they can use directly or indirectly for nefarious purposes. PowerShell, Windows Command Shell, Windows Management Instrumentation (WMI), PsExec and RDP often come pre-installed, and are frequently exploited by hackers during targeted ransomware attacks.

This attack technique is also called ”Living-off-the-Land” as it involves leveraging legitimate tools already present for malicious purposes. The technique makes it difficult to distinguish between legitimate and malicious activity. For in-depth description of the threat of abuse of legitimate programmes see the threat assessment ”Hackers leverage legitimate programmes in cyber attacks”, which is available on CFCS’ website.

③ Network reconnaissance

With their tools at hand, hackers will often scan the network to find ways to move laterally to other clients and servers.

Hackers typically scan the network using legitimate network scanners or pen-testing scanners, which in some cases are supplemented with more specialized network monitoring programmes such as Process Hacker or BloodHound. These scans can generate lists of open ports on particular devices and servers in the network. An open port means that the units is “listening” to communication on that particular port. Because specific services communicate over specific ports, hackers are able to figure out which services can be used to communicate with other devices in the same network.

An open 3389 port usually means that you can communicate over Remote Desktop Protocol (RDP). Server Message Block (SMB) is another widely used service that is used by numerous organizations for file sharing. SMB operates over port 445 or 139 in older versions. Both ports will typically be open in most organizations. Legitimate network administrators use RDP to administer devices and servers in the network, and SMB facilitates file access, which most organizations rely on – a fact that hackers know and exploit to move laterally in the network.

4 Lateral movement

Armed with an overview of devices and servers with open ports, hackers will often try to move laterally across the network. One of the ways they usually try to move laterally is by trying to log into other devices or servers using local admin credentials via RDP over port 3389. When an administrator establishes connection to a device or server, they must verify their identity with a password. Administrators thus have to keep track of every password for all devices in a network, which may be as many as hundreds or thousands of individual passwords depending on the network, and thus prove a challenging task for the administrators. Consequently, passwords tend to be similar or very predictable across devices and servers, posing a great security risk if hackers are able to guess or otherwise gain access to the passwords. If this happens, hackers are free to establish connections to the devices or servers on the network with administrator rights.

This is usually where credential stealers are used. Hackers among other use credential stealers to steal the password for the local administrator account on the first compromised machine if they do not already have it. Hackers often use Mimikatz, which is capable of extracting passwords from a computer’s memory in clear text. Other techniques to steal login credentials include LaZagne and ProcDump. With access to the password from the first device, hackers will typically test the password on other devices with open port 3389 in the network to gain access via RDP. Hackers have been known to test hundreds of password combinations if the password, for example, seems to be a sequence of numbers. For instance, if the password on the first compromised machine is ’Admin112’, hackers will try every combination of numbers after ’Admin’ until they find the right one. They can subsequently repeat this technique on other machines connected to the network. If successful, they can move freely between the machines with privileged rights.

Every Windows 7 computers at a Danish victim all used the same local administrator password. Hackers was able to take advandtage of this to move freely between the computers via RDP among other.

Exploitation of vulnerabilities offers another possibility of lateral movement. Usually this form of lateral movement is associated with so-called cryptoworms, which is a special kind of ransomware that automatically exploits vulnerabilities to move laterally, encrypting systems as it moves through them. Unlike targeted ransomware attacks that require manual deployment, cryptoworms operate autonomously once it is deployed to a device. WannaCry is the most famous example of a cryptoworm, which managed to cripple thousands of computers worldwide in 2017 using the EthernalBlue/DoublePulsar SMB vulnerability to spread globally.

5 Persistence

Having gained access to compromised accounts across the network, hackers will usually cement their presence in the network by establishing several entry points into the victim's network to safeguard their presence in case one access is lost. If, for instance, hackers gained access to an organization via stolen login credentials and the particular employee changed his/her password, the hackers would lose access to the network. Generally, hackers use three different types of extra external accesses into an organization's network.

- Legitimate remote access services.
- Malware Remote Access Tools (RATs).
- Pen-testing Remote Access Tools (RATs).

Exploitation of legitimate remote access services is one of the most widely used techniques to establish persistence. Again, RDP is sometimes exploited, where hackers intentionally open an external port thus allowing any computer with Internet connection to access it. Hackers have also been known to download commercial remote access systems such as TeamViewer or similar systems, which provide hackers with an alternative entry point into the system.

A second technique to establish persistence is malware-based, where hackers for instance place so-called web shells that opens an external access via the Internet. In April 2020, the US National Security Agency (NSA) and the Australian Signals Directorate (ASD) published an in-depth report on web shells, which is available on their websites.

Web shells
A web shell is a piece of code hidden in a file that enables remote access via the Internet.

Web shells thus function as so-called "Remote Access Tools" (RAT), enabling hackers to read, write, change, download or delete files on a server.

A final technique involves exploitation of pen-testing tools with built-in remote access functions. For example, hackers have been known to hide the pen-testing tool CobaltStrike on more than ten different computers during the same attack, which opened backdoors for the hackers. In addition, several pen-testing tools facilitating persistence have been built in a number of hacker malware.

6 Privilege escalation to domain administrator

Having established several backdoors into an organization's network, the hackers now begin the hunt for the crown jewels of the organization: Administrator access to Active Directory on the Domain Controller Server. Domain Control Servers are the heart of most organization networks. They provide access to the entire domain of the organization from where hackers can control large parts of the organization's IT infrastructure. These privileges are extremely valuable to hackers with the ambition to launch a paralyzing ransomware attack. Instead of having to gain access to each device and server in the network, hackers with administrator access to a Domain Controller can deploy ransomware to the entire domain in one sweep. Domain administrators with access to Domain Controllers are thus highly attractive targets for hackers, and their accounts should be given special protection.

Hackers first face the challenge of identifying these highly privileged accounts. Hackers often use the same tools that they initially used for network scanning supplemented with specialized tools, including the open-source tool BloodHound, to locate these accounts. BloodHound is a tool capable of quickly mapping an organization’s hierarchy of privileged accounts and has a very user-friendly graphical user interface, allowing hackers to plan how to most effectively compromise different users with higher privileges in order to gradually seek out domain administrators.

If BloodHound or a similar tool fails to expose the domain administrators, hackers will typically wait for domain administrators to expose themselves. Hackers may hide on compromised devices and regularly check for active RDP connections. As mentioned, RDP is not used exclusively for external remote access but also internally by legitimate administrators to make changes to the user systems. By regularly keeping an eye out for active RDP connections, hackers are able to identify accounts with administrator privileges, which they can target.

Once the hackers have identified privileged accounts, they typically gain access to them by stealing their login credentials. This sometimes happens when administrators establish RDP connections to devices that have already been compromised. If the administrators connect to the devices via RDP, their login credentials may be stolen as the connection has to be authenticated by a login from the administrator. This login exposes their login credentials to the hackers. The hackers thus wait patiently for the RDP connections to be established and continuously steal login credentials, hoping that a domain administrator account might pop by one day. Mimikatz is a particularly popular credential stealer currently used in many targeted ransomware attacks. However, attackers also use credential dumping such as LaZagne and ProcDump to gain access to login credentials.

In some cases, hackers create new domain administrator accounts once they have gained access to the Domain Controller. They do this partly to bypass logging, and partly to avoid being locked out in case the compromised domain administrator decides to change password.

7 Destruction of backups

Armed with the keys to the kingdom in the form of domain administrator privileges, hackers will often make sure that their attacks cannot be mitigated merely by rebooting their systems from backups. If hackers have domain administrator rights, backups are typically the best bet to combat a crippling ransomware attack.

Domain administrator privileges provides access to the entire network, enabling the hackers to quickly map and access the entire data infrastructure of the organization. Often the data infrastructure has already been mapped by the organization itself to facilitate updates, but alternatively PowerShell scripts or integrated search strings within the Active Directory user interface are used to generate a complete list of every device in the domain.

Backups are usually stored both locally on the individual device, i.e. shadow copies, and on a centralised backup solution. Attackers will attempt to either delete or encrypt these systems.

Hackers will typically access the local backup files with legitimate programmes such as PowerShell or Windows Management Instrumentation (WMI) and subsequently delete shadow copies with VSSADMIN.EXE or WMIC.EXE.

Central backup systems come in many different varieties, but hackers will actively seek to render them inoperable. If hackers fail to access these backups directly, they have been known to encrypt backups for longer periods of time before encrypting the rest of the organization’s systems in an effort to increase data losses and thus raise the incentive to pay the ransom. Some hackers have even timed the encryption of the systems to start while backups are ongoing.

8 Possible exfiltration of sensitive data

In late 2019, a new trend started to emerge in which hackers threatened to leak sensitive information from their victims if the ransom was not paid. In other words, hackers increasingly started using the deep insight they gained into their victims’ organization to exfiltrate data and extort them even further. Several criminal groups threaten to publish sensitive data on public Internet sites if the victims fail to pay ransom. Others tries to sell the information to interested buyers. Most recently, the Sodinokibi/REvil operators have launched an online auction site selling stolen victim data to the highest bidder. Some organizations have even been extorted into paying ransoms in exchange for the hackers “promising” to delete the stolen data without any guarantees of this actually happening.

Data exfiltration may occur in a number of ways, for example through the extra backdoors or malware hidden in the network by the hackers. In 2019, an IT security company came across a new tool called Sidoh, which has been used for data exfiltration purposes in connection with targeted ransomware attacks. The tool searches for specific keywords such as ”Spy”, ”Government” and ”Secret” and exfiltrate documents containing these or similar words.

9 Deactivation of security systems

Right prior to the deployment of ransomware, hackers will typically deactivate antivirus and other security systems on the individual devices to make sure that the ransomware is not detected and disabled on the machines.

Windows’ TASKKILL.EXE or Net Stop commands are often used, while others use commercial solutions such as ProcessHacker, PCHunter, PowerTool x64, GMER, Total Uninstall Portable or Defender Control to this end. Such commands are relatively easy for hackers to deploy as they already have the highest possible privileges within the domain.

In addition to stopping antivirus and other security systems, the hackers also stop other processes that could possibly prevent encryption, such as Exchange Servers and SQL Servers.

10 Ransomware deployment and extortion

Only at this stage, do the hackers deploy ransomware and encrypt systems across an organization. The encryption itself does not take long and is often carried out over night when system administrators are usually not aware. In the morning, compromised staff will have been locked out of their systems, receiving a message that their encrypted data is held hostage for a ransom.

Sometimes hackers set a specific time delay on the encryption to make it appear as though the encryption came out of nowhere.

Hackers typically spread their ransomware through legitimate programmes such as PsExec in Microsoft SysInternals, a logon-logoff script via Group Policy Object (GPO) or Windows Management Interface (WMI).

It is important to bear in mind that although ransomware and the criminal landscape are constantly evolving, most types of ransomware use the same encryption algorithms that are used to secure regular online communication. Even though the encryption mechanisms themselves are very similar across different types of ransomware, knowing the particular type of ransomware used in an attack might help in the efforts to remediate an attack as each hacker group usually use a particular ransomware and, to some extent, uses the same techniques across cases.

Even though the type of ransomware victims is hit by varies, the hackers typically leave nearly identical ransom notes with instructions and demands trying to convince organizations that their files are now inaccessible but that access may be restored if they pay a ransom. Some leave email addresses for direct communication. Hackers typically want the ransom to be paid in cryptocurrency such as Bitcoin or Monero via a TOR browser in order to seek to maintain anonymity. The victims are sometimes put under time pressure, meaning that the ransom increases the longer it takes for the victim to pay, raising the incentive to pay the ransom quickly.

In the effort to achieve the largest ransom possible and maximize the likelihood of an actual payment, hackers carefully adjust the size of ransoms to reflect the size and characteristics of the targeted organization. More specifically, several hacker groups carefully weigh the ransom amounts against the organization’s earnings base and significance to society. The amounts vary from a few hundred thousand to two-figure million USD in targeted ransomware attacks. According to some security companies, the amount may sometimes be negotiated down.

Hackers typically employ the same strong encryption algorithms used to secure everyday online communication. For this very reason, it is not possible to decrypt files without using the hackers’ decryption key, despite several online decryption services advertise of such services. However, in some instances security experts have managed to find errors in the hackers’ implementation of the algorithms, which sometimes lead to solutions that may lead to ways to decrypt files. This is a relatively rare scenario, though, and hackers quickly learn from their mistakes and correct their errors along the way. Together with a number of companies, Europol has put together a list of decryption tools that are actually capable of decrypting some of the older types of ransomware. The site can be reached at: https://nomoreransom.org.

The CFCS generally recommends that organizations do not pay the ransom.

Payment of the ransom perpetuates criminal activities, and paying the hackers does not guarantee that an organization will actually regain access to their data. In some cases, hackers do not provide the decryption key despite the victims actually paying the ransom. In other cases, the victims' data has not just been encrypted but deleted, rendering restoration impossible. Hackers have also been known to encrypt the same systems more than once, meaning that even if they did provide a decryption key, the victims would only be able to decrypt the first layer of encryption, leaving the rest of the data inaccessible.

In addition, an important issue to raise is that decryption using keys may take as long as recreating the data from backups. Furthermore, it is important to bear in mind that hackers have probably hidden backdoors across the network that still have to be removed even if ransom is paid. Even if a victim chooses to pay for decryption keys, decrypting every single machine and removing potential backdoors are a difficult and time-consuming task.

If possible, restoration through backup is preferable. However, awareness must be on the risk of copying the backdoors during the restoration process. This happens if the hackers were already present in the systems when the backup was run. Consequently, it is important to ascertain the exact time when the hackers initially gained access to the system and then subsequently recreate the system with a backup created prior to this time.

Preservation of data credibility is also a key element to consider. A successful targeted ransomware attack typically allows hackers to access and manipulate sensitive data. If, for example, the target is a hospital, it may prove very important to establish whether data credibility in patient files for example, has been preserved or not.

Although every target ransomware attack is unique and each stage could vary in sequence or be repeated several times, most attacks follow the steps described in this report. Knowing how the hackers act when they enter a network provides the best basis for protecting against them. In the final part of this report, we bring this knowledge described above in play to provide specific recommendations that may help public authorities and private companies to improve their defence against targeted ransomware attacks.

How to defend against targeted ransomware attacks

In this final section we match the attack techniques most commonly used in the real-world targeted ransomware attacks this report is based upon with the specific defensive measures that counter them.

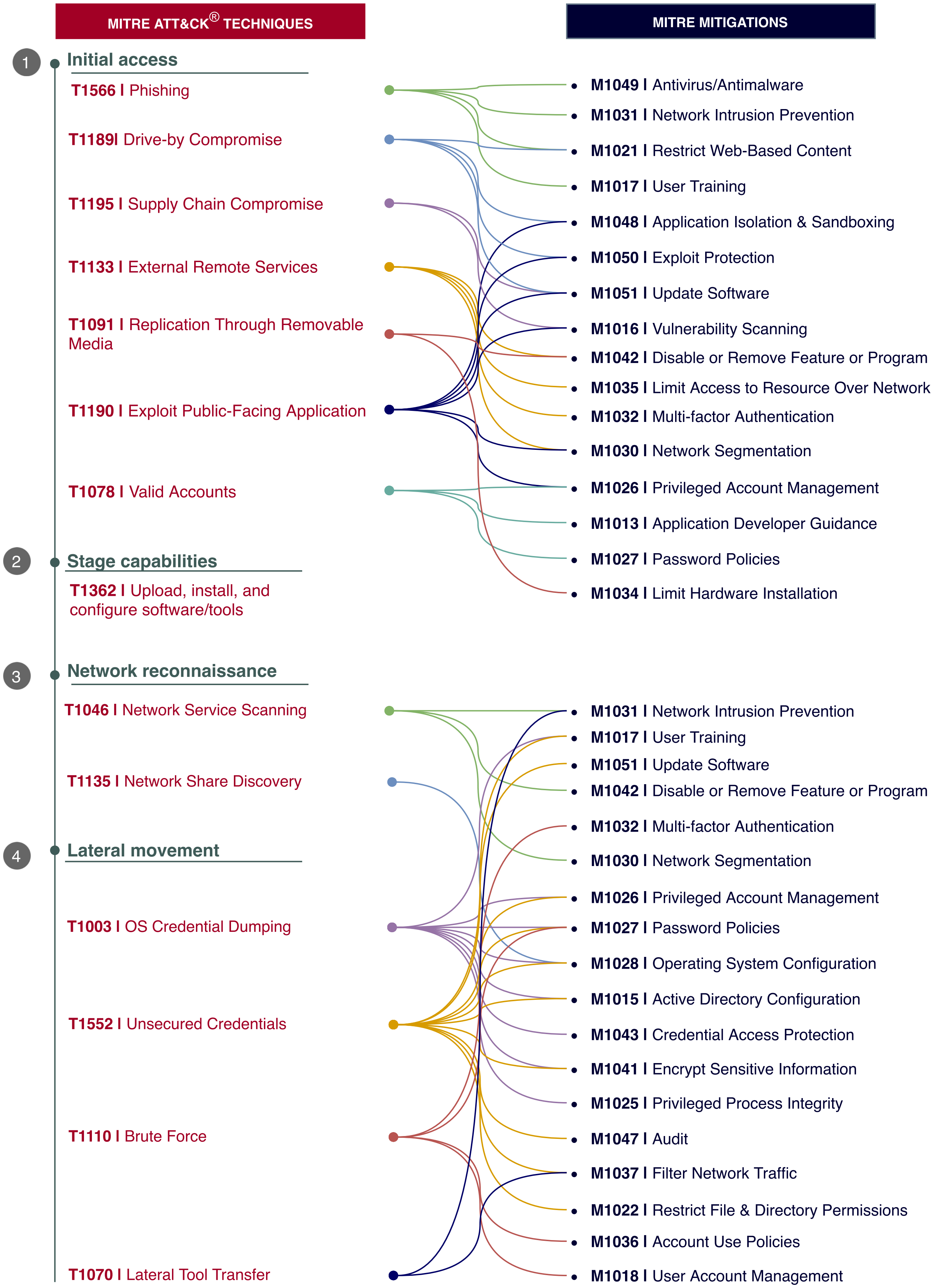
The pairing of attack techniques and defensive measures are based on MITRE's ATT&CK® framework. Organizations could use the illustrations in figures 3-5 actively in their cyber defence as guidelines on how to improve their defence in every stage of a typical targeted ransomware attack. As no attacks or organizations are identical, the measures should be adjusted to fit the individual organization's systems, policies and processes and not be considered exhaustive. The defence recommendations are specifically adapted to large private companies and public institutions.

The measures are based on the "defence in-depth" principle, meaning that rather than relying on a single security solution, organizations should utilize a multi-layered security approach that ensures that even if one layer is breached, other layers of security will prevent an attack. This will improve the chances of detecting, stopping and limiting the consequences of an attack.

There are a number of basic security initiatives that need to be in place first. These initiatives are described in the guide "Cyberforsvar der virker", which is available on CFCS' website [only in Danish].

As this report is primarily based on ransomware attacks in Microsoft-based environments, the following general recommendations for Microsoft environments could advantageously be incorporated into the general security recommendations:

- **Best practices for securing Active Directory**
  This guideline contains Microsoft's recommendations on how to reduce the attack surface of Active Directory (AD), secure privileged accounts/groups and administrator workstations, and establish secure Domain Controllers, as well as recommendations on logging and monitoring.
- **Windows security baselines**
  These baselines contain Microsoft's recommended security configuration settings and could be used as a guide line when creating the specific setup requested by an organization. The Policy Analyzer Tool, which is a utility included in the Microsoft toolkit, can be used to compare sets of Group Policy Objects with Microsoft's recommended baseline or other Group Policies.



MITRE ATT&CK® TECHNIQUES

1 Initial access

T1566 I Phishing

T1189I Drive-by Compromise

T1195 I Supply Chain Compromise

T1133 I External Remote Services

T1091 I Replication Through Removable Media

T1190 I Exploit Public-Facing Application

T1078 I Valid Accounts

2 Stage capabilities

T1362 I Upload, install, and configure software/tools

3 Network reconnaissance

T1046 I Network Service Scanning

T1135 I Network Share Discovery

4 Lateral movement

T1003 I OS Credential Dumping

T1552 I Unsecured Credentials

T1110 I Brute Force

T1070 I Lateral Tool Transfer

MITRE MITIGATIONS

- **M1049 I** Antivirus/Antimalware
- **M1031 I** Network Intrusion Prevention
- **M1021 I** Restrict Web-Based Content
- **M1017 I** User Training
- **M1048 I** Application Isolation & Sandboxing
- **M1050 I** Exploit Protection
- **M1051 I** Update Software
- **M1016 I** Vulnerability Scanning
- **M1042 I** Disable or Remove Feature or Program
- **M1035 I** Limit Access to Resource Over Network
- **M1032 I** Multi-factor Authentication
- **M1030 I** Network Segmentation
- **M1026 I** Privileged Account Management
- **M1013 I** Application Developer Guidance
- **M1027 I** Password Policies
- **M1034 I** Limit Hardware Installation

- **M1031 I** Network Intrusion Prevention
- **M1017 I** User Training
- **M1051 I** Update Software
- **M1042 I** Disable or Remove Feature or Program
- **M1032 I** Multi-factor Authentication
- **M1030 I** Network Segmentation
- **M1026 I** Privileged Account Management
- **M1027 I** Password Policies
- **M1028 I** Operating System Configuration
- **M1015 I** Active Directory Configuration
- **M1043 I** Credential Access Protection
- **M1041 I** Encrypt Sensitive Information
- **M1025 I** Privileged Process Integrity
- **M1047 I** Audit
- **M1037 I** Filter Network Traffic
- **M1022 I** Restrict File & Directory Permissions
- **M1036 I** Account Use Policies
- **M1018 I** User Account Management

Figure 3: Attack techniques and defensive mitigations - phase 1-4

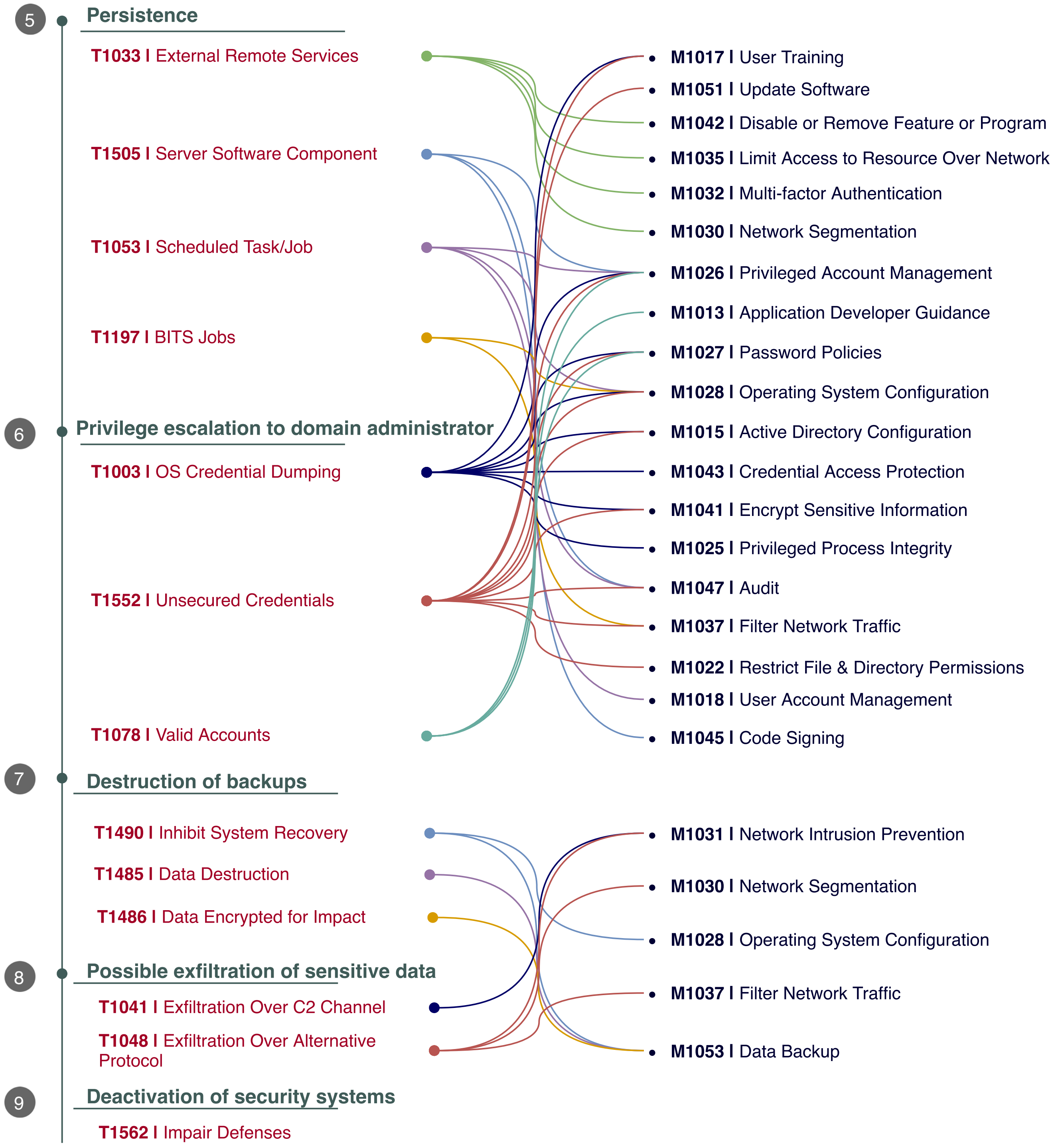

5
Persistence
T1033 I External Remote Services
T1505 I Server Software Component
T1053 I Scheduled Task/Job
T1197 I BITS Jobs
6
Privilege escalation to domain administrator
T1003 I OS Credential Dumping
T1552 I Unsecured Credentials
T1078 I Valid Accounts
7
Destruction of backups
T1490 I Inhibit System Recovery
T1485 I Data Destruction
T1486 I Data Encrypted for Impact
8
Possible exfiltration of sensitive data
T1041 I Exfiltration Over C2 Channel
T1048 I Exfiltration Over Alternative Protocol
9
Deactivation of security systems
T1562 I Impair Defenses
M1017 I User Training
M1051 I Update Software
M1042 I Disable or Remove Feature or Program
M1035 I Limit Access to Resource Over Network
M1032 I Multi-factor Authentication
M1030 I Network Segmentation
M1026 I Privileged Account Management
M1013 I Application Developer Guidance
M1027 I Password Policies
M1028 I Operating System Configuration
M1015 I Active Directory Configuration
M1043 I Credential Access Protection
M1041 I Encrypt Sensitive Information
M1025 I Privileged Process Integrity
M1047 I Audit
M1037 I Filter Network Traffic
M1022 I Restrict File & Directory Permissions
M1018 I User Account Management
M1045 I Code Signing
M1031 I Network Intrusion Prevention
M1030 I Network Segmentation
M1028 I Operating System Configuration
M1037 I Filter Network Traffic
M1053 I Data Backup

Figure 4: Attack techniques and defensive mitigations - phase 5-9

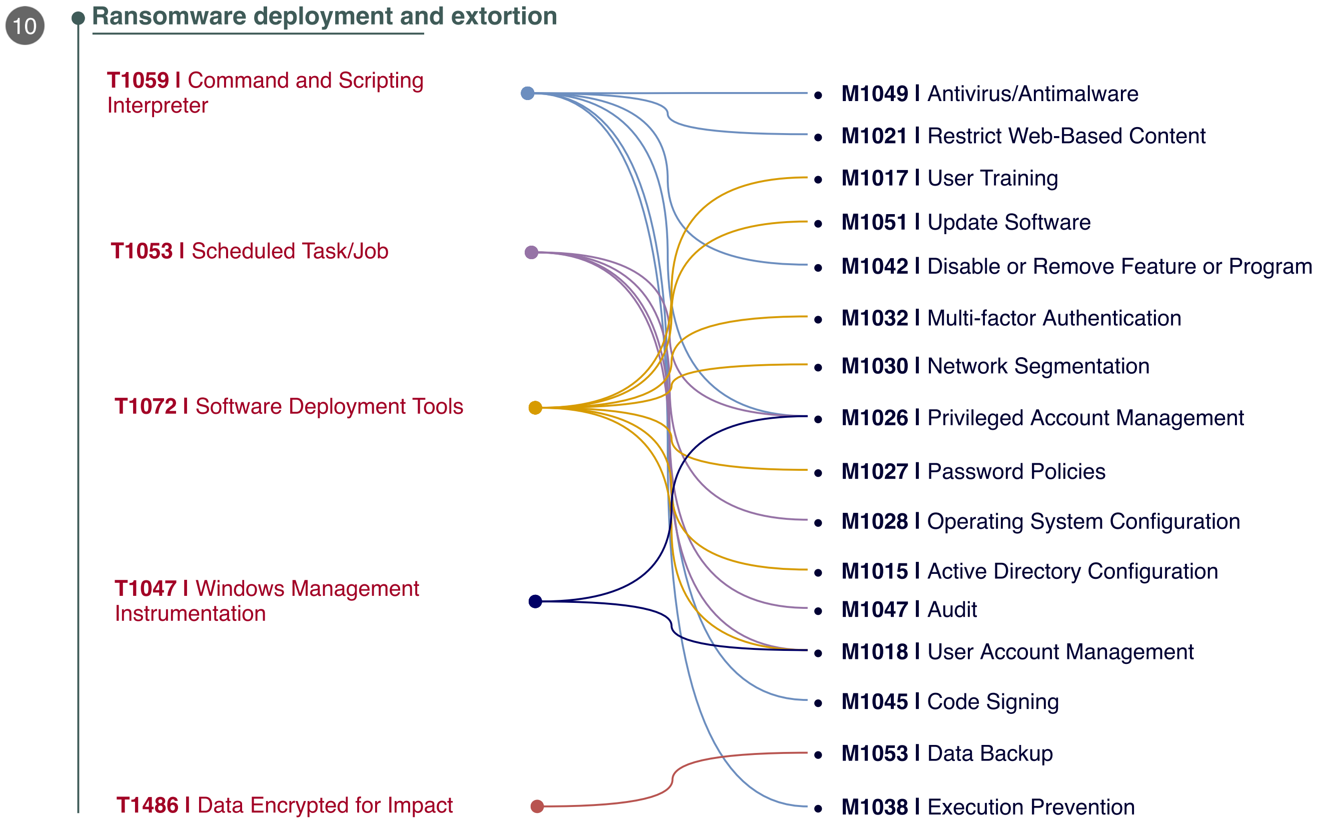

10
Ransomware deployment and extortion
T1059 I Command and Scripting Interpreter
T1053 I Scheduled Task/Job
T1072 I Software Deployment Tools
T1047 I Windows Management Instrumentation
T1486 I Data Encrypted for Impact
M1049 I Antivirus/Antimalware
M1021 I Restrict Web-Based Content
M1017 I User Training
M1051 I Update Software
M1042 I Disable or Remove Feature or Program
M1032 I Multi-factor Authentication
M1030 I Network Segmentation
M1026 I Privileged Account Management
M1027 I Password Policies
M1028 I Operating System Configuration
M1015 I Active Directory Configuration
M1047 I Audit
M1018 I User Account Management
M1045 I Code Signing
M1053 I Data Backup
M1038 I Execution Prevention

Figure 5: Attack techniques and defensive mitigations - phase 10

M1013	Application Developer Guideline
Description and advice	Ransomware attackers target account credentials anywhere they can. Thus, it is essential that applications do not store sensitive data or account credentials insecurely, for example account credentials in clear text in code, in version control/source code tools or configuration files. System administrators and application developers should always ensure that account credentials are stored and handled securely.
Recommendations	
Further reading	https://cfcs.dk/en/forebyggelse/vejledninger/passwords/

M1015	Active Directory configuration
Description and advice	Configure Active Directory to reduce the risk of compromise of login credentials through techniques used in connection with ransomware attacks. For example, avoid storing login credentials in the registration database and logging on to clients with Domain Administrator accounts. If the resources are available, Kerberos events could be monitored in order to detect pass-the-hash attacks. If an organization has access to Azure ATP, it could be used for monitoring. If AD compromise is suspected, the KRBTGT password should be changed immediately and on a regular basis, for example once a year. The KRBTGT account is used to encrypt and sign all Kerberos tickets for the domain. Be aware that the KRBTGT password should be changed twice in order to reset existing Kerberos tickets.
Recommendations	• Use accounts with no redundant user rights for remote support of clients.
Further reading	https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/ https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard https://www.microsoft.com/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/

M1016	Vulnerability scanning
Description and advice	Regular vulnerability scans of internal as well as Internet-facing networks could help identify vulnerabilities. Identified vulnerabilities could then be addressed before malicious actors can leverage them. Vulnerability scans could be supplemented by actual penetration tests in which security experts actively try to identify and exploit vulnerabilities. In several of the analysed incidents described in this report, the initial compromise happened through exploitation of known vulnerabilities that could have been identified through a vulnerability scan.
Recommendations	• Conduct regular scans of Internet-facing systems and applications. • Conduct regular scans of internal networks and systems.

	• Have security experts conduct penetration tests of new and existing systems and networks. • Monitor third party components for publicized vulnerabilities.
Further reading	https://owasp.org/www-community/Vulnerability_Scanning_Tools https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment https://www.zaproxy.org https://owasp.org/www-project-dependency-check https://cve.mitre.org https://nvd.nist.gov
M1017	**User Training**
Description and advice	In addition to technical security measures, security conscious users are the strongest line of defence against ransomware. In many ransomware incidents, initial access was achieved using credentials harvested from successful phishing attacks. Users should continuously be trained in recognizing signs of phishing and social engineering tricks. All users and administrators should be familiar with in-house password policies and avoid password recycling.
Recommendations	
Further reading	https://www.ncsc.gov.uk/collection/you-shape-security https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/user-education-and-awareness https://www.social-engineer.org/framework/attack-vectors/phishing-attacks-2/ https://cfcs.dk/en/forebyggelse/vejledninger/passwords/
M1018	**User Account Management**
Description and advice	User account management is crucial in the fight against ransomware attacks. Having a clear user account policy describing how accounts are provisioned, maintained and disabled can help reduce the attack surface. Self-monitoring is a key tool for ensuring implementation of the processes and policies. Also, it is important to eliminate unnecessary user privileges that could be leveraged by hackers if the account was to be compromised. To this end, the Least-Privilege principle could be applied that states that any user, programme or process should only have the bare minimum of privileges required to perform its function. Respond quickly and proactively reset passwords to accounts that have been used in connection with leaked credentials. Do it as soon as the breach – or brute force attempt – is detected.

Recommendations	• Establish a clear policy with well-defined processes and administration of user accounts and privileges. • Administrator privileges should only be assigned to users temporarily and on a case-by-case approach based on if they actually have an operational need or not.
Further reading	https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
M1021	**Restrict Web-Based Content**
Description and advice	The initial malware infection in connection with a ransomware attack often happens by tricking the user into visiting a malicious website or downloading and running an unwanted script or application (Potentially Unwanted Application). An effective link in the defence chain may thus be to block access to known malicious websites and prevent the downloading and execution of bad files (application control). From a security perspective, it may also be worth considering blocking ads in the users' browser.
Recommendations	• Limit the users' possibility of running scripts based on file type or application control. • Monitor and respond to alarms on attempts to run blocked scripts and applications. • Use a secure DNS service or implement another solution to block access to malicious websites.
Further reading	https://support.microsoft.com/en-us/help/4562299/protect-your-pc-from-potentially-unwanted-applications https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control
M1022	**Limit file and directory permissions**
Description and advice	To avoid detection, hackers will often try to deactivate security measures such as antivirus and Endpoint Detection and Response (EDR) and hide their tracks by deleting logs. It should thus be confirmed that users do not have permission to change files in critical application or system folders. In addition, users should not have permission to change or delete logs, which could be used to detect ongoing malicious activities or to investigate previous breaches. Similarly, access to shared folders should only be granted on a strictly necessary basis in order to minimize the risk that a compromised account is used to harvest other login credentials or gain access to private encryption keys on common drives, for example. The Sysinternals Accesschk and AccessEnum could potentially be used to identify folders and show which users have been granted access.
Recommendations	• Restrict user's permission to reset or delete logs. • Monitor and respond to alarms on attempts to access protected folders. • Monitor and respond to alarms on attempts to delete logs.

Further reading	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders https://docs.microsoft.com/en-us/sharepoint/deploy-file-collaboration https://docs.microsoft.com/en-us/sysinternals/
M1024	**Restrict Registry Permissions**
Description and advice	Access to critical parts of the registration database could be compromised to prevent security tools, including antivirus, EDR, firewall or logging solutions, from starting or running.
Recommendations	• Limit user access to the parts of the registration database relating to security tools. • Monitor and respond to alarms on changes in the registration database related to security tools.
Further reading	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/prevent-changes-to-security-settings-with-tamper-protection
M1025	**Privileged process integrity**
Description and advice	The LSA process that validates users and upholds security policies may come under attack in an attempt to circumvent restrictions or access account credentials. LSA Protection or Windows Defender Credential Guard can help protect against this attack vector.
Recommendations	
Further reading	https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard
M1026	**Privileged account management**
Description and advice	In several ransomware attacks, local administrator accounts or local administrator passwords was used to retain persistence or move laterally across the network. In Microsoft environments, Local Administrator Password Solution (LAPS) can be used to secure unique passwords on local administrator accounts. The risk of compromise will be reduced by exclusively using privileged accounts on dedicated administrator workstations and only to perform designated tasks that require special privileges.
	• Only use privileged accounts for activities that require special rights. • Use regular user accounts without special rights for everyday administrative tasks. • Administrative rights should only be assigned to users on a case-by-case basis and only when specifically required.
Further reading	https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview https://www.microsoft.com/en-us/download/details.aspx?id=46899

M1027	**Password policies**
Description and advice	Implementation of a password policy based on best practices may reduce the risk of account compromise in a ransomware attack. Never recycle passwords across multiple accounts, including local administrator accounts, and other privileged accounts. In Microsoft environments, LAPS can be used to generate unique passwords on local administrator accounts. Multi-factor authentication can make it difficult for hackers to use compromised login credentials to gain access to, and embed themselves in, an organization's systems.
Recommendations	For recommendations regarding passwords and password policies, please read the CFCS's Password guide referenced below.
Further reading	https://cfcs.dk/en/forebyggelse/vejledninger/passwords/ https://www.microsoft.com/en-us/download/details.aspx?id=46899
M1028	**Operating system configuration**
Description and advice	Some operating system (OS) settings may be exploited by ransomware actors to access cached account credentials, limit the organization's possibility to quickly restore encrypted data, and to escalate privileges. Because previous NTLM versions are insecure, it should be investigated whether the organization's environment can be configured to require NTLMv2 if Kerberos-based authentication is not successful. This configuration and the standard setting for WDigest (UseLogonCredential=0) that disable caching of credentials in memory can be forced through GPO. As some ransomware groups are known to change these settings, monitoring of the settings may give an indication of whether an attack is under way. Ransomware also exists that delete Volume Shadow Copies by means of Wmic, Powershell or Vssadmin in order to complicate data restoration. Thus, backups should be sent to another protected system, and activities between the systems should be monitored. Privilege escalation from an account with Server Operator privileges can be carried out by using the "at" command to schedule tasks that are conducted in context of the SYSTEM account on a Domain Controller. To this end, a GPO can be used that enforces the disabling of the setting: "Domain controller: Allow server operators to schedule tasks".
Recommendations	• Implement OS security policies automatically and limit the number of administrators with privileges to change items.
Further reading	https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-controller-allow-server-operators-to-schedule-tasks https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares

M1030	Network segmentation
Description and advice	In network segmentation, critical systems, functions or resources can be isolated and the traffic between them can be reduced to the bare minimum. Online services should be isolated (for example in a DMZ), preventing full access to other networks or services in the event of a compromise. Remote access to internal resources should be protected using encryption and multi-factor authentication. Remote access from trusted units can take place via a VPN solution. Several known ransomware attacks have started through misuse of remote access services such as Remote Desktop Protocol, using account credentials that have been compromised or obtained through brute force attacks. Remote Desktop servers should not be accessible directly from the Internet but instead go through an RD Gateway and protected by multi-factor authentication. This solution could furthermore be supplemented by an Azure AD Application Proxy providing additional protection. Segmentation of the network can hamper an attacker's efforts to map and move through the network. If a crypto worm is deployed, segmentation can also help limit the spread to accessible network segments.
Recommendations	• Use encrypted connections and multi-factor authentication for remote access. • Divide the network into segments, ensuring that units (devices, servers or network equipment) are placed in different segments according to their use and sensitivity. • Network traffic between individual network segments should be limited and monitored according to documented needs.
Further reading	https://tools.cisco.com/security/center/resources/framework_segmentation https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/network-level-segmentation https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-security https://docs.microsoft.com/en-us/azure/virtual-network/ https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares
M1031	**Network intrusion prevention**
Description and advice	Intrusion Prevention Systems (IPS) are designed to detect and remove malicious traffic between network segments. In a ransomware context, IPS can block vulnerability scans, malicious links and attachments in phishing emails or detect attempts to exfiltrate data among other. Placement of such system within the network should be decided based on a risk assessment to ensure maximum effect.

	The solution should be actively monitored and potential alarms timely addressed.
Recommendations	
Further reading	https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50951
M1032	**Multi-factor authentication (MFA)**
Description and advice	Multi-factor authentication is very effective in the fight against ransomware. Multi-factor authentication can reduce the risk of compromised account credentials being used to gain access to an organization's systems or to conduct critical actions. There are several examples where remote access services without multi-factor authentication have been accessed by means of brute force or recycled passwords.
Recommendations	• Use multi-factor authentication whenever possible and as a minimum on all remote access or other privileged accounts. Further information on multi-factor authentication can be found in the CFCS password guide.
Further reading	https://cfcs.dk/en/forebyggelse/vejledninger/passwords/
M1034	**Limit hardware installation**
Description and advice	Organizations should have a defined policy on the use of USB devices and other removable external media. Consider preventing users and user groups from connecting non-approved hardware to systems, including USB devices. Make sure that all USB devices are scanned for malware before they are plugged into units connected to the network, for example on an offline but updated malware scanning station.
Recommendations	• Prepare a policy on external removable media.
Further reading	https://docs.microsoft.com/en-us/windows/security/threat-protection/device-control/control-usb-devices-using-intune
M1035	**Limit access to resources over network**
Description and advice	Remote access services such as Webmail, VPN, Citrix and Remote Desktop Services are often exploited to gain initial access to an organization's systems by means of compromised login credentials. Access to these services should thus only take place through gateways or proxies, ensuring that the user is validated by multi-factor authentication. Gateways and proxies can also ensure that traffic is encrypted before access is granted. (See also M1030)
Recommendations	• Remote-access sessions should operate over an encrypted connection and use multi-factor authentication.
Further reading	https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-security

	https://docs.citrix.com/en-us/citrix-gateway-service.html
M1036	**Account use policies**
Description and advice	Login policies could be used to limit the number of allowed login failures and specify when a login is allowed and from where. Such security initiatives could help reduce the risk of ransomware actors compromising login credentials by means of brute-force attacks, including the risk of password spraying and credential stuffing. However, when very restrictive policies are employed, legitimate users' risk being locked out of their accounts. Signs of brute-force attacks may be an early indication of attempts at compromise that could result in the deployment of ransomware and should thus be timely addressed.
Recommendations	The CFCS's password guide contains additional advice on account and password policies.
Further reading	https://cfcs.dk/en/forebyggelse/vejledninger/passwords/
M1037	**Filter network traffic**
Description and advice	Ransomware actors have been known to exfiltrate data for extortion purposes. This can happen over existing C2 channels or through any other allowed communications channels. By allowing only relevant servers to handle outbound traffic over necessary ports, exfiltration can be hampered. Blocked attempts at outbound traffic from servers, or unusual data transmission patterns may be an indication of data exfiltration attempts.
Recommendations	• Only allow necessary outbound traffic from servers. • Use a secure DNS service.
Further reading	https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-exfiltration-alerts
M1038	**Execution prevention**
Description and advice	Scripts and executable programmes are used during most of the stages in a typical targeted ransomware attack. They may be created by actors themselves, made by others, or come preinstalled with the operating system (for example Powershell). Application control may be a useful tool to limit the use and detection of unauthorized actions that may be part of an active ransomware attack. Windows Defender Application Control and Applocker can, for example, be used to control which programmes and scripts are allowed to run on a standard workstation and are powerful supplements to Antivirus and EDR platforms. (See also M1045)
Recommendations	• Limit the user's ability to run scripts based on file type or application control. • Limit the user's ability to run non-approved applications. • Monitor and respond to alarms on attempts to run blocked scripts and applications.
Further reading	https://support.microsoft.com/en-us/help/4562299/protect-your-pc-from-potentially-unwanted-applications https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

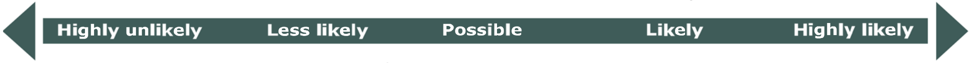
M1041	**Encrypt sensitive information**
Description and advice	If an organization’s Windows environment still allows RC4 encryption of Kerberos tickets, a service account’s NTLM password hash may be found via Kerberoasting. Updated Windows environments can use AES encryption instead, and Azure Security Center can be used to detect attempts at Kerberoasting. Non-encrypted backups of Domain Controllers may also be interesting for hackers, as may encryption keys that are not securely stored.
Recommendations	
Further reading	https://adsecurity.org/?p=3458 https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group https://docs.microsoft.com/en-us/archive/blogs/motiba/detecting-kerberoasting-activity-using-azure-security-center
M1042	**Disable or remove feature or program**
Description and advice	Every available service may be attacked by hackers, and potential vulnerabilities may be exploited. Consequently, the attack surface should be reduced, and servers should only offer the necessary services. Additional services should be uninstalled, deactivated or blocked. Ransomware actors often use standard scripting and administration tools from the operating system to perform reconnaissance, lateral movement and escalate privileges. If standard scripting and administration tools are not used for administration purposes, they could be removed from devices and servers and blocked, including by using Windows Defender Application Control and/or Applocker. In addition, Execution Policies could be used to limit which Powershell scripts could be run. Alternatively, access to these tools should be limited to relevant IT administrators and reduced to the bare minimum required to do the job, for example by following the Just Enough Administration (JEA) principle.
Recommendations	• Deactivate unnecessary services on systems to reduce the attack surface. • Only allow the newest edition of necessary script interpreters and administration tools. • Limit the ability to execute scripts and use administration tool rights and monitor logs on their usage.
Further reading	https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/winrmsecurity
M1043	**Credential access protection**
Description and advice	Ransomware actors will often try to access cached account information or attack the authentication process itself to compromise accounts.

	In order to limit caching of account information locally on stationary devices and servers, disabling caching using GPO may be considered, based on a relevant WMI filter. However, laptops may need to cache account information to allow login when the users are not directly connected to the organization’s network. Windows Defender Credential Guard can also reduce the risk of hackers gaining access to account information.
Recommendations	
Further reading	https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication
M1045	**Code signing**
Description and advice	By only allowing cryptographic code signing with approved signatures, it is possible to limit executable scripts, thereby hampering hacker efforts. Powershell Execution policies can control Powershell scripts but not prevent manual execution of Powershell commands. (See also M1038)
Recommendations	
Further reading	https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies
M1047	**Audit**
Description and advice	Account information stored in the registration database, in scheduled tasks or in scripts or other files may be extremely valuable to ransomware actors. Thus, it is important to limit the practice of account information being stored in random locations. The accounts used should have restricted rights. It is also important to conduct regular scans for stored account information to locate sensitive account information before potential ransomware actors do.
Recommendations	• Regularly search for stored account information in systems and files.
Further reading	https://adsecurity.org/?p=2288
M1048	**Application isolation and sandboxing**
Description and advice	Limiting the execution of applications to a virtual sandbox environment may limit the possibility of malicious code spreading to systems outside the sandbox. Isolated execution of the programme helps limit the data, processes and system functions accessible to the malicious code.
Recommendations	
Further reading	https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/
M1049	**Antivirus/antimalware**

Description and advice	An updated antivirus programme can be used to protect against malicious programmes and code. It can automatically quarantine suspicious files and warn of suspicious programme behaviour. In several of the analysed ransomware attacks, the installed antivirus actually detected the hackers' malicious activity days prior to the actual deployment of the ransomware.
Recommendations	• Install and maintain updated antivirus/antimalware software. • Monitor and respond to alarms from antivirus/antimalware programmes.
Further reading	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-microsoft-defender-antivirus-features
M1051	**Update software**
Description and advice	All software should be subject to regular updates to ensure that potential vulnerabilities are patched as quickly as possible in order to prevent compromise of the system by publicly available exploits.
Recommendations	• Keep all software updated with the latest security patches.
Further reading	
M1052	**User account control**
Description and advice	Trusted accesses from suppliers and other partners could, if compromised, be used as an entry point into an organization's systems. Thus, it is important to make sure that third party accounts are issued and administered in accordance with organization policies. This could, for instance, entail that personal accounts are only issued to identifiable individuals, are temporary and based on the principle of least-privilege. It should also be ensured that the terms of the agreement deal with third-party responsibilities and third-party obligation to report own data compromises, and have relevant security requirements. It should also be ensured that the use of third-party accounts is logged and that logging is extended in relation to the level of third-party non-privileged accounts.
Recommendations	• Accounts issued to third parties should follow organization security policies and security responsibility should be assigned in the agreement.
Further reading	https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/ [only in Danish]
M1053	**Backup**
Description and advice	In order to increase the likelihood of receiving ransom payment, attackers will often try to destroy potential backups before deploying the ransomware. Thus, it is important to keep an offline backup of critical data and ensure that compromised administrator accounts do not have access to the backup system and its data. For instance, administration of the backup system could be restricted to accounts outside the domain and only allow access to dedicated, hardened and isolated administrator workstations. Also, it is important to conduct regular inspections if the intended data is actually included in the backup and that the possibility of restoring data from the backup is tested.
Recommendations	• Conduct a backup of business-critical data and system configurations and regularly test that the backup contains the intended data. • Keep an offline backup copy of critical data.

	• Regularly test that data can be restored from the backup. • Protect access to the backup system and backup data.
Further reading	

The DDIS applies the below scale of probability



”We assess” corresponds to ”likely” unless a different probability level is indicated.