BEST PRACTICES FOR PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS

Document Metadata:

Document publication date: 21/05/2024
Version: 1.1

Table of Contents

INTRODUCTION **3**

RANSOMWARE INCIDENT RESPONSE PLAN **4**

PREPARATION 4
Summary of Attacker Tactics *5*
Summary of Possible Mitigations to Implement in the Organization *6*
IDENTIFICATION 9
CONTAINMENT 10
EXTERNAL COMMUNICATION AND REPORTING 11
INCIDENT ANALYSIS 14
RECOVERY 16
LESSONS LEARNED 17

CONCLUSION **17**

APPENDIX 1: DETAILED DESCRIPTION OF MITIGATIONS 18
1. Initial Access *18*
2. Execution *21*
3. Privilege Escalation *22*
4. Defense Evasion *23*
5. Credential Access *24*
6. Discovery *26*
7. Lateral Movement *26*
8. Persistence: *27*
9. Command and Control: *28*
10. Exfiltration *28*
11. Impact *29*
APPENDIX 2: SAMPLE CONTACT LIST TEMPLATE IN THE ESCALATION PATH (LIST FOR CUSTOMIZATION/MODIFICATION) 30

Introduction

In the face of the ever-growing threat of ransomware attacks, which constitute one of the most serious challenges to the security of IT systems in contemporary organizations, it is necessary to take effective measures aimed at continuously increasing the level of security of these systems. Ransomware attacks pose not only significant threats to data security and ICT system stability, but can also lead to substantial financial losses, materialization of reputational risk, and consequently, loss of trust from clients or other external stakeholders.

The most common attack vectors in ransomware attacks are:

- **Phishing:** manipulating the user e.g. by sending fraudulent emails aimed at prompting the recipient to open an attached file or click on a link to download a file containing malicious software
- **Vulnerable, outdated services**: many ransomware attacks exploit known software vulnerabilities that have not been updated to the latest recommended version by the manufacturer
- **Improperly secured remote access**: attackers often exploit publicly available remote access services by breaking passwords using brute force methods

In this document, we describe best practices that can help protect an organization from ransomware attacks and propose ways to respond to such incidents, should they occur. The proposed technical measures and organizational safeguards aim to increase resistance to ransomware attacks and minimize the impact of such incidents. In addition, to the term “ransomware attack”, the document interchangeably uses terms such as “incident” or “event.”

We hope the information contained in this document will significantly contribute to increasing the resilience of your organization.

Ransomware Incident Response Plan

This chapter describes the procedure for responding to incidents, including the organization's preparation stage. The following compilation is based on the experiences of CSIRT KNF staff in handling ransomware-related incidents, feedback from representatives of the financial market, recommendations from CISA's[1] "Stop Ransomware" project[2], and independent security experts.

This part of the document is dedicated to the process of responding to a security incident such as a ransomware attack, divided into 7 stages:

1. Preparation
2. Identification
3. Containment
4. External communication and reporting
5. Remediation
6. Recovery
7. Lessons learned

PREPARATION

This is a crucial stage where no incident has occurred yet, and the actions taken are aimed at preventing its occurrence or mitigating the consequences if a ransomware attack happens. At this stage, it is also important to address organizational issues. We encourage keeping a printed version of the document in case of unavailability of IT systems due to a ransomware attack. Additionally, it is advisable to ensure that those responsible for responding to security incidents are well-acquainted with this document, which can significantly improve quality of response during a ransomware incident. Furthermore, it is recommended to establish alternative communication channels and contacts in the escalation path and designate individuals with physical access to data processing locations (collocations, server rooms, etc.) should their personal intervention during a ransomware attack be required.

As part of the initial stage of responding to a potential ransomware attack, variants of mitigation recommended by CSIRT KNF for implementation in the organization have been described. These aim to protect the environment from such criminal activities,

[1] CISA - Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/
2 https://www.cisa.gov/stopransomware

increase the security level, and/or mitigate the impact of such an incident. However, it should be noted that these do not constitute an exhaustive list of solutions. A detailed description of each element is provided in Appendix 1.

Summary of Attacker Tactics

The division has been prepared based on the MITRE ATT&CK framework[3]:

1. **Initial Access** - Techniques and procedures (TTP) in this tactic allow the identification of actions, processes and mechanisms through which attackers attempt to access the organizational IT network. This includes various methods that attackers may use in the preparation stage of the attack.
2. **Execution -** This phase involves the infection process, i.e. executing malicious code on the victim's system or network. This phase also intertwines with other attack phases, including Defense Evasion, Lateral Movement, Credential Access, Privilege Escalation, and Command and Control.
3. **Privilege Escalation** - In this phase, attackers try to obtain as much data as possible to gain the highest possible privileges within the system or network to access the organization's resources widely.
4. **Defense Evasion -** In this tactic, attackers try to bypass the organization's defense mechanisms to avoid detection.
5. **Credential Access -** This attack phase focuses on obtaining as much authentication data as possible. This phase may include techniques already applied in the Privilege Escalation phase.
6. **Discovery -** Techniques used by attackers to explore the internal IT infrastructure to move on to Lateral Movement tactics.
7. **Lateral Movement -** In this phase, attackers use stolen credentials to gain access to additional systems.
8. **Persistence -** Techniques used in this tactic aim to ensure the attackers can survive in the compromised system and/or re-infect the system if the attack has been detected.

[3] https://attack.mitre.org/

9. **Command and Control -** This tactic describes the mechanisms of communication between the infected infrastructure or systems and the attackers' command servers.
10. **Exfiltration** - This is one of the final elements of the attack, involving the extraction of data from the targeted organization.
11. **Impact -** In this phase, attackers may take actions to disrupt, destroy or alter the victim's systems to affect the quality, integrity and stability of the organization's services. This tactic may be used, for example, in the event of disconnecting infected systems from the attackers' command & control servers upon detecting the attack.

Summary of Possible Mitigations to Implement in the Organization

For each of the tactics mentioned above, below we present the associated possible mitigations. **Detailed descriptions of the mitigations have been included in Appendix 1 of the document.** It should be noted that the scope of implemented and used mitigations should be tailored to the specific organization, depending on its technical and organizational capabilities.

1.	Initial access
1.1	Blocking or monitoring non-standard email attachment extensions
1.2	Adding warnings for incoming emails from outside the organization
1.3	Verification and detonation of links and attachments in a sandbox system
1.4	Configuration of email security SPF, DMARC, DKIM
1.5	Taking inventory and verification of services exposed on public interfaces available from the Internet
1.6	Regular scanning of services visible from the Internet
1.7	Securing remote access interfaces
1.8	Monitoring published vulnerabilities
1.9	Monitoring system, device, and service configuration integrity
1.10	Using Web Application Firewall and IPS solutions
1.11	Using multi-factor authentication (MFA) for logging into services accessible from the Internet
1.12	Regularly raising user awareness of cybersecurity threats
1.13	Monitoring and limiting Password Spraying attacks
1.14	Monitoring and limiting Brute Force attacks
1.15	Maintaining up-to-date network documentation and schematics
1.16	Using proxy mechanisms

1.17	Increasing restrictions for externally available RDP[4] services.
1.18	Analyzing the configuration of services and applications
1.19	Regular software updates and security patch management
1.20	Conducting tests and participating in cybersecurity exercises
2.	**Execution**
2.1	Enhancing the monitoring of PowerShell script execution
2.2	Restricting the use of the PsExec tool
2.3	Limiting network connections initiated by PowerShell scripts and system tools
2.4	Restricting the execution of macros in office document files
2.5	Monitoring the process tree for unusual behavior
2.6	Signing internally developed and used scripts and tools
2.7	Monitoring or blocking the execution of script files .bat, .cmd, .js, .ps1, .py
2.8	Detecting changes to PowerShell ExecutionPolicy
2.9	Monitoring the installation of new services via PsExec
2.10	Monitoring login processes and log clearing operations
3.	**Privilege Escalation**
3.1	Limiting the use of local administrator accounts and employing PAM[5] solutions
3.2	Monitoring and limiting the use of LOLBins[6] and their presence in process trees
3.3	Verifying LDAP[7] queries
3.4	Monitoring and verifying new domain controllers and their synchronization
3.5	Creating Canary user accounts
3.6	Detecting SMB[8] enumeration
4.	**Defense Evasion**
4.1	Using a whitelist of approved applications
4.2	Monitoring the deactivation of security mechanisms
4.3	Mutual monitoring of security agents
4.4	Enforcing updates to security system signatures and rules
4.5	Monitoring the use of net.exe stop and net.exe start commands
4.6	Monitoring registry keys responsible for security solutions
4.7	Monitoring changes in backup configuration (VSSADMIN)
4.8	Monitoring the use of taskkill.exe and Pskill.exe commands
4.9	Detecting new hosts in the network
4.10	Monitoring changes to scheduled tasks configuration
4.11	Monitoring the use of sc.exe command
5.	**Credential Access**
5.1	Implementing multi-layered security measures
5.2	Identity hygiene
5.3	Monitoring user activity
5.4	Building employee awareness
5.5	Protecting administrator accounts
5.6	Domain administrator privilege separation

[4] RDP – Remote Desktop Protocol
5 PAM- Privileged Access Management
6 LOLBins - Living Off The Land Binaries, Scripts and Libraries
7 LDAP - Lightweight Directory Access Protocol
8 SMB – Server Message Block

5.7	Detecting and blocking programs that perform memory dumps of the LSASS process
5.8	Implementing LAPS[9]
6.	**Discovery**
6.1	Monitoring network connection reconnaissance attempts via arp.exe
6.2	Monitoring reconnaissance attempts via nslookup.exe
6.3	Monitoring the use of other tools and commands
7.	**Lateral Movement**
7.1	Network segmentation
7.2	Monitoring the use of RDP
7.3	Securing domain controllers
8.	**Persistence**
8.1	Monitoring registry keys used by attackers
8.2	Monitoring registry keys created for new services
9.	**Command and Control**
9.1	Monitoring connections to known Command & Control (C2) servers
9.2	Implementing rules and monitoring detected beaconing attempts to C2 servers
9.3	Implementing rules to detect commercial tools like Cobalt Strike
10.	**Exfiltration**
10.1	Limiting traffic to TOR network exit nodes
10.2	Restricting DNS over HTTPS (DoH) traffic
10.3	Monitoring or blocking traffic to file-sharing services
10.4	Monitoring or blocking SMB/TFTP/FTP/SFTP traffic to the Internet
10.5	Monitoring network anomalies
11.	**Impact**
11.1	Creating rules to monitor mass file overwriting and integrity breaches
11.2	Creating rules to detect the execution of libraries like pycrypto used in encryption processes
11.3	Ensuring secure access to backups
11.4	Preparing and maintaining critical data backups

9 LAPS - Local Administrator Password Solution

Ransomware Incident Response Process

The preparation stage is the time when the organization does not yet suspect the occurrence of a ransomware attack, but is aware of the risk. An essential element of the incident response process is designating an incident coordinator (permanent or rotational) who will have the authority to make key decisions, at minimum, regarding the response, protection and impact mitigation areas. This role is crucial for handling a wide range of security incidents, not just ransomware attacks.
Further in the document, we present the subsequent stages of responding to a suspected or confirmed ransomware incident.

IDENTIFICATION

At this stage, the detection and confirmation (or dismissal) of a ransomware attack take place. It is recommended that the organization has prepared procedures and internal instructions to optimize the actions of staff receiving the initial report of a ransomware attack. Personnel handling such an event should have appropriate training and knowledge, including collecting malware samples to extract IOCs[10] and use them in systems like EDR[11]/XDR[12]. Prioritization of tasks and awareness of treating such a report as a priority is also essential. Efficient and systematic actions will help avoid unnecessary mistakes and shorten the time needed to identify an incident. Preliminary analysis of the event should be conducted, and further steps taken based on the factual situation.

1. Identification and confirmation of the incident:
    - preliminary analysis of security system logs to confirm the incident,
    - determining the current state of infection: whether servers, virtualizers and/or backups have been infected, and whether attackers have access to the AD structure using privileged accounts.
2. Reviewing system logs:
    - verifying potential alerts indicating the presence of malicious software or attacker activity

[10] IOC – Indicator of Compromise
[11] EDR – Endpoint Detection and Response
[12] XDR – Extended Detection and Response

- securing logs from Active Directory, security systems and perimeter devices (antivirus, EDR/XDR, IDS, IPS, FW, WebFB, etc.)
- securing logs from proxy and DNS to assess whether data exfiltration from infected workstations and/or servers has occurred

3. Initial assessment of the event and assigning priority.
4. Verifying if a message from the attackers has been delivered to the organization, e.g. information about a ransom proposal.
5. Activating the internal escalation path:
    - the potential impacts of a ransomware incident can significantly affect the organization's stability. In the event of such an incident, it is recommended to inform immediate superiors and the organization's management
    - as that attackers may have access to the organization's IT infrastructure (e.g. email systems, ticketing systems or internal direct communication systems), they may monitor actions taken by the organization to see if the attack has been noticed and identified. Therefore, using external communication channels such as phone calls is recommended to avoid informing the intruders about the detection and the actions taken by the organization
    - preparing contact lists with phone numbers in advance and keeping them ready in case of an attack, also in paper form (attackers may be monitoring the organization's IT network)
6. Initiating the incident response team's work.

CONTAINMENT

After the preliminary analysis of the event and classifying it as a security incident related to a ransomware attack, steps must be taken to minimize the attack's impact and prevent further escalation of the incident while securing materials necessary for further analysis. It is recommended to:

1. Immediately isolate potentially compromised systems:
    - determine the current state of infection and the extent of attackers' access to infected systems

- if multiple systems or subnets are infected, consider isolating entire subnets at the network device level, as isolating individual hosts may be ineffective
- during network isolation, focus on systems critical to the organization's functioning first
- if network isolation from network devices is not possible, consider physically disconnecting network connections from infected devices or networks
- attackers may observe the organization during the attack; it is recommended to carry out network isolation in a manner as inconspicuous as possible to the attackers
- Be aware that disconnecting potentially compromised devices from power may result in losing access to important information and proof of the related attack. Shutting down systems should be considered when isolation is not possible, remembering to collect evidence.

2. Monitoring the uncompromised part of the network for potential infection traces.

EXTERNAL COMMUNICATION AND REPORTING

At this stage, it is mandatory to maintain cooperation between personnel handling the incident and those responsible for internal and external communication within the organization. It is recommended that the communicated message be balanced, without causing unnecessary chaos or panic. Information which is being provided should be accurate and verified before publication. At this stage, it is also necessary to engage individuals responsible for reporting to fulfill formal and operational obligations.

It is worth considering establishing a crisis team (unless internal incident response procedures already mandate it) comprising of at least an incident coordinator, representatives from the communication department, legal department, reporting personnel and members of the organization's management.

To achieve the above, we suggest the following steps:

1. Preparing an external communication plan:

- involving departments responsible for communication in the incident handling process (at the identification stage by establishing the incident response team)
- the organization should have a developed crisis communication plan for ransomware attacks. If no communication plan exists, it should be created immediately
- if decided that the information will not be disclosed outside the organization in the initial incident handling phase, prepare to instruct employees not to disclose the attack, and ensure that those in contact with external stakeholders are prepared to issue appropriate communication. It should be remembered that that attackers might disclose the attack themselves

2. Reporting the incident to the national or sectoral CSIRT team[13]. Due to the potential sensitivity of transmitted information, messages should be secured. Using encrypted communication, e.g. PGP keys, is recommended. At this stage, the organization may not have full knowledge of the attack's scale and scope, which should not however provide grounds for lack of, or delays in reporting the incident. It is recommended to make reports promptly and without causing significant delays in the incident handling process. Individuals other than those directly responsible for technical tasks in the incident handling should be involved in the reporting process. Remember that the initial incident report can be updated if new information arises.

   In the initial stage, directly after detecting and identifying the incident:

   - determine the current state of infection and ongoing actions
   - provide information about receiving a ransom demand message from attackers and the content of that message (this may help identify the criminal group responsible for the attack more quickly)

   In subsequent stages of incident handling, the report should be supplemented with the following information:

   - identified or probable initial attack vector and the status of mitigation or elimination of the threat

[13] If a CSIRT team has been established for a specific sector.

- assessing the impact of the event on the organization's functionality and service availability
- status of internal escalation implementation
- information on whether external communication about the incident is planned, including the form of the message
- status of available backups and the plan for restoring infrastructure and business services
- status of notifications sent to other entities, including whether a report has been filed with law enforcement and/or an incident report has been submitted to the National Personal Date Protection Entity.
- identified risks related to the potential spread of ransomware infection to other organizations' systems or ICT service providers
- potential identified risks that may pose threats to other entities collaborating with the organization
- sending the following files[14]:
    - at least 2 encrypted files
    - ransom note from attackers (if provided)
    - sample malware that infected workstations or servers
    - logs from the infected machine(s) and security systems during the infection
    - original files that were encrypted, if preserved or restored from backup (sample files post-encryption and their original versions)
- other steps taken so far

3. If a data breach has been identified, the incident must be reported to a specified law enforcement unit, as stated by national law.
4. Filing a crime report with law enforcement. During the reporting process, the organization may be asked to provide information, including but not limited to the following:
    - when and how the attack was detected
    - actions taken by the victim in response to the incident
    - the attack vector/method of infection and any available details

[14] https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

- the number of affected devices and the incident's impact, including identified losses to the company/clients
- whether data was stolen during the attack (including its type) and whether the victim is being extorted with the possibility of public disclosure or sale of stolen data
- whether the location of the server where the attackers intend to or have already publicized the stolen data is known
- details of the ransom demand, including the attackers' specified payment method if the attackers provided such details
- has the organization contacted the criminals

When submitting a written crime report, it is advisable, if possible, to include the above information in the prepared document. Additionally, at this stage, the law enforcement unit(s) may also wish to secure necessary devices, system logs and expand the scope of required information beyond what is mentioned above.

INCIDENT ANALYSIS

At this stage organization should determine the actions to be taken and the tools to be used to eliminate the threat sources and repair the damages to the organization. It is also the right time to conduct a detailed analysis of the causes of the incident in order to understand how the ransomware attack occurred, and how to prevent such attacks in the future. Conducting a detailed analysis requires possessing necessary information and, first of all, system logs. It is recommended that the organization be prepared to potentially look up information up to 3 months back before the incident date, and have a process for securely storing chronological records with information about events and activities in the organization's IT infrastructure.

At this stage, we recommend:

1. Starting the Threat Hunting process, focusing on:
    - identifying the initial attack vector and potential access points and pinpointing access routes and systems used by attackers in the early stages of the attack

- identifying and securing other systems that attackers may have access to through compromised credentials and accesses
- newly created accounts in Active Directory, particularly those with elevated privileges (e.g. domain administrator)
- verifying logs of remote connections to the organization (e.g. VPN) to identify potential unauthorized logins or unauthorized devices with remote access to the infrastructure
- identifying modifications to backup settings on workstations (e.g. shadow copy). Built-in Windows tools such as fsutil.exe (deletejournal), vssadmin.exe, wbadmin.exe, wmic.exe (shadowcopy) are often used for this purpose
- traces of communication with systems like Cobalt Strike beacon/client. Cobalt Strike is commercial software used in penetration tests, but likewise, often utilized by criminals in real attacks. (The software processes are often hidden under standard Windows process names)
- traces of non-standard use of remote monitoring and management (RMM) software
- non-standard PowerShell commands or operations using tools from the PSTools package
- traces of Active Directory resource enumeration attempts
- traces of memory dump attempts from the LSASS process using tools like Mimikatz, Sysinternals ProcDump, PPLdump, HandleKatz, nanodump
- traces of non-standard internal or external communication with Command & Control (C2) servers
- traces indicating data exfiltration from the organization, such as:
    - unusual network traffic outgoing from the organization before the incident, which may be tunneled via different ports and services
    - communication with file storage services, FTP/SFTP or tools like Rclone, Rsync
- if data on the server was encrypted through an infected workstation:
    - reviewing logs: Review Computer Management > Sessions and Open Files lists to determine users or systems accessing files

    - reviewing the properties of encrypted files or files with ransom note content to identify associated user accounts
    - reviewing logs: TerminalServices-RemoteConnectionManager for potential RDP connections
    - reviewing logs: Windows Security log, SMB event logs and others that may identify attempts to access server resources
    - running software on the server to capture network traffic, e.g. Wireshark, to identify IP addresses associated with processes saving or renaming files on the server, using commands like smb2.filename contains ransomware_name
  - newly created services, added entries in task schedules, non-standard software, generating unusual files, or standard software initiating atypical processes
  - traces of logon process modifications and log clearing operations
2. Extended analysis of attackers' access and initial attack vector:
  - complete identification and securing of attack vectors used by criminals
  - permanent removal all potential accesses and mechanisms used by attackers

RECOVERY

At this stage, the organization conducts actions to restore standard functioning of systems and services. Due to the possibility of system infection before executing backup, it is recommended to test restored systems and applications from backups to ensure they are free of threats, primarily those identified as attackers' entry vectors.
Restoring systems according to the prioritization of critical services in the organization:

- conducting an analysis for restoration, identifying critical systems for the organization's operation to be restored first
- resetting passwords in all systems related to the incident, reviewing security measures and implementing updates and security patches in the infrastructure that were not previously implemented
- restoring systems and infrastructure elements according to the prioritization of critical services
- reconnecting restored systems and resuming business process functions

LESSONS LEARNED

After completing the incident handling process and restoring the organization to full operation of business and operational processes, it is recommended to conduct an additional analysis to evaluate the incident response process.
We recommend:

1. Documenting incident details and drawing lessons from the incident handling process.
2. Preparing a post-incident report that should include a detailed description of the event, actions taken, and future recommendations.
3. Updating the incident register.
4. Conducting a “Lessons Learned” process from incident handling and related events.
5. Submitting final incident handling reports to the relevant CSIRT team.

Conclusion

The risk of a ransomware attack is a threat that every organization must face. Implementing appropriate procedures and security mechanisms significantly reduces the likelihood of a successful attack. Equally important is the ability to respond to such incidents when they occur. Quick, well-thought-out, and well-coordinated actions often help mitigate the consequences of the incident. Therefore, we hope that the best practices in preventing and responding to ransomware attacks collected in this document will be helpful both in preparing for such attacks, and in the event of a ransomware incident. However, it is essential to remember that the scope of actions and the shape of internal procedures should be prepared according to the specifics of your organization's operations.

This material was created in collaboration with entities from the Polish financial market and external consultants who shared their knowledge and experience in this field. We sincerely thank you for your work on the material and all the feedback sent to us!

Appendix 1: Detailed Description of Mitigations

1. Initial Access

1.1. **Blocking or monitoring non-standard email attachment extensions** – Implementing rules that block or additionally verify emails containing attachments with specific extensions. Examples of such extensions include: .iso, .dmg, .img, .exe, .vbs, .lnk, .bat, .cmd, .ps1.

1.2. **Adding warnings for incoming emails from outside the organization** – This aims to increase email users' awareness and highlight the need for caution when opening emails from outside the organization. It's a good practice to change messages periodically to prevent users from becoming accustomed to the displayed message.

1.3. **Verification and detonation of links and attachments in a sandbox system** – Implementing mechanisms to verify potentially dangerous links and attachments in incoming emails. The solution should include:

- checking links in reputation services contained in emails sent to the organization,
- some security solutions allow automatic unpacking of archives and attempts to decrypt them using strings found in the message and a known list of passwords,
- checking checksums of attachments or attempting to run them in a sandbox system, then, depending on the pre-defined parameters, deliver the message or move it to the appropriate quarantine.

1.4. **Configuration of SPF, DMARC, DKIM email security** – Verifying and configuring SPF, DMARC, and DKIM mechanisms to exclude sender impersonation. Using reputation lists to filter emails from known spam or malicious content addresses. When configuring security measures, it is worth using help guides and correct configuration pattern testing:
https://cert.pl/posts/2021/10/mechanizmy-weryfikacji-nadawcy-wiadomosci/
https://bezpiecznapoczta.cert.pl/

1.5. **Inventory and verification of services available on Internet-facing public interfaces** – Conducting regular scans of own IP addresses to identify services exposed to the Internet and verifying whether visibility and availability of identified services is justified. Configuring management interfaces for various services so that access is only possible from local infrastructure or using whitelisting.

1.6. **Regular scanning of services visible from the Internet** – Implementing mechanisms to scan external IP addresses belonging to the organization to detect unauthorized services and servers.

1.7. **Securing remote access interfaces** – The organization should consider limiting access to remote interfaces so that they are only available to users logged in via VPN. At a minimum, it is recommended to limit the list of IP addresses that can log into these services.

1.8. **Monitoring published vulnerabilities** – Regularly monitoring information about vulnerabilities and threats to systems, applications, infrastructure elements, devices, and network services on the edge between the Internet and local infrastructure. Regular security scans of external infrastructure elements for vulnerabilities and threats.

1.9. **Monitoring system, device, and service configuration integrity** – Regularly monitoring perimeter infrastructure to verify unauthorized configuration changes.

1.10. **Using Web Application Firewall and IPS solutions** – For infrastructure elements visible from the Internet – to automatically detect and block attack attempts. Updating signatures and rules in these solutions (including testing to exclude False-Positive) to ensure continuous quality of protection.

1.11. **Using multi-factor authentication (MFA) for logging into services accessible from the Internet.** Enforcing complex and secure passwords compliant with the organization’s password policy.

1.12. **Regularly raising user awareness of cybersecurity threats** – Conducting educational activities to increase user awareness of cyber threats with practical examples of techniques used by attackers and various scenarios of attacks.

1.13. **Monitoring and limiting Password Spraying attacks** – Implementing mechanisms to detect and block Password Spraying attacks.

1.14. **Monitoring and limiting Brute Force attacks** – Implementing mechanisms to detect and block (e.g. via captcha) Brute Force attacks.

1.15. **Maintaining up-to-date network documentation and schematics** – Identifying IT infrastructure elements participating in internal network access from the Internet (in both directions) with documentation of data flow directions. Documentation should be kept up-to-date.

1.16. **Using proxy mechanisms** – Implementing proxy communication mechanisms in the organization. It is also recommended to link proxy mechanisms with dangerous domain lists, e.g., in Poland the list is maintained by CERT Polska: https://cert.pl/en/posts/2020/03/malicious_domains/.

1.17. **Increasing restrictions for externally available RDP services.** If these services should not be accessible, it is recommended to block them on edge devices. If RDP services are essential for business or organizational reasons, it is recommended to secure access with VPN mechanisms. To access RDP services, strong & secure passwords should be used that comply with the security policy and procedures of the organization. MFA protection should be implemented for remote access interfaces.

1.18. Analyzing the configuration of services and applications to eliminate default or non-compliant with internal policies settings, redundant services, and information.

1.19. **Regular software updates and security patch management** – Missing security updates significantly increases the risk of a successful ransomware attack on the organization. It is recommended to implement mechanisms for managing vulnerabilities within the organization, with high priority placed for systems accessible from external networks, particularly the Internet.

1.20. **Conducting tests and participating in cybersecurity exercises** – During a real incident, crucial decision-making is time-restricted. Preparing the organization through regular security testing and procedure drills is a critical element in handling ransomware incidents.

2. Execution

2.1. Enhancing the monitoring of PowerShell script execution – Utilizing two levels of logging available in Windows: PowerShell Windows Event Log and PowerShell Operational Log. Analyzing situations where unauthorized PowerShell scripts are executed.

2.2. Restricting the use of the PsExec tool – It is recommended to restrict the use of the PsExec tool by enforcing the UAC mechanism, limiting the tool only to selected administrative accounts, and logging and verifying every invocation of the PsExec tool. Example SNORT rule detecting PsExec use is available here: https://medium.com/@DatBoyBlu3/sigma-rule-psexec-command-execution-684bbc036cbe

2.3. Limiting network connections initiated by PowerShell scripts and system tools – Configuring restrictions for network connections initiated by PowerShell scripts, particularly connections to the Internet, such as *cmd /c powershell.exe iwr and other system tools (LOLBINs) like Bitsadmin, certutil, netuse, netcat, tftp, wget, debug, etc.* This limits the risk of downloading malicious payloads and progressing to further attack stages. Similar restrictions can be applied to other scripting engines like wscript, cscript, python. For development environments, an individualized approach to implementing restrictions is recommended.

2.4. Restricting the execution of macros in office document files – Hardening the configuration of office suites to limit the execution of unsigned macros. Blocking macros can be done via GPO: *Administrative templates > Microsoft Word > Word options > Security Trust Center > Block macros from running in Office files from the Internet* or *Disable all macros except digitally signed macros*.

2.5. Monitoring the process tree for unusual behavior – Monitoring for unusual behaviors such as document editors invoking programs like *conhost.exe, cmd.exe, cscript.exe*, etc. Creating rules that may indicate the execution of malicious software from macros in office documents.

2.6. Signing internally developed and used scripts and tools – Blocking the execution of unsigned scripts, and for mature environments, unsigned scripts with internal certificates generated for the organization.

2.7. **Monitoring or blocking the execution of script files .bat, .cmd, .js, .ps1, .py** – Implementing mechanisms to monitor the execution of scripts by non-administrator users. It is recommended to create a specific role for users who need to run scripts in their work. More restrictive permissions may also apply to executable files from outside the list of approved software in the organization.

2.8. **Detecting changes to PowerShell ExecutionPolicy** – Monitoring and verifying scripts that attempt to downgrade ExecutionPolicy levels, e.g., *jsRun.Run("cmd.exe /c PowerShell -ExecutionPolicy Bypass")*.

2.9. **Monitoring the installation of new services via PsExec** – Monitoring the installation of new services using PsExec, for example, through Auditing Windows Services event ID 7045 and keywords psexec in the content.

2.10. **Monitoring login processes and log-clearing operations** – During an attack, common actions by attackers include modifying login processes and clearing logs on infected devices. Implementing mechanisms to monitor such events is recommended.

3. Privilege Escalation

3.1. **Limiting the use of local administrator accounts and employing PAM (Privileged Access Management) solutions** – To reduce the direct use of administrator accounts, it is recommended to implement PAM solutions in the organization. These solutions enable secure access to administrative accounts and monitoring of their usage. Separate login mechanisms or session recording should also be considered.

3.2. **Monitoring and limiting the use of LOLBins[15] and their presence in process trees** – Solutions like EDR/XDR can help here. Consider excluding their use.

3.3. **Verifying LDAP queries** – Implementing mechanisms to monitor LDAP queries for Password Spraying, BruteForce, and LDAP enumeration attempts. Example SIGMA rule, SIGMA LDAP Recon:

[15] More information about LOLBins: https://socprime.com/blog/what-are-lolbins/

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/ldap/win_ldap_recon.yml

3.4. **Monitoring and verifying new domain controllers and their synchronization** – Implementing mechanisms to monitor the appearance of new domain controllers.

3.5. **Creating Canary user accounts** – Establishing dedicated Canary accounts in the organization that no one uses. Activity and login attempts on these accounts should be monitored and alerted, as they may indicate potential security breaches or privilege escalation attempts.

3.6. **Detecting SMB enumeration** – Implementing rules to monitor SMB share enumeration attempts. Example commands: *smbmap -u "" -p "" -P 445 -H <DC IP> && smbmap -u "guest" -p "" -P 445 -H <DC IP> smbclient -U '%' -L //<DC IP> && smbclient -U 'guest%' -L //*.

4. Defense Evasion

4.1. **Using a whitelist of approved applications** – Users should not be able to install and use (portable) applications that have not been vetted for security and approved for organizational use. The list of applications should be regularly updated and maintained. A central repository of approved applications for user download should also be maintained.

4.2. **Monitoring the deactivation of security mechanisms** – Implementing detection and alert mechanisms against disabling of antivirus/EDR/XDR/HIPS services/processes. Monitoring Event ID 7040 in Auditing Windows Services for changes in security services.

4.3. **Mutual monitoring of security agents** – Reporting when any security mechanism is disabled while others are still running. If possible, detecting the process of reinstalling antivirus software, for example.

4.4. **Enforcing updates to security system signatures and rules** – Ensuring timely updates to signatures and rules in security systems.

4.5. **Monitoring the use of net.exe stop and net.exe start commands** – Example usage of *net.exe stop "service_name"* to stop a service.

4.6. **Monitoring registry keys responsible for security solutions** – Implementing mechanisms to monitor and alert on modifications to registry keys responsible for security solutions and systems, such as: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*.

4.7. **Monitoring changes in backup configuration (VSSADMIN)** – Implementing mechanisms to detect and alert on changes in backup configurations using built-in tools like *vssadmin.exe*.

4.8. **Monitoring the use of taskkill.exe and Pskill.exe commands** – These commands may be used to disable security mechanisms and agents installed on the host. Example command disabling Sophos antivirus: *cmd.exe /C taskkill /F /IM SavService.exe*.

4.9. **Detecting new hosts in the network** – Implementing mechanisms to detect new unauthorized devices in the internal network.

4.10. **Monitoring changes to scheduled tasks configuration** – Implementing mechanisms to monitor modifications to scheduled task configurations in the system.

4.11. **Monitoring the use of sc.exe command** – It is recommended to monitor the use of the built-in *sc.exe* utility. Ransomware may use it to install, modify, or disable services and security mechanisms.

5. Credential Access

5.1. I**mplementing multi-layered security measures** – To better protect the organization, particularly critical systems, it is worth considering a "Defense in Depth" approach. This includes implementing multi-layered security measures (such as protecting the network perimeter, intrusion detection systems, network segmentation, and workstation protection) and mechanisms to restrict access at various levels of the network infrastructure (e.g., access levels, network

segmentation). It is also worth considering implementing access control lists (ACLs) to limit access to resources only to authorized users and devices.

5.2. **Identity Hygiene** – Implementing a requirement in the organization to use multi-factor authentication (MFA). Establishing a process for identity and access management (IAM), including regular reviews of permissions to minimize situations where employees have unnecessary permissions for their job roles and removing unused or inactive user accounts.

5.3. **Monitoring user activity** – Implementing systems to monitor logins and user activity and ensuring alerts are handled at the highest acceptable level.

5.4. **Building employee awareness** – Conducting regular training on cyber threats and information resource protection, recognizing attack attempts, and procedures for reporting incidents.

5.5. **Protecting administrator accounts** – Implementing additional security measures for privileged user accounts, including those with administrative rights. These accounts should not be used for daily work that does not require elevated privileges. Minimizing the number of accounts with Enterprise Administrator or Domain Administrator rights.

5.6. **Domain administrator privilege separation** - AD Tier model – Implementing a separation of administrator privileges, such as the AD Tier model, which separates administrative rights into three levels according to Microsoft's recommendations[16].

5.7. **Detecting and blocking programs that perform memory dumps of the LSASS process** – To obtain credentials from this process, cybercriminals often use tools such as Mimikatz, Sysinternals ProcDump, PPLdump, HandleKatz, and nanodump. Implementing mechanisms to detect the operation of such tools and attempts to perform memory dumps is recommended, as well as mechanisms to protect against such actions, e.g., ASR for LSASS.

[16] https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model; https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges

5.8. **Implementing LAPS (Local Administrator Password Solution)** – Where possible, implementing LAPS mechanisms for local administrator accounts is recommended.

6. Discovery

6.1. **Monitoring network connection reconnaissance attempts via arp.exe** – Implementing mechanisms to detect the invocation of the *arp.exe -a* command, which may be used by malicious software to discover the infrastructure.

6.2. **Monitoring reconnaissance attempts via nslookup.exe** – Implementing mechanisms to detect reconnaissance attempts using the nslookup command.

6.3. **Monitoring the use of other tools and commands** – Implementing mechanisms to detect the use of tools and commands only used by qualified and authorized personnel in specific cases but also available to attackers, e.g., commands like net: *net view* / *GetIPNetTable*.

7. Lateral Movement

7.1. **Network segmentation** – It is recommended to separate individual networks and subnets within the organization. Implementing appropriate network segmentation will significantly hinder attackers from spreading the ransomware attack.

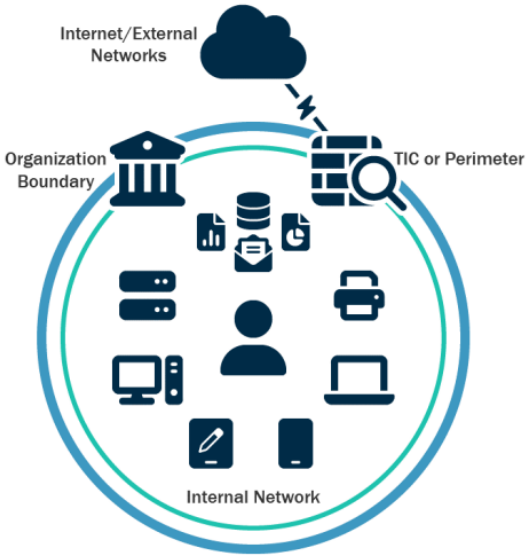

Figure 2: Flat (Unsegmented) Network

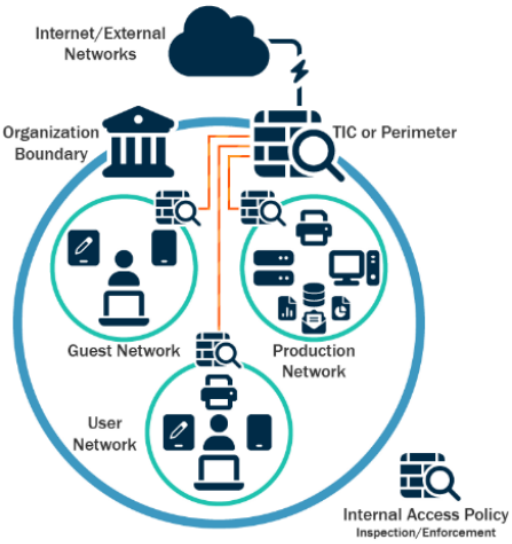

Figure 3: Segmented Network

Figure 1 Sample Network Segmentation Diagram[17]

7.2. **Monitoring the use of RDP** – Implementing mechanisms to monitor attempts to connect via the RDP protocol where the source hosts are not jump stations.

7.3. **Securing domain controllers** – Domain controllers are often targeted during ransomware attacks due to their potential to gain wider access to other infrastructure elements. Special care should be taken to secure them. Implementing security measures according to Microsoft's recommendations[18] and conducting security tests on domain controllers to verify their security level with tools like BloodHound, Adalanche, or PingCastle is recommended.

8. Persistence:

8.1. **Monitoring registry keys used by attackers** – Implementing mechanisms to monitor and alert on modifications to registry keys used by attackers to maintain access to the infrastructure (persistence), e.g.:

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

[17] https://www.cisa.gov/resources-tools/resources/stopransomware-guide
[18] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

8.2. **Monitoring registry keys created for new services** – Implementing mechanisms to monitor the addition of new services by modifying registry keys: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*

9. Command and Control:

9.1. **Monitoring connections to known Command & Control (C2) servers** – Implementing mechanisms to monitor network traffic for communication with C2 servers. It is also recommended to link proxy mechanisms with dangerous site lists, e.g., those maintained by CERT Polska[19].

9.2. **Implementing rules and monitoring detected beaconing attempts to C2 servers** – It is recommended to enable network traffic analytics in proxy, IDS/IPS, or firewalls to find patterns of connections indicating beaconing (cyclical connections to C2 with similar time intervals) [20] . Alternatively, enabling appropriate rules in SIEM systems if they analyze network flows. More about beaconing detection rules can be found here [21] .

9.3. **Implementing rules to detect commercial tools like Cobalt Strike** – Attackers often use popular commercial tools used in penetration testing, such as Cobalt Strike, in their attacks. It is recommended to create or enable built-in security solution rules to detect the use of such tools in the organization's infrastructure.

10. Exfiltration

10.1. **Limiting traffic to TOR network exit nodes** – Implementing monitoring and limiting network traffic exiting to detect attempts to connect from the internal network to the TOR network, e.g., by blocking known TOR exit nodes or restricting ports 9001, 9030, and 9090 on edge devices. It is also recommended

[19] https://cert.pl/en/posts/2020/03/malicious_domains/
[20] https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic
[21] https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic

to limit the ability to install and use TOR communication software by users, such as torify, Tor browser, torsocks.

10.2. **Restricting DNS over HTTPS (DoH) traffic** – Attackers use DNS over HTTPS to mask their communication. It is recommended to analyze the possibility of restricting such communication and implementing mechanisms to limit users' ability to enable it in the web browser[22]. Example use of DNS over HTTPS: https://8.8.8.8/resolve?type=TXT&name=onet.pl.

10.3. **Monitoring or blocking traffic to file-sharing services** – If there is no business or organizational justification, it is recommended to restrict access and the ability to upload files to file-sharing services. Monitoring and restricting the ability to upload to specific services is advised.

10.4. **Monitoring or blocking SMB/TFTP/FTP/SFTP traffic to the Internet** – If there is no business or organizational justification, it is recommended to block the ability to connect using TFTP/FTP/SFTP protocols on edge devices or restrict connections to trusted services/hosts within the organization.

10.5. **Monitoring network anomalies** – Implementing mechanisms to monitor network anomalies, such as a large volume of data being sent to the Internet or unusual times when network traffic occurrs. Setting up monitoring rules, if possible, enabling anomaly analytics, and defining thresholds for outgoing traffic transfer to trigger alerts and event analysis.

11. Impact

11.1. **Creating rules to monitor mass file overwriting and integrity breaches** – Mass modification of files and integrity breaches may indicate encryption attempts.

11.2. **Creating rules to detect the execution of libraries like pycrypto used in encryption processes** – It is recommended to create rules in EDR/XDR antivirus or sysmon tools to monitor the use of cryptographic libraries used for file

[22] https://techdocs.akamai.com/etp/docs/disable-doh-browsers

encryption by unknown software not on the authorized software list, or unsigned. Examples of such libraries include: bcrypt.dll, pycrypto, pycryptodome, cryptography. Below is an example sysmon rule. Exceptions should be applied to limit potential false-positive detections.

```
<Sysmon schemaversion="4.0">
  <EventFiltering>
    <ImageLoad onmatch="include">
      <ImageLoaded condition="end with">bcrypt.dll</ImageLoaded>
    </ImageLoad>
  </EventFiltering>
</Sysmon>
```

11.3. **Ensuring secure access to backups** – Ensuring that unauthorized users and malicious software cannot access or interfere with backups. Backups should not be stored on the same servers they were created from. When creating backups sent to the backup location over the network, it is recommended to create rules allowing backup tools and systems to create new backups without the ability to delete or overwrite them. The role of the Backup Administrator should be particularly protected (usually it has access to all storage spaces).

11.4. **Preparing and maintaining critical data backups** – During a ransomware attack, the availability and integrity of backups are crucial for maintaining organizational continuity. Regularly testing backups to ensure they are correctly executed and can be restored is essential. It is also worth maintaining and regularly updating a “Golden Image” – reference images of systems that significantly streamline the process of restoring infrastructure availability.

Appendix 2: Sample Contact List Template in the Escalation Path (list for customization/modification)

It is advisable for the organization to establish a notification path, considering that different individuals/units will require varying levels of information to take actions based on their respective competencies and internal procedures. Additionally, where possible, it is also beneficial to establish alternative contacts in case those listed are unavailable, as well as alternative communication channels.

Operation Units:

PERSON'S DETAILS/ POSITION/ROLE/ TEAM NAME	PHONE	E-MAIL	PREFERRED CONTACT METHOD	WORKING HOURS

Managment/Reporting Units:

PERSON'S DETAILS/ POSITION/ROLE/ TEAM NAME	PHONE	E-MAIL	PREFERRED CONTACT METHOD	WORKING HOURS

Vendors:

VENDORS	PHONE	E-MAIL	PREFERRED CONTACT METHOD	WORKING HOURS

References:

https://attack.mitre.org/

https://cert.pl/lista-ostrzezen/

https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf (PL language version)

https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://medium.com/@DatBoyBlu3/sigma-rule-psexec-command-execution-684bbc036cbe
https://socprime.com/blog/what-are-lolbins/

https://techdocs.akamai.com/etp/docs/disable-doh-browsers

https://unit42.paloaltonetworks.com/trigona-ransomware-update/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

https://www.cisa.gov/resources-tools/resources/stopransomware-guide

https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf

https://www.cisa.gov/stopransomware

https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic

https://www.hhs.gov/sites/default/files/medusalocker-ransomware-analyst-note.pdf