Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Ransomware incident response plan

The incident response cycle, applied to ransomware

Version managment

Version	Reason / amendments	Date
0.1	First draft	Nov. 2021
0.3	Review from NCSC theme incident response processes	Nov. 2021
0.8	Review within NCSC unit operation	Jan. 2022
0.9	External review	March 2022
1.0	Final format	May 2022
1.0	English translation	June 2022

This document was produced with contributions from Ahold Delhaize, the Betaalvereniging, CIBG, Equens and the Police.

Permitted distribution: TLP WHITE

(Traffic Light Protocol)

This guide contains the label TLP: WHITE and is distributed by the NCSC. The NCSC uses the Traffic Light Protocol (TLP) to define clearly and unambiguously what may be done with the information it provides. If information has a TLP designation, you will know with whom you may share it. This is described in the First standard (www.first.org/tlp). Recipients may share the information from this guide within their organisation and outside it, and the information may also be published.

We welcome your responses at info@ncsc.nl

Contents

Intended use of this plan 4

Incident response 5

Preparation 6
Continuity management 6
Design and design principles 6
Inventory and configuration management 6
Monitoring and detection 7
Processes and procedures 7
Accounts and rights 8
Technical measures 8
Employee awareness 8

Identification 10

Containment 11

Eradication 12

Recovery 13

Lessons learned 14

Related information 15
Sources of information 15
Contact details 15

Appendix 1: Schematic representation of a ransomware attack 16

Intended use of this plan

This plan is intended to prepare for and support incident response. Also known as a playbook, this plan serves organisations that have been, or think they may be, affected by a ransomware attack. It is important to stress that good preparation is essential for an effective incident response. Ransomware can be a serious threat to (ICT) services for an organisation with a long-term and costly impact. In the light of such a potentially serious incident, it is good not to have to think about what to do from scratch, but to have an initial outline to work from.

This document is organised according to the steps described in the SANS incident response cycle[1]. If it is used to increase resilience to a ransomware incident, the first phase will be particularly important. It includes a wide range of aspects that will not suit all organisations equally. First of all, these are basic measures that can be used in recovery operations. In addition, there are more advanced measures to limit the impact of an attack or to detect an attack early. Due to the diverse nature of the measures, their implementation will also vary greatly. Existing measures can sometimes be tightened up to make them more effective. In other cases, the introduction involves an entire project, including appropriate processes and procedures.

When an organisation has already been affected by a ransomware attack, an effective response is essential and the phases from 'identification' onwards can provide a handle for the approach.

When using this plan, it is important to select only the relevant parts and translate them into the current situation. In addition, specific measures and activities for the organisation will have to be added in order to obtain an appropriate approach.

[1] The SANS Incident Handler's Handbook can be found at: https://www.sans.org/white-papers/33901/

Incident response

Definition

For the purpose of this incident response plan, we define a **ransomware incident** as a digital attack that disables systems or files by encrypting them and holding data hostage. This hostage-taking is accompanied by extortion, whereby decryption is offered in return for a payment, usually in crypto-currency.

There are variations of ransomware extortion where, in addition to encryption, data is also stolen and threatened to be leaked if payment is not made (*double-extortion*) and where there are threats to disclose data to customers or to extort customers with the captured data (*triple-extortion*).

Appendix 1 contains a schematic representation of how a ransomware attack works, as described by the New Zealand National CERT (CERT NZ).

It is important to note that *ransomware is not just a technical problem*. In most cases, this involves serious, organised cybercrime. The police and the Public Prosecution Service are making efforts to combat this, but can only do so if cooperation is sought with them. This can be done by reporting the matter to the police.

When carrying out incident response, it is important to always keep a number of points of attention in mind. When resolving the disruption under pressure, these are easily lost out of sight. We list these below.

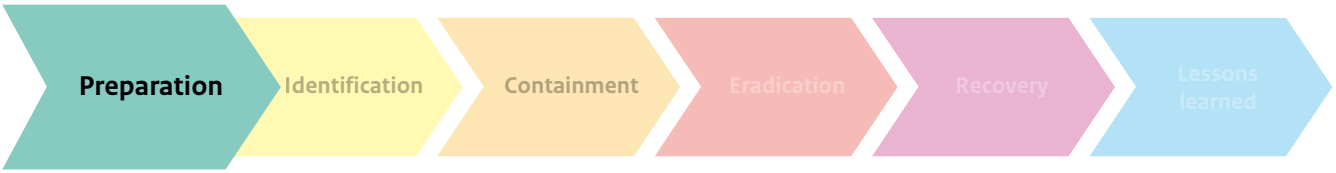
Points of attention for the incident response

- Adhere to agreed incident response procedures and agreements;
- Proceed systematically;
- Make notes of your findings and activities (keep a log with date and time);
- When communicating and recording, confine yourself to facts, explicitly state what conclusions are drawn and avoid assumptions;
- Make sure that all those involved are kept informed of the current status and information;
- Communicate regularly and announce the next communication moment each time;
- Stay calm and keep in contact with the incident response team, CERT or CSIRT.

Communication

Communication is one of the strategic processes that help manage a disaster and/or crisis. For the internal organisation, it is important to offer employees clarity in order to prevent noise and unrest on the shop floor. To the outside world, communication is used to protect and/or restore the organisation's reputation and trust. This requires that as much uncertainty as possible be removed by carefully providing information, offering a perspective for action and making sense of what is happening. Stakeholders benefit most from open communication to limit consequential damage.

Preparation



In preparing for this type of incident, the following actions can be carried out per theme.

Continuity management

- Where appropriate, there will be a need for an integrated approach coordinated with network partners. Therefore, have contracts and service level agreements (SLAs) in place that regulate the presence and availability of the partners involved;
- Ensure that there are 24x7 standby managers on duty for the critical facilities. Pay attention to the application of and compliance with the terms and conditions of employment law;
- Have images (quickly) available to provide critical systems with a basic setup when deploying in a clean environment;
- Provide (rapidly) available spare hardware and available software to redeploy critical systems in a clean environment;
- Provide a recovery plan (dependencies, manner and order of recovery, responsibilities, system owners) of the ICT systems and the critical systems and test and update this regularly.

Back-up

- Determine what form of backup (incremental or full) is necessary and what retention time should be used;
- Provide a periodic offline backup of central and decentralised data;
- Ensure that all systems and virtual machines (VMs) are periodically backed up;
- Check each backup result and periodically the backup process for possible errors;
- Regularly verify the integrity of the backup (by performing a restore, for example);
- Regularly test the backup against the agreed recovery point objective (RPO) and recovery time objective (RTO) (*see related information*);
- Store backups or backup media offline and off-site;
- Ensure that online and offline backups cannot be accessed using the same accounts; use accounts other than standard management accounts (including multi-factor authentication).

Design and design principles

- Segment the network according to both functionality and security level. Preferably follow the *zero trust* principle (*see related information*);
- Apply system hardening according to vendor guidelines or CIS benchmarks (*see related information*);
- Give users and administrators minimum rights, apply the principle of least privilege;
- Use a secure VPN solution that complies with TLS guidelines (*see related information*);
- Only connect management interfaces to a management (V)LAN;
- Use strong passwords and do not reuse them. Where possible, supplement authentication with multi-factor authentication (MFA) (*see related information*);
- Limit the use of local administrative accounts;
- Ensure that local administrative accounts on different systems have different (random) passwords. For example, use the Microsoft Local Administrator Password Solution (LAPS);
- Limit, protect and monitor the use of Active Directory domain administrator accounts;
- Turn off access to systems via RDP unless there is no other way. If no alternative is available, secure remote access channels and RDP with, for example, MFA and a VPN solution, and log their use.

Inventory and configuration management

- Identify critical systems and determine the impact when they are affected by ransomware;
- Provide an up-to-date and complete overview of systems and interdependencies;
- Record the configuration of systems with each change;
- Develop and maintain infrastructure designs containing critical systems and data flows. Take account of supply chain partners and outsourced services;
- Ensure that product maps and architectural records of the critical facilities are available and up-to-date.

Monitoring and detection

- Ensure the security of the email environment, including scanning for attachments or internet links;
- Provide (secure and centralised) logging in the network of:
- Executed (powershell) scripts and attempted excution of (powershell) scripts;
- Event-Ids for authentication;
- Event-Ids for creating services and persistent processes;
- (Large) outgoing data streams;
- Event-Ids for creation or modification of (privileged) accounts
- Use canary files (documents or files that should not be used and modified) to detect unauthorised changes to the file system;
- Monitor the use of sensitive management accounts, such as Domain Admin accounts.

Processes and procedures

Communication

- Take account of the breakdown of regular communication channels (telephone, email, address book access, chat), prepare, test and keep up-to-date confidential alternatives or fall-back options;
- Define an internal and external communication strategy. Ensure that stakeholders (employees, spokespersons/press officers, chain partners, customers, board of directors, data protection officers, etc.) are informed in a timely manner and take into account:
  - The purchasing department may be able to help by providing an overview of suppliers;
  - Involve the legal department in the preparation and possibly have an external communication manual approved in advance;
- Determine the communication strategy when stolen data is published, including:
  - Which senders and recipients are important;
  - Which messages should be sent;
  - Which supervisory authority or authorities (including the Dutch Data Protection Authority) must be informed;
  - Which other organisations need to be informed (NCSC, police, etc.);
- Determine a strategy for dealing with the ransom note. Contacting the hostage takers can be important in order to determine whether data has been stolen and what data sources have been accessed. In addition, criminals should share information during negotiations; this increases the chances of successful detection. *It is important to note that having contact with the hostage takers does not mean that a ransom has to be paid.* The urgent advice from the police and from the Government remains not to pay a ransom after a ransomware attack, as this maintains the criminal revenue model.[2]

Moreover, payment does not guarantee that the problem is resolved: there are known cases where the decryption does not take place (completely) even after payment; the attacker may still be in your network even after payment; the attacker may have stolen your data and blackmail you again later (the perpetrator now knows that you are willing to pay). For the contact about the ransom note, take account of:

- Who should be called in to hold a discussion with the hostage takers;
- What information must be established in a negotiation/ discussion;
- How a ransom demand is handled;
- Who reports the matter to the police and when is it reported.

Incident response

- Prepare an incident response plan, including:
  - Who should be involved in a cyber security incident;
  - How, on the basis of which criteria and by whom is it determined that there is a security incident;
  - Who is responsible for resolving the incident;
  - How and when to connect to regular (ITIL) incident management procedures;
- Know who the internal key players and external stakeholders are;
- Make the mandate of those involved explicit, especially which officer has the power to switch off a service or facility;
- Describe the role and structured work process of the incident response team. Also describe the desired requirements and competences per role of the team, in the form of job descriptions;
- Introduce a standard structure for crisis consultations, in which situational awareness can be shared and decisions can be reached. A process of crisis decision making within a crisis management team could be:
  1) establish the situation (perception of data);
  2) comprehension (determine the meaning of the situation, identify the issues and analyse them and set the direction);
  3) take action (determine what to do with the issues; can we solve them ourselves, who do we need to involve and what strategic decisions do we need).
  And practice the consultation according to this structure;
- Ensure that the members of the incident response team have sufficient rest and sleep during the performance of the incident response;
- Equip those involved with the means to communicate quickly and easily as a team even outside office hours. Make it possible for those involved to work from the office environment (including the back-up location) outside office hours;
- As various ransomware incidents have shown that ransomware is often executed on the systems on Friday evenings, it is useful to take this into account for picket roles and the availability of incident response team members;Arrange for a contract with a service provider or incident response party to support and carry out, for example, recovery and forensic investigations;

[2] https://www.nomoreransom.org/en/ransomware-qa.html https://www.politie.nl/nieuws/2020/februari/6/00-politie-%E2%80%98niet-betalen-bij-ransomware.%E2%80%99.html https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2021Z16018&did=2021D37453

- Simulate and practice a ransomware attack with employees. Evaluate this exercise and use it as input to update the incident response plan where necessary;
- Take into account guidelines, legislation and regulations (e.g. for informing supervisors, stakeholders and authorities) and incorporate this in the incident response plan. Also take into account the possibility of making a voluntary WBni report or a mandatory WBni report to the NCSC or the CSIRT DSP;
- Be prepared to report the matter to the police. This will give the police better insight into the phenomenon of ransomware and enable them to give it the appropriate priority. Refer to the brochure 'Samen tegen Cybercrime, Stappenplan voor IT-specialisten' (Together against Cybercrime, Step-by-step plan for IT specialists), which has been drawn up by the police to take measures that support the investigation of crime (*see related information*). Making a report or announcement can also prevent new attacks. This allows the police to warn other organisations or disable servers with malicious software.

Accounts and rights

- Delete unnecessary or unused user accounts and groups;
- Assign minimum domain, admin and root privileges to accounts;
- Restrict access to domain controllers to a separate domain administrator group;
- Limit the rights of the domain administrator group and use the member accounts only for administration on the domain controllers. Create separate administrator accounts for other management tasks;
- Log the use and login of management accounts (both successful and unsuccessful login attempts).

Miscellaneous

- Make sure that the network can be monitored on:
  - Which (unknown) files have been or are being executed;
  - Which (powershell) scripts have been or are being executed;
  - Which 'lateral movement' between workstations/endpoints is taking place or has taken place;
  - Which (large amounts of) data is or has been exfiltrated;
  - Who logged on to which system or used resources;
- Establish a procedure for forensic image creation of workstations and servers and test it regularly;
- Have an implemented patch and upgrade policy and update systems (servers and workstations) regularly; base the priority and schedule of patching on the severity of the remedied vulnerabilities;
- Provide an emergency patch and update process to immediately mitigate critical vulnerabilities.

Technical measures

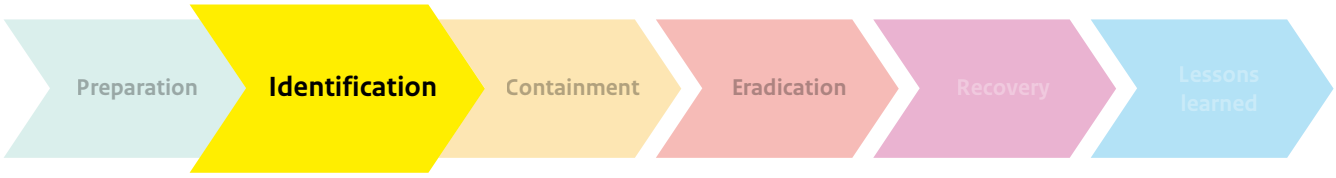
- Install an Endpoint Detection and Response (EDR) tool on both clients and servers;
- Implement network segmentation based on function (development, test, acceptance and production) and data classification (public, internal, confidential, secret, personal data, special data);
- Implement multi-factor authentication (MFA);
- Maintain and check antivirus software; scan any software downloaded from the internet before running it;
- Centrally disable macros in office software so that macros in infected files cannot be executed;
- Turn off following web links or opening images in emails;
- Turn off the Remote Desktop Protocol (RDP) on the internet side (ransomware often spreads by malicious actors who have compromised organisations via RDP);
- Check the periphery of the network for the presence of management interfaces on the outside and switch them off;
- Consider using PowerShell constrained language mode to limit PowerShell usage;
- Consider applying additional PowerShell logging measures, such as: Module logging, Script-Block logging and Transcript logging;
- If you use Windows operating systems, consider applying Applocker and Windows Defender Application Control to limit the use of unwanted scripts and software;
- Use the 'Protected Users' Active Directory group in Windows Active Directory for privileged user accounts to make pass-the-hash attacks more difficult;
- Consider application whitelisting;
- Do not install additional software on domain controllers or on other systems, and remove already installed software that is not needed;
- Disable unnecessary services on domain controllers and other servers, and disable the print spooler service on domain controllers;
- Block internet connectivity on the domain controllers. Updates can be retrieved via a WSUS solution;
- Consider implementing additional Local Security Authority (LSA) security on Windows servers (the LSA process validates (local and remote) user login and ensures the application of security policies);
- Determine and configure the use of Bit-Locker or other disk encryption (if not used, it can be used by attackers);
- Block the use of unauthorised USB devices and configure the permitted use of authorised USB devices;
- Consider filtering outgoing traffic on the firewall, configure which applications and servers are allowed to communicate with the outside world.

Employee awareness

- Employees include temporary staff, advisors and seconded staff.
- Ensure there is knowledge and awareness among employees about:
  - Phishing variants and how to recognise them;
  - Identifying social engineering;
  - The spread of malware and ransomware;

  - Recognising a ransomware infection and how to respond to this;
  - How to report suspicious observations or possible contaminations;
  - Using different passwords for different systems and environments (support employees in this by offering a password manager);
  - The desired use of company property and mobile devices;
  - The organisation's social media policy;
- Make it easy for employees to report suspicious email messages, for example by providing a menu option or button for this;
- Make a list of key officials and make them aware of the possible espionage risks due to their function or position within the organisation;
- Provide a policy plan for education, training and exercise of, among others, the above aspects, and implement the plan

Identification

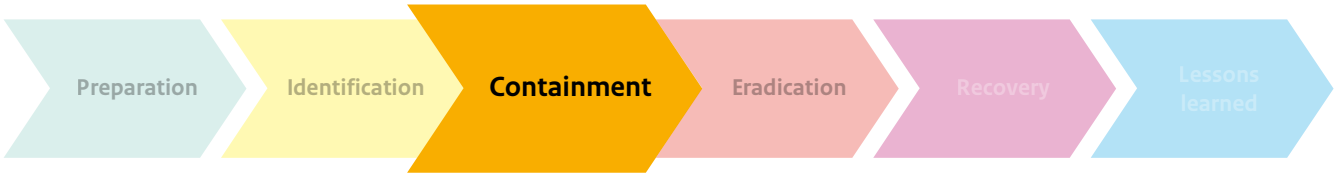


Preliminary remark: A ransomware incident may manifest itself with a large-scale disruption of (ICT) services because file systems have been encrypted. This may require an immediate start to restoring a (clean) environment in order to resume services as soon as possible. *However, it is still necessary to run through the incident response cycle in parallel with recovery, starting with identification.* After all, it is important to deny malicious actors access to the network and keep them from regaining access to the network in the future.

The following may be an indication of a ransomware incident. This also includes a number of activities, which can be carried out for identification purposes:

- Unusual invoices or other business emails, possibly with malicious attachments or links;
- Ransomware messages on the file system;
- Ransomware messages on the screen;
- Ransomware messages via email;
- Employees report that they can no longer open their files;
- Large numbers of files are (successively) modified on a (network) file system;
- An unusual (large) amount of data is diverted;
- System analysis leads to identification of server-side encryption. Investigate:
  - In Windows under computer management under 'Sessions' and under 'Open Files'; check for connected systems/users;
  - Ownership of encrypted files; check the account that is writing these files;
  - The RDP event log; check for unexpected successful RDP connections;
  - The Windows Security log and SMB log; check for authentication events;
  - Network communication via the SMB protocol to identify open connected systems;
- Unusual activity is observed on a system or malware is found that can encrypt a file system (or can download modules that can encrypt a file system). Examination:
  - Unusual binaries;
  - Forensic images of memory;
  - Unusual processes;
  - Unusual tasks in the Task Scheduler
  - Unusual patterns of email attachments;
  - Unusual network or web browsing activity, for example TOR traffic or traffic to cryptocurrency payment sites;
- Malicious communications or network traffic may be taking place. These include:
  - Known patterns of exploit kits;
  - Connections to (known) C2 servers;
  - Unusual network traffic or web browsing activity, for example TOR traffic or traffic to cryptocurrency payment sites;
  - Emails with links to suspicious or malicious websites;
  - Unusual attachments in emails (attachments of a type that an employee does not normally receive, attachments from a sender who does not normally send attachments or attachments from an unknown sender);
- Announcements are made of a successful ransomware attack by known actors on the dark web;
- Exfiltrated data or files from a ransomware attack are offered on the dark web;
- A phishing attack is carried out with characteristics that can be traced back to known ransomware attacks (use DMARK logs or DNS logs if necessary);
- After observing a ransomware attack, provide an up-to-date situational picture (which systems have been affected and what is the function of those systems, who is responsible for that system) and an impact assessment so that measures to be taken are consistent with this;
- It is important to identify 'Patient Zero' in order to understand how the attacker got in and to deny access at a later stage (e.g. look for where unusual activity occurred after receiving a phishing email, from where C2 communication occurs or where common ransomware-related tooling is used, such as installation of a keylogger, exploitation of a vulnerability using Metasploit, execution of Mimikatz or Cobalt Strike);
- Based on the current situational picture, determine whether it is necessary to make a voluntary or mandatory Wbni report to the NCSC or to CSIRT DSP;
- Monitor supply chain partners (customers, suppliers or cooperation partners) for reports of possible ransomware infections.

Containment



To contain the consequences of this type of incident, the following actions can be taken:

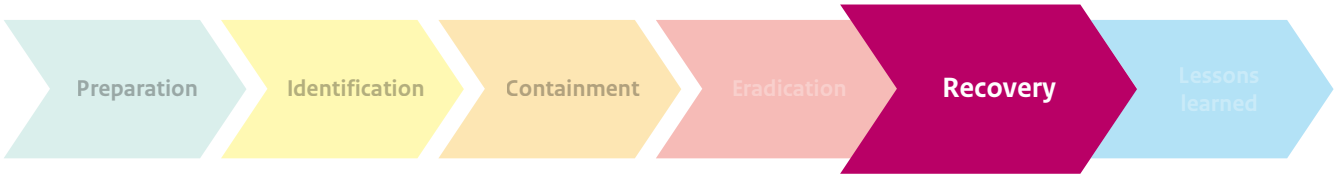
- Immediately disconnect systems from the network (on all interfaces: wired, Wi-Fi or mobile) that have been identified or are suspected of being compromised (with ransomware) (disconnection is also possible by activating aeroplane mode);
- Do not turn systems off, but put them in sleep mode or possibly hibernate mode (if available, e.g. on laptops). This is so as not to disrupt the system's condition and thus obtain the best possible image, to prevent the loss of any key material present and not to lose any forensic traces for possible investigation;
- In the event of a major attack, consider disconnecting network infrastructure, such as Wi-Fi, routers and switches and internet connectivity; if possible, disconnect networks or network parts not yet affected by the ransomware;
- Immediately disconnect external devices, such as USB/external drives, mobile phones or other devices that may become infected;
- Disconnect the network file storage if a system cannot be isolated or disconnected from the network;
- Block or deactivate all accounts (potentially) involved in the ransomware attack;
- Reset passwords and other forms of authentication for administrator and other system or service accounts (note: resetting the password of the KRBTGT service account must be performed twice in succession otherwise access with the old password will remain possible) (see related information);
- Reset user passwords;
- Remove write permissions on file systems from processes or accounts with which ransomware is executed;
- Check that MFA is still set on the accounts and for access to services where it is intended and correct where necessary if a malicious user has disabled MFA;
- Block traffic with potentially identified C2 servers;
- Submit the (characteristics of) as yet unknown malware found in the incident response process or forensic analysis to the endpoint security provider and the NCSC;
- Submit as yet unknown malicious URLs, domain names or IP addresses to the network security provider and the NCSC;
- Report the incident as soon as possible to prevent further damage (contact information can be found at the end of this document);
- Collect possibly relevant log files, such as: Windows Security logs, Email logs, Firewall logs and Linux System logs;
- If a supply chain partner is potentially infected, block the exchange of email and network traffic with this organisation until it is clear that the risk of infection has been eliminated;
- Consider informing the police in this incident response phase. There have been occasions when the police have been able to intervene in the channelling of information to leak pages. It may also be possible for the police to warn other (potential) victims in time. It is also relevant at this stage to think about securing evidence, such as communication channels and BTC addresses. Refer to the brochure 'Samen tegen Cybercrime, Stappenplan voor IT-specialisten' (Together against Cybercrime, Step-by-step plan for IT specialists), which has been drawn up by the police to support the investigation of crime (*see related information*).

Eradication

Note: *Do not proceed with eradication until it is clear that the entire scope of the attack has been mapped and no new infected machines are found. Moving too quickly with eradication may inform an attacker of the incident response actions taken and may leave behind an attacker's backdoor or dormant malware.*

- To eradicate the breach or impact of this type of incident, the following actions can be taken:
- Delete the malicious binaries and, if applicable, corresponding registry values from (centrally stored) compromised user profiles and systems (also consider %ALLUSERPROFILE%, %APPDATA% and %SystemDrive%). If cleaning is not possible, consider deleting (centrally) stored user profiles;
- Reinstall affected systems with a clean image after any locally stored data and files have been quarantined;
- Record metadata such as signatures and origin of the malware, domains and IP addresses and block known malware (communication);
- Update antivirus signatures so that the identified malware is blocked;
- Identify the system where the first breach occurred and remedy the cause or potential vulnerabilities.
- Implement the established internal and external communication strategy. Ensure that stakeholders (employees, chain partners, customers, board of directors, etc.) are informed in a timely manner.

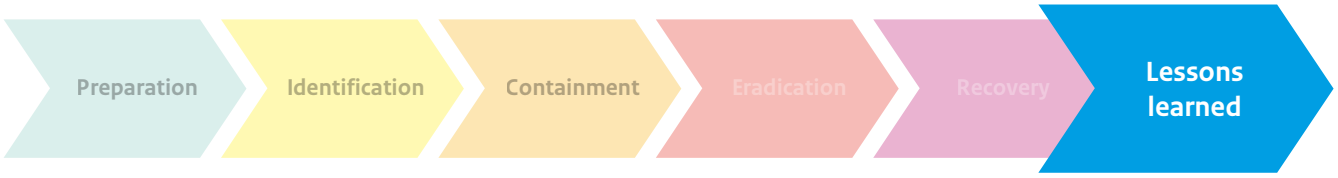
Recovery



To recover from this type of incident, the following actions can be taken:

- In the event of a major attack, consider building the network and associated systems in parallel to the existing environment. Do not import systems or data without thoroughly checking them for the presence of malware. Do not connect systems to the clean environment that have been connected to the infected environment;
- If it is not possible to build a new environment parallel to the existing one in the event of a major attack with possible compromise of the Active Directory, consider building a new permission structure with new accounts, including management and service accounts, and (permanently) deleting all old accounts;
- Only use carefully certified secure systems for recovery;
- Make sure all malicious binaries that were present are removed from the systems if they need to be reconnected and cannot be reconfigured;
- Check with the No More Ransom project (*see related information*) if there are any known decryption keys or software available for the ransomware used in this incident;
- Contact law enforcement agencies to report the incident and obtain possible decryption keys;
- Share (technical) information about the incident with the police. This can be by means of an official report, but also by providing information. This can assist with the (international) detection and disruption of offender groups and it can lead to the notification of other (potential) victims;
- Scan backups for malware before restoring. The malicious actors may have been in the network for a long time, so that malicious files could have ended up in the backups;
- Scan quarantined data and files and remove any malware found;
- Restore encrypted or compromised servers or systems from an uncompromised backup;
- Recover encrypted files from an uncompromised backup;
- If decryption or recovery from a backup fails and there is a data loss, a copy of the encrypted information can be retained. If a method of decrypting the information is found later, it can still be retrieved.
- Correct any unwanted configuration changes that may have been made by the malicious parties;
- Test and verify whether the abnormal behaviour (e.g. network traffic) has disappeared after restoring all systems and processes;
- Monitor the network intensively for some time to make sure that the attacker has disappeared from the network and cannot get back in;
- Upgrade and update outdated software and systems.

Lessons learned



Lessons can be learned from such incidents after recovery, which in turn can lead to further preparatory actions. As these lessons learned are specific to each incident, they cannot be determined in advance. However, it is vitally important to go through this phase. All preparatory actions already carried out can also be evaluated in this step. In order to obtain useful feedback for the lessons learned, an after-action review can be performed with those involved at the conclusion of the active incident response, so that experiences can be shared fresh from the experience.

The quality of reporting is improved if there is always someone present who performs the role of reporting at all stages so that all steps, decisions, documents, etc. are recorded correctly, on time, completely and in a verifiable manner (in addition to the individual logs kept by employees).

It is recommended that the lessons learned be included in a report. It is recommended to pay attention to the following issues, among others:

- Dissemination: who will receive the report;
- Target group of the report;
- Initial infection;
- Activities and timeline;
- Targeted systems;
- Impact on availability;
- Influence on or dependency on (supply chain) partners, customers, suppliers or other stakeholders;
- Characteristics of the ransomware used (IOCs);
- Risks of possible leaked data in the outside world;
- Effectiveness and execution of the incident response process (what went well and what could be improved);
- Costs and lead time of the incident;
- Which documentation needs to be modified on the basis of the lessons learned and who will do this;
- How do you inform the organisation of these changes;
- Changes to be implemented to prevent future similar incidents or to reduce their impact, relating to:
  - System adaptation and technical modifications;
  - Adjustments to procedures and policies;
  - Adjustments to incident response procedures or to specific incident response plans;
- Share found indicators and report with the NCSC so that other organisations can be alerted or informed.

Related information

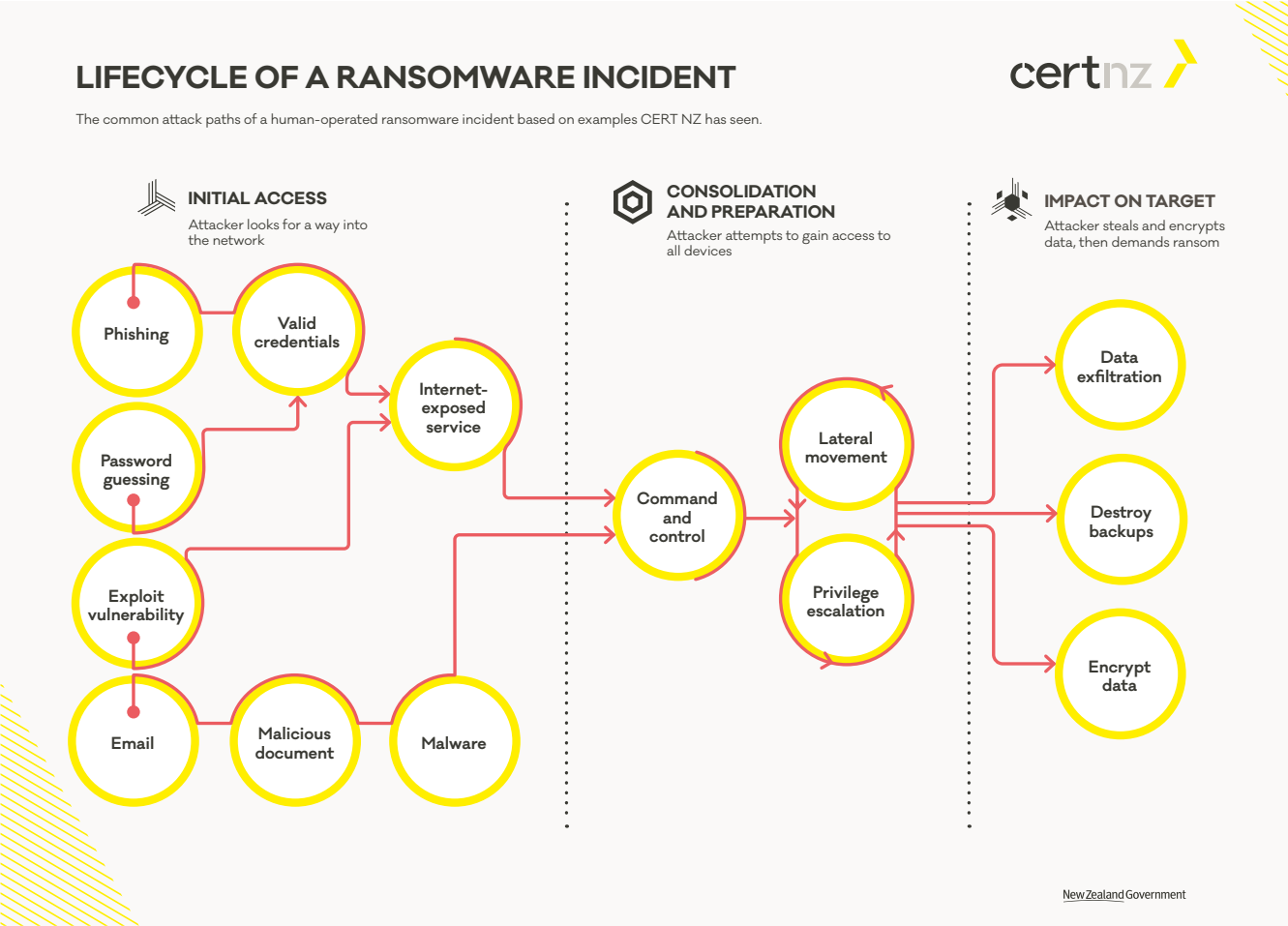
Sources of information

Document	*Location*
NCSC factsheet ransomware	https://english.ncsc.nl/publications/factsheets/2020/june/30/factsheet-ransomware
NCSC factsheet 'Prepare for Zero Trust'	https://english.ncsc.nl/publications/factsheets/2021/augustus/18/factsheet-prepare-for-zero-trust
NCSC ICT security guidelines for Transport Layer Security (TLS) v2.0	https://english.ncsc.nl/publications/publications/2019/juni/01/it-security-guidelines-for-transport-layer-security-tls
NCSC factsheet mature authentication – use of secure authentication tools	https://english.ncsc.nl/publications/factsheets/2022/juni/9/factsheet-mature-authentication---use-of-secure-authentication-tools
No More Ransom project	https://www.nomoreransom.org/en/index.html
Ransomware Guide (CISA)	https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
Ransomware Infographic (Police)	https://www.politie.nl/binaries/content/assets/politie/onderwerpen/ransomware/infographic-cybercrimes-ransomware.pdf
Back-up strategy	https://business.gov.nl/running-your-business/business-management/cyber-security/all-about-good-backups/ https://www.digitaltrustcenter.nl/back-up/geavanceerde-informatie-over-back-ups
CIS benchmarks	https://www.cisecurity.org/cis-benchmarks/
Microsoft white paper 'Mitigating Pass-the-Hash and Other Credential Theft, version 2'	http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf
Samen tegen Cybercrime, Stappenplan voor It-specialisten (Together against Cybercrime, Step-by-step plan for IT specialists)	https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/brochure-stappen-plan-cybercrime.pdf

Contact details

Organisation	*Contact details*
NCSC CERT service	cert@ncsc.nl
NCSC general	info@ncsc.nl
Police (report)	https://www.politie.nl/aangifte-of-melding-doen

Appendix 1: Schematic representation of a ransomware attack



Source: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Publication
National Cyber Security Centre (NCSC)
PO Box 117, 2501 CC The Hague, The Netherlands
Turfmarkt 147, 2511 DP The Hague, The Netherlands
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

June 2022