TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Instructions – Ransomware

Traficom Research Reports
23/2022

Contents

1 Introduction

1.1 Purpose of the instructions

The purpose of these instructions drawn up by the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency Traficom is to offer advice to organisations in situations in which it is suspected that ransomware has caused an attack or prevents normal operations. The instructions are focused on how to deal with the special characteristics of this type of information security incident. In order to resolve the situation completely, the organisation should maintain the incident response plan it has drawn up in case of information security incidents and follow it.

These instructions offer guidance on a general level on how to act in case of an information security breach and recover from it. It is recommended that the organisation should draw up a separate guide for its own use that takes its technological and operational environment into account in more detail. The project is funded by the National Emergency Supply Agency.

1.2 What does ransomware mean?

Ransomware is used in cyber attacks, in which cyber criminals aim to encrypt the organisation's data with an encryption algorithm and demand a ransom to restore the data. Criminals often also steal confidential information and may blackmail the organisation by threatening it with data leaks.

Criminals have found ransomware an effective way to benefit financially, because organisations unprepared for the threat are easy targets. Paying the ransom to resolve the situation is not the right solution, however. Payment does not necessarily guarantee that the data will be restored or even prevent the blackmail or other attacks from continuing. The attacker's objective may also be simply to destroy the data, which means that the blackmail is just a smokescreen. In that case, the data cannot be restored even by paying the ransom.

The right kind of preparation for ransomware attacks clearly improves the level of information security of organisations and their resilience against ransomware as well as other potential attacks. In addition to these instructions, the National Cyber Security Centre Finland has also published instructions for the management on what to do in case of a ransomware incident.[1]

[1] https://www.kyberturvallisuuskeskus.fi/en/publications/what-do-case-ransomware-incident-instructions-management

2 Preparation

Preparing for security incidents is a good way to reduce their severity and make it possible to recover quickly and continue the business. Organisations can assess their own readiness by using the Kybermittari (Cybermeter) cyber security evaluation tool of the National Cyber Security Centre Finland, for instance.[2] An incident response plan that has been drawn up in advance is a good starting point for what to do in case of a security incident. The organisation must also ensure that measures such as locking user IDs, isolating servers and terminal devices from the network and restricting network traffic to harmful IP addresses or domain names are technically possible and that the personnel have the expertise required to carry them out.

Gathering, compiling and monitoring log data is important in order to detect incidents in time. Log data also make it possible to investigate incidents thoroughly, which speeds up the cleaning and restoration of the environment. The National Cyber Security Centre Finland has drawn up a guide on how to collect and use log data.[3] Depending on the systems used by the organisation, comprehensive monitoring typically also requires network- and system-level solutions in addition to this.

2.1 Administrative measures

Immediate actions

- Draw up an incident response plan for your organisation in case of a ransomware attack.
- Train the personnel on how to act during incidents like those described in these instructions.
    - Also offer basic training for regular employees advising them on how to act if a ransomware attacks the employee's own terminal device.
- Find out in advance how you can report an information security breach to the National Cyber Security Centre Finland.[4] Start monitoring the news by the National Cyber Security Centre Finland.[5]
- Review attack scenarios together with the company's management and agree on the practical measures as well as management responsibilities and authority in case of an information security breach.
- Develop[6] the incident response plan and practice it regularly with tabletop exercises, in which responsible persons and interest groups practice the information security incident response process in imaginary scenarios.
- Consider whether your organisation should have a cyber insurance policy that may cover the damage caused by a ransomware attack. Contact insurance companies for further information. However, do not under any circumstances state publicly that your organisation has a cyber insurance policy, because cyber criminals may choose such organisations as targets of their attacks, hoping that they are more likely to pay the ransom.

Measures that support cyber security more extensively

- Identify the components critical to the business and create and maintain lists of what needs to be protected.

[2] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter
[3] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/collecting-and-using-log-data
[4] https://www.kyberturvallisuuskeskus.fi/en/report

[5] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news

[6] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

- Make sure that your organisation and subcontractors have implemented continuous vulnerability and update management.
- Specify the necessary access rights carefully based on the needs of the users and the technical functionalities.
- Consider establishing a security operations centre or purchasing a similar service. The purpose of the security operations centre is to monitor the network traffic of your company and information security events in the systems.

2.2 Technical measures

- Back up your critical systems regularly and automatically by following the 3-2-1 rule. That is, have at least three copies in two different formats and keep one of these copies completely outside the network.
- Test the functioning of the backups regularly and practice restoring the backups of at least the critical systems.
- Take advantage of network segmentation, data encryption and access control to ensure that the attack surface of your company and the amount of material exposed to an attack at the same time are as small as possible.
- Aim to detect attacks as early as possible by using different kinds of centralised monitoring solutions and make sure that their functionality is also tested regularly.
- Install anti-malware software on terminal devices that can be used to restrict the running of programs, investigate suspected information security breaches and isolate the computer from the network, if necessary.
- Implement mechanisms for filtering out emails that contain harmful content, spam and unwanted network traffic.

2.3 Preparation and training in practice

One important part of preparation is practicing threat scenarios. By practicing the scenario below in advance, you can make sure that your organisation is ready to meet situations like the one described. Training ensures, among other things, that the personnel of the organisation understand what the different parts of the workflow and checklist in the instructions mean and they have the capability to act according to the instructions.

For instance, the scenario in this case could be a situation in which ransomware has locked the files of a system critical to operations while preventing the use and operation of the system. This becomes apparent to the organisation when the system stops working. The attackers have breached the organisation through a phishing message and managed to navigate to a critical system via an infected workstation by taking advantage of a vulnerability in the server. The personnel and customers overload the IT and customer support, and the pressure to restore operations or find alternative ways to operate increases.

What would your organisation do in a situation like the one described? With the help of practice, try to assign responsibilities and allocate sufficient resources to the four parallel lines of activities that are key to a fast recovery:

1. Returning back to the normal status (recovery).
2. Finding the root cause and preventing further damage (investigation and corrective measures).

3. Workarounds/stopgap measures used during recovery and dismantling them in a controlled manner after recovery.

4. Communication between the team reacting to the incident as well as the rest of the personnel, interest groups, management and the public, providing information and coordination (coordination).

Practice at least the following steps of these instructions:

- Reporting the incident and escalating the situation.
- Isolating the devices identified from the network immediately.
- Locking down the infected IDs and disconnecting active sessions.
- Ensuring the continuity of operations during the information security breach.
- Gathering identification information of the malware and log analysis.
    - Is it possible to find out how and where the malware came from?
    - Which user IDs have been compromised?
- Using the identification information gathered to check other servers and terminal devices in case of infection.
- Finding out the recipients of the phishing message.
    - Who have opened a harmful attachment?
- Restoring the infected systems.
    - Servers and terminal devices. Use of backups.
- Final investigation process of the security incident.

In connection with all of the tasks being practiced, you should think about how the organisation leads the incident management, how the internal communications work and who is the person responsible or their deputy at which stage. It is also recommended that you study the materials of the National Cyber Security Centre Finland related to exercises.[7]

[7] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

3 Detecting an information security breach

There are two types of attacks: a ransomware attack and a wiperware attack. The effect of both types is the same: you cannot access files or systems important for the operations of your organisation. An attack can be detected in the following ways, for instance:

- The attacker sends a blackmail message to the target organisation, or such a message appears on the display of a workstation.
- The organisation is notified about the attack by a party outside the organisation via social media, customers, partners or the authorities, for example.
- The organisation's files cannot be opened from a network drive, for instance, or they are otherwise corrupted.
- The equipment in a factory or production environment stops working without a visible or identifiable cause.
- An information security product or service provider sends an alarm.

Report the information security breach to the National Cyber Security Centre Finland.[8] We advise you confidentially and free of charge on how to limit the damage, analyse the incident and take recovery measures. At the same time, you support the national information security situation awareness and make it possible to warn other potential victims.

See the guide on how to detect data breaches by the National Cyber Security Centre Finland (in Finnish).[9]

[8] https://www.kyberturvallisuuskeskus.fi/en/report

[9] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

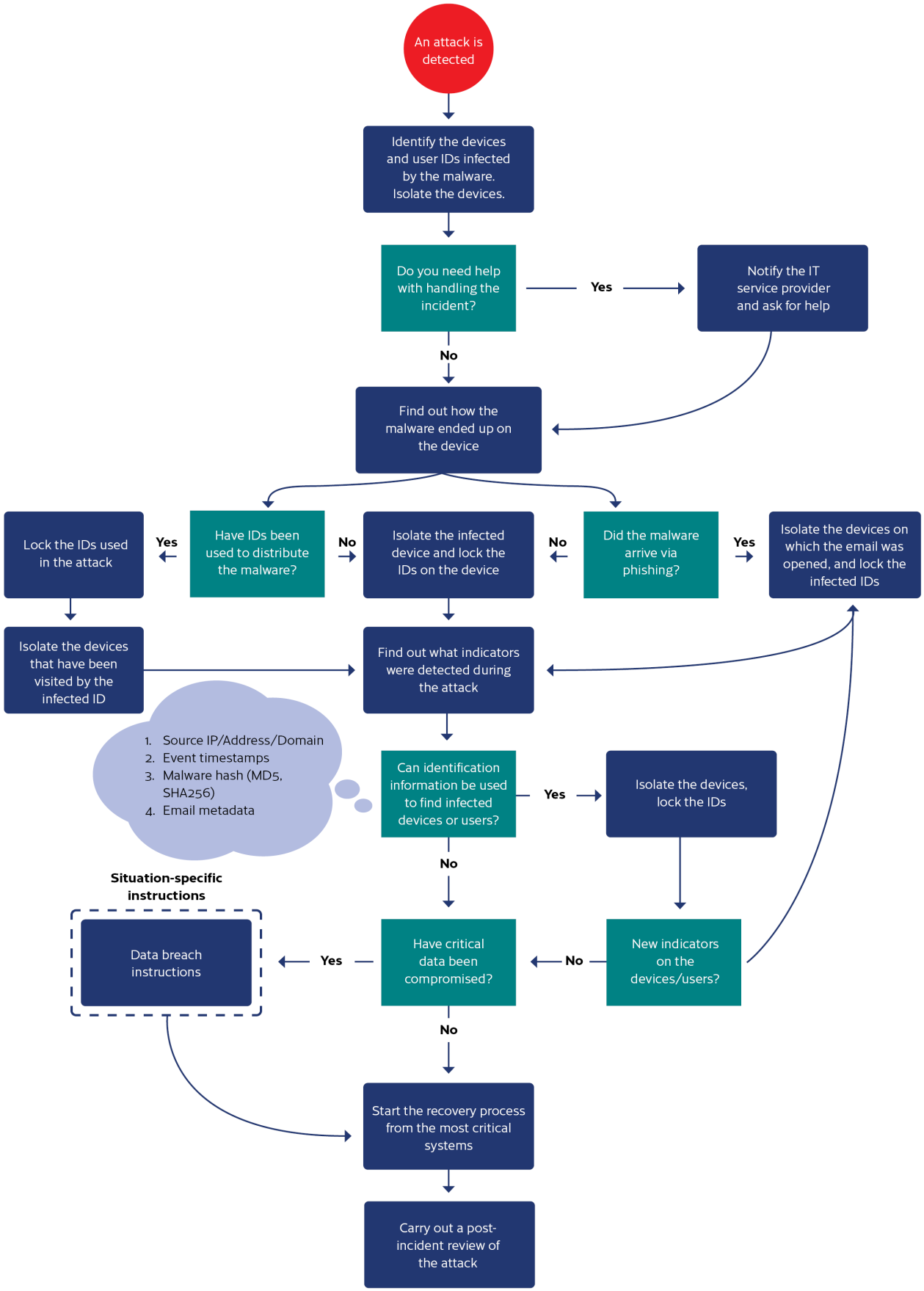
4 Instructions

Use the attached checklist to find measures to help you, if you suspect that you have become a victim of ransomware. The checklist helps organisations to prioritise and use a phased approach when investigating information security incidents.

4.1 Workflow of an information security breach investigation

The flow chart below describes the right order of measures when investigating the incident. The flow chart supports the use of the checklist. During the investigation, it is also crucially important to keep an accurate event log of the measures taken. The log should show the measure taken, the timestamp and the party that implemented the measure.

The gathering of potential evidence should also be documented carefully. You should record who gathered the data, what it was, and when and how it was gathered. A carefully drawn up event log makes the investigation as well as the cooperation with the police and information security investigators significantly easier.


An attack is detected
Identify the devices and user IDs infected by the malware. Isolate the devices.
Do you need help with handling the incident?
Yes
Notify the IT service provider and ask for help
No
Find out how the malware ended up on the device
Lock the IDs used in the attack
Yes
Have IDs been used to distribute the malware?
No
Isolate the infected device and lock the IDs on the device
No
Did the malware arrive via phishing?
Yes
Isolate the devices on which the email was opened, and lock the infected IDs
Isolate the devices that have been visited by the infected ID
Find out what indicators were detected during the attack
1. Source IP/Address/Domain
2. Event timestamps
3. Malware hash (MD5, SHA256)
4. Email metadata
Can identification information be used to find infected devices or users?
Yes
Isolate the devices, lock the IDs
No
Situation-specific instructions
Data breach instructions
Yes
Have critical data been compromised?
No
New indicators on the devices/users?
No
Start the recovery process from the most critical systems
Carry out a post-incident review of the attack

4.2 Immediate measures

Goals of the phase	The accuracy and speed of the measures are both important. The goal of the immediate measures is to stop the malware from spreading, prevent the attackers from gaining a foothold in the network and prepare for the start of the recovery process. Do not go along with the attackers' blackmail. Paying the ransom does not guarantee that the situation would end or that data could be restored.

Phase	Purpose	Measures
Identify the infected systems and user IDs	The aim is to identify all of the servers and terminal devices to which the ransomware has managed to spread. In addition, the aim is also to identify the user IDs that may have ended up in the hands of the attacker.	In order to identify the infected devices and IDs, check the infected computers with your monitoring products. Check the users that have logged in to the infected devices, and find out where else they have logged in. Among other ways, you can do this based on Active Directory logs, by using an endpoint detection and response product, or based on identity management logs.
Isolate the devices identified as infected	By isolating devices that have been identified as infected from all data networks, it may be possible to stop the attack from spreading.	Isolate the devices by using the features of endpoint detection and response. If necessary, disconnect the network cables of the devices. Keep the devices on after they have been isolated. This will make it possible to restore them, if the encryption keys used by the ransomware can still be found in their memory. Memory-based investigation is also an effective way to investigate information security breaches.
Identify the IDs used in the attack	Malware is often disseminated by using IDs that have extensive access rights (such as administrator accounts)	Investigate how the malware ended up in the infected devices based on endpoint detection and response or the logs of infected devices. All IDs that are logged in to the infected servers and terminal devices must be treated as lost. Take also account of the local IDs and service accounts of servers and terminal devices that may have ended up in the hands of the attacker. Attackers often use tools (e.g. Mimikatz) to steal the IDs in the memory of a device. This means that such IDs should be locked, too.
Contact your IT service provider	Often a part of the organisation's IT infrastructure has been outsourced to a service provider. In that case, the assistance of service providers may be needed for some of the measures related to limiting the scope of the incident.	In this phase at the latest, find out what parts of the IT infrastructure of your organisation have been outsourced to service providers. Contact the service provider's contact person in case of crisis situations. Among other things, you may have to ask your service provider to disconnect your servers from networks, restore them, or send their logs.

		IT service providers often also have experienced personnel who can help with resolving the security incident.
Notify the partners in cooperation and interest groups that may be affected by the incident about the information security breach	The security breach may cause the partners, customers and service providers risks or problems with the availability of services. An attack against the delivery chain may also endanger the safety of all partners.	Notify the contact persons in case of crisis situations of different interest groups about the incident if you believe that it may affect their data or the availability of the services, or if there is a chance that the malware may spread between organisations. You should also communicate actively about the incident internally. If the malware has already spread widely, it may be a good idea to instruct the employees not to turn on their computers if possible in order to prevent further damage.
Evaluate whether you need external help to handle the information security breach or not	The organisation may need help with organising measures, managing the security breach and technical measures. If your own organisation or IT service providers do not have the necessary expertise, you should consider getting external help.	Technical measures to handle the incident may require external expertise. Such measures may include collecting identification information, investigating the threat based on it, identifying the type of ransomware, and carrying out memory analysis of the infected devices. The National Cyber Security Centre Finland can help organisations especially during the first response to the incident as well as by offering additional information on similar cases in Finland and abroad. You can find Finnish service providers in the resources listed in the footnote.[10]
Report the information security breach to the authorities	Report the security breach to the authorities. The organisation may have an obligation to report the security breach based on regulations or the cyber insurance.	File a report of an offence about the incident with the police.[11] Also notify the National Cyber Security Centre Finland[12] of the incident to maintain situation awareness and get help. If there is a risk that personal data or other information subject to data protection legislation (GDPR) have ended up in the hands of the attacker, report the incident to the Office of the Data Protection Ombudsman.[13] The infrastructure operators and service providers critical to the

[10] https://dfir.fi/
https://www.fisc.fi/fi/about-us
https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/ (in Finnish)

[11] https://poliisi.fi/en/report-a-crime

[12] https://www.kyberturvallisuuskeskus.fi/en/report

[13] https://tietosuoja.fi/en/data-breach-notification

		security of supply that are subject to the NIS directive of the EU on the security of network and information systems must notify the supervisory authorities about information security incidents in network and information systems.[14]

[14] https://www.kyberturvallisuuskeskus.fi/en/services/report-security-incident-nis-notification-obligation

4.3 Investigating an information security breach

Goals of the phase	The goal of investigating the security breach is to determine the extent of the attack and its impact on the organisation. A careful investigation ensures that malware, access rights that have fallen into the wrong hands and potential backdoors have been removed from the environment.

Phase	Purpose	Measures
Identify harmful activity and collect identification information	Identification information is collected to make it possible to map how widely the infection has spread to devices and how the stolen access rights have been used. Once attackers have gained a foothold, they may use different kinds of attack methods. In fact, identification information should be collected extensively and signs of their use should be studied carefully to ensure that the cleaning of the environment can be done reliably. Recovery can only start after the attacker has been removed from the environments.	The identification information gathered includes, among other things, the time when the incidents occurred, such as when a login to the server occurred, or when a certain command was run on the server. The malware often communicates with the attacker's command and control server. By studying the network traffic of infected devices or domain name resolution (DNS logs), the source IP addresses or domain names used by the attacker can be identified. When harmful files are identified, their hashes (MD5/SHA256) can be extracted and used to identify harmful files on other devices, too. Authentication events related to infected devices and measures taken by the user accounts linked to them can be used to determine the IDs used to spread the malware. Endpoint detection and response often has features for collecting and using the identification information mentioned above. Otherwise, the measures should be taken manually by using a centralised log server. If no such server is available, either, the logs of individual servers and terminal devices should be examined. If the malware was originally delivered into the organisation via email or other means of communication, the identification information of messages should be collected. Important information includes the timestamps, subjects, attachments, senders and recipients of the messages as well as their content. This information can be used to find all of the parties that may have received a harmful message and whose device has become infected by malware in that way.
Use the identification information to help with identifying all infected systems	The identification information can be used to find out how far into the organisation the attacker was able to penetrate. By collecting identification information and searching for it in the target systems, it is possible to ensure that all infected devices and identifiers are found and cleaned.	Identification information can be used to find infected devices, such as by using the endpoint detection and response features that often directly offer the option of searching for events on devices based on different identifiers. If the organisation also has a centralised log server, it can be used to search for events efficiently based

		on identifiers from several different devices at the same time. If neither of the solutions mentioned above is available, identifiers should be searched separately from each device. Different kinds of remote control solutions can be used for the purpose, however; they often enable running PowerShell commands simultaneously on several servers, for instance. There is a risk that the attackers have attempted to cover their tracks by disabling logging after gaining access to a device. In that case, it may not be possible to find all of the collected identification information in the device logs. For this reason, it is important to aim to use a wide variety of identification information and event sources.
Save all available log files and other evidence on a hard drive isolated from the network for later investigation	The aim of collecting and storing evidence is to guarantee a high-quality investigation after the incident so that the root causes of the incident can be determined. Evidence may be needed during the criminal investigation and for the court proceedings. If the organisation has a cyber insurance policy, the insurance company may also require more detailed information on the security incident as well as evidence for the investigation.	Save log files that contain information relevant to the investigation of the incident on a hard drive isolated from the network. Also collect harmful email and other messages, if any. Aim to keep the evidence, such as complete disk images and memory samples, as intact as possible. Extract integrity hashes from them to ensure this. Aim to save samples of the malware detected. They should be handled with extreme care. Professional expertise is often required to carry it out safely. Send the samples to the National Cyber Security Centre Finland.[15]

[15] https://www.kyberturvallisuuskeskus.fi/en/news/transmitting-e-mail-and-sending-samples-national-cyber-security-centre-finland

4.4 Recovery

Goals of the phase	Start the recovery from the systems that are the most critical to the business. The organisation should aim to restore the business back to normal as quickly as possible, but only after the recovery can be carried out safely.

Phase	Purpose	Measures
Restore the infected systems from backups	The aim is to restore the systems and return to normal operation. Restoring the systems is done as safely as possible to ensure that the attacker cannot get back into the system.	Restore the systems from backups. Also take account of the risk that previous daily (incremental) backups may already have been infected. When restoring old backups, keep in mind that the backup may include the vulnerabilities that the attacker used in the attack. You can try to prevent the risk by restoring the systems without a network connection and updating the operating system and its applications before connecting to the network. If there is no suitable backup available, do a clean install of the operating system and its applications, starting from scratch. Also take the risk factors mentioned in the previous section into account. Do not try to clean an infected system by using anti-malware or automated tools, because there is no guarantee that they will be able to clean the system completely. Save the encrypted files or hard drives, in case a way to decrypt them is found later. Check the systems with anti-malware tools before connecting them back to the network again.
Restore the infected IDs and ensure that the system administrator IDs are safe.	Ensure that the login information of all of the infected IDs is changed so that the attacker can no longer use the IDs to access the organisation's systems. Strengthen the user login requirements, if possible.	Change the passwords of infected IDs and start using the IDs again. To make sure, change the password of administrator accounts and service accounts in case some of them have fallen into the hands of the attackers. Deliver the new passwords to users either verbally in person, in a text message or by telephone. Do not use the organisation's email or instant messenger, because the attacker may still have access to them. Consider adding two-factor authentication to administrator accounts as well as the IDs that were exploited during the attack. In addition, monitor the IDs used in the attack more carefully after the attack in case the attacker gains control of them again. If it is still unclear to the organisation how the attacker was able to gain control of certain IDs, consider creating completely new IDs. In this way, you can ensure that the attacker cannot gain control of the IDs

		again by using the method that could not be identified. If the organisation uses Active Directory and it is suspected that the attacker has gained control of the whole domain at some point, you also need to change the password of your KRBTGT account twice in order to make the golden ticket expire. Also re-provision the certificate services of the Active Directory in case the attacker obtained certificates from the certificate service that can be used for identification.

5 Post-incident review of an information security breach

When the crisis is over and business operations have returned to normal, it is important to start the post-incident review of the attack and learn as much as possible about what happened for the future. At the same time, crisis management systems should be updated based on the observations made. The organisation may become a victim of a similar attack again, if the root causes of the incident cannot be determined and no lessons are learned from it.

During the post-incident review, the activities during the crisis are studied: what measures were done well, what could have been done better, and how the plans and the security level could be improved. A report should be drawn up on the post-incident review that examines at least the following questions in addition to the course of the events:

- Root causes of the incident:
    - What technical or functional weaknesses led to the situation?
- Effectiveness of the organisation's own protection:
    - Were the controls used to detect attacks sufficient?
    - Did the attacker's actions raise any alarms?
    - What was the reaction to the alarms like? Was the information about alarms transmitted to the right responsible persons?
- Actions during the crisis:
    - Was the crisis plan followed? How usable was it?
    - Were the responsibilities of the crisis management team assigned to the right people?
    - How successful was limiting the scope of the attack and removing the attacker?
    - How successful were the communications of the crisis management team? How were the interest groups taken into account?
- Recovery:
    - How did the recovery of critical information and services go?
- Post-incident review:
    - Have the course of events and the investigation work been documented?
    - Was the technical investigation of the incident sufficient? Has it been possible to submit sufficient data on the attack for the use of the authorities, for example?
    - Evaluate the actions of the service providers. Were the response time and the services that were agreed upon sufficient for the investigation of the incident?

The organisation should update its own incident response plan and more detailed playbooks designed for combating different types of security incidents after the fact. Practicing different scenarios at regular intervals is also recommended to ensure that you can benefit from them in crisis situations.

The National Cyber Security Centre Finland hopes that the companies and organisations share the most important lessons they have learned from the incident with the Centre, too. With incident reports, the National Cyber Security Centre Finland can help other organisations in Finland as well as internationally to investigate similar cases. The lessons learned from recovery help with developing the preparedness of all organisations.

Finnish Transport and Communications Agency
Traficom
National Cyber Security Centre Finland
PO Box 320, FI-00059 TRAFICOM
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-815-7

NATIONAL EMERGENCY SUPPLY AGENCY

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre