National Cyber Security Centre
Ministry of Justice and Security

Ransomware

Measures for preventing, limiting and recovering from a ransomware attack

Fact sheet FS-2020-03 | Version 1.0 | June 2020

The threat of ransomware has increased worldwide in recent years. This malicious software can affect any organisation that has not taken the right measures. A new trend has emerged over the past few years: malicious parties are carrying out more specific ransomware attacks on targets that can afford a higher ransom amount.

This fact sheet highlights the different types of ransomware, describes various measures that organisations can take to prevent ransomware attacks and offers advice on what to do if your organisation is infected with ransomware.

Background

For criminals, the ransomware revenue model used to be based on economies of scale: untargeted attacks were aimed at large numbers of users with vulnerable systems. A low ransom amount was often requested.

A new method has emerged over the past few years: malicious parties are carrying out more targeted ransomware attacks on victims that can afford a higher ransom amount. After they have managed to gain access to a target's system, this system is thoroughly analysed for a long time. As a result, a criminal will know the 'value' of the organisation and will modify the ransom requested in line with this subjective value.

Target group

Chief Information Officers, Chief Information Security Officers, Security Officers and Information Security Officers.

Collaboration partners

Created in collaboration with CERT-BE, NCSC-UK, Digital Trust Center (DTC), Maastricht University, Z-CERT, De Volksbank, Achmea, Ahold Delhaize, ASML, KPN, Heineken and Netherlands Police.

Copyright

Key facts

1. The impact of ransomware attacks is increasing.
2. Measures against ransomware also help to combat other malware.
3. The revenue model of ransomware has changed. Malicious parties are carrying out more targeted ransomware attacks on victims that can afford a higher ransom.

What is ransomware?

Ransomware is malware that encrypts users' data files, with the aim of decrypting them later in exchange for a ransom. In extreme cases, the ransomware blocks access to the IT system by also encrypting system files that are essential for the proper functioning of the system. Given the destructive nature of ransomware attacks, it is often difficult to recover the log files and find out what actually happened. Hackers may have stolen intellectual property or personal data, using ransomware to hide their real intentions.

There are two types of ransomware: a *locker* locks the access screen of a system, whereas a *cryptor* encrypts the files on the infected system using encryption algorithms. Advanced types of ransomware can encrypt not only local IT systems but also hard disks, databases, backups, USB flash drives and data in the cloud. Both types of ransomware require the victim to pay a ransom in order to regain the normal use of the computer. This ransom is often demanded in the form of a cryptocurrency, such as Bitcoin.

Ransomware infections differ very little from other malware infections. In addition, the measures that an organisation can take against ransomware are largely the same. Depending on the maturity of your organisation, the impact of a ransomware attack can range from a minimum of annoyance to the large-scale disruption of the primary process.

How much is the ransom?

There is a major difference between an opportunistic ransomware attack and a targeted attack. In an opportunistic attack, attempts are made to infect a considerable number of victims and a few hundred or few thousand euros are usually demanded. The amount is deliberately kept low to ensure that paying the ransom is the fastest and cheapest way of getting the victims' IT systems back to normal.

In a targeted, carefully prepared attack by malicious parties, the ransom can amount to millions of euros. Malicious parties want the ransomware to have the greatest possible impact on their target. Such an attack can have big consequences: after a ransomware infection, critical files and processes may no longer be accessible. Threats may also be made to erase the data or to make it public. These types of attacks are becoming more common.

Malicious parties who are more interested in sensitive information also use ransomware to cover their tracks. In this case, they use ransomware as a *wiper*, which can mean that it will no longer be possible to recover your data from your hard disk.

The NCSC recommends not paying a ransom. There is no guarantee that the key (*decryptor*) or password will be provided after you have paid the ransom requested. In addition, there are cases in which the same victim was targeted again after making the payment.

How does ransomware infect your system?

There are various ways in which a malicious party can infect your system with ransomware. Ransomware is a form of malware. Opening a malicious attachment in an email or visiting a malicious web page is enough to get infected. Many victims install ransomware without realising.

Ransomware attacks also use unpatched vulnerabilities in a system. Examples include vulnerable web browsers and legacy protocols such as SMBv1, as well as Remote Desktop Protocol (RDP) access. Other malware, such as trojans, can also be used in order to access your system.

Ransomware as a service

Cybercrime is characterised by specialisation and increasing professionalism. Some groups of cybercriminals specialise in gaining and then selling access to networks.

There are also groups of cybercriminals who specialise in exploiting this access; for example, via ransomware. They have developed various ways of identifying and abusing vulnerable RDP sessions. For instance, credentials and other sensitive information could be stolen. The use of RDP access offers advantages: it is easier to blend into a victim's network usage with the aid of existing credentials. As existing credentials are used, attackers can disguise their actions and blend into 'normal' network usage. Precisely because there is little to no visible or malicious network traffic, the attacker may not be noticed as quickly by system monitoring or a vigilant system administrator.

Despite the increasing professionalism of ransomware as a service, both untargeted and targeted ransomware attacks still require specialist knowledge.

Preventing ransomware

1. Protect against phishing
2. Organise vulnerability management, patch management and network segmentation
3. Limit the possibilities for code execution
4. Filter web browser traffic
5. Limit USB usage

There is no silver bullet for ransomware attacks. Ransomware is one among many variants of malware. As a result, the measures that you can take against ransomware largely correspond to measures that protect your systems against other kinds of malware.

The purpose of ransomware is often financial gain. It is therefore advisable to protect your network with an in-depth defence system so malicious parties will need to make a greater effort in order to carry out a successful ransomware attack. Criminals will estimate the potential gain and give up if the attack is likely to take too much time in proportion to the prospective ransom.

1. Protect against phishing

Phishing is a form of social engineering in which people are coaxed into handing over sensitive data. The most common phishing method is sending fake emails that appear to come from reliable senders. These emails often contain a link to a fake Internet page, which will either offer an infected file or ask the recipient to enter personal data. Combating phishing requires both a technical and a human-oriented approach. You can train your employees to recognise phishing emails on the one hand, while there are also technical measures that you can take on the other. In any case, we recommend the following measures:

- Improve email security using SPF, DKIM and DMARC. Also see the fact sheet *Protecting domain names against phishing* [1] (in Dutch) from the NCSC. Check incoming email traffic with these standards as well. This measure will prevent malicious parties from sending emails on behalf of your organisation.
- Use spam filters to prevent phishing emails from reaching employees.
- Perform phishing tests on a regular basis. Make users realise the importance of not clicking on everything and teach them how to recognise spam as well as phishing emails. Coordinate these tests properly within your organisation in order to avoid inconvenience.
- Set up a process that allows users to report phishing emails and train your staff in how to deal with them. Almost identical phishing emails are often sent, e.g. emails in which only the link to the infected page differs slightly.
- Increase your employees' awareness and adopt a positive safety culture; make sure that employees know where to report phishing and that they feel confident enough to do so, even if they have already clicked on a malicious link themselves.
- Email software sometimes contains visual tools that alert users to malicious emails. These tools make it possible to label external emails, for example.

2. Organise vulnerability management, patch management and network segmentation

Some versions of ransomware exploit vulnerabilities in operating systems, web browsers, browser plug-ins and applications. These vulnerabilities have often been public for some time and patches are available which can mitigate the risk of infection.

Updates

Performing system updates makes it significantly harder to infect your systems with recent vulnerabilities. Most software is updated on a regular basis. These updates may include patches to provide the software with better protection against new threats.

It is important to patch all the systems within your network in a timely manner, not just the systems that are directly connected to the Internet. An attacker may move laterally through your network, particularly in the case of a targeted attack. Patching all the systems promptly will make it harder for an attacker who succeeds in penetrating to access your network further. The NCSC recommends the following measures:

- Follow the NCSC RSS feed with security updates for commonly used software. In addition, ask your suppliers to keep you informed about updates to their product.
- Install the latest updates of your operating system.
- It is essential to install updates on a regular basis. Using a step-by-step approach to do so is a good idea (test phase followed by implementation).
- Make sure that the antivirus software is up to date and that all relevant features are enabled.

1 https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing/20151028+-Factsheet-Bescherm-domeinnamen-tegen-phishing.pdf

Network monitoring

A successful ransomware attack relies on timing: malicious parties will try to stay unnoticed for as long as possible. When preventing (or limiting) a ransomware attack, it is therefore important to identify these activities as quickly as possible. The NCSC recommends the following measures:

- Create and manage an up-to-date inventory of your assets; you must have a clear overview of what is present on your network. In case of a ransomware infection, you must be capable of tracing to whom a system belongs and where it is located in the network.
- Recognise the basic behaviour of the network; use a solution that knows what is normal for your network.
- Set up detection to identify threats from digital attacks or malicious activities. Detection is important for quickly identifying and stopping an attack. Also see the NCSC web page about detection [2]. This page contains the publications (in Dutch) *Guidance for the implementation of detection solutions* and *Indicators of Compromise Fact Sheet*.
- Monitor whether credentials may have been compromised.
- Make sure that logging takes place at a central location.
- Apart from logging, it is also a good idea to set up monitoring; determine which logs should always generate an alarm and set up a process to respond accordingly. For example, this process could take the form of an alarm when your antivirus is switched off.
- Improve the visibility of security incidents. Explore the possibility of implementing a Security Information and Event Management (SIEM) system.
- Explore the possibility of implementing Endpoint Detection and Response (EDR). This software makes it possible to monitor the endpoints (mostly PCs) in your organisation continuously. You will then also be capable of responding to an attack in real time.

Network segmentation

Network segmentation provides an additional security layer in your network. It is very important for preventing lateral movement through your network. Lateral movement means that a malicious party is intent on gaining deeper and broader access to your network. Dividing your network into functional segments makes it harder for malicious parties to achieve their goal. After all, the part of the network where the attacker entered could be completely screened off from the intended target. The NCSC recommends the following measures:

- Limit external access to systems as well as their interfaces to traffic that is strictly necessary. Ensure that employees can only gain access to your internal network via a VPN connection.
- Segment your network. Systems that do not require interaction or communication must be divided into different segments. Users will only be given access to the segments that they need. Block cross-segment traffic. This measure implies a zero-trust principle; only allow traffic that is explicitly trusted.
- Limit administrator privileges and the sharing of these privileges.
- Ensure that attackers cannot log into your systems from the outside. Use long, complex passwords and implement an account-locking policy to protect you from brute-force attacks. Authenticate users by means of Multi-Factor Authentication (MFA).

Hardening management interfaces

A management interface such as the Remote Desktop Protocol (RDP) makes it possible to access and operate systems remotely. There are functional advantages; for example, an employee does not have to be physically present on site. However, this direct access via the Internet also makes management interfaces a popular target for malicious parties. Among other things, they can be abused by SamSam ransomware, which tries to exploit Internet-accessible RDP servers with weak passwords.

Restricting access to an organisation's network is also known as system hardening. Although virus scanners and firewalls contribute to this goal, the restriction of access via management interfaces also deserves attention. It is very important in this context only to open relevant network interfaces and restrict specific access rights to production environments/data.

- Check whether it is necessary to have RDP available on systems; if so, limit connections to specific and reliable hosts (whitelisting).
- Also protect your RDP or other connections against brute-force attacks; make sure that users connect via a VPN and authenticate these users by means of Multi-Factor Authentication (MFA).
- Ensure that cloud environments comply with recent best practices. Also limit the use of RDP ports in these environments.
- Properly protect the use of RDP (including the ports).

Please note: when it comes to information security, it is important for you to carry out your own risk analysis that focuses on your organisation. The above description is not an exhaustive list and not all measures are appropriate to each organisation.

3. Limit the possibilities for code execution

Consider protecting your organisation from unauthorised code execution, which is the execution of malicious code and malware. Using macros is a common method of attack; a malicious party will tempt users to execute malicious code by allowing macros in the document that they have opened. This attack can be prevented by disabling macros within your organisation.

From a security perspective, it is also desirable not to give end users the option of installing software on their own device. Of course, there are also legitimate reasons to install software or execute code on a device. Create a process to facilitate this option for users. This way, you will prevent them from being tempted to do so behind your back.

2 https://www.ncsc.nl/onderwerpen/detectie

In any case, we recommend the following measures:
- Use application whitelisting to ensure that only approved programs can run on your computer systems.
- Disable macros in Office files.
- Disable ActiveX in Office files.
- Disable AutoPlay.

4. Filter web browser traffic

It is advisable to use a proxy for your outbound web traffic. This measure allows you to filter the websites that your users wish to visit, e.g. blocking known malicious websites.

5. Limit USB usage

Data carriers such as USB flash drives can infect a system with malware. It is possible to close USB ports or block USB storage. You can also limit USB storage to specific users who use special USB flash drives. Consider whether one of these measures would suit your organisation.

What is the impact of a ransomware attack?

Ransomware restricts access to systems or data until a solution is found. This attack can lead to serious damage such as unsafe working situations, financial damage and loss of reputation. Ransomware not only affects your own organisation but also your environment. Even with carefully configured backups, it may take some time for your organisation's primary processes to be restored. During this downtime, an organisation may need to activate its business continuity processes.

In targeted ransomware attacks, malicious parties gain access to your organisation's IT systems. This situation may jeopardise the integrity and confidentiality of your data. The system may also be infected with other types of malware, in addition to the ransomware.

A successful ransomware attack will not only affect the encrypted data. It may also lead to indirect or even permanent damage.

Reduce the impact of a ransomware attack

1. Limit access to data and file systems
2. Create a backup strategy

1. Limit access to data and file systems

You can prevent ransomware from spreading freely within your organisation; restrict access to data as well as file systems to people (or systems) that have a valid reason for using them. Remember that this measure will also benefit your backup systems and cloud facilities.

It is very important to implement good access controls, i.e. the strict application of user rights. It is important to ensure good user administration for this purpose. Keep track of the joiners-movers-leavers process in your organisation; modify the access rights when a user is assigned a different role or leaves the organisation.
Good access controls are even more relevant to administrator accounts (admin); these accounts require extensive rights and access to systems. Users with a system admin role should not send emails or browse using admin accounts, or be logged into workplace systems. This measure may limit a ransomware attack to specific domains of the infrastructure.

The principle of zero trust is also becoming increasingly popular. This information security framework does not rely on the existence of a 'secure personal network', thus eliminating the distinction between internal and external networks. Such a conceptual framework can provide guidance for organisations that have an open Bring Your Own Device (BYOD) policy, for example. Measures that can mitigate risks in this area include micro-segmentation or a Privileged Access Management (PAM) solution. Among other things, micro-segmentation means that an organisation specifies what each individual system can access (whitelisting). Monitoring can also be applied to each system, in addition to the monitoring of the entire network. Privileged Access Management involves monitoring and logging admin activities as well as consciously authorising users for specific tasks. These authorisations are valid for a limited period; the user may perform this task for a short period of time. Such a solution may complement your existing Identity Access Management system.

2. Create a backup strategy

Backups are essential for restoring your files after a ransomware incident. Creating backups of all your vital files and systems can limit the impact of a ransomware infection.

- Data can only be restored to the time of the last backup.
- Online backups can also become infected. (An online backup means that the backup is connected to the network, in contrast to offline backups. Examples of offline backups include a hard disk in a safe or the use of tapes.)
- Backup files must not be directly accessible from a system that may become infected.
- These backup files must be tested regularly; check that the data are complete and not corrupt.

Make sure that backups are not your only protection against ransomware; good cyber security measures can prevent your organisation from becoming infected in the first place.

If you need to decide on the number of potentially feasible backups, evaluate which information is the most critical to your organisation. This evaluation should also include your critical processes; which functions must your organisation be able to perform again (within a few hours or days)?

- Apply the **3-2-1 rule**. Make sure that you have at least **three** different copies of your data and applications. These backups must be on at least **two** different storage media. Make sure that **one** carrier is in a different location. The **3-2-1 rule** also specifies that **one** of these backups must be an offline copy.
- Limit the number of users who have access to your backups; the fewer, the better.
- The logs must also form an integral part of your backup strategy.

It is essential to check how long it takes for you to restore a backup. This information is crucial for drawing up your business continuity plan; there is a major difference between a restore that takes a few days and one that takes a few weeks. Define a recovery time objective and adapt your backup strategy accordingly, then test this strategy.

It is risky to base the backup on the same technology as the operational infrastructure. Consider making the backup infrastructure work in its own environment (thus limiting lateral movement). In addition, consider using completely different technology. One example would be the use of Linux-based solutions for backing up a Windows system.

What to do if your organisation is infected with ransomware

Ransomware encrypts your files. Restoring data by means of a backup is the most reliable solution for regaining access to these files.

If it is not possible to restore the files by means of a backup, it is advisable to check whether a decryptor exists. For example, you can do so on the website of the 'No More Ransom' project [3], an initiative set up by police forces and private parties.

In case of a limited infection:

Please note that the infected system is considered to be lost in the next steps. This situation may disrupt a possible decryption process.

- Remove the infected system from the computer network.
- Remove the ransomware from the infected computer system. The system will then be completely reinstalled if necessary.
- Report the infection to the police.
- Restore the IT system using a backup.

In case of a network-wide infection:

- Activate your emergency plan.
- Close your network off from the outside world, e.g. by closing your firewall(s).
- Get help from a cyber security expert and/or a cyber security partnership.
- Report the infection to the police.
- Restore the IT systems using a backup.

Also check whether you have a reporting obligation to the NCSC, a supervisory authority, a client or another body[4]. Among other things, consider the applicable privacy legislation (if you are a processor, for example).

Communication employee care

A lot of work is required if your organisation is affected by ransomware. Many things are unclear and numerous questions will come up, especially during the initial exploration ('What is the extent of the problem?'). It is therefore advisable already to consider your communication about the ransomware infection at an early stage, preferably before an attack occurs.

Explore ways to inform the parties concerned if your email systems are also encrypted. Other organisations have used social media and/or physical information points in such situations, among other things. Record these plans in a script and practise/evaluate them regularly.

In addition to communication, it is also advisable to determine which partner organisations you need during a ransomware attack. During the downtime, check which processes are vital to your organisation and draw up a business continuity plan.

Be aware that a ransomware infection places significant demands on the employees involved and that the adverse effects can persist for weeks. Make sure that your employees get enough rest during this period. This situation will allow them to keep up their energy throughout the recovery period.

Should you pay up?

Paying the ransom is not recommended, especially as it does not guarantee a solution to the problem. There is a strong probability that numerous problems will arise during the decryption. The decryptor provided by cyber criminals has often received far less attention than the encryption software. As a result, it will no longer be possible to recover the data in the worst-case scenario.

Paying the ransom also preserves a business model; it encourages cyber criminals to use ransomware, as it is a profitable undertaking. Cyber criminals will then continue their activities and seek out new ways of exploiting systems, resulting in more infections, more victims and more harm to society.

Some victims who paid the ransom indicated that a higher amount was demanded after an initial payment was made. In some cases, the victims were later affected by the same ransomware once again.

3 https://www.nomoreransom.org/nl/index.html

4 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/datalek-door-ransomware-wat-moet-u-doen

Reporting the incident

You can report the incident to a police station. Call +31 34 357 88 44 to make an appointment.
In order to prepare for your statement, you must ensure that the person making the statement on behalf of your company has written authorisation to do so. Take any log files with you (which may contain clues, indications and evidence) and write down the contact details of the complainant in advance.

When making a statement, you can expect the following questions:

- Which systems were affected?
- What are the network addresses and what is the network infrastructure?
- Which security measures (such as virus scanners and firewalls) did you take?
- Was there a threat or were there other special circumstances?
- What is the estimated damage (both economic and to your reputation) and what amount of personal data has been affected?
- Which recovery actions did your company take after discovering the incident?

In conclusion

As long as organisations do not pay sufficient attention to cyber security, malware such as ransomware will continue to exist. The revenue model is based on the idea that an organisation will have no choice but to pay up. By preventing a ransomware attack, you not only help your own organisation but also contribute to disrupting this criminal activity.

At the same time, not all ransomware attacks can be prevented. As a result, make sure that you are also prepared for the potential impact of a ransomware attack.

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

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

FS-2020-02 | version 1.0 | June 2020