RANSOMWARE

HOW TO PREDICT, PREVENT, DETECT & RESPOND

F-Secure

CONTENTS

REVISION HISTORY
v2.0: Published November 2019
v1.0: Published November 2016

CYBER SECURITY IS A PROCESS

Many organizations still follow an outdated approach to cyber security, relying solely on a defensive perimeter to protect their infrastructure. We recommend a more robust, iterative approach, which can be broken down into four phases [1] —**Predict**, **Prevent**, **Detect**, and **Respond**.

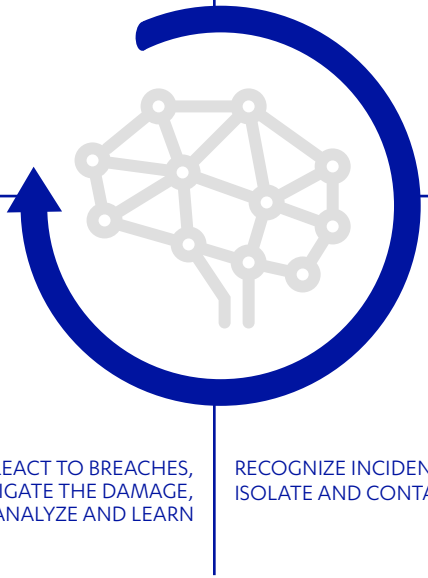
In sequence, the phases are:

PREDICT

A corporate exposure analysis is performed to assess the attack surface of the organization's infrastructure. The findings of these analyses are used to plan the construction of a solid defensive perimeter for the organization.

UNDERSTAND YOUR RISK, KNOW YOUR ATTACK SURFACE, UNCOVER WEAK SPOTS

MINIMIZE THE ATTACK SURFACE, PREVENT INCIDENTS



PREVENT

Defensive solutions are deployed to harden infrastructure and reduce its attack surface. Security software is deployed, vulnerabilities are patched, employees are trained, and the security culture of an organization is generally improved.

RESPOND

Forensic evidence is examined to determine how the breach happened and what impact it had on systems, data and infrastructure. An incident response process is initiated to restore the environment to a known-good state and to fix any security problems found. The findings of this phase are fed back into the next Predict phase, and the cycle continues.

REACT TO BREACHES, MITIGATE THE DAMAGE, ANALYZE AND LEARN

RECOGNIZE INCIDENTS AND THREATS, ISOLATE AND CONTAIN THEM

DETECT

The infrastructure is carefully monitored for signs of intrusion or other suspicious behavior, so that breaches can be pinpointed quickly and accurately.

In this whitepaper, we examine how this approach to security can be applied to dealing with a notable threat: **ransomware**.

ABOUT RANSOMWARE

Ransomware is a form of **crimeware** - malicious programs that are used, typically by individuals or organized criminal groups, to extort money. Ransomware has attracted attention in the mainstream media in the last few years as major corporations and goverments reported being compromised by the threat [2, 3].

TYPES OF RANSOMWARE

There are two main types of ransomware: **crypto-ransomware**, and **police-themed**, which use different forms of fear to motivate the user into paying the ransom. Crypto-ransomware directly preys on a user's fear of never recovering their affected content or device, while police-themed ransomware tries to make the user believe they have commited a crime that requires payment of a 'fine'.

Many ransomware programs share similar characteristics that group them into *families* - for example, the way they infect the device, what kind of files they target, how they demand payment and so on. Knowing which specific family is involved in an incident can be critical in determining what should be done to contain any damage and remove the threat from an affected device.

Crypto-ransomware

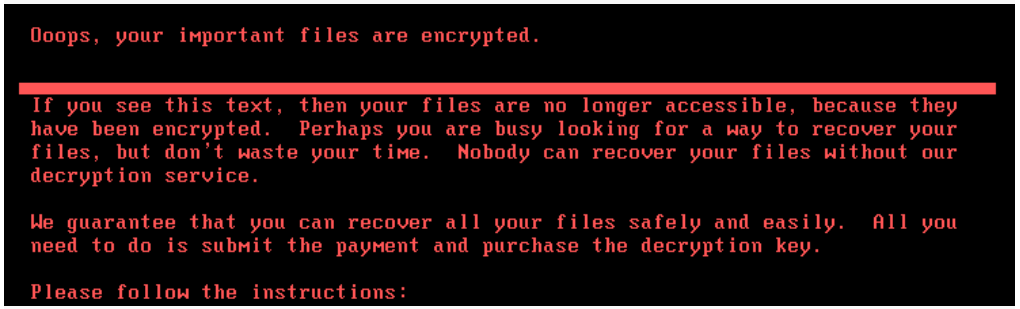


IMAGE SOURCE: F-SECURE BLOG

The device or files are encrypted so they cannot be accessed without a decryption key. A message is then displayed, providing instrutions for paying the ransom. Some crypto-ransomware will also perform other actions, such as deleting files, if payment is not made, or not made according to a deadline

Notable families GandCrab, Petya, WannaCry

Police-themed ransomware

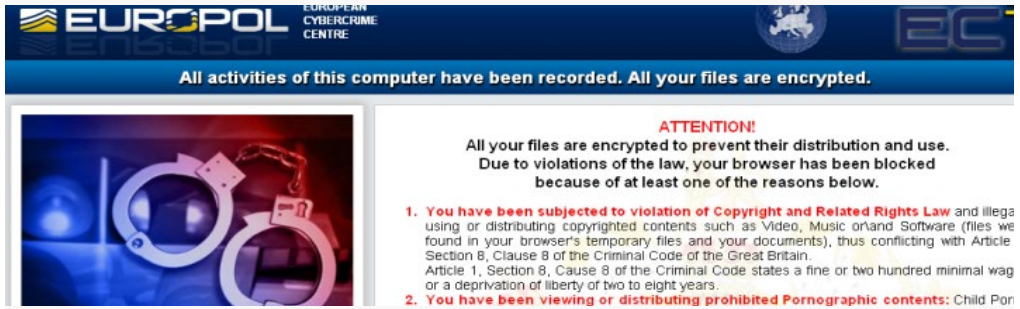


IMAGE SOURCE: F-SECURE BLOG

Displays a message saying the device/files have been 'locked' by a local or national law enforcement authority, supposedly because the device was used for criminal activity (child pornography, digital fraud, etc). Some will actually encrypt the device or files, while others only alter access to the device/files to make it appear to be 'locked'

Notable families Reveton, Browlock, Urausy

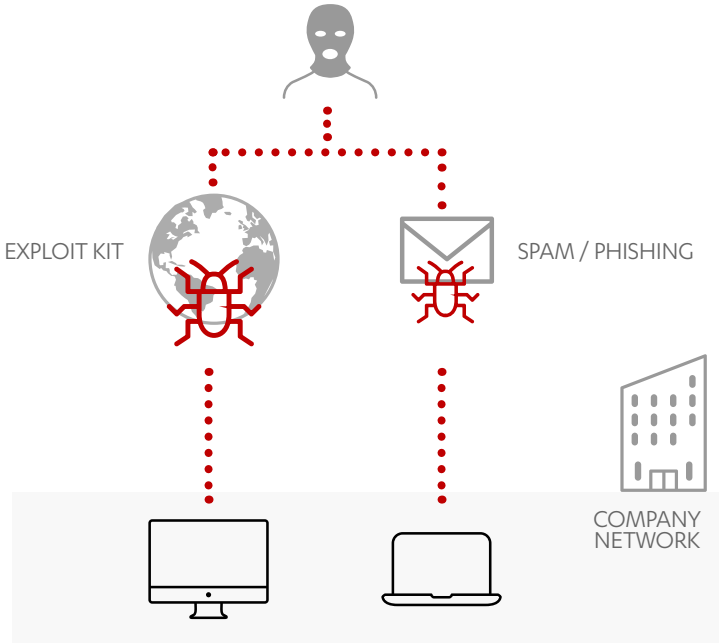
HOW IT SPREADS

SPAM OR PHISHING EMAIL MESSAGES

Email is the most common distribution method for ransomware, either as indiscriminate spam, or as *phishing* messages that are tailored to the recipient. A file is attached to the message (usually a Microsoft Office document, a zip file or an executable program) and if the recipient opens the attachment, it installs and launches the ransomware.

EXPLOIT KITS

These are toolkits that are planted by attackers on a website. The site may be a compromised legitimate one, or a malicious site where attackers lure or redirect their targets. Exploit kits probes the devices of each site visitor for vulnerabilities, and if found, exploits it so that the kit can download ransomware onto the device.



EFFECTS

ENCRYPTS THE DEVICE OR FILES

Ransomware encrypts a file by using a mathematical algorithm to 'scramble' the contents, making it impossible to use the file without a decryption key that can 'unscramble' the contents. The user is basically paying to obtain the decryption key needed to recover their content.

'BRICKS' THE DEVICE

In some cases, failure to pay the ransom - or to pay it within a specific timeframe - can lead to total loss of the affected files. If this includes operating system files or other critical components, this leaves the device useless, or 'bricks' it.

DEMANDS PAYMENT

Ransom demands usually require use of prepaid electronic cash transfer (for example, Ukash or MoneyPak), or digitial cryptocurrency such as Bitcoin. This makes it more difficult for law enforcement authorities to trace the payments and catch the criminals operating the ransomware. These payment methods can be a major stumbling block for users who do not have the knowledge or facility to obtain the necessary funds. Often, punitive action is threatened if the demand is not paid within a given time limit.

CYBER SECURITY VERSUS RANSOMWARE

Ransomware is one of the most prominent cyber threats today. Yet just like any other threat, a four-phase approach to cyber security - **Predict**, **Prevent**, **Detect**, and **Respond** - can help an organization defend against, cope with or recover from a ransomware incident.

Despite the alarming nature of the threat, the way ransomware most commonly gains entry onto a user's device - via emails or vulnerability exploits - are relatively predictable, and can be successfully identified and defended. To do so requires identifying weaknesses in the device and any installed software, then setting the appropriate safeguards in place to block any potential intrusion attempts, as well as to raise the alarm if any penetration does occur.

The four-phase approach also means that even in the event that a threat does manage to bypass protective measures, all is not lost. The affected device can still be identified and isolated, so that the damage can be contained. The findings from a forensic investigation of the device can then be used to further improve the organization's infrastructure, hardening it against future incidents.

PREDICT

- Identify software with vulnerabilities that may serve as entry points to devices, data or local network
- Identify program settings that can be configured for optimal security
- Evaluate user behavior patterns and security awareness

For more on evaluating an attack surface, see page 7.

PREVENT

- Take regular backups and ensure they are clean
- Regularly patch any installed software
- Use robust, multilayered security software
- Educate users in best security practices and threat awareness

For more preventative measures, see page 8.

DETECT

- Use security software with behavioral analysis capabilities to identify suspicious behavior on a device in the local network
- Identify the resources (devices, network shares) connected to an affected device to estimate potential exposure
- Identify changes done on the affected device by the threat

For more investigative steps, see page 9.

RESPOND

- Immediately disconnect affected devices from the local network and the Internet
- Scan all connected devices, network shares and cloud storage for evidence of the threat
- Examine the affected device for information on how the threat was able to install and run

For more on incident response, see page 10.

PREDICT

Ransomware exploits human behavior and software vulnerabilities to gain access to a device or network. Evaluate your infrastructure accordingly

HUMAN NATURE

Very often, the emails used to deliver ransomware are designed to look like legitimate messages, ones that the user would assume to be trustworthy. The user clicks on the attachment in good faith - and gets infected.

This is known as *social engineering* - and despite its simplicity, it is still surprisingly effective. Evaluating how vulnerable the users in an organization are to social engineering means considering things like:

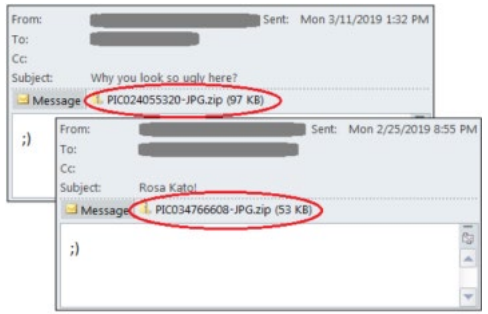


IMAGE SOURCE: F-SECURE BLOG

- Are the users regularly informed about ongoing spam campaigns that may affect them?
- Which users are most likely to receive emails from external sources?
- Can the users recognize the difference between a legitimate email and a fake that closely resembles one?
- Is there a simple mechanism in place for users to report suspicious emails?

SOFTWARE VULNERABILITIES

Ransomware that use vulnerability exploits to run are only effective if the device has software installed that has unpatched vulnerabilities. Assessing the state of all software in use on the network is therefore the single most effective proactive measure to take against vulnerability-based intrusions. Evaluating the software-related attack surface involves questions such as:

- What devices are Internet-accessible, and what programs are installed on them?
- How regularly are these programs updated? Do they have the latest security updates installed?
- Can the users manually delay or prevent updates being applied to their devices?
- Do the devices have any security programs or mechanisms in place to protect against newly discovered vulnerabilities (*zero-days*) that do not yet have a patch from the program vendor?

PREVENT

It's trite but true - prevention is better than cure
Take precautions to reduce your attack surface

Make regular backups of critical files, test them to make sure they're reliable and store them in a location not easily accessible from the internal network. This is by far the most important step in proactively guarding against any kind of infection, not just ransomware.

Keep all software up-to-date with the latest security patches from the respective vendor. If software in use has a known zero-day vulnerability, employ applicable mitigation or workaround strategies until a security patch becomes available.

Use a reputable email filtering system to minimize exposure to spam and phishing emails, disable macro scripts from Office files received via email, and educate employees on current spam and phishing schemes.

As Microsoft Windows is the most widely used - and targeted - operating system in the world, harden the settings for devices and networks using it to make it harder for potential infections to spread. Some steps that can be taken are:

- Restrict user's write access rights to network shares and connect to partitions only when necessary. Disconnect from partitions after use.
- Enable "Show hidden Files, Folders and Drives" and disable "Hide extension of known file types".
- Implement rules in Group Policy Objects to restrict execution of executable files in %APPDATA%, %LOCAL_APPDATA%, and their sub-directories, and apply exclusions for known good files [6].
- Limit users to accounts without administrator rights to prevent silent installations and modifications.
- Enable the Applocker feature available in Windows 7 and 2008 R2 [7].
- On Windows Vista and later operating systems, enable application restriction strategies.
- Activate User Account Control to prevent 'elevation of privilege' attacks on user accounts.
- Configure your anti-spam solution to filter email messages with attachments that are executable programs, as well as those of the file types ZIP, DOC, DOCX, XSL, XSLX, and XML.
- Some ransomware use the macros in Microsoft Office programs to encrypt files. Disable macros in these programs [4, 5]:
  - For all applicable versions, set the Group Policy settings for 'Macro Settings' to 'Disable macros with notification'. This blocks macros from running automatically when an Office document is opened.
  - Office 2013 and 2016: Edit the Group Policy settings to block macros from running at all in Word, Excel and PowerPoint documents that come from the Internet.

DETECT

Ransomware infections are hard to miss. What's harder to spot is the full extent of an infection, which is crucial to containment

Unlike other threats, ransomware is neither stealthy nor subtle. An infection will usually announce itself quite dramatically, as the malicious program first cuts off access to the device or files, then displays the ransom demand. Despite the immediate urgency of dealing with the affected device, it is also important to consider whether the ransomware is able to spread to other connected machines or shared storage, where it can potentially magnify the impact of an infection.

To assess the full extent of a ransomware incident, the following questions need to be addressed:

- **Is a network / device monitoring system in place that alerts administrators to suspicious behavior?** A monitoring system that uses behavioral analysis to detect suspicious activity on devices in a local network can give system administrators the critical time they need to identify an infection and mobilize resources to contain it.
- **Is the device connected to the Internet, or the local network?** If there is still an active Internet connection, the threat may still be sending or receiving data to or from the attackers operating the ransomware. If it is still connected to the local network, some ransomware can move laterally to affect other connected devices.
- **Is it connected to network shares or shared cloud storage?** Some ransomware will encrypt or block access not only to files on the device, but also to those on any accessible shares or cloud storage. This can then lead to a domino effect as other users who try to use the affected files in the shared location encounter the ransomware.
- **Have the encrypted files been synchronized to a backup solution? Are there other, clean backups of the data available?** If an automated backup process is in place, it may inadvertently transfer the affected files to the backup, making it more difficult to contain and recover from the infection.
- **What changes did the threat make to the device or files?** For example, what domains does the threat try to contact, what values were edited in the registry, processes, system parameters, etc. Forensic analysis of the changes made by the threat help to identify the same changes in other devices, which might indicate a spreading infection. This information can also be used to identify and block any subsequent reinfection attempts.
- **Can you identify the ransomware that infected the device?** Some ransomware identify themselves quite obviously, while others are less helpful. Knowingthe specific family involved makes it easier to search online for information about remedial options. The ID-Ransomware project site may be able to help identify the ransomware involved.

RESPOND

An incident response process should not only include restoring the device, files or network, but also hardening them to prevent a recurrence

CONTAINMENT

In the event of a ransomware infection, there are a couple of steps you can take to contain the fallout:

> **IMMEDIATELY** disconnect the affected device or devices from the local network and/or the Internet. Doing so prevents the infection from spreading to other connected devices. It is recommended to perform this on the network layer, or by unplugging network cables from the device.

> **Do NOT** power the devices down as you may lose valuable evidence which could be retrieved during forensic analysis.

> If several machines are infected or the infection continues to spread, it is highly recommended to ensure that your backups are completely isolated from your network. This may require you to pause synchronisations to backup servers in order to avoid overwriting your backups with infected data.

> If you do not have any backups in place, you may consider preserving at least one Domain Controller for each affected Windows Domain. Domain Controllers (DCs) are seen as the heart of Windows networks and handle all authentication events on the Domain.

Prior to initiating the recovery process following a ransomware attack, it is highly recommended that a root cause investigation is conducted. This would require preserving forensic evidence and using it to discover how the ransomware was deployed.

The outcomes of the investigation would provide guidance on how to prevent re-infections. Without having performed this due diligence, it is possible that threat actors could re-infect networks and cause further damage if appropriate security controls are not applied.

This is especially true in recent times, where threat actors first achieved a high level of privilege on the network prior to orchestrating a targeted ransomware deployment. Without an extensive investigation and cleanup operation, it is highly likely that re-infections would incur.

Should you require assistance from our global Incident Response team when experiencing a targeted ransomware attack, please refer to: https://f-secure.com/en/consulting/incident-response.

REMEDIATION

Once the extent of the attacker's foothold on the network is understood, remediation efforts can begin. It is important to note that recovering files that have been encrypted by crypto-ransomware is technically extremely difficult; in most cases, it is simpler to wipe the device clean and restore from clean backups.

Remediation efforts typically include rebuilding affected machines, resetting user accounts, applying security patches, removing persistence mechanisms of active malware, blocking the malware from executing, and monitoring for signs of re-infection while making use of existing hardware and software solutions.

GENERAL REMOVAL TOOL

In many cases, F-Secure's free Online Scanner removal tool is able to remove police-themed ransomware, restoring normal access to the system and files.

FAMILY-SPECIFIC REMOVAL TOOLS

For certain crypto-ransomware families, the No More Ransom! project have been able to obtain the decryption keys from the attackers' servers, and use them to create special removal tools that can recover the cotent of files encrypted with the keys.

These tools generally require technical knowledge to use. They are also only effective for these specific ransomware families, or even just for threats that were distributed in specific campaigns.

ABOUT NO MORE RANSOM

This initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre and security researchers aims to help victims of ransomware retrieve their encrypted data without having to pay the criminals responsible for the threat

POST INCIDENT ACTIVITY

Lastly, it is important to review what happened during the incident to determine which security controls or processes failed. Most importantly, existing policies should be updated to address the observed short comings.

SOURCES

1. F-Secure; F-Secure Rapid Detection Service (RDS) service description; https://www.f-secure.com/documents/10192/1617120/RDS-ServiceDescription.pdf
2. CNN; In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks; published 8 October 2019; https://edition.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html
3. Washington Post; Pharmaceutical giant rocked by ransomware attack; published 28 June 2017; https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/
4. TechNet; New feature in Office 2016 can block macros and help prevent infection; published 22 March 2016; https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help- prevent-infection
5. TechNet; Office 2013 can now block macros to help prevent infection; published 26 October 2016; https://blogs.technet.microsoft.com/mmpc/2016/10/26/office-2013-can-now-block-macros-to-help-prevent- infection/
6. TechNet; Using Software Restriction Policies to Protect Against Unauthorized Software; published 25 May 2004; https://technet.microsoft.com/en-us/library/bb457006.aspx
7. How-to Geek; Restrict Access to Programs with AppLocker in Windows 7; http://www.howtogeek.com/howto/6317/block-users-from-using-certain-applications-withapplocker/


F-Secure