RANSOMWARE

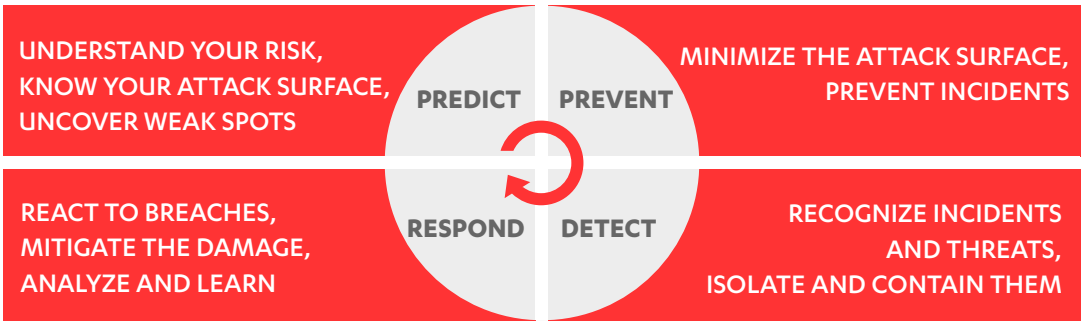
HOW TO PREDICT, PREVENT, DETECT & RESPOND

PUBLISHED
NOVEMBER 2016

F-Secure

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Many organizations still follow an outdated approach to cyber security, relying solely on a defensive perimeter to protect their infrastructure.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.

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.

DETECT

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

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, in turn, fed back into the next **Predict** phase, and the cycle continues.

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

F-SECURE LABS
THREAT RESPONSE
Whitepaper

VERSION HISTORY
First published: November 2016

CONTENT

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

The malicious programs known as **ransomware** have attracted a significant amount of coverage in the mainstream media over the last few years, as major companies and organizations announced that their operations had been affected by the threat. Examples of affected businesses include hospitals, universities and major international corporations [2, 3].

Despite the alarming nature of the threat, the way ransomware gains entry onto a user's device is actually no different from the methods used by other threats. Ransomware is most commonly spread by two methods:

- Email messages that trick users into opening a malicious file attachment, and
- Exploit kits that silently download the threat onto the user's device while they are visiting a website

These pathways onto the user's device are relatively predictable, and can be successfully identified and defended. This requires identifying potential weaknesses in the device and setting the appropriate safeguards in place, both to block any potential intrusion attempts and 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 6.

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 7.

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 8.

RESPOND

- **Immediately** disconnect the affected machine 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 9.

ABOUT RANSOMWARE

Programs that take control of a user's device or data, then demand payment to restore normal access to the ransomed content or system

Ransomware is a form of **crimeware** - malicious programs that are used, either by an individual or by organized criminal groups, to extort money from an affected user.

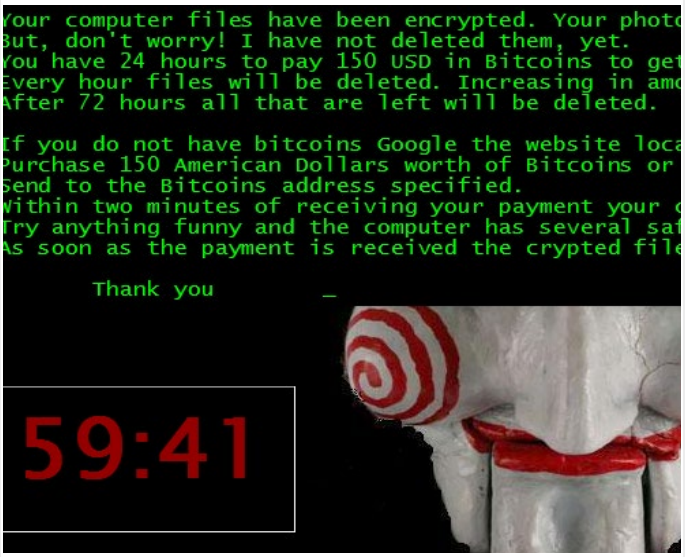
There are two main types of ransomware: **crypto-ransomware**, and **police-themed**. The types differ mainly in the kind of fear they use to motivate the user into paying the ransom: police-themed ransomware tries to scare the user into believing they need to pay a 'fine' for committing a crime of some sort, while crypto-ransomware exploits the user's fear of never recovering their content or device.

There are many different ransomware **families**, or sets of individual programs (*variants*) that are similar enough to be grouped together. Each family has unique characteristics, such as how 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 figuring out what should be done next in order to contain any damage and remove the threat from an affected device.

Types of ransomware

CRYPTO RANSOMWARE



Characteristics

Device or files are encrypted so they cannot be accessed without a decryption key

Message is displayed saying the device or files have been encrypted, as well as instructions 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

Locky, CryptoWall, TeslaCrypt, Petya, Jigsaw

POLICE-THEMED RANSOMWARE

Characteristics

Message is displayed saying the device/files have been 'locked' by a local law enforcement authority

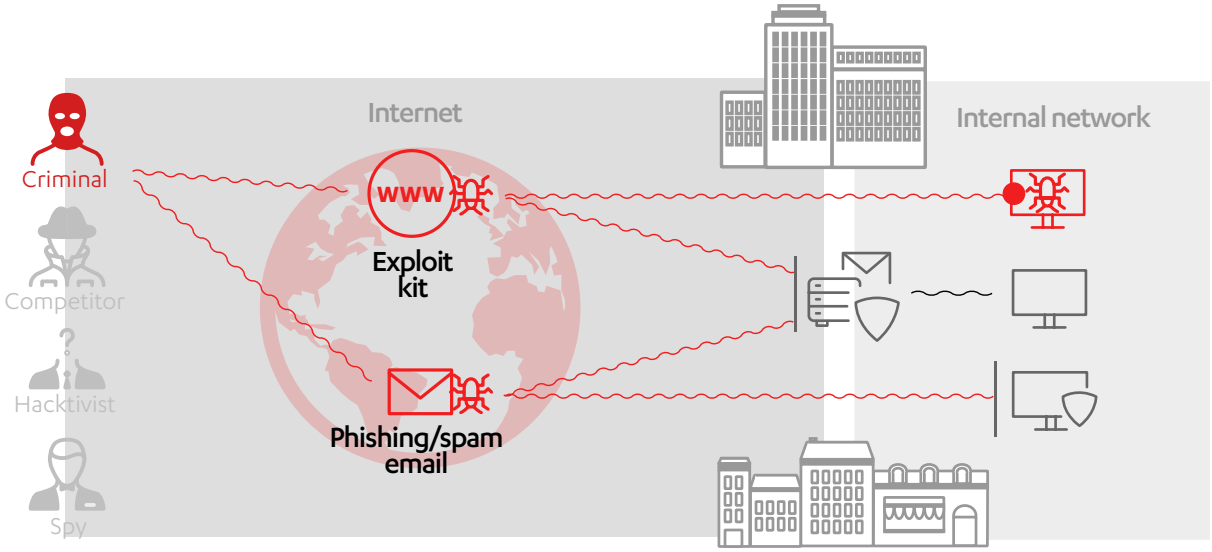
Message includes instructions for paying the 'fine', supposedly to the law enforcement authority

Some police-themed ransomware will also encrypt the device or files; others alter access to the device or files to make it appear to be 'locked'; others only display the message

Notable families

Reveton, Browlock, Urausy

How it spreads



PHISHING / SPAM EMAIL

Ransomware is most commonly spread via email, usually either in the form of mass spam messages, or more carefully crafted messages tailored to the recipient (also known as *phishing*). The email messages include a file attachment, which is most commonly a Microsoft Office document, a zip file or an executable program. If the user opens the attachment, it will run code that installs and launches the ransomware on the machine.

EXPLOIT KIT

Exploit kits are another common distribution method. These are toolkits that are planted by attackers on a website. In some cases, the site is deliberately created for malicious use, while in others, the site is a legitimate one that has been compromised. Once installed, the exploit kit probes the devices of each website visitor for any vulnerabilities that can be targeted. If a flaw is found, the kit exploits it to download ransomware onto the device.

Effects

ENCRYPTS THE DEVICE OR FILES

Crypto-ransomware (and some police-themed ransomware) will **encrypt** a file by using a mathematical algorithm to 'scramble' the contents, making it impossible to use the file without the *decryption key* that allows the contents to be unscrambled. The user is basically paying the attacker(s) behind the ransomware to obtain the decryption key needed to recover their content.

'BRICKS' THE DEVICE

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

DEMANDS PAYMENT

Ransom payments are most commonly demanded in some form of prepaid electronic cash transfer (for example, Ukash or MoneyPak), or digitial cryptocurrency such as Bitcoin. These payment options are chosen to make it more difficult for law enforcement authorities to trace the payments and catch the criminals operating the ransomware.

For some users, the requirement of using only digital cryptocurrency is a major stumbling block, as they may not have the knowledge or facility to obtain the demanded currency.

In most cases, there is a time limit on how long the user has to respond before the attacker takes some sort of punitive action.

PREDICT

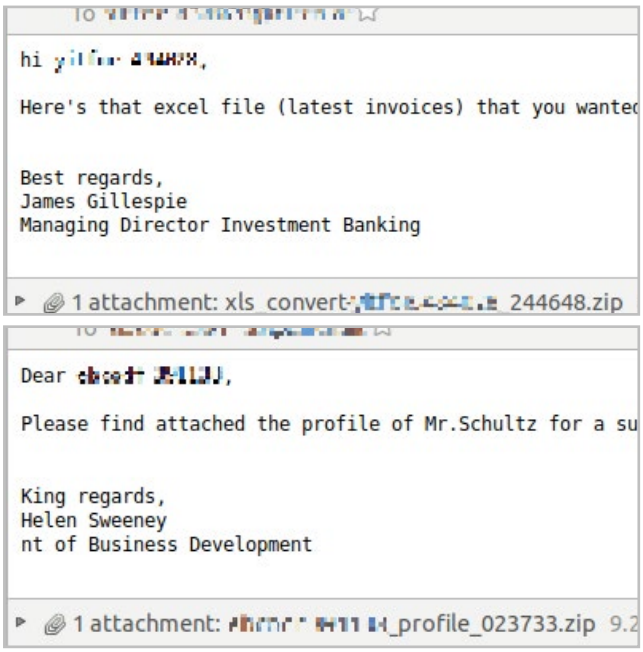
Ransomware typically exploits software vulnerabilities and human behavior to gain access to a device or network. Evaluate your infrastructure accordingly

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:

- 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

Exploit kits that distribute ransomware are only effective against software that have unpatched vulnerabilities. Assessing the state of all software in use in 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?

SPECIAL MENTION

JAVA & FLASH PLAYER

The Java development platform and Flash Player are very popular productivity and media programs, found on millions of devices around the world.

Unfortunately, their ubiquity also makes them perfect for attackers, who can use vulnerabilities in these programs to reach millions of potential targets.

Security researchers now routinely give the following advice when it comes to Java and Flash Player:

If you do not need it, uninstall it. If you do not use it regularly, disable it until it Is needed.

PREVENT

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

KEY STEPS

1. **Take regular backups of files** and test them to make sure they're reliable. This is by far the most important step in proactively guarding against any kind of infection, not just ransomware. In case you do get hit, you won't be put in the difficult position of deciding whether to pay.

2. **Keep all software up to date.** Ransomware often infects by taking advantage of security flaws in outdated software, so keeping software current will go a long way.

3. **Use robust security software** that employs a layered approach to block known threats as well as brand new threats that haven't yet been seen.

   F-Secure offers the following relevant services and technologies:

   - RAPID DETECTION SERVICE
   - F-SECURE PROTECTION SERVICE FOR BUSINESS
   - DEEPGUARD (PDF)

4. **Watch out for spam and phishing emails.** For example, the post office will never send a document as a .zip file. And so-called legal documents that ask you to "enable content" are traps. Businesses should also use a good email filtering system, disable macro scripts from Office files received via email, and educate employees on current spam and phishing schemes.

DISABLING MACROS IN MICROSOFT OFFICE

Some ransomware variants need macros to be enabled in Microsoft Office programs before they can encrypt files on the machine.

Disabling macros in these programs stops ransomware from being able to tamper with files on the machine.

To disable macros [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.
- In 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.

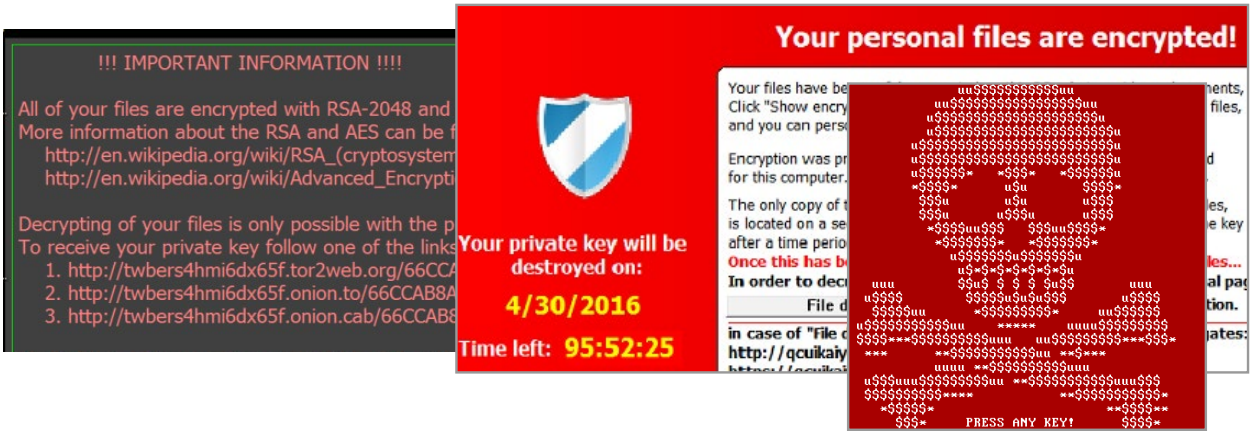
ADDITIONAL

On Microsoft Windows:

- 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 (.exe) 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 system 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 (UAC) to prevent 'elevation of privilege' vulnerability attacks on the user accounts.
- Configure your anti-spam solution to filter email messages with file attachments of the type ZIP, DOC, DOCX, XSL, XSLX, and XML, in addition to all file attachments of executable programs.

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. The images above are the ransom demands made by some of the more common ransomware families, and are clearly designed to cause fear and alarm in the users.

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:

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **Can you identify the ransomware that infected the device?** Some ransomware identify themselves quite obviously, while others are less helpful. Knowing the 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:

ID-RANSOMWARE

RESPOND

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

1. **IMMEDIATELY disconnect the device from the local network.** Contain the infection as much as possible by disconnecting the affected device from any network.
2. **Scan all connected devices and shares for similar flaws and additional threats.** Not only should other connected devices and shares be checked for infection by the same threat, but also for any other threats that may have been installed on the side.
3. **If possible, format and reinstall the device.** For larger companies, it may be more expedient to simply wipe the affected device clean and start afresh. Alternatively, there are removal tools available for specific ransomware families.
4. **Reinstate data from backups.** If available and clean, the affected data can be restored from backup files. It may be more efficient to restore files in network shares or cloud storage first, to maintain continuity and productivity for other users.
5. **Use incident response findings to reassess attack surface.** Based on the results of investigations into the incident, update any relevant security precautions or systems.
6. **Report the incident to the appropriate local law enforcement authority.** Each country handles incidents of electronic crime differently, but in general most national law enforcement agencies urge companies to report incidents and avoid paying any ransom demanded.

Removing ransomware

GENERAL REMOVAL TOOL

In most cases, F-Secure's free **Online Scanner** removal tool is able to remove police-themed ransomware, restoring normal access to the system and files. For more information about this removal tool, go to:

ONLINE SCANNER

FAMILY-SPECIFIC REMOVAL TOOLS

Crypto-ransomware is much harder to remove from an infected device. In most cases, it is simpler to wipe an infected device clean and reinstall the operating system, then recover the data from a clean backup.

For certain crypto-ransomware families, security researchers have been able to obtain the decryption keys from the attackers' servers, and use them to create special removal tools that can recover the contents of files that were encrypted with the keys. These tools generally require some level of 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. For more information about these tools, visit the **No More Ransom!** project site:

NOMORERANSOM.ORG

About the No More Ransom project

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

MANUAL REMOVAL

For instructions on manually removing infections by variants in the **Trojan:W32/Reveton** and **Trojan:W32/Urausy** ransomware families, see the **Trojan:W32/Reveton** Threat Description:

TROJAN:W32/REVETON

Caution: Manual removal is a risky process; it is recommended only for advanced users. Otherwise, seek professional technical assistance.

SOURCES

1. F-Secure; *F-Secure Rapid Detection Service (RDS) service description*; https://www.f-secure.com/documents/10192/1617120/RDS-ServiceDescription.pdf

2. BBC; *Three US hospitals hit by ransomware*; published 23 March 2016; http://www.bbc.com/news/technology-35880610

3. United States Federal Bureau of Investigations; *Ransomware is on the rise*; published 29 April 2016; https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

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/

THIS PAGE IS INTENTIONALLY LEFT BLANK


F-Secure