CRYPTO-RANSOMWARE

A quick guide to crypto-ransomware - what it is, how it works, what happens when your computer is infected and what you can do to protect your computer

Crypto-ransomware is a type of harmful program that encrypts files stored on a computer or mobile device in order to extort money.

Encryption 'scrambles' the contents of a file, so that it is unreadable. To restore it for normal use, a decryption key is needed to 'unscramble' the file.

Crypto-ransomware essentially takes the files hostage, demanding a ransom in exchange for the decryption key needed to restore the files.

Using shock and fear tactics

Unlike other threats, crypto-ransomware is neither subtle or hidden. Instead, it prominently displays lurid messages to call attention to itself, and explicitly uses shock and fear to pressure you into paying the ransom.

A few so-called crypto-ransomware do not perform the encryption at all, and just use the threat of doing so to extor money. In most cases however, the threat is actually carried out.

NOTABLE RANSOMWARE:

- Trojan:W32/Petya.F (https://www.f-secure.com/v-descs/trojan_w32_petya_f.shtml)
- Trojan.Ransom.WannaCryptor (https://www.f-secure.com/v-descs/trojan_w32_wannacryptor.shtml)
- Trojan-Downloader:JS/Locky (https://www.f-secure.com/v-descs/trojan-downloader_js_locky.shtml)

Encountering crypto-ransomware

There are two common ways you can encounter crypto-ransomware:

- Via files or links delivered through emails, instant messages or other networks
- Downloaded onto your device by other threats, such as trojan-downloaders (https://www.f-secure.com/v-descs/trojan-downloader.shtml) or exploit kits (https://www.f-secure.com/v-descs/articles/exploit-kit.shtml)

Delivered as files

Users most commonly come into contact with crypto-ransomware via files or links that are distributed in email messages:

- The email message contain links to 'documents' saved online. In fact, the documents are executable programs (the crypto-ransomware itself)
- The emails have attached files that download crypto-ransomware onto the device. Common files formats used to deliver crypto-ransomware include:
- Microsoft Word document (file name ends with .doc or .docx)
- Microsoft XSL document (.xsl or .xslx)
- XML document (.xml or .xslx)
- Zipped folder containing a JavaScript file (.zip file containing a .js file)
- Multiple file extensions (e.g., <INVOICE#132435>.PDF.js)

Tricking the recipients

Receiving the email itself does not trigger an infection; the attached or linked file would still need to be downloaded or opened.

Attackers often craft the email messages using social engineering tricks to lure the recipients into opening the links or attached files. For example, they use the name and branding of legitimate companies, or intriguing or legal-sounding texts.

Opening the attachments

If the opened file is JavaScript, it will try to download and install the crypto-ransomware itself from a remote website or server.

If the attached file is a Microsoft Word or Excel document, harmful code is embedded in the file as a macro. Even if the user does open this file, the macro can only run if one of the following conditions is present:

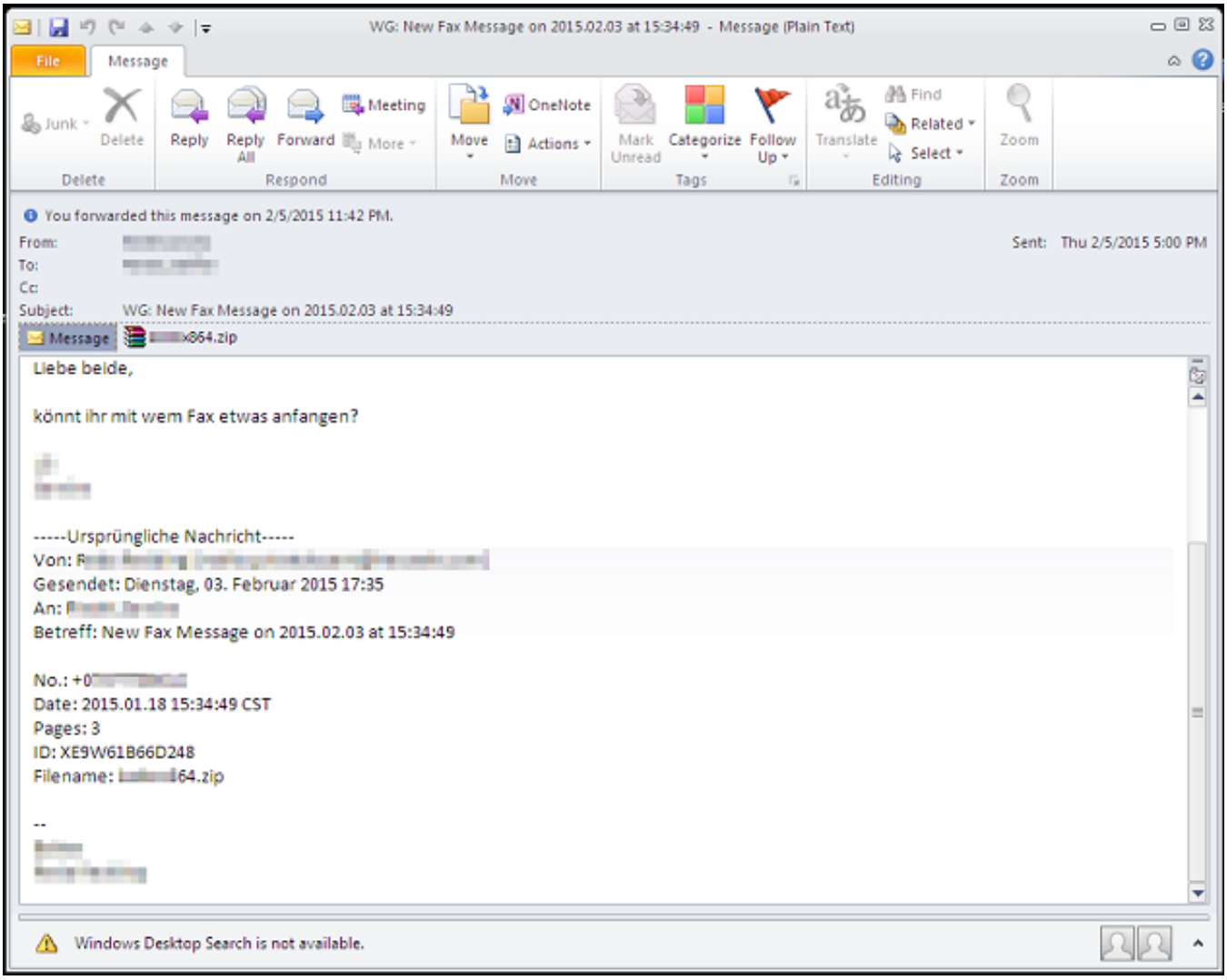
- Macros are already enabled in Word or Excel
- The user is tricked into enabling macros

Macros are disabled by default in Microsoft Office. If they happen to be enabled when the file opened, the macro code run immediately.

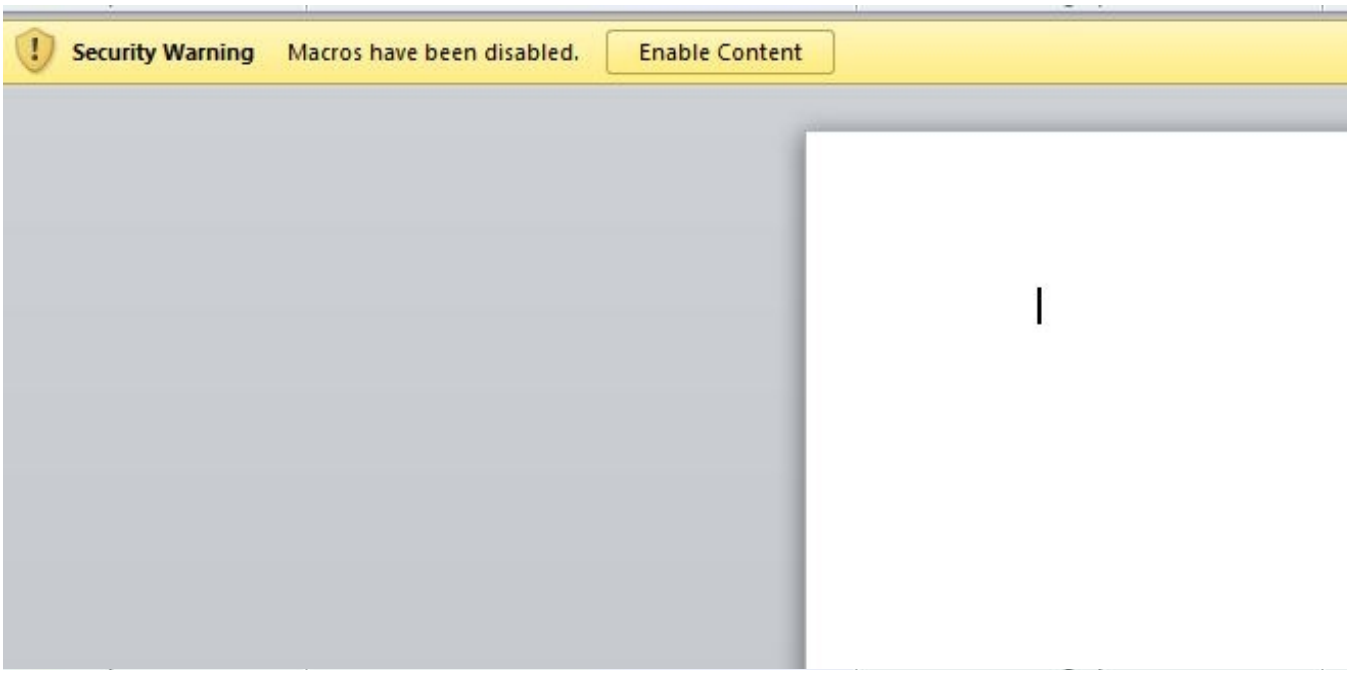
If macros are not enabled, the file will display a notification prompt asking the user to enable them. If the user clicks 'Enable Content', macros are enabled and the embedded code will run immediately.

Delivered by exploit kits

Crypto-ransomware can also be delivered by exploit kits, which are toolkits that are planted by attackers on websites. There are



SPAM USED TO SPREAD THE CTB-LOCKER CRYPTO-RANSOMWARE
(SOURCE:F-SECURE WEBLOG)



NOTIFICATION MESSAGE IN WORD ASKING USERS TO ENABLE MACROS

numerous exploit kits currently delivering ransomware in the wild, such as Angler, Neutrino and Nuclear.

These kits probe each website visitor's device for flaws or vulnerabilities that it can exploit. If a vulnerability is found and exploited, the exploit kit can immediately download and run crypto-ransomware on the device.

Encrypting files and demanding ransom
When the crypto-ransomware is downloaded and run on a device, it hunts for and encrypts targeted files.

Some crypto-ransomware, such as older variants of TeslaCrypt, will only encrypt specific types of files. Others are less discriminating and will encrypt many types of files (for example, Cryptolocker). There is also one known family, Petya, that encrypts the Master Boot Record (MBR), a special section of a computer's hard drive that runs first and starts (boots) its operating system, allowing all other programs to run.

After the encryption is complete, the crypto-ransomware will display a message containing the ransom demand. The amount will vary depending on the specific ransomware, and the payment is often only in Bitcoins, or a similar digital cryptocurrency. Specific instructions are also provided.

In some cases, the attackers put extra pressure on victims to pay the ransom by allowing only has a limited time period to meet the demand. After the stipulated time, the decryption key may be deleted, or the ransom demand may be increased.

F-SECURE WEBLOG: THE RANSOM NOTICE DISPLAYED BY CTB-LOCKER CRYPTO-RANSOMWARE.

Consequences
If the affected files contain valuable data, encrypting them means losing access to that information. If the data is critical to a business - for example, a patient data in a hospital, or payroll details in a finance firm - the loss of access can impact the entire company.

If the affected files are used by the device's operating system, encrypting them can stop the device from working properly. If the device is critical to a company's operations - for example, a server, hospital medical equipment, or industrial control system - the business impact can be siginificant.

In recent years, there have been multiple cases of ransomware spreading through entire company networks, effectively disrupting or even halting normal business until the infected machines can be cleaned and the data recovered.

TO PAY OR NOT TO PAY?

Ransomware works on the assumption that the user will be inconvenienced enough at losing access to the files that they are willing to pay the sum demanded.

Security researchers and law enforcement authorities, in general, strongly recommend that the victims refrain from paying the ransom. In some reported cases however, the crypto-ransomware infections have been so disruptive that the affected organizations and users opted to pay the ransom to regain the data or device access.

Respond & recover
If the worst happens and crypto-ransomware does infect your device, there are a couple of steps you can take to contain the damage:

- **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.
- **Scan all connected devices and /or cloud storage for similar flaws and additional threats.** Not only should other connected devices and storage media be checked for infection by the same threat, but also for any other threats that may have been installed on the side.
- **If possible, identify the specific ransomware responsible.** Knowing the specific family involved makes it easier to search online for information about remedial options. The ID-Ransomware (https://id-ransomware.malwarehunterteam.com) project site may be able to help you identify the ransomware involved.

Once you are certain the infection is contained, you can then try to remove the infection, recover the device and the data saved on it.

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 reinstall the operating system, then recover the affected data from a clean backup.

You can take the following steps for recovery:

- **If possible, format and reinstall the device.** Usually, this is the most expedient way to remove a ransomware infection. In a small handful of cases, there are removal tools available for specific ransomware families (see *Family-specific removal tools* below) which you may consider as an alternative.
- **Restore data from clean backups**. If available and clean, the encrypted data can be recovered by restoring from backup files. In cases where no decryption is possible, this is the method recommended by law enforcement authorities and security experts to avoid paying the operators responsible for crypto-ransomware.
- **Reevaluate the security of any software installed.** To prevent a recurrence, ensure any software installed (including the operating system) is up-to-date with the latest security patches.
- **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 affected individuals or companies to report incidents and avoid paying any ransom demanded.

Family-specific removal tools

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.

Do note however that 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.

No More Ransom

For more information about these tools, visit the No More Ransom! project site. 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 retrieve their encrypted data without having to pay the criminals responsible for the threat.

Prevention

As an individual user, you can take a number of simple precautions to avoid becoming a victim of crypto-ransomware:

- Backup all necessary files regularly, and store them in a location not connected to the computer or network. This means that even if your computer is affected, you always have unaffected backups available.
- Apply all critical and important security patches for all installed operating systems and applications. This prevents scenarios where the attack vector is not simply email file attachments, but vulnerability exploit attacks.
- Enable all your antivirus solution's security features and keep it up-to-date with the latest signature databases.
- Avoid opening emails sent by an unknown sender, especially if it contains an attachment or a link.
- Enable "Show hidden Files, Folders and Drives" and disable "Hide extension of known file types". This helps you spot files that have multiple file extensions.
- In Microsoft Office, make sure that the settings for 'Macro Settings' are set to 'Disable macros with notification'. This will block macros from running automatically when the document file is opened.

- In Office 2016, you can modify the settings to block macros from running at all in documents that come from the Internet. This new feature was added in response to the resurgence of macro malware. More information and instructions are available at: https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/ (https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/)