CERT.be

Ransomware Whitepaper

TLP: WHITE

Author: CERT.be

1. Introduction

Lately many computer users will have heard/read a lot about the following malware: Cryptolocker, TorrentLocker, Cryptowall, TeslaCrypt, CTB-Locker, PadCrypt, Locky, Petya, ... All of them are Ransomware. Ransomware is a type of malware which tries to extort users of the infected systems. This document tries to give a quick view about the characteristics of this type of malware, what we can do to prevent it, and what to do when infected.

2. About Ransomware

2.1. Two types of ransomware

Currently, literature makes a distinction between non-encrypting and encrypting ransomware:

- Non encrypting ransomware threatens you with the diffusion of collected personal information, e.g.: browsing history.
- Encrypting ransomware (cryptoware), which is the most common type nowadays, will encrypt the user's files. It doesn't encrypt the computer as a whole, since the computer remains generally operational. However it does encrypt all the files which might hold some value for the user, even if these documents don't reside on the computer itself, but are accessible through network shares. In order to recover the encrypted files, the ransomware urges you to buy the decryption key. Some newer variants target the database of your website, the data on your phone... The most common encryption algorithms used by these ransomware are AES 256 bits and RSA 2048 bits. Each day, new variants of ransomware appear. Most of the ransomware works for Windows but this is not exclusive. There is also ransomware on MacOS, iOS, Linux, Android, ...

In this document we will mainly talk about the encrypting type of ransomware, as it is the most commonly seen these days.

2.2. Distribution

Ransomware is distributed using multiple vectors:

- Phishing Mails: Some phishing campaigns are used to spread ransomware. These mails contain a malicious attachment which serves as a Downloader/Dropper. It is the dropper's job to download and install the cryptolocker without being noticed. At the end of this section we describe the most commonly used droppers.
- Compromised Web page: When you visit a compromised page, a script downloads a malicious payload which could be a ransomware.

The malicious actors remain creative, thus this is no exclusive list. Other distribution methods might be used.

The most commonly used downloaders/droppers are:

- Microsoft office documents that contain malicious macro's
- Malicious javascript documents
- Malicious LiNK (.lnk) files. Lnk is the file extension used for icons that launch applications on windows.
- Microsoft Compiled html help (.chm), is a format made by Microsoft to distribute help documents.

3. Preventive Measures

There are different measures that can be taken on different levels to prevent or reduce the impact of cryptoware. A quick search will reveal dozens of "tips to prevent ransomware articles". We will enumerate some of the most relevant ones.

3.1. Users

Keep your users informed: an infection almost always begins with a human error. Keeping your users informed about the risks of opening attachments, suspicious software, or links is the first line of defense. However, even trained personnel is error-prone, NEVER count on the human element to keep you safe.

3.2. On Workstation

1. Disable macros: We mentioned in the previous section that office documents can contain malicious macro's. When you don't use macro's, you can disable them. More info Office 2007 and Office 2010.
2. Disable vvsaexe: prevent ransomware from encrypting your Volume Shadow Copy which is a copy of the files, by disabling the vssaexe service. This is a standard builtin functionality to administer the VSC. The shadow copies will be stopped when you disable the service. The ransomware will no more be able to encrypt these files that could be used to recover a part of the files.
3. Disable Windows Script Host (WSH): Disabling WSH prevents the execution of javascript when they are opened under windows. However, this measure should be carefully considered as it might have an impact on production software.

4. Show hidden extensions on Windows. A simple way to trick users into opening an executable file is to add another extension. And attacker could, for example, name a file "MyFile.pdf.exe". Windows will hide the ".exe" extension by default, making the file appear as a simple pdf. Untrusted ".exe" files should, off course, never by opened.

5. Install a Script blocking application: To avoid the execution of malicious scripts on a website, you can install plugins that block scripts.

6. Restrict file permissions. Windows users can prevent the execution of files in %TEMP% and %AppData% directories. This is usually where malware is installed, and restricting permissions can prevent it from running.

7. Take variant-specific preventive measures. Some ransomware variants have know flaws which can prevent them from executing (for example, creating a HKCU\Software\Locky registry key will prevent certain Locky versions). Putting these measures in place will require a varying level of technical expertise and will only be effective against a given program/version.

8. Keep your system and your antivirus up to date.

3.3. On Fileserver

Fragment your shares. To reduce the impact of the encryption, you should reduce the rights on different shares. What a malware can't edit, it can't encrypt. You can also check the creation of specific extension used by ransomware

3.4. On Mail-server

Filter on attachements at the e-mail gateway: Block e-mails containing executables, but don't hesitate to block attachements with filetypes that shouldn't be or don't often get e-mailed around like .chm, .lnk and .js.

3.5. On the Network

1. Use a proxy with webfiltering: Some proxies allow you to filter the traffic from blacklisted domains. This could reduce the risk of infection, if the list is up-to-date.

2. Fragment your network: Often cryptoware scans for network shares to encrypt. If your network is fragmented you will reduce the number of shares available.

3.6. With your backup

When all your shared network resources (also called shares) are encrypted by ransomware, it is useful to have a backup. It is really important to keep your backup offline, unconnected to your network and computer, to avoid them also being encrypted. You have to backup regularly and ensure that your backups actually work. If employees are responsible for backing up their own machines, ensure that this is done according to a policy.
NOTE: Backups are the only SURE way to recover files after a ransomware infection.

3.7. Commercial Solutions

Each day new dedicated protection software are published. Security companies are constantly trying to thwart ransomware and publish software designed to stop these programs from executing (see section 5.1). However ransomware keeps evolving, so these solutions are **not guaranteed** to work against all ransomware variants and versions.

4. What to do when infected

Once infected, it is often too late. The only surefire way to recover files is through the use of backups. If you are victim of an attack, the first step is to identify the variant (and potentially version) of the program. This this usually mentioned explicitly in the ransom message or in the program window. Be as specific as possible when looking for information or seeking help for the problem.

4.1. Immediate action

Disconnect the infected machine from the network and all the storage devices that are connected on the machine as quickly as possible. It could reduce the data loss if all the files are not yet encrypted.

4.2. Report the incident

If you were the victim of a ransomware, it is always usefull to report this to CERT.be. We are specifically interested in the type of ransomware you were victim of, what dropper was used (how you got infected) and an extract of the dropper or the malware itself. You may also contact your local police department. CERT.be can help you determine what information to send them.

4.3. Restoring your files

Before trying to recover your files it is important to remove the ransomware from your machine. This can be done by either reinstalling the machine entirely or by using a third party malware

removal software (usually part of a commercial anti-virus). You should also isolate the infected machine from the rest of your network. Once the cryptolocker is removed, you can restore the lost files using your backup.

On Windows, you might be able to restore files to previous unencrypted versions using the Shadow Volume Copies created by the System Restore features. Recent cryptoware will often target and delete these copies, however. Some cryptoware only encrypts a part of the disk, you may be able to recover files using File recovery tools.

4.4. To pay or not to pay

We strongly discourage paying, as it is only encouraging the malicious actors to continue their activities. As soon as a certain type of attack becomes uninteresting, criminals will no longer invest in it.

If you pay, you can never be 100% certain that you will get your files back. The attacker may simply choose to withhold the key, or bugs in the ransomware could prevent the correct decryption (there are cases where files were corrupted during encryption which made any decryption impossible). Furthermore, backdoors or other malware can be invisibly installed along with the ransomware, so you can't be sure your machine is actually clean.

4.5. Reverse engineered cryptoware

If you have no backups, then there is one last resort. Some older versions of cryptoware have been cracked. For these versions, scripts to decrypt your files are available on the web (see section 5.2). Even more so than for prevention software, this approach is extremely dependent on the program and version used in the attack (and many current versions are virtually unbreakable).

5. External Resources

Software presented here is not intended to provide an up-to-date or exhaustive list on options. Most instances are limited to specific malware variants and versions.

5.1. Ransomware prevention examples:

- https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/
- https://www.foolishit.com/cryptoprevent-malware-prevention/
- https://blog.malwarebytes.org/malwarebytes-news/2016/01/introducing-the-malwarebytes-anti-ransomware-beta/

5.2. Ransomware decryption examples:

- https://www.nomoreransom.org/
- https://www.talosintel.com/teslacrypt_tool/
- https://noransom.kaspersky.com/
- https://labs.bitdefender.com/2016/01/third-iteration-of-linux-ransomware-still-not-ready-for-prime-time/
- https://github.com/Googulator/TeslaCrack
- http://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/

5.3. Other links

- Awarness(NL): https://www.safeonweb.be/nl/nieuws/laat-je-niet-gijzelen-door-ransomware
- Awarness(FR): https://www.safeonweb.be/fr/actualites/ne-vous-laissez-pas-prendre-en-otage-par-des-virus-de-ran
- Advisory: https://www.us-cert.gov/ncas/alerts/TA16-091A
- Advisory: http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ALE-015/index.html [French]
- Advisory: https://www.circl.lu/pub/tr-41/
- Identify: https://id-ransomware.malwarehunterteam.com/
- Tips: https://isc.sans.edu/diary/Tips+for+Stopping+Ransomware/20903