Mohd Amirul Kasyful Nur bin Zulkifli

From: UUMIT
Sent: 12 April 2016 14:13
To: UUM - All Staff; UUMstudgroup
Subject: IT SECURITY ALERT : Recent Threat of TeslaCrypt Ransomware

UUM Information Technology

To All UUM communities;

Recent Threat of TeslaCrypt Ransomware

Introduction

Ransomware is a type of malicious software (malware) that infects a computer and restricts access to it until a ransom is paid to unlock it. This type of malware, which has now been observed for several years, attempts to extort money from victims by displaying an on-screen alert. These alerts often state that their computer has been locked or that all of their files have been encrypted, and demand that a ransom is paid to restore access. This ransom is typically in the range of $100–$500 dollars, and sometimes the cybercriminal demanded the ransom in Bitcoin.

Recently, MyCERT is aware about the spreading of ransomware in the constituency that affects computers belong to individual users and commercial business. Majority of the ransomware incidents that we receive lately are related to the TeslaCrypt variant, apart from a few related to CryptoLocker variant.

Brief Description

The recent incidents we received is a new variant of the TeslaCrypt ransomware in which the file extension for the encrypted files is **.MP3**. Initially, TeslaCrypt is a ransomware that targets computers installed with specific games, such as Call of Duty series, World of Warcraft, Minecraft. However, newer versions of TeslaCrypt also targets computers without these specific games installed. As for the newer variant, it targets for Word, PDF and JPEG files.

The new ransom note filenames are now in the format:

_H_e_l_p_RECOVER_INSTRUCTIONS+[3-characters].png,**_H_e_l_p_RECOVER_INSTRUCTIONS+[3-characters].txt**, and **_H_e_l_p_RECOVER_INSTRUCTIONS+[3-characters].HTML**.

Other than that, the ransom notes are worded the same way. Below are the screenshot of the TeslaCrypt Ransomware note:

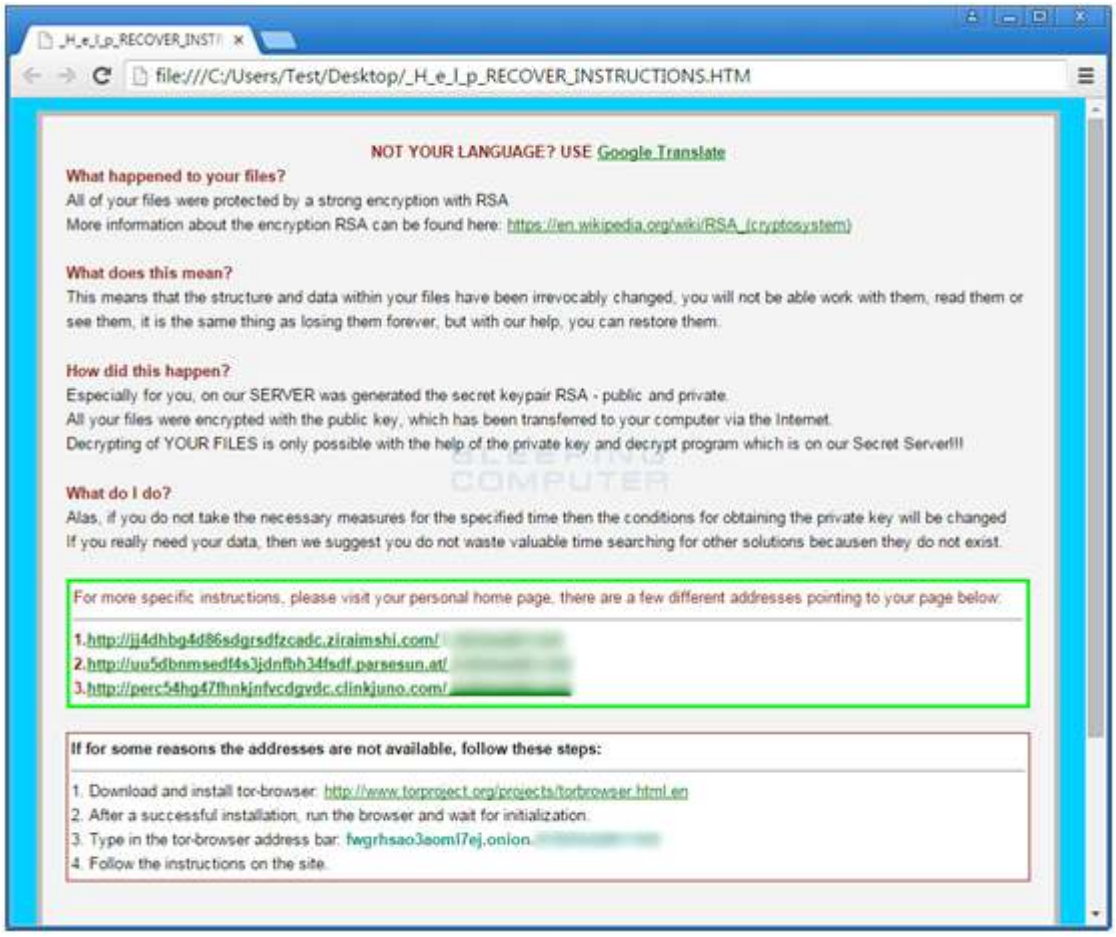

Figure 1: TeslaCrypt's ransom note

TeslaCrypt encrypts original files in the infected computers with the **.MP3** extension. That means that if the original filename is **hello.jpg**, once it is encrypted it will be changed to **hello.jpg.mp3**. Below is the screenshot of the encrypted files with the .MP3 extension.

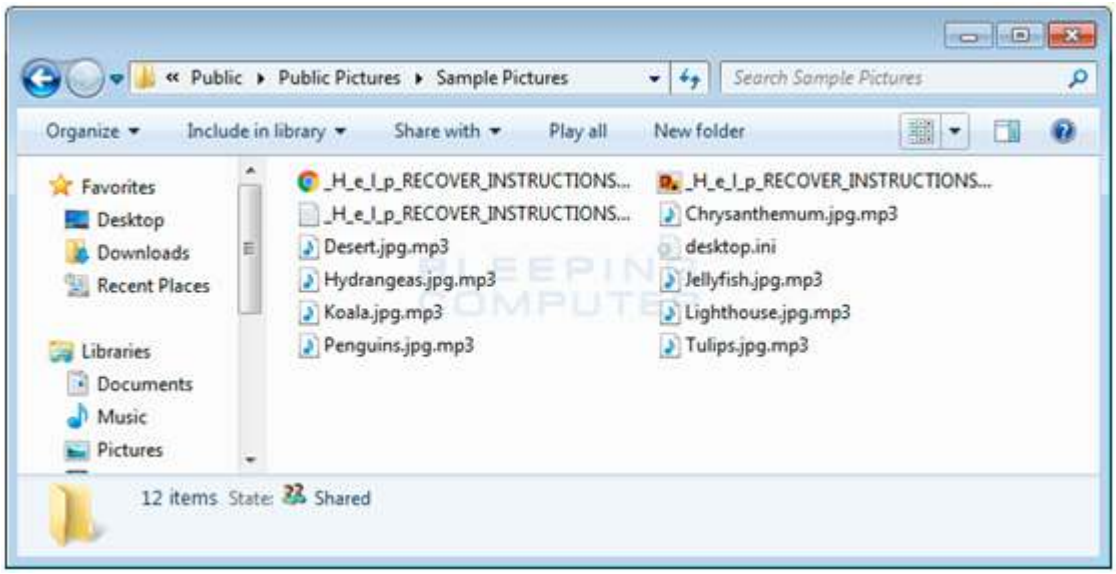

Figure 2: Files encrypted with .MP3 extension

Impact

Ransomware not only targets home users; businesses can also become infected with

ransomware, leading to negative consequences, including:

- Temporary or permanent loss of sensitive or proprietary information
- Disruption to regular operations
- Financial losses incurred to restore systems and files
- Potential harm to an organization's reputation

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Recommendations

MyCERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.

- Prevent execution of Files in %AppData% Directories - for the malware to execute it usually resides in various temporary directories in Windows (%AppData%). It is possible to disable the ability to execute binaries in these directories via Group Policy or Security Policy which means when a user double-clicks on Invoice.exe, the malware will not run.

- Keep your operating system, softwares, Java, Shockwave and Flash up-to-date as exploit kits rely on vulnerabilities on the client machine to get malware to execute. Usually this involves vulnerabilities in Java, Shockwave, Flash, and Adobe Reader. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

- Maintain up-to-date anti-virus software, and scan all software downloaded from the Internet prior to executing.

- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For

enterprises or organizations, it may be best to block email messages with attachments from suspicious sources. Many ransomware emails use attachments with executables, simply disabling e-mails with executables will prevent users from receiving. Also look for emails with "double file extensions". Another common trick is attachments with a zip file that may include an executable or an html document (using other tricks to download an executable).

- Do not follow unsolicited Web links in emails.

For any inquiries, please contact UUMIT at 04-9286666 or email to itservices@uum.edu.my.

Thank you.

UUM Information Technology (UUMIT) | Universiti Utara Malaysia | 06010 UUM Sintok, Kedah, Malaysia | Office : +6049286666 | Fax : +6049282343 | Email : it@uum.edu.my | Website : http://it.uum.edu.my

Get in touch with us via :

Stop by UUMIT

Fill Up Online Form

Visit at http://servicedesk.uum.edu.my

Call +6049286666

Email to itservices@uum.edu.my

Contact Onsite Support Team