Ransomware Analysis and Recommendations

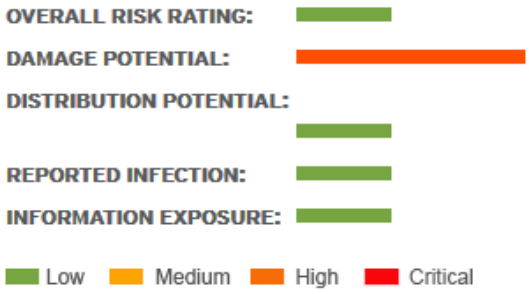
RANSOM_CRYPTESLA.YUYAIF

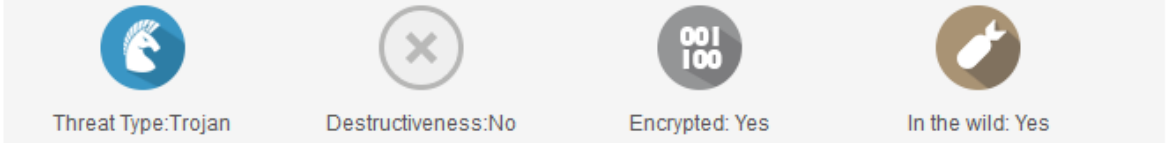
Publish date: March 08, 2016

ANALYSIS BY

Francis Xavier Antazo

PLATFORM: Windows





Malware family as well as additional ransomware information:

- Crypto-ransomware family (Crypto Locker\wall V3-4\Locky\TeslaCrypt) has the capability to encrypt your files.
- After execution of its malicious routine, some variants have been observed to delete themselves from the system.
- It is recommended to restore from back-up all encrypted files Crypto-ransomware uses a high level of encryption.
- The malware uses asymmetric type of encryption, which means a private key is needed coming from the malware author to decrypt the files.
- The files cannot be decrypted manually or by a tool within any reasonable amount of time. Thus, restoring the encrypted files/systems from backups is the only recommended option.
- Always consider having a critical file backup strategy in case of a serious infection or other major issue such as a system or hard drive crash.
- One good safe computing practice is to ensure you have accurate back-ups of your files.
- The 3-2-1 principle should be in play: three copies, two different media, one separate location.
- Windows has a feature called Volume Shadow Copy that allows you to restore files to their previous state, and is enabled by default.

- Cloud storage services (such as SafeSync) can be a useful part of your backup strategy. Although, some new variants of crypt ransomware will disable or remove the volume shadow copies it is always a good idea to enable these types of backups.

Ransomware History:
http://www.trendmicro.com/vinfo/us/security/definition/Ransomware
Cryptesla Variant:
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom_CRYPTESLA.YUYAIF
Ransomware: What it is and how can you protect yourself
http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-what-it-is-and-how-you-can-protect-yourself

Specific tips when dealing with infections:

How to try and pinpoint the infected or source computer:

- Locate computer with files with encrypted extensions or the Help_decrypt\Help_your_files\recover files\Recovery*.txt
- Isolate the computer taking it off the Network as soon as possible as a proactive measure.
- To locate the source of the infection if a file server or NAS/SAN is affected, look for the last user who modified the files or current open sessions to encrypted files.
- If NAS/SAN audit is enabled check the audit logs to find out which user encrypted the files.
- Isolate the encryption source by finding out which people/departments have access to the encrypted shares
- Run ATTk scan tool on the encryption source (as mentioned previously, many variants remove themselves after executing the encryption payload to prevent reverse engineering, so it is possible no malware will be found on the system):
- Download the Anti-Threat Toolkit by clicking your operating system version below:

    - 32-bit
    - 64-bit

Once we've verified that there are no more malware on the machine please be guided our recommendations below to help prevent similar future infections:

Trend Micro Recommendations

1. Optimize your OfficeScan (OSCE) server security settings to help prevent future malware infection:

- Apply OSCE best practice settings for malware http://esupport.trendmicro.com/solution/en-US/1054115.aspx
  On the best practice guide make sure to enable and configure the following settings:
    - Enable Behavior Monitoring (AEGIS) to block the infection routine

- Enable Web Reputation Service feature to block communications between the malware and its C&C server.
- Enable Meerkat in OfficeScan (OSCE) to notify users before executing newly encountered files that can be a new undetected malware http://esupport.trendmicro.com/solution/en-US/1103392.aspx
- Enable the Ransomware Protection feature in OfficeScan (OSCE) 11.0 Service Pack 1 – http://esupport.trendmicro.com/solution/en-US/1111377.aspx

2. Optimize your SPAM/E-mail protection.

- Make sure that you have a mail scanning solution implemented on your network.
- Several variants of the ransomware malware were detected to have originated from spam emails -- as a malicious attachment.
- Crypto-ransomware related threat normally enters a network via spam/phishing emails with malicious attachments.
- Since the malware writers can easily mutate or repack the malicious files to create different samples to avoid pattern signature detection, then one of the best preventive measures is to use attachment scanning and blocking methods at the email or gateway level.
- Some of Trend Micro's solutions for this include ScanMail for Exchange (SMEX), InterScan Messaging Security Suite (IMSS) and InterScan Messaging Security Virtual Appliance (IMSVA).

2.1. Detect & quarantine executable file type (EXE, JS…) inside a zip or compress file.

IMSx & SMEX provide a feature to detect and quarantine executables file inside a compress file.

Recent wave of Crypto ransomware malware use JS file inside a compress file. This best practice can stop it as well.

http://esupport.trendmicro.com/solution/en-US/1099665.aspx
http://esupport.trendmicro.com/solution/en-US/1101849.aspx

2.2. Enable New-Born URLs Handling Function in messaging products.

New-Born URLs handling feature had proved to be very effective to stop spam and also malicious email which carry ransomware.

Both IMSx and SMEX (11 SP1) support this feature.

Ref Link - http://esupport.trendmicro.com/solution/en-US/1108290.aspx

The settings should be:

- Scanning Conditions [Default spam rule]
- Take rule action when: any condition matched (OR)
- Spam/Phishing/Social Engineering Attack
- (Checked) Spam detection settings
- (Checked) Phishing email
- Web Reputation
- (Checked) Web Reputation Settings

3. Disable or limit file sharing.

Once a machine is infected, and any mapped or shared drives are detected, then the ransomware will also attempt to encrypt files on those drives. So for files which are hosted on shared/mapped drives those will be encrypted as well.

Therefore it is recommended to turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts.

Good practices to prevent ransomware infections via email:

- Always check who the email sender is. If the email is supposedly coming from a bank, verify with your bank if the received message is legitimate. If from a personal contact, confirm if they sent the message. Do not rely solely on trust by virtue of relationship, as your friend or family member may be a victim of spammers as well.
- Double-check the content of the message. There are obvious factual errors or discrepancies that you can spot: a claim from a bank or a friend that they have received something from you? Try to go to your recently sent items to double-check their claim. Such spammed messages can also use other social engineering lures to persuade users to open the message.
- Refrain from clicking links in email. In general, clicking on links in email should be avoided. It is safer to visit any site mentioned in email directly. If you have to click on a link in email, make sure your browser uses web reputation to check the link, or use free services such as the Trend Micro Site Safety Center. (http://global.sitesafety.trendmicro.com/)
- Block executable file types, including those in compressed file attachments in emails. A file with an executable file extension means that the file format supports some ability to run an automatic task. This is in contrast to other file formats that simply display data, play a sound or video, etc. If you open a file with one of these file extensions, your computer could, without your continued permission, run one or more operations programmed into that file. For new malware samples or variants which may not be in a detection pattern yet, this would allow the malware to infect the system it is run on.