2017. 03. 02

Tech Report

Ransomware Trends to Watch

Notorious ransomware in 2016 and changes in ransomware trends

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com

Table of Content

Introduction

On November 27, 2016, ransomware infected San Francisco's Municipal Transportation Agency (SFMTA, or 'Muni') system and disabled the ticketing system. Known as HDDCryptor, this malware encrypts files and overwrites the MBRs to prevent a PC from booting up. Almost 25 percent of Muni's network was compromised, which included more than 2,000 payment and scheduling systems. Attackers demanded 73,000 USD for the decryption key. SFMTA announced that they refused to pay the ransom demand and are conducting an ongoing investigation. While they claimed there was "no impact to the transit service" (passengers were simply allowed to ride for free that day), one thing that this incident makes clear is that ransomware no longer just disables files and computers, but now also poses a threat to critical infrastructure.

Starting in 2015, ransomware has steadily increased to become a matter of concern for cyber security in 2016. According to AhnLab Security Emergency-response Center (ASEC), only 10 types of ransomware were roughly in existence from 2013 to 2015; however, in 2016 alone, the number increased to about 160 types including their variants (as of December 15, 2016). For the past year, ASEC noted a rapid increase in new ransomware, with 15 to 20 new versions emerging each month in the second half of the year. Including ransomware that are as of yet unknown, the total number will surely exceed this number.

The reason for the rampant increase of ransomware is, in short, money. For attackers, ransomware has been something of a proven means for raising immediate funds in a short period of time. Many security experts thus anticipate that the number of ransomware will continue to increase in 2017.

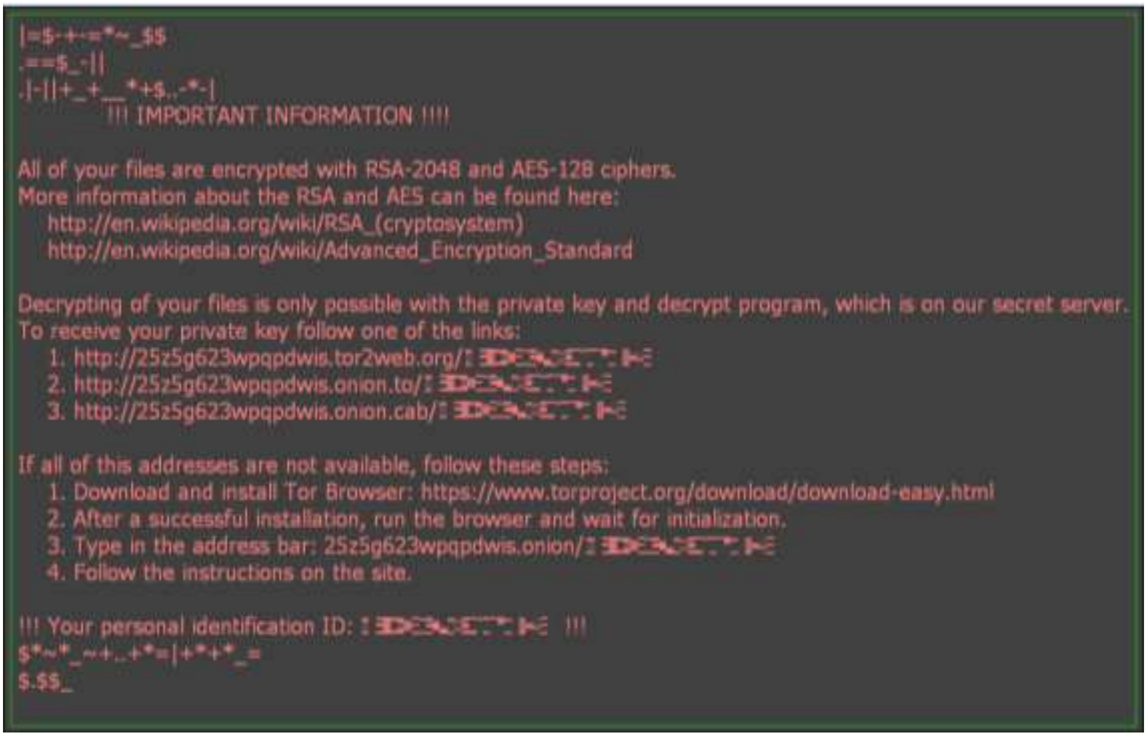
This report presents ransomware trends for 2016 and beyond.

Findings 1: Representative ransomware in 2016

1. Locky: No. 1 ransomware of 2016

Locky ransomware, which caused widespread global damage, expanded by changing its distribution and infection methods. It usually distributes malware via spam email containing infected attachments or links to malicious websites, and became notorious for the sheer volume of spam mail sent during the past year alone.

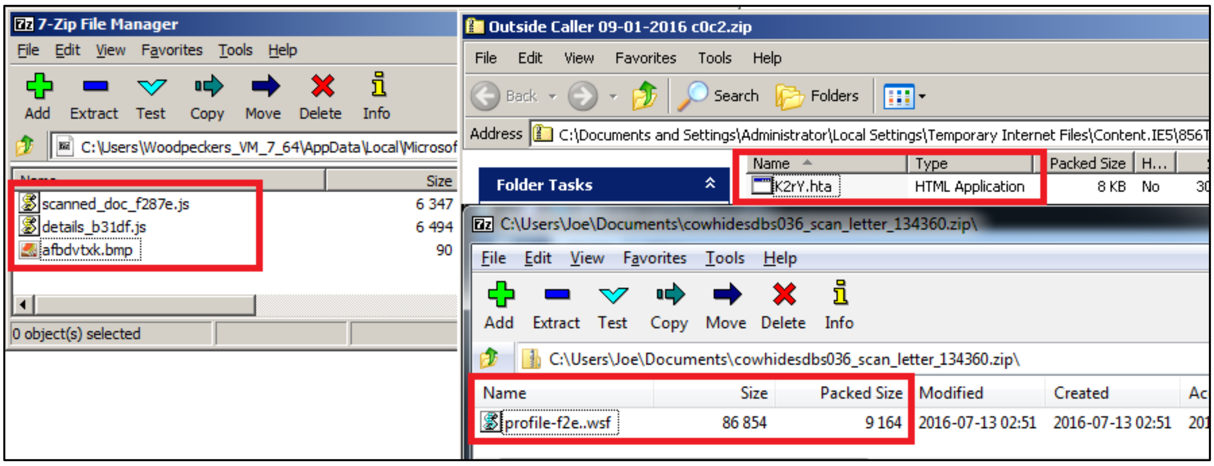
Locky ransomware was first discovered in February 2016. In collusion with the Dridex botnet, infamous for its online banking fraud malware, Locky ransomware was distributed via spam emails with a Word file (.doc) attached to them.



```
|=$-+-=*~_$$
.==$_-||
.|-||+_+__*+$..-*-|
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
   1. http://25z5g623wpqpdwis.tor2web.org/[redacted]
   2. http://25z5g623wpqpdwis.onion.to/[redacted]
   3. http://25z5g623wpqpdwis.onion.cab/[redacted]

If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
   2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: 25z5g623wpqpdwis.onion/[redacted]
   4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted] !!!
$*~*_~+_+*=|+*+*_=
$.$$_
```

Figure 1. Extortion threat message of Locky ransomware

Since March 2016, Locky ransomware has changed its spam email attachment from a Word file (.doc) to a compressed file (.zip) containing an obfuscated JavaScript file. The script file contained in the compressed file also changed repeatedly: from JavaScript (JS) in March, to HTA (HTML Application) in May and later, to WSF (Windows Script File) in July 2016. It is assumed that the creators of the Locky ransomware continuously changed their tactics in order to evade detection by spam filters or other security solutions.


7-Zip File Manager
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
Outside Caller 09-01-2016 c0c2.zip
File Edit View Favorites Tools Help
Back Search Folders
Address
Folder Tasks
Add Extract Test Copy Move Delete Info
0 object(s) selected

C:\Users\Woodpeckers_VM_7_64\AppData\Local\Microsof

Name	Size
scanned_doc_f287e.js	6 347
details_b31df.js	6 494
afbdvtxk.bmp	90

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\856T

Name	Type	Packed Size	H...
K2rY.hta	HTML Application	8 KB	No

C:\Users\Joe\Documents\cowhidesdbs036_scan_letter_134360.zip\

Name	Size	Packed Size	Modified	Created
profile-f2e..wsf	86 854	9 164	2016-07-13 02:51	2016-07-13 02:51

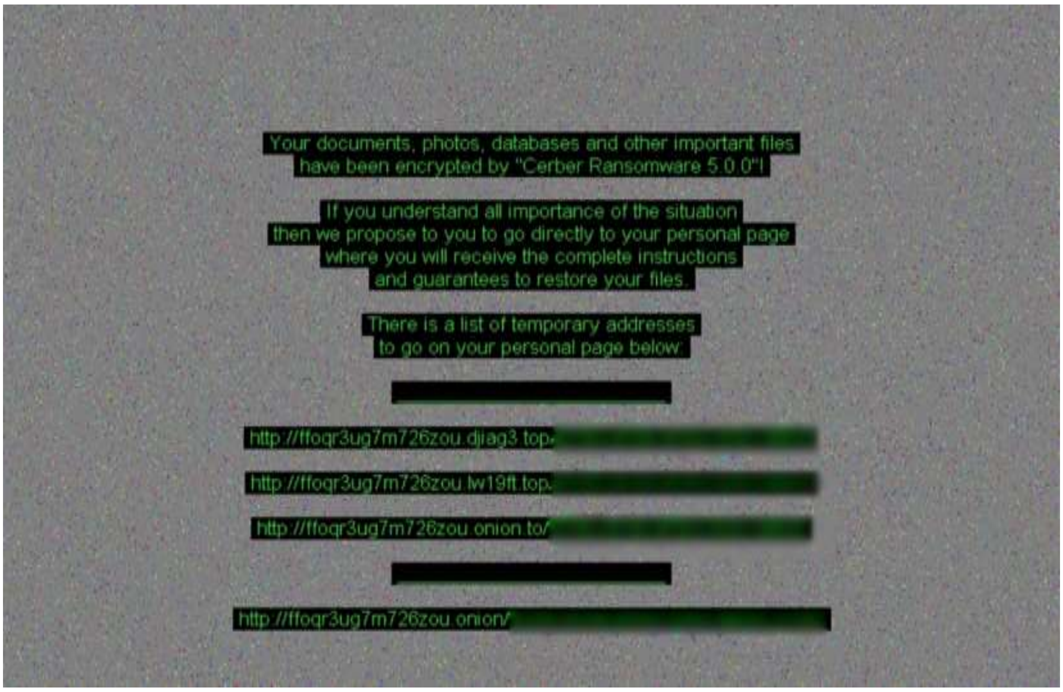
Figure 2. Locky ransomware attachments

There have also been changes in the extensions added to the files that Locky ransomware encrypts. An early version of Locky ransomware added “.locky” to the encrypted files, then switched to the extension “.zepto” in June 2016, and then “.odin” in September. By the end of October, “.shit” and “.thor” extensions were appended. This was followed by “.aesir” and “.zzzzz” at the end of November, and “.osiris” at the beginning of December.

There are a few features that should be noted. The frequency of new Locky variants has increased in the latter half of 2016. Many of the extensions are named after gods from Norse mythology (Odin, Thor, and Aesir) and Egyptian mythology (Osiris), but random names are also used, such as “.shit” and “.zzzzz”. This could indicate that there are at least two groups of Locky ransomware creators.

2. Cerber: ransomware with audio guidance

Once it infects a PC, Cerber ransomware encrypts files and then announces its presence via audio message. It first appeared in March 2016, and then ran rampant in the latter half of 2016. Unlike Locky ransomware, Cerber ransomware variants used to carry version numbers, such as the latest 5.0.1 (as of late 2016). However, the new Christmas decorated version of Cerber no longer had a version number. It is likely that this ransomware will be created and distributed without a version number from now on.



Your documents, photos, databases and other important files
have been encrypted by "Cerber Ransomware 5.0.0"!

If you understand all importance of the situation
then we propose to you to go directly to your personal page
where you will receive the complete instructions
and guarantees to restore your files.

There is a list of temporary addresses
to go on your personal page below:

[redacted]

http://ffoqr3ug7m726zou.djiag3.top[redacted]

http://ffoqr3ug7m726zou.lw19ft.top[redacted]

http://ffoqr3ug7m726zou.onion.to/[redacted]

[redacted]

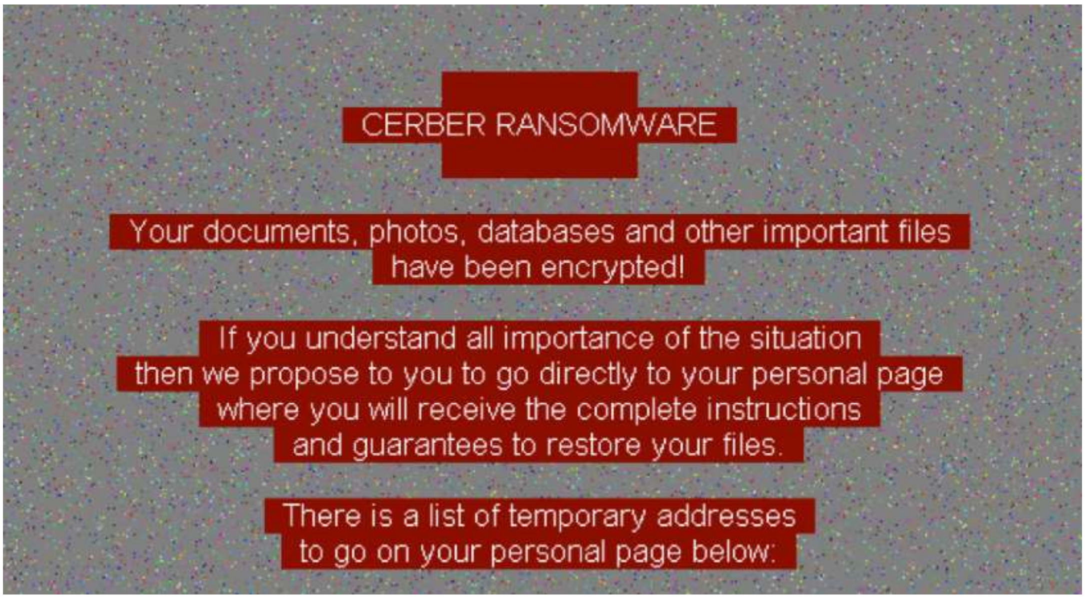
http://ffoqr3ug7m726zou.onion/[redacted]

Figure 3. Extortion threat message: Cerber v5.0

Like Locky ransomware, Cerber is distributed via spam emails or exploit kits. Initially, it was distributed in the form of a Word file, but the latest variants include Word Open XML Macro-Enabled Document (DOCM) file, HTML Application (HTA) and Visual Basic Script (VBS).

Exploit kits (EKs) are used for Web site vulnerability attacks and malvertising attacks. They were used to deliver pharming attacks and distribute online game hacking malware. Cerber versions 1 and 2 were distributed via Nuclear, Angler, and Neutrino exploits kits. When Nuclear and Angler EKs disappeared during the first half of 2016, the third version of Cerber was delivered via RIG and Magnitude EKs. From version 4 onwards, RIG (including RIG-E and RIG-V), Neutrino, and Magnitude EKs were used.

Meanwhile, Cerber creators used malware distribution networks operated by a different group to distribute the ransomware. In addition, Cerber has been sold on the Russian black market ever since the first version.



CERBER RANSOMWARE

Your documents, photos, databases and other important files
have been encrypted!

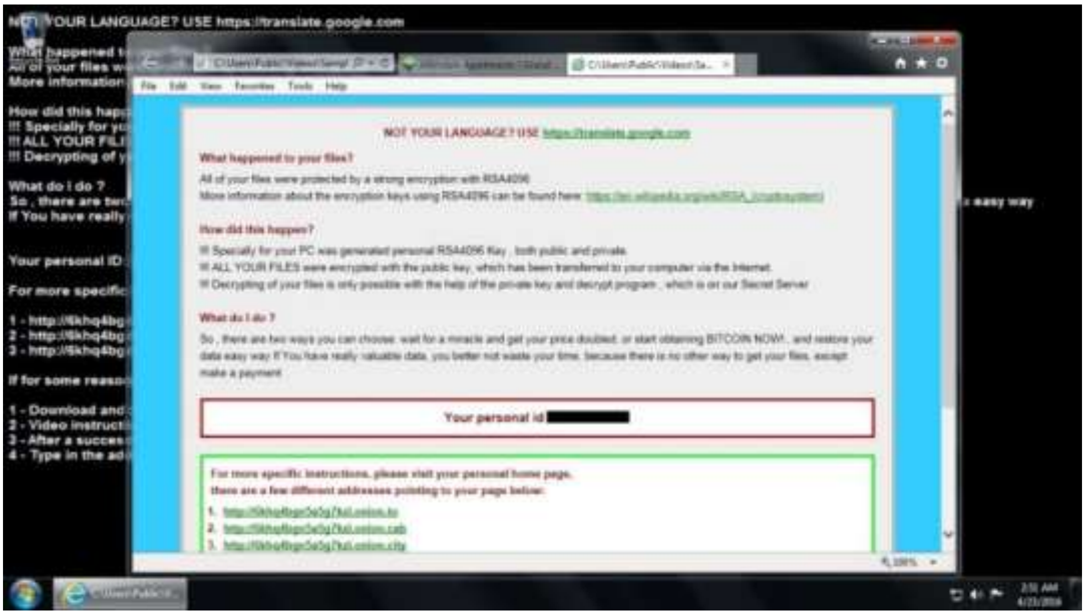
If you understand all importance of the situation
then we propose to you to go directly to your personal page
where you will receive the complete instructions
and guarantees to restore your files.

There is a list of temporary addresses
to go on your personal page below:

Figure 4. Christmas decorated Cerber version

3. CryptXXX: suddenly vanishing ransomware

CryptXXX ransomware was especially notorious in South Korea. In the beginning of June 2016, it infected personal computers via a compromised popular smartphone-related website in the country.



NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files?

All of your files were protected by a strong encryption with RSA4096
More information about the encryption keys using RSA4096 can be found here: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen?

!!! Specially for your PC was generated personal RSA4096 Key , both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?

So , there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment

Your personal id [redacted]

For more specific instructions, please visit your personal home page,
there are a few different addresses pointing to your page below:

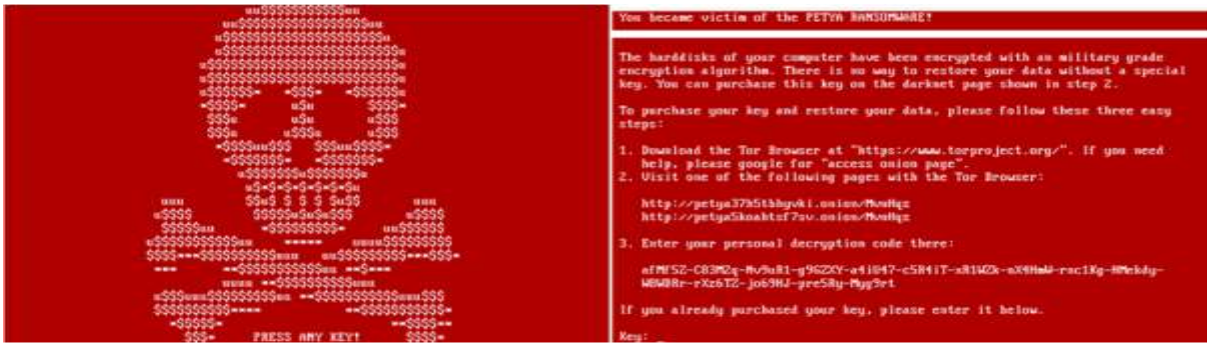
1. http://6khq4bgn5e5g7kul.onion.to
2. http://6khq4bgn5e5g7kul.onion.cab
3. http://6khq4bgn5e5g7kul.onion.city

Figure 5. Extortion threat message: CryptXXX ransomware

CryptXXX ransomware emerged around May 2016 around the time that TeslaCrypt, which had been highly active from the beginning of 2016, suddenly disappeared. However, CryptXXX itself disappeared by the end of July 2016. With the announcement of the end of TeslaCrypt's campaign, the TeslaCrypt ransomware creators made the decryption key public. As of yet, no announcement for CryptXXX's shut down has been made, but the malware has not re-appeared in South Korea, where CryptXXX was more active than Locky and Cerber, for five months. Thus, it does not seem that CryptXXX is in a momentary lull.

4. Types of ransomware that encrypt MBR

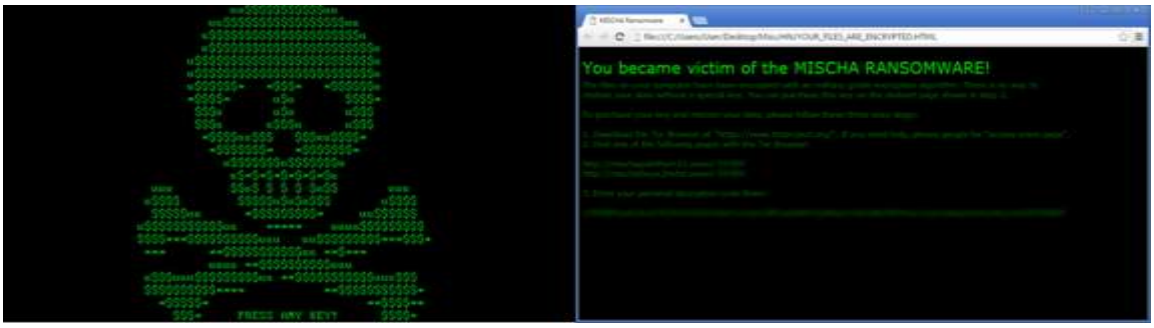
Petya ransomware, which overwrote the Master Boot Record (MBR), was discovered in March of last year. This ransomware replaces the Master Boot Record (MBR) and encrypts the Master File Table on an infected Windows computer's hard drive to prevent victims from booting up. Even if the MBR is manually restored, the MFT is still encrypted, making infected computers inaccessible.



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/MvnHqz
   http://petya5koahtsf7sv.onion/MvnHqz

3. Enter your personal decryption code there:

   afMF5Z-C83M2q-Mv9uR1-g96ZXY-a41047-c5R4iT-xR1WZk-aX4HmW-rac1Kg-HMekdy-
   W8W8Rr-rXz6TZ-jo69HJ-gre5Ry-Myg9rt

If you already purchased your key, please enter it below.

Key:
```

Figure 6. Screenshot of Petya ransomware

Following Petya, Mischa ransomware was discovered in May 2016. Mischa is a somewhat interesting ransomware in that it selectively encrypts the MBR and files. When the MBR is encrypted, it shows an image similar to the Petya ransomware, but on a black background with green text as shown in Figure 7.


PRESS ANY KEY!
MISCHA Ransomware
file:///C:/Users/User/Desktop/Mischa/YOUR_FILES_ARE_ENCRYPTED.HTML

You became victim of the MISCHA RANSOMWARE!

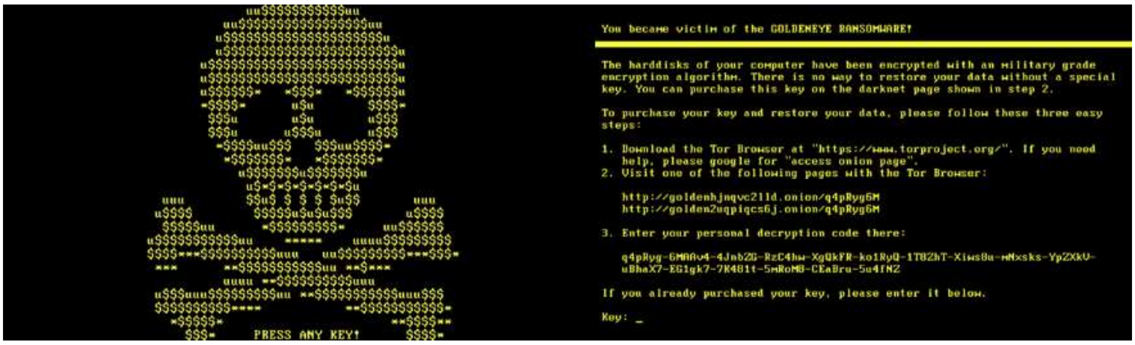
[illegible]

Figure 7. Screenshot of Mischa ransomware

GoldenEye ransomware made its appearance in December 2016, seven months after the emergence of Mischa ransomware. It is the latest version of the Petya ransomware and displays an image similar to that of

Mischa – only the color of the text, which is gold, differs.

Unlike Petya, which only encrypted the MBR, or Mischa, which only encrypted user files of the MBR, GoldenEye encrypts both the MBR and files. It encrypts files first and adds an extension with eight random characters. It then overwrites the MBR to load the ransom note below (see Figure 8).



```
PRESS ANY KEY!
```

```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://goldenhjnqvc211d.onion/q4pRyg6M
   http://golden2uqpiqcs6j.onion/q4pRyg6M

3. Enter your personal decryption code there:

   q4pRyg-6MAAv4-4Jnb2G-RzC4hw-XgQkFR-ko1RyQ-1T8ZhT-Xiws8u-mNxsks-YpZXkV-
   uBhaX7-EG1gk7-7K481t-5mRoM8-CEaBru-5u4fNZ

If you already purchased your key, please enter it below.

Key: _
```

Figure 8. Screenshot of GoldenEye ransomware

All three ransomware – Petya, Mischa, and GoldenEye – were created by Janus Syndicate, a cybercrime syndicate. Janus Syndicate is also the name of a fictional crime syndicate featured in the 1995 James Bond film, *GoldenEye*.

Findings 2: Key changes in ransomware trends

The latest ransomware trends can be summarized by: an expanded range of damage by ransomware; diversification of ransomware distribution; and changes in the aspect of ransomware creation.

1. Expanded range of ransomware damages

Today, ransomware is being discovered simultaneously across the world, regardless of country or region. Particularly, the number of infections by TeslaCrypt, Locky, Cerber, and CryptXXX has been high. There were slight regional differences based on distribution frequency via spam emails or exploit kits and number of PC users, but the ransomware has proliferated over all regions – North America, Europe, and Asia. That is, while ransomware has been dominant in North America and Europe, including Russia, it has extended its territory to Asia, including South Korea, Japan, India, and Taiwan.

In 2016, ransomware damages were reported not only by personal users but also by medical institutions and public organizations. We cannot rule out the possibility of ransomware attacks spreading to various service sectors, including finance and manufacturing in the near future. With ransomware activity gradually expanding, it is highly possible that the scope of damage will expand as well.

2. Diversification of distribution methods

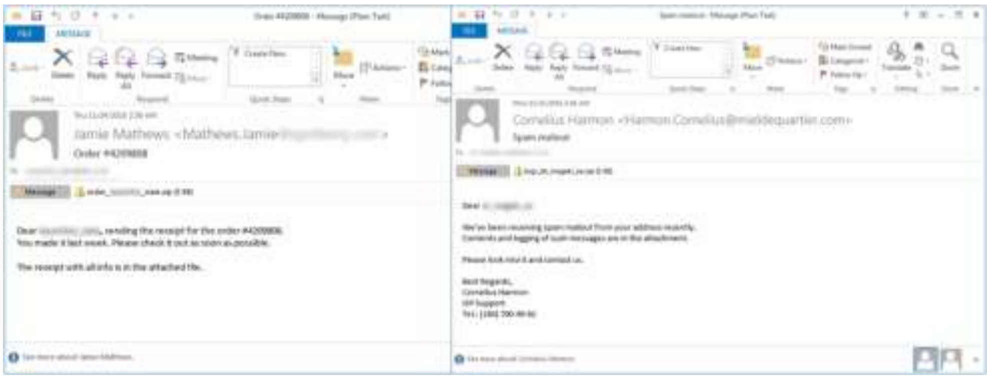
With the methods of ransomware distribution diversifying, the damage is becoming more severe. There are three main distribution methods – spam email, exploit kits, and malvertising.

Distribution Method	Descriptions
Spam email	• Traditional malware distribution technique • Deceives users with email subjects, messages, and attachments to open malicious attachments and contained links.
Exploit Kits (EK)	• Uses web vulnerability and drive-by-download • Effective in infecting a number of random victims • Many active EK groups
Malvertising	• Combined EK and advertisement module • Effective in infecting a number of random victims

[Table 1] Ransomware distribution methods

Spam email, a traditional malware distribution method, is also actively used. Both Locky and Cerber ransomware were distributed via spam emails. Social engineering techniques are also used in spam emails to lure users. They are usually disguised as promotions, prize drawings or purchase-related emails in South Korea, whereas in the US and Europe, they are disguised as invoice, payment or resume related emails.

However, there is a built-in hurdle to ransomware infection via spam emails in that users must manually execute the malicious attachments. With more email security solutions blocking executable attachments, attackers are using encrypted compressed files or obfuscated script files to evade detection by security solutions.



Jamie Mathews <Mathews.Jamie[redacted]>

Order #4209808

order_[redacted]_.zip

Dear [redacted], sending the receipt for the order #4209808.
You made it last week. Please check it out as soon as possible.

The receipt with all info is in the attached file.

Cornelius Harmon <Harmon.Cornelius@middequartier.com>

Spam mailout

Dear [redacted]

We've been receiving spam mailout from your address recently.
Contents and logging of such messages are in the attachment.

Please look into it and contact us.

Best Regards,
Cornelius Harmon
ISP Support
Tel.: (180) 700-49-81

Figure 9. Spam emails that distribute ransomware

Exploit Kits (EK) are required for drive-by-download attacks, a technique that distributes malware via vulnerable websites. When a user visits a compromised website, the ransomware is downloaded and executed without the user’s awareness. This method is effective in attacking a number of random victims, and has been used to distribute online game hacking or pharming malware.

There are three prerequisites for successfully attacking random victims via EK – vulnerable websites with traffic, people who use vulnerable software, and new malware not yet detected by antivirus programs. The prime targets would be structurally vulnerable Internet-based applications or programs that are applied to many websites and used by many users such as Internet Explorer, Flash Player, Java, and Silverlight.

There are many different types of EKs. RIG, RIG-E, Neutrino, and Magnitude are actively used these days. Nuclear EK and Angler EK were terminated in the first half of 2016. Attackers then started using Neutrino and RIG EKs.

As mentioned above, in order to infect as many random victims as possible with drive-by-downloads, the website needs to be vulnerable and have high traffic. However, not many websites meet both of these conditions. To overcome this problem, cybercriminals are using online advertising modules or servers instead of vulnerable websites. Most of the advertisements on popular websites use the advertising agency’s server, and most agencies are usually small and cannot afford to maintain secure servers.

Attackers distribute compromised advertisements with malware via vulnerable advertisement servers. Even if the website is not vulnerable, malware can be downloaded to a user’s computer through advertisements. This technique is so-called “Malvertising”, a portmanteau of "malicious” and “advertising". In the case of malware infection via malvertising, it is difficult to trace the infection path.

In addition, ransomware distribution via Remote Desktop Protocol (RDP) has recently increased. Remote Desktop Protocol (RDP), developed by Microsoft, provides users with a graphical user interface (GUI) to remotely connect to another computer over a network connection. It is usually used for server management or remote connection. In order to execute RDP, information regarding the server administrator or user account is required. The problem is that users as well as administrators usually use very security-weak passwords such as ‘1’, ‘1234’, ‘abcd’, ‘password,’ etc. In some cases, the passwords are shared accounts used with others or owners who do not bother to change the password.

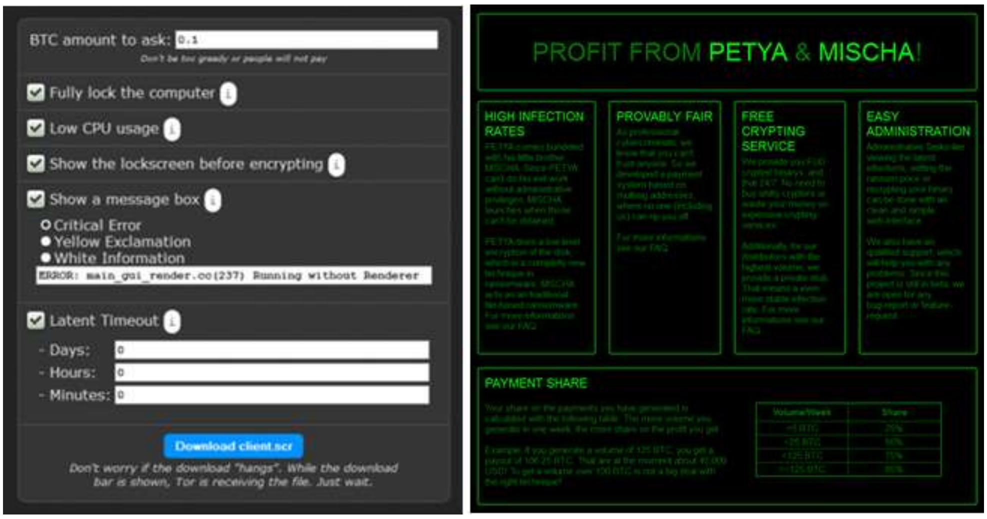
Cybercriminals attempt to login through brute-force attacks, and when they succeed, they copy and run the ransomware file on the system. Ransomware infection using this technique is on the rise, and thus, security experts continue to emphasize the use of strong passwords that are changed on a regular basis.

3. Changes in ransomware creation

To briefly summarize the process of ransomware creation to infection, the attacker creates the ransomware and passes it over to a malware distributor; the group then distributes the ransomware to infect victims’ computers. When the victim pays the ransom, the ransomware creator and distributor divide the earnings.

In the case of some notorious ransomware that have reaped huge profits, some of the money is reinvested into improving the ransomware. The creators either change the infection technique, evade detection by security solutions, expand the encryption scope or enhance the encryption method. They even have a Quality Assurance (QA) process to check for errors. The creators then deliver the enhanced ransomware to the distributor to earn more money, and continue reinvesting to enhance the ransomware's functions. Examples of such ransomware include Cerber, Locky, CryptoLocker, TeslaCrypt, CryptXXX, CTB-Locker, and Cryptowall.

One of the most remarkable trends in ransomware is Ransomware as a Service (RaaS), which enables any potential cyber criminal to purchase and use malware without IT expertise. All that is required is payment of a service charge to an RaaS provider. Buyers then receive a user-friendly panel that gives them simple instructions on how to manage ransomware that even include "product details" such as the number of daily infections, the number of people who have paid the ransom, and the income generated. The RaaS provider receives a certain sum as a commission for their services.



BTC amount to ask: 0.1

Don't be too greedy or people will not pay

☑ Fully lock the computer

☑ Low CPU usage

☑ Show the lockscreen before encrypting

☑ Show a message box

○ Critical Error
● Yellow Exclamation
● White Information

ERROR: main_gui_render.cc(237) Running without Renderer

☑ Latent Timeout

- Days: 0
- Hours: 0
- Minutes: 0

Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.

PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

PROVABLY FAIR

FREE CRYPTING SERVICE

EASY ADMINISTRATION

PAYMENT SHARE

Figure 10. Ransom32 and Mischa

RaaS also provides some advantages to ransomware creators who lack the initial capital to earn money. Locky and Cerber were initially spread via RaaS, as were Ransom32, Petya, Mischa, Stampado, Philadelphia, Shark, and Atom.

There is another recent ransomware trend: open-source ransomware. These are usually published for educational purposes and to raise a user's security awareness. Here are the following types of open-source ransomware: Hidden Tear, EDA2, and Heimdall, Most open-source ransomware has been developed based on Hidden Tear and EDA2. Although open-source ransomware creators give notice about the limits of their usage, criminals illegally exploit these well-intended ransomware, and many of the ransomware found last year were generated from open-source-based ransomware.

Conclusion

Ransomware has started to evolve more quickly and has become more diverse since 2016. In the first half of 2016, ransomware used to encrypt files only, but now it has begun encrypting both the MBR and files. In addition, multiple RaaS have started to increase in the latter half of the year. Attackers also have begun to exploit open-source ransomware that were originally developed for educational purposes.

This rapid increase in ransomware over the past two years is expected to evolve further. There will be more new variants that will not only encrypt the MBR, but also other areas of the system. The infection techniques will become more sophisticated in disabling antivirus programs or bypassing detection by security solutions.

Ransomware, however, is not a new form of malware that suddenly appeared out of nowhere. There is also nothing new about its distribution methods. Drive-by-download attacks via spam emails or exploit kits have existed for many years. In this regard, existing security solutions and following traditional security guidelines are still effective in preventing ransomware infection.

In order to prevent infection via malvertising or drive-by-download attacks using exploit kits, it is important to keep operating systems and programs updated to the latest version. In addition, it is crucial to back up important data on a regular basis to minimize the possibility of damages caused by such attacks.

When it comes to ransomware prevention for corporations, the implementation of centralized security management and control for individual systems in the organization is absolutely critical. Companies must urge employees to follow security guidelines. In addition, it is necessary to deploy multi-layered security systems that detect and respond to malware in both the network and at endpoints. In particular, it is necessary to come up with an effective system for coping with ransomware for the initial victim as well as for preventing lateral proliferation at the endpoint level.

References

1. Locky

1) Locky ransomware, disguised in Word docs, latest from Dridex creators
http://www.scmagazine.com/dridex-actors-likely-behind-vicious-locky-ransomware-strain/article/475420/

2)New Locky version adds the .Zepto Extension to Encrypted Files

https://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/

3) Locky / Zepto Ransomware now being installed from a DLL

https://www.bleepingcomputer.com/news/security/locky-zepto-ransomware-now-being-installed-from-a-dll/

4) Locky Ransomware now uses the .ODIN extension for Encrypted Files

https://www.bleepingcomputer.com/news/security/locky-ransomware-now-uses-the-odin-extension-for-encrypted-files/

5) Locky Ransomware's new .SHIT Extension shows that you can't Polish a Turd

https://www.bleepingcomputer.com/news/security/locky-ransomwares-new-shit-extension-shows-that-you-cant-polish-a-turd/

6) Locky Ransomware switches to THOR Extension after being a Bad Malware

https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-thor-extension-after-being-a-bad-malware/

7) Locky Ransomware now using the Aesir Extension for Encrypted Files

https://www.bleepingcomputer.com/news/security/locky-ransomware-now-using-the-aesir-extension-for-encrypted-files/

8) Locky Ransomware putting us to sleep with the ZZZZZ Extension

https://www.bleepingcomputer.com/news/security/locky-ransomware-putting-us-to-sleep-with-the-zzzzz-extension/

9) Facebook Spam Campaign Spreading Nemucod Downloader and Locky Ransomware

https://www.bleepingcomputer.com/news/security/facebook-spam-campaign-spreading-nemucod-downloader-and-locky-ransomware/

10) Locky Ransomware switches to Egyptian Mythology with the Osiris Extension

https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/

2. CERBER

1) The three heads of the Cerberus-like Cerber ransomware

https://blogs.technet.microsoft.com/mmpc/2016/03/09/the-three-heads-of-the-cerberus-like-cerber-ransomware/

2) Cerber Ransomware – New, But Mature

https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/

3) Cerber Ransomware version 2 Released, Uses .Cerber2 Extension

https://www.bleepingcomputer.com/news/security/cerber-ransomware-version-2-released-uses-cerber2-extension/

4) Cerber Ransomware switches to .CERBER3 Extension for Encrypted Files

https://www.bleepingcomputer.com/news/security/cerber-ransomware-switches-to-cerber3-extension-for-encrypted-files/

5) Cerber Ransomware switches to a Random Extension and Ends Database Processes

https://www.bleepingcomputer.com/news/security/cerber-ransomware-switches-to-a-random-extension-and-ends-database-processes/

6) Cerber Ransomware 4.10 now shows the Version Number in Ransom Notes

https://www.bleepingcomputer.com/news/security/cerber-ransomware-4-10-now-shows-the-version-number-in-ransom-notes/

7) Cerber Ransomware 5.0 Released with a Few Changes

https://www.bleepingcomputer.com/news/security/cerber-ransomware-5-0-released-with-a-few-changes/

8) Cerber Ransomware Spreads via Fake Credit Card Email Reports

https://www.bleepingcomputer.com/news/security/cerber-ransomware-spreads-via-fake-credit-card-email-reports/

3. TeslaCrypt / CryptXXX

1) TeslaCrypt shuts down and Releases Master Decryption Key

https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

2) TeslaCrypt Developers recommend TeslaDecoder to Decrypt Files

https://www.bleepingcomputer.com/news/security/teslacrypt-developers-recommend-tesladecoder-to-decrypt-files/

3) CryptXXX: New Ransomware From the Actors Behind Reveton, Dropping Via Angler

https://www.proofpoint.com/us/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler

4) Decrypted: Kaspersky releases free decryptor for CryptXXX Ransomware

https://www.bleepingcomputer.com/news/security/decrypted-kaspersky-releases-free-decryptor-for-cryptxxx-ransomware/

5) Kaspersky releases updated Decryptor for CryptXXX 2.0

https://www.bleepingcomputer.com/news/security/kaspersky-releases-updated-decryptor-for-cryptxxx-2-0/

6) CryptXXX updated to version 3.0, Decryptors no longer Work

https://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/

7) CryptXXX ransomware again updated, can now encrypt network shared files

https://www.scmagazine.com/cryptxxx-ransomware-again-updated-can-now-encrypt-network-shared-files/article/528252/

8) CryptXXX Ransomware moves from the Crypz extension to a Random One

https://www.bleepingcomputer.com/news/security/cryptxxx-ransomware-moves-from-the-crypz-extension-to-a-random-one/

9) CryptXXX providing free keys for .Crypz and .Cryp1 Versions

https://www.bleepingcomputer.com/news/security/cryptxxx-providing-free-keys-for-crypz-and-cryp1-versions/

10) New CryptXXX changes name to Microsoft Decryptor

https://www.bleepingcomputer.com/news/security/new-cryptxxx-changes-name-to-microsoft-decryptor/

11) CryptXXX Ransomware is now scrambling the filenames of Encrypted Files

https://www.bleepingcomputer.com/news/security/cryptxxx-ransomware-is-now-scrambling-the-filenames-of-encrypted-files/

4. PETYA / Mischa / GoldenEye

1) Petya Ransomware skips the Files and Encrypts your Hard Drive Instead

https://www.bleepingcomputer.com/news/security/petya-ransomware-skips-the-files-and-encrypts-your-hard-drive-instead/

2) Petya Ransomware's Encryption Defeated and Password Generator Released

https://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/

3) Petya is back and with a friend named Mischa Ransomware

https://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/

4) The Petya and Mischa Ransomware are part of a new Affiliate Service

https://www.bleepingcomputer.com/news/security/the-petya-and-mischa-ransomwares-part-of-a-new-affiliate-service/

5) Petya Ransomware Returns with GoldenEye Version, Continuing James Bond Theme

https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/

5. HDDCryptor (Mamba)

1) HDDCryptor Ransomware Overwrites Your MBR Using Open Source Tools

https://www.bleepingcomputer.com/news/security/hddcryptor-ransomware-overwrites-your-mbr-using-open-source-tools/

2) Ransomware Hits San Francisco Public Transit System, Asks for $73,000

https://www.bleepingcomputer.com/news/security/ransomware-hits-san-francisco-public-transit-system-asks-for-73-000/

3) San Francisco SFMTA Denies That Hacker Stole 30GB of Data from Its Servers

https://www.bleepingcomputer.com/news/security/san-francisco-sfmta-denies-that-hacker-stole-30gb-of-data-from-its-servers/

6. RaaS

1) Stampado Ransomware campaign decrypted before it Started

https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/

2) Stampado: Taking Ransomware Scumbaggery to the Next Level

https://www.bleepingcomputer.com/news/security/stampado-taking-ransomware-scumbaggery-to-the-next-level/

3) The Philadelphia Ransomware offers a Mercy Button for Compassionate Criminals

https://www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/

4) The Shark Ransomware Project allows you to create your own Customized Ransomware

https://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/

5) Shark Ransomware Rebrands as Atom for a Fresh Start

https://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/

7. Ransomware delivered via social engineering

1) VindowsLocker Ransomware Mimics Tech Support Scam, Not the Other Way Around

https://www.bleepingcomputer.com/news/security/vindowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/

2) PokemonGo Ransomware installs Backdoor Account and Spreads to other Drives

https://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/

3) New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses

http://blog.trendmicro.com/trendlabs-security-intelligence/new-open-source-ransomwar-based-on-hidden-tear-and-eda2-may-target-businesses/

4) The Donald Trump Ransomware tries to Build Walls around your Files

https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/

8. Ransomware variants

1) Bart Ransomware being Spammed by the same devs behind Locky

https://www.bleepingcomputer.com/news/security/bart-ransomware-being-spammed-by-the-same-devs-behind-locky/

2) Side-by-side comparisons of the CrypMIC and CryptXXX Ransomware Infections

https://www.bleepingcomputer.com/news/security/side-by-side-comparisons-of-the-crypmic-and-cryptxxx-ransomware-infections/

3) MarsJoke Ransomware Mimics CTB-Locker

https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker

4) Polyglot – the fake CTB-locker

https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

5) Hucky Ransomware: A Hungarian Locky Wannabe

https://blog.avast.com/hucky-ransomware-a-hungarian-locky-wannabe

9. Educational ransomware

1) The EduCrypt Ransomware tries to teach you a Lesson

https://www.bleepingcomputer.com/news/security/the-educrypt-ransomware-tries-to-teach-you-a-lesson/

2) New educational ShinoLocker Ransomware Project Released

https://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/

3) Heimdall Open-Source PHP Ransomware Targets Web Servers

https://www.bleepingcomputer.com/news/security/heimdall-open-source-php-ransomware-targets-web-servers/

10. Other ransomware

1) Telecrypt Ransomware Uses Telegram as C&C Server

https://www.bleepingcomputer.com/news/security/telecrypt-ransomware-uses-telegram-as-candc-server/

2) Telecrypt Ransomware Cracked, Free Decryptor Released by Malwarebytes

https://www.bleepingcomputer.com/news/security/telecrypt-ransomware-cracked-free-decryptor-released-by-malwarebytes/

3) New Scheme: Spread Popcorn Time Ransomware, get chance of free Decryption Key

https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

4) This Ransomware Unlocks Your Files For Free If You Infect Others

http://thehackernews.com/2016/12/ransomware-malware.html

5) Popcorn Time ransomware, pay up the ransom or spread it to decrypt the files

http://securityaffairs.co/wordpress/54237/malware/popcorn-time-ransomware.html