RANSOMWARE

Battling A Rapidly Changing And Booming Industry

By : Jaaziel Sam Carlos
Ransomware 101

Ransomware Attacks

Identifying Ransomware

Solution and Prevention
A type of malware which **limits** or **prevents** users from using a system. It forces its victims to pay **ransom** through certain payment methods. There are at least **110** known Ransomware Family today.
The first ransomware was discovered in Russia around 2005. It was detected as PGPCODER.

**OUTSIDE RUSSIA**

During 2012, Ransomware variants spread in countries across Europe. Mostly uses Fake Police Notification.

**CRYPTOLOCKER**

In 2013, CryptoLocker was discovered and the use of military grade encryption and TOR among ransomwares became common.
RANSOMWARE | Ransomware Threat

- DAMAGE POTENTIAL: HIGH
- DISTRIBUTION: LOW
- UPDATE FREQUENCY: HIGH
RANSOMWARE | New Ransomware

2014: 21
2015: 32
2016: 60
RANSOMWARE | New Ransomware

2014: 32
2015: 21
2016: 60
RANSOMWARE | Kinds of Ransomware
ALERT! YOUR COMPUTER HAS BEEN LOCKED

To regain access to your computer enter the key which you can have by paying 500$ in the following account

Enter

RANSOMWARE | Kinds of Ransomware
SPAM MAIL

EXPLOIT KITS
Hey there!

I just found your website, I am very interested in a position or perhaps an internship. I attached my CV for you, please go through it and you will see that I am very qualified. You will not be disappointed, I assure you.

Take care.
A SPAM with a malicious link that redirects to a download site or exploit serve kit
A SPAM with a malicious document which disguises as a CV
A SPAM with a malicious script file which downloads ransomware.
A normal site can redirect to an exploit server kit with the use of "Malvertisement"
The malvertisement will redirect the network traffic to an Exploit Server Kit.
The Exploit Kit will be responsible for checking the system for vulnerability that will be exploited and using it to download the Ransomware.
A Compromised Site is a site which is hacked/stolen by a cybercriminal. This can be used to redirect a user to a Exploit Server Kit.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Angler Exploit Kit</td>
<td>CryptoWall, TeslaCrypt, CryptoLocker</td>
<td>CryptoWall, TeslaCrypt, CryptoLocker,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CryptoXXX</td>
</tr>
<tr>
<td>Neutrino Exploit Kit</td>
<td>CryptoWall, TeslaCrypt</td>
<td>CryptoWall, TeslaCrypt, Cerber, CryptoXXX</td>
</tr>
<tr>
<td>Magnitude Exploit Kit</td>
<td>CryptoWall</td>
<td>CryptoWall, Cerber</td>
</tr>
<tr>
<td>Rig Exploit Kit</td>
<td>CryptoWall, TeslaCrypt</td>
<td>Ransom_GOOPIC</td>
</tr>
<tr>
<td>Nuclear Exploit Kit</td>
<td>CryptoWall, TeslaCrypt, CTB-Locker, Trolodesh</td>
<td>TeslaCrypt, Locky</td>
</tr>
<tr>
<td>Sundown Exploit Kit</td>
<td></td>
<td>CryptoShocker</td>
</tr>
<tr>
<td>Hunter Exploit Kit</td>
<td></td>
<td>Locky</td>
</tr>
<tr>
<td>Fiesta Exploit Kit</td>
<td>TeslaCrypt</td>
<td></td>
</tr>
</tbody>
</table>
Ransomware is downloaded or dropped onto the system.
The Ransomware will connect the C&C to receive a Key and send victim information.
The ransomware will now start searching the system for target file types and directories.
Once the ransomware finds a target it will encrypt the said files.
The ransomware will now display a ransom note that instructs the victim on how to pay the ransom.

We ENCRYPTED your FILES
Pay 1.5 BTC to Unlock your Precious files
WHAT IS ITS IMPACT TO THE VICTIMS?
ALERT! YOUR FILES ARE NOW ENCRYPTED

To regain access to your computer enter the key which you can have by paying 500$ in the following account

Enter

Permanent or temporary lost of important files
Disruption from regular operations

RANSOMWARE | Impact of Ransomware Infection
ALERT! YOUR FILES ARE NOW ENCRYPTED

To regain access to your computer enter the key which you can have by paying 500$ in the following account

Enter

Financial loss when paying the ransom
Average payed ransom by victim

$30M every 100 days collected by CryptoLocker threat actors

A Hospital from L.A. payed a ransom amounting to 17,000$
IDENTIFYING RANSOMWARE
LOCKY’s arrival vector is either through SPAM mail or through Nuclear Exploit Kit.
LOCKY needs an argument to run properly
Encrypts the file name and adds “.locky” or “.zepto”
The ransomnote dropped by Locky has the string “HELP_instructions”

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:

Decryption 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:

If all of these 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: mphdadhc5mrd1ju.onion/342947139CF2DFF7
4. Follow the instructions on the site.

!!! Your personal identification ID: 342947139CF2DFF7 !!!
Latest variants lock the screen after encrypting the files on the system.

Covers legitimate rundll32.exe to its current folder use it to load the malware (some variants rename the rundll32).

RANSOMWARE | CryptXXX
<table>
<thead>
<tr>
<th>Version</th>
<th>File Extension</th>
<th>Loader</th>
<th>Note Filename(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.crypt</td>
<td>none</td>
<td>de_crypt_readme</td>
</tr>
<tr>
<td>2</td>
<td>.crypt</td>
<td>use of svchost.exe</td>
<td>{unique ID}</td>
</tr>
<tr>
<td>3</td>
<td>.crypt</td>
<td>use of svchost.exe</td>
<td>!Recovery_{ID}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>{unique ID}</td>
</tr>
<tr>
<td>3</td>
<td>.cryp1</td>
<td>use of rundll32.exe</td>
<td>!{unique ID}</td>
</tr>
<tr>
<td>3.2</td>
<td>.crypz</td>
<td>use of explorer.exe</td>
<td>!{unique ID}</td>
</tr>
<tr>
<td>3.205</td>
<td>.[Random]</td>
<td>use of rundll32.exe</td>
<td>@{unique ID}</td>
</tr>
</tbody>
</table>
Petya is a type of lockscreen. And is able to encrypt, not the files, but the Master File Table.
Cerber
CERBER’s arrival vector is either through SPAM mail or through Neutrino Exploit Kit.
Encrypts the file name and adds “.cerber” also drops a speaking ransomnote.
CERBER RANSOMWARE

Cannot you find the files you need?
Is the content of the files that you looked for not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Great!!!
You have turned to be a part of a big community #CerberRansomware.

!!! If you are reading this message it means the software !!! "Cerber Ransomware" has been removed from your computer.

*********************************************************
RANSOMWARE
IDENTIFICATION TOOLS
SOLUTION AND PREVENTION
# Ransomware Overview

<table>
<thead>
<tr>
<th>Name</th>
<th>Extensions</th>
<th>Extension Pattern</th>
<th>Ransom Note Filename(s)</th>
<th>Comment</th>
<th>Encryption Algorithm</th>
<th>Also Known as</th>
<th>Decryptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoHasYou</td>
<td>.enc</td>
<td>_timestamp__email__777</td>
<td>read_this_file.txt</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="https://decrypter.crusader.com/">https://decrypter.crusader.com/</a></td>
</tr>
<tr>
<td>7ev2in</td>
<td>.RST</td>
<td>e.g. <em>14-05-2016-11-59-36</em></td>
<td></td>
<td></td>
<td>XOR</td>
<td>7ev2in-HONEST</td>
<td><a href="https://github.com/has">https://github.com/has</a></td>
</tr>
<tr>
<td>.7fr</td>
<td>.7fr</td>
<td>README.TXT</td>
<td>info.txt</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="http://www.bleepingcomputer.com">http://www.bleepingcomputer.com</a></td>
</tr>
<tr>
<td>Black8</td>
<td>.Block3</td>
<td>READ_IT.txt</td>
<td>Based on HiddenTear</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="http://www.bleepingcomputer.com">http://www.bleepingcomputer.com</a></td>
</tr>
<tr>
<td>Alpha Ransomware</td>
<td>.encrypt</td>
<td>Read Me (How Decrypt)!!!.txt</td>
<td></td>
<td></td>
<td>AES(256)</td>
<td>AlphaLocker</td>
<td><a href="http://www.bleepingcomputer.com">http://www.bleepingcomputer.com</a></td>
</tr>
<tr>
<td>Apocalypse</td>
<td>.encrypted</td>
<td>How_To_Decrypt.txt</td>
<td>info.html</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="https://decrypter.crusader.com/">https://decrypter.crusader.com/</a></td>
</tr>
<tr>
<td>AutoLocker</td>
<td>.locky</td>
<td>info.txt</td>
<td>info.html</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="https://decrypter.crusader.com/">https://decrypter.crusader.com/</a></td>
</tr>
<tr>
<td>BadRig</td>
<td>.id[0-9][EMAIL_ADDRESS]</td>
<td>Help Decrypt.html</td>
<td>Files might be partially encrypted</td>
<td>AES(256)</td>
<td></td>
<td>Rakheli</td>
<td><a href="https://decrypter.crusader.com/">https://decrypter.crusader.com/</a></td>
</tr>
<tr>
<td>BitCryptor</td>
<td>.cif</td>
<td>Has a GUI.</td>
<td>CryptoGraphic Locker family. Newer CoinVault variant.</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="http://www.bleepingcomputer.com">http://www.bleepingcomputer.com</a></td>
</tr>
<tr>
<td>BlackShades Crypter</td>
<td>.silent</td>
<td>Hacked_Read_me_to_decrypt_files.html</td>
<td></td>
<td></td>
<td>AES(256)</td>
<td>SilentShade</td>
<td><a href="http://www.bleepingcomputer.com">http://www.bleepingcomputer.com</a></td>
</tr>
<tr>
<td>Bloccato</td>
<td>.blocatto</td>
<td>Based on HiddenTear</td>
<td>EXE was replaced to neutralize threat</td>
<td>AES(256)</td>
<td></td>
<td>Salam!</td>
<td><a href="http://www.bleepingcomputer.com">http://www.bleepingcomputer.com</a></td>
</tr>
<tr>
<td>Boobyah</td>
<td>.locky</td>
<td>MENSAهام.txt</td>
<td>Based on EDA2</td>
<td></td>
<td>AES(256)</td>
<td></td>
<td>Salam!</td>
</tr>
<tr>
<td>Brazilian</td>
<td>.locky</td>
<td>MENSAGEM.txt</td>
<td></td>
<td></td>
<td>AES</td>
<td></td>
<td>Salam!</td>
</tr>
<tr>
<td>BtLock</td>
<td>.btlock</td>
<td>Ransomware.bt</td>
<td></td>
<td></td>
<td>GOST</td>
<td></td>
<td>Salam!</td>
</tr>
<tr>
<td>Bwlock</td>
<td>.btlock</td>
<td>Ransomware.bt</td>
<td></td>
<td></td>
<td>GOST</td>
<td></td>
<td>Salam!</td>
</tr>
</tbody>
</table>

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#
Never open unverified email
Follow the 3-2-1 Rule

Creating Backup

RANSOMWARE | Ransomware Prevention
Update OS & Applications Regularly

[Image of a computer screen with a download icon and text: "Updating Software"]

RANSOMWARE | Ransomware Prevention
Avoid posting your company email online.

We have an opening.

Send your resume to JuanDC@company.com.
THANK YOU