Topics

- What is Ransomware?
- Basic Ransomware Operation
- A Little History
- Ransomware Characteristics
- Actual Compromises
- Some Help With Recovery
- A Plan for Protection
What is Ransomware?

- Windows ransomware, such as Cryptolocker, Cryptowall, Locky, and Samas, does not bother to steal your critical files (Office documents, photos, videos) as it is much easier to just encrypt them in-place and give you a ransom note.
- If the ransom is not paid by its due date, you do not get the decryption key needed to decrypt your files.
- Depending on the variant of Ransomware you’ve been infected with, you may be able to recover your files.

It’s not just Windows:
- Linux.Encoder, which exploits a security vulnerability in the Magneto e-commerce platform.
- OS X KeRanger, distributed through compromised Transmission BitTorrent client.
**Basic Ransomware Operation**

- Infect system via email attachment, Angler exploit kit (0-day Flash exploit), or GameOver Zeus Botnet.
- Contact CnC server to generate / receive encryption key.
- Perform a depth first search of all disk folders (including network drives), encrypting files with targeted extensions using with one of several algorithms, such as RSA, ECC, AES.
- Place ransom notes in all folders where files were encrypted.
- Delete malware when encryption is complete and display final ransom note.
Basic Ransomware Operation

• Depending on which variant of Ransomware a system has been infected with, other activities shown here may also take place:
  • Deletion of Shadow Volume copies:
    – "C:\Windows\SYsWOW64\cmd.exe" /C "C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet
  • Secure deletion of original files after they’ve been encrypted.
  • Malware setup as a scheduled task to run whenever system boots.
  • Encrypt filename extensions and also filenames.

Zcryptor exhibits worm-like spreading behavior by copying itself to external drives.
A Little History

• Cryptolocker arrives in September 2013.
  – Spread via infected email attachments and via the GameOver Zeus botnet until shut down by Operation Tovar.
• CryptorBit / HowDecrypt arrives in December 2013.
• CBT Locker / Critroni arrives in July 2014.
• CryptoWall arrives in September 2014.
  – Followed by CryptoWall 2.0 in October and CryptoWall 3.0 in January 2015.
• CryptoDefense arrives in January 2014.
• TeslaCrypt arrives in February 2015.
  – Files associated with video games also encrypted.
• AlphaCrypt arrives in April 2015.
A Little History

• Chimera arrives in September 2015.
  – First ransomware to contain a doxing threat if ransom is not paid.
• January 2016: Ransom32 appears.
  – First ransomware written in javascript.
  – Organized as SaaS, allows user to craft ransomware to their liking.
A Little History

• Android ransomware debuts in September 2015.
  – Green Dot MoneyPak, Ukash, PaySafeCard used to pay fines.

• Koler ransomware.
  – Distributed via fake applications, such as BaDoink and PhotoViewer, and SMS messages with malicious links.

• FBI ransomware.
  – Distributed via PornDroid application.

• Reboot Android device into Safe Mode and delete malicious app.
Ransomware Characteristics

- File types that are targeted for encryption can include the following:

```
.7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .sc2save, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .b kp, .qic, .b kf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .h plg, .hkdb, .mdb backup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mcgame, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .001, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpgge, .kdb, .db0, .DayZProfile, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, .unity3d, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, . pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rw1, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbfv, .m df, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsx, .xls, .ods, .odt
```
Ransomware Characteristics
Ransomware Characteristics

All your documents, photos, databases and other important files have been encrypted with strongest encryption RSA-2048 key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main encryptor red window, examine it and follow the instructions. Otherwise, it seems that you or your antivirus deleted the encryptor program. Now you have the last chance to decrypt your files.

Open in your browser one of the links:
http://is6xosotjdy4qtgur.afnwdsy4j32.com
http://is6xosotjdy4qtgur.9isernvur33.com
https://is6xosotjdy4qtgur.tor2web.blutmagie.de

They are public gates to the secret server.
Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
12kpdMak91BF5PKr1NdUNyi42froMwa8tB

Follow the instructions on the server.

If you have problems with gates, use direct connection:
1. Download Tor Browser from http://torproject.org
2. In the Tor Browser open the http://is6xosotjdy4qtgur.onion/
   Note that this server is available via Tor Browser only.
   Retry in 1 hour if site is not reachable.
Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
12kpdMak91BF5PKr1NdUNyi42froMwa8tB

Follow the instructions on the server.
Ransomware Characteristics
Ransomware Characteristics

- If the ransomware is allowed to finish encrypting files, it deletes itself. Since it was discovered relatively quickly, it still existed on disk:
Knowing the specific variant of ransomware may assist with file recovery.
Actual Compromises

• Company A: Health Care provider
  – Employee computer infected via email attachment.
  – No malware scanning on Exchange server or employee computer.
  – Files on computer and all company network shares mapped to the employee computer were encrypted.
  – Company used Carbonite for real-time backup.
  – All Carbonite files were replaced with (new) encrypted versions.
  – IT staff located offending email on Exchange server and deleted it.
  – The company paid the Bitcoin ransom.
Actual Compromises

- **Company B: Educational Institution**
  - Remote employee laptop infected via personal email attachment.
  - Files on laptop were encrypted. College policy dictates no files are stored locally…. But this policy was not fully complied with.
  - Husband of employee was security savvy and disconnected computer from VPN connection. This was a *good thing*!
  - A limited number of files on the schools network shares mapped to the employee computer were encrypted.
  - Spread was limited due to proper permissions in effect.
  - The company reimaged the laptop and restored other encrypted files from a current backup.
  - Endpoint protection did not stop the malware.
Actual Compromises

• Company C: Town Police
  – Administrative assistant’s computer infected via email attachment.
  – Files on computer and department file server were encrypted.
  – Files were restored from a recent backup.
  – An IT security audit was suggested but not performed due to budget concerns.
  – Three months later the same employee infected her computer a second time.
  – Many encrypted files were lost due to a failed hardware backup process.
State Court <adrian.pierson> 4:02 AM (3 hours ago)

Be careful with this message. It might contain a virus or a malicious link. Learn more

Dear Anton,

This is to inform you to appear in the Court on the April 20 for your case hearing. Please, prepare all the documents relating to the case and bring them to Court on the specified date. Note: If you do not come, the case will be heard in your absence.

The copy of Court Notice is attached to this email.

Regards,
Adrian Pierson,
Court Secretary.
Do you see any patterns at work here that would help you begin deobfuscating this sample?
Some Help With Recovery

This turned out to be a Trojan downloader and installer for TeslaCrypt. One payoff for analyzing the file is the list of all Registry keys and file locations that are utilized in the infection.
Some Help with Recovery

• Be aware that others have already suffered through ransomware attacks and some tools are available.
  
  • [https://decryptcryptolocker.com/](https://decryptcryptolocker.com/) provides relief for Cryptolocker victims.
Some Help with Recovery

- Varonis provides instructions on detecting and cleaning Cryptolocker infections.

- Bleeping Computer provides the ListCwall tool that will scan the Windows Registry for the Cryptowall key that contains the list of encrypted files. This is helpful for finding out what files were encrypted prior to recovery from backup.
Some Help with Recovery
Some Help with Recovery

- For TeslaCrypt visit [http://blogs.cisco.com/security/talos/teslacrypt](http://blogs.cisco.com/security/talos/teslacrypt) for information about what the ransomware does and access to a decryption tool to recover encrypted ECC files.

- AlphaCrypt is a variant of TeslaCrypt, but the Cisco decrypting tool does not work for its EZZ files. However, Bleeping Computer has a decrypting tool that works for ECC and EZZ files, located here: [http://www.bleepingcomputer.com/forums/t/574900/teslacrypt-ransomware-changes-its-name-to-alpha-crypt/page-4](http://www.bleepingcomputer.com/forums/t/574900/teslacrypt-ransomware-changes-its-name-to-alpha-crypt/page-4)

Some Help with Recovery

This version of Tesla/AlphaCrypt decryptor can decrypt files only when decryption key is still present in a data file or Tesla/AlphaCrypt’s registry key. Data file can be manually selected if you are trying to decrypt files on different computer.

Trying to load data from windows registry...
ERROR - Registry entry not found or incorrect.

Trying to load data file from disk...
ERROR - Data file not found.

*** You can load data file manually by clicking on Load data file button. ***

Loading data file from >> I:\key.dat
Data file version 4 recognized.
Decryption key found >>
122CC20E7EC2A0412E446DFDEA4C76D9C13EFD08E52E84232383654F0EF93C

Load data file
Save data file
Decrypt Folder
Decrypt All
Close

*** You can try to decrypt your files now. ***

*** It is highly recommended to copy few encrypted files into a new folder and try to decrypt this folder by clicking on button Decrypt Folder. ***

Decrypting files in folder: I:\
Please wait...
Decryption finished. (3 files decrypted, 0 files skipped)
See log file for more information: C:/Users/jantonak/Downloads/TeslaDecoder\TeslaDecoder.log.txt

Load data file
Save data file
Decrypt Folder
Decrypt All
Close

Trustwave SpiderLabs
Some Help with Recovery

• Here are the original and decrypted versions of some sample files from an AlphaCrypt infection:
A Plan for Protection

• Helping prevent future ransomware infections requires a combination of several things:
  – Maintain multiple current backups.
  – Proper (and limited, ie: mostly Read-only) access permissions.
  – Use Firewall, IDS / IPS, and anti-virus to assist with real-time detection and mitigation.
  – Have an Incident Response team in place, ready to quickly respond to an infection.
  – Disable synching on Internet-based file storage.
  – Ongoing security awareness training.
  – Employ Software Restriction Policies.
  – Block access to TOR network.
  – Maintain up-to-date patches.
A Plan for Protection

• Additional suggestions:
  – Check for Shadow Volume copies.
  – Read the blog post located here, which provides interesting insight into the network communications employed by Ransomware and how server event logging may be used to detect an infection:
    • https://blog.logrhythm.com/tags/cryptolocker/
  – Keep looking for tools provided by others.

Should you pay the ransom? That is a personal or business decision. Experts, including the FBI, say No. Also, paying the ransom does not guarantee you’ll be able to decrypt your files.
Thank You and Questions?

Thank you all for attending!

James L. Antonakos
SpiderLabs Incident Response Consultant
jantonakos@trustwave.com