Analysis of the TeslaCrypt Family

and How to Protect Against Future Ransomware/Cyber Attacks

Sophia Wang

COMP 116 F17
Final Project

What is ransomware?

- It is a subgroup of malware
- Infects a machine through compromised websites, email phishing, drive-by downloads, and vulnerability exploitations
- 2 types:
  - Encrypt, obfuscates, and denies users access from their files
  - Locks users out of their systems
- Uses highly complex encryption key to encrypt and obfuscate user's files
- Any device is susceptible to a ransomware attack
- Extremely damaging and can lead to the loss of important files, data, memories, money, jobs, etc.

What are the steps of a ransomware attack?

1. Deployment
2. Installment
3. Command-and-control
4. Destruction
5. Extortion

Step 1: Deployment

- The components of the malicious software infect the system
- Methods:
    - Strategic web compromise: multiple drive-by downloads, this method is employed mostly when a specific victim is targeted, aka watering-hole attacks
    - Drive-by downloads: when a victim downloads a piece of malicious software without their knowledge of the malicious contents
    - Phishing emails: the email has misleading links or attachments to deceive the victim into clicking/downloading them, usually untargeted
    - Vulnerability exploitation: the ransomware scans internet in search for vulnerabilities to exploit
    - Exploit kits: legitimate (or illegitimate) websites are hacked to redirect user to the cyber criminal’s server that hosts the exploit kit, the exploit kit can identify vulnerabilities on a machine and exploit them

Step 2: Installment

- Once the payload has been dropped into the system — infection ensues
- The executables from the malicious payload receive commands to download the ransomware itself
- Ransomware installs itself into the system
- Ensures the malicious code is run every time the machine starts up
- Method:
    - Download dropper methodology: small pieces of code are delivered at a time to avoid detection and then reconstructed

Step 3: Command-and-control (C&C)

- The malicious software connects the machine back to the cyber criminal’s C&C server
- Information about the machine (IP address, geographical location, permissions of the account, operating system details) is sent back to the C&C server
- With the information now in the cyber criminal’s hands, additional attacks may be launched
- The C&C server then proceeds to send the encryption key to encrypt the files on the machine

Step 4: Destruction

- The ransomware has received the encryption key
- Encryption of files begin
  - First local files
  - Followed by files from any removable devices (USB, external hard drive)
  - Finally mappable network locations
- Takes any amount of time ranging from hours to days to fully encrypt
- Ransom note is created and dropped into every directory containing encrypted files
- Desktop background is changed to display the ransom note
- Then the ransomware destroys itself to avoid any security companies getting ahold of and analyzing the software

Step 5: Extortion

- The ransom note demands payment from victim for the decryption key
- Victim is provided with a web address/download link to Tor server to provide their payment
- Most ransomware demands payment in the form of cryptocurrency (Bitcoin, prepaid vouchers, Litecoin, Zcash, etc.)
- Some threaten to completely wipe out files if victim does not provide the payment within x number of days
- Ransom amount varies from a couple hundred dollars to over $1,000

Why is ransomware relevant?

- Cybercrime is the greatest threat to corporations today
- Ransomware accounts for the majority of cyber security attacks
- In the first three months of 2016 alone ransomware extorted $209 million from victims
- More and more ransomware variants are released everyday — so the chances of any individual being attacked by ransomware is increasing
- The ransom sums are also increasing — the average demand is now over $1,000
- Just a small amount of reconnaissance of the victim and exposure to vulnerabilities of a system is required for a ransomware attack

Examples

- WannaCry (May 2017)
  - $300 ransom, doubled every three days
  - Claims to delete files if no payment after seven days
  - Spread to over 150 countries in just 5 days
  - Exploits vulnerabilities of unpatched Windows systems
  - Great negative impact on the healthcare industry
  - Extorted approximately $41,000 from its victims throughout its lifetime
- GoldenEye (June 2017)
  - $300 ransom
  - Encrypts entire hard drive and locks user out of system completely
  - Started in Ukraine
  - Attacked the national bank, state power company, and Kiev’s largest airport
  - Uses EternalBlue exploit kit — exploit vulnerabilities found in the Server Message Block protocol

What is TeslaCrypt?

- Introduced in February of 2015
- Trojan ransomware
- Targeted online gamers, but affected many businesses and average individuals as well
- Ransomware encrypted common file formats and mostly game files (save files, configurations, Steam accounts, game softwares, etc.)
- Asked for an average of 2.5 bitcoins (~$550)
- Garnered $76,522 from victims in less than the first four months of its release
- Demanded a ransom ranging from $250 to $1,000
- Payment in bitcoins or through paypal (which required the full payment of $1,000)

Associated CVEs

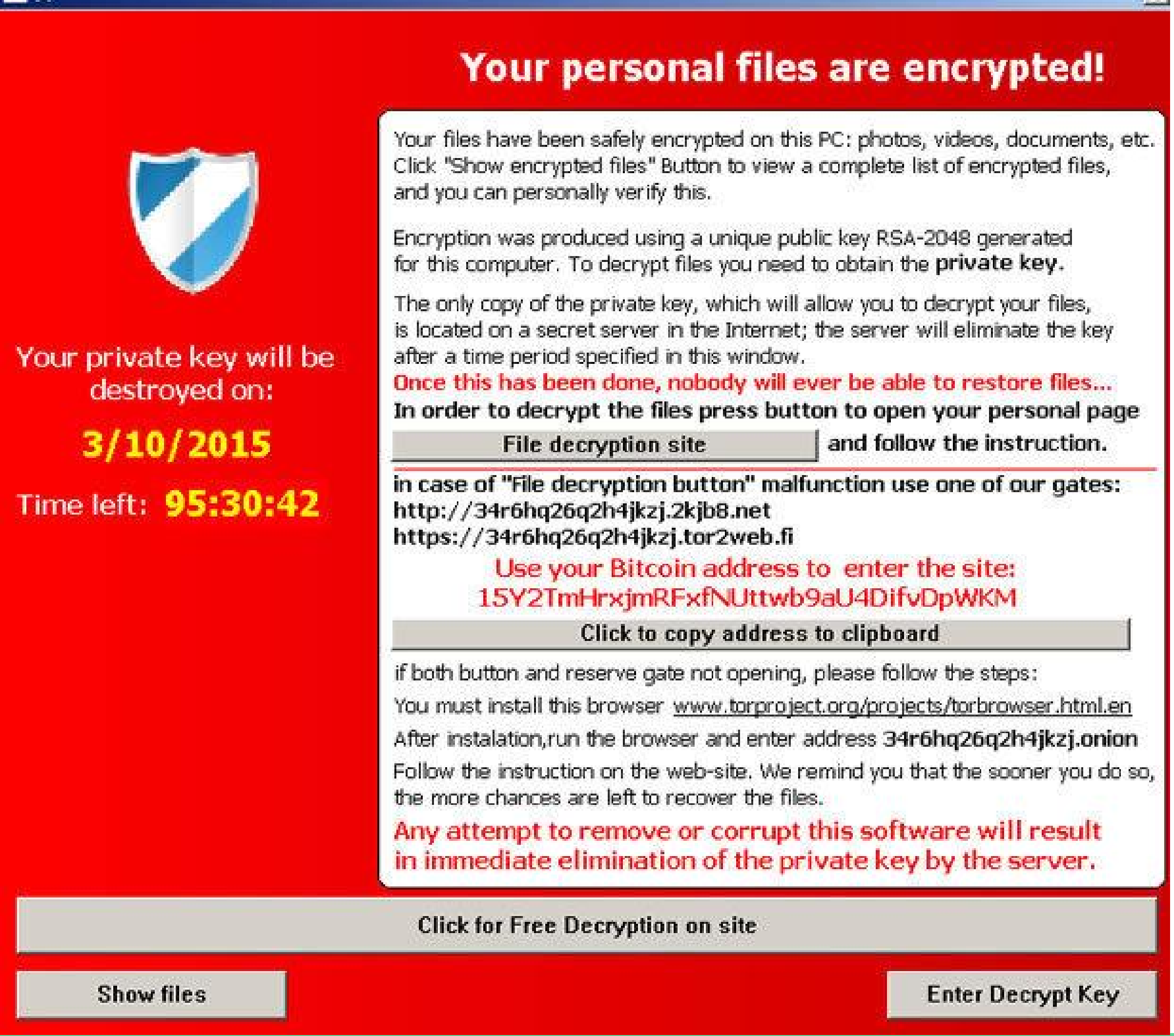
- CVE-2015-0311: Unspecified vulnerability in Adobe Flash Player
- CVE-2013-2551: Use-after-free vulnerability in Microsoft Internet Explorer 6
- CVE-2016-0034: Vulnerability of Microsoft Silverlight 5
- CVE-2014-6332: Vulnerability in Microsoft Windows Servers allows remote attackers to execute arbitrary code via crafted web site
- CVE-2015-8651: Integer overflow in Adobe Flash Player

How does TeslaCrypt work?

- Spread through spam, phishing emails, malicious links, compromised websites
- Enacted through the Angler exploit kit
  - Masks the infection from detection from most antivirus tools
  - Adds infected machine to botnet
  - Sends back information about machine to C&C server
  - Exploits vulnerabilities of applications and plugins such as the Flash clip, Silverlight, VBScript, Internet Explorer
  - Drops TeslaCrypt payload into machine
- Executable file from malicious payload which contains TeslaCrypt’s main component is written to memory

How does TeslaCrypt Work? (con.)

- Once system infected, all drives scanned for files
- Common file types and files associated with gaming are encrypted using the AES-256 encryption algorithm
- The ransom message is dropped into all directories with encrypted files
- Once encrypted, the ransom message replaces the desktop background, alerting victims of the infection
- Ransom message provides victim with the link to TeslaCrypt server or a link to download the Tor server to reach the ransom payment site
- Victim was offered 1 free file decrypted to show that their files were still existing and decryptable



Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page

File decryption site **and follow the instruction.**

in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.2kjb8.net
https://34r6hq26q2h4jkzj.tor2web.fi

Use your Bitcoin address to enter the site:
15Y2TmHrxjmRFxfNUttwb9aU4DifvDpWKM

if both button and reserve gate not opening, please follow the steps:

You must install this browser www.torproject.org/projects/torbrowser.html.en

After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**

Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Your private key will be destroyed on:

3/10/2015

Time left: 95:30:42

Click to copy address to clipboard
Click for Free Decryption on site
Show files
Enter Decrypt Key

What the Ransom Message Looks Like

Who did TeslaCrypt affect?

- From February 7, 2015 to April 28, 2015:
    - A total of 1,231 victims visited the TeslaCrypt page to attempt to decrypt a file
    - 139 individuals paid 0.5 to 2.5 bitcoins
    - 20 individuals paid the full $1,000
- Specifically targeted online gamers
- Gamers were estimated to spend approximately $111 billion in 2015 — so the attacker's chose their victim intelligently
- Some targeted games: Call of Duty, Star Craft 2, Diablo, Minecraft, Skyrim, Star Wars: The Knights Of the Old Republic, Metro 2033, WarCraft 3, Resident Evil 4, Assassin's Creed, World of Warcraft, League of Legends, EA Sports games, etc.

  —> the point is A LOT of games, regardless of popularity, were affected

How did it all end?

- The beginning of 2016 a researcher at ESET noticed that TeslaCrypt activity was dwindling — the developers were slowly starting to shut down the project
- May of 2016 the researcher reached out to ask the group behind TeslaCrypt if they would be willing to release the master decryption key — they agreed
- With the release of the master decryption key many security companies created decryption softwares
- Victims who did not pay the ransom were then able to regain access to their files
- TeslaCrypt did end on a comewhat positive note...but we still need to remain vigilant!

Defenses

- Keep software/firmware updated
- Apply necessary patches
- Use spam filters
- Use adblock
- Have latest antivirus software installed
- Do not click on any links from an unknown source
- Do not download anything from an unknown source
- Restrict administrative rights
- Block connections to I2P and Tor servers via a firewall
- Regularly backup all files and systems

Defenses (con.)

- Sandboxing — scan files before opening them, the technique in which files from email attachments or any web downloads are opened and run in a virtual environment first and checked for suspicious behavior, only once file is cleared is it released to the user
- Keep full backups of your files as well as your system
  - Keep these backups disconnected from your machine, as viruses can spread to external memory as well
  - Keep these backups unmappable from your server since viruses can propagate through networks and servers
- Have a plan if your machine/company does get hit!

Defenses (con.)

- If the precautionary steps were not enough and you get infected anyway…
  - If the infected machine is part of a network, remove the machine from the network and disconnect from wifi right away — the virus may spread to more machines otherwise
  - Do not shut down machine, as our data may just all be lost
  - Decide whether or not you want to pay the ransom
    - This decision is based on your own values: significance of data in the files, backup availability, financial situation, any other personal risks
  - If it was a company that is infected, be wary of how the situation is handled — if company decides to pay ransom and the incident is publicized, the company may become a target for other cyber criminals as they will seem “easy” to probe money from
  - Try to compromise with the attacking group — most cyber criminals prefer to receive some money over no money
- Spread awareness of proper cyber hygiene and how prevalent and harmful infections can be if they are not careful on the internet

The future of cyber warfare

- As we move into a world filled with more technology and we increase our dependence on technology, our risks of being attacked also increase
- More and better malicious softwares are developed everyday
- Currently a company is hit with a ransomware attack once every 40 seconds — this rate is only going up
- With the cyber criminals becoming more creative and the technology becoming more devious and advanced, we as users of technology need to learn, enact, and spread the proper defenses to fight back

Call to action!

- Educate your co-workers! Educate your friends, family, classmates, professors…everyone and anyone who uses the internet!
- Nobody is immune to being infected
- The top threat for corporations as of now is cybercrime
- CSO predicts that in just 5 years cybercrime will need to become the greatest concern for every individual, thing, and place
- It is estimated that the global loss from ransomware alone will exceed $5 billion in 2017 — 15 times that of 2015
- The world of cybercrime is only growing, which is why we need to educate ourselves and others and properly defend against these malicious attackers

Works Cited

Common Vulnerabilities and Exposures: The Standard for Information Security Vulnerability Names. (n.d.). Retrieved December 4, 2017.

Donaldson, S. (2017, May 19). WannaCry Ransomware: Who It Affected and Why It Matters [Web log post].

How do I clean a TeslaCrypt infection using the ESET TeslaCrypt decrypter? (2016, May 26).

Koller, S. (2016, May 27). TeslaCrypt Ransomware Developers Retire, Release Master Decryption Key. Mondaq Business Briefing, p. Mondaq Business Briefing, May 27, 2016.

Liska, A., & Gallo, T. (2016). Introduction to Ransomware. In *Ransomware*. O'Reilly Media, Inc.

Lord, N. (2017, July 27). Ransomware Protection & Removal: How Businesses Can Best Defend Against Ransomware Attacks [Web log post].

Massive GoldenEye ransomware attack affects users worldwide [Web log post]. (2017, June 27).

Morgan, S. (2017, October 19). Top 5 cybersecurity facts, figures and statistics for 2017.

Pande, R., & Malik, A. (2016, June 6). Angler Exploit Kit Evading EMET.

Ransomware: How an attack works. (2016, August 18).

Sidharth Shekhar. (2016). Burrp Compromised to Deliver TeslaCrypt Ransomware. *PC Quest,* PC Quest, March 16, 2016.

Skuratovich, S. (2016). *Looking Into TeslaCrypt V3.0.1* (Rep.).

Sophos News — The current state of ransomware: TeslaCrypt. (2016, June 1).

Stevenson, A. (2015, May 27). Hackers using Angler exploit kit to spread TeslaCrypt ransomware. *V3.co.uk*, p. V3.co.uk, May 27, 2015.

Storm, D. (2015, March 16). Gamers targeted by TeslaCrypt ransomware: $1,000 to decrypt games, mods, Steam [Web log post].

Zorabedian, J. (2015, March 16). TeslaCrypt ransomware attacks gamers – “all your files are belong to us!”.