Malware 101

Introduction to ransomware and how to protect your organization against these emerging threats

UCCSC 2016
July 11th 2016
David Lam
IT Security
UC Davis Medical Center
davlam@ucdavis.edu
Why should we care?

• Hospitals are easy targets for attackers.
  • Many hospitals are already in the headlines for its association with ransomware: Hollywood Presbyterian, Kansas Heart, MedStar Health.

• Ransomware can bring down critical assets and systems.

• Ransomware is a business – Criminals collected over $209 million in the first three months of 2016 - FBI
What is Ransomware?

**ransomware**

'ransəmˌwe(ə)r/

*noun*

- a type of malicious software designed to block access to a computer system until a sum of money is paid.

- Google
Types of Ransomware

- Non-Encrypting Ransomware / Trojans / Hoaxes
- Encrypting Ransomware (common ransomware)
- Web-based Ransomware
Non-Encrypting Ransomware / Trojans / Hoaxes

• Arrives through the user’s inbox, web browser, or other telecommunications means.
• Threatens the user that adverse action would be taken against them or their account(s).
• Does not encrypt files, but demands financial information or a ransom to resolve adverse action.
“Police” Ransomware

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America (Article 1, Section 8, Clause B; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your MoneyPak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.
Deadly Consequences of Ransomware

Joseph Edwards, 17

• Suffered from Autism
• Received an email from Cheshire police demanding a ransom of £100 or face prosecution due to extreme pornography, breach of copyright, and terrorism.
• Hanged himself in his own home after receiving false email
Encrypting Ransomware (common ransomware)

- Encrypting ransomware returned back to prominence with the introduction of *CryptoLocker* in 2013.
- Many different variants and strains released since that time.
- Many infection vectors, including malvertising, drive-by download, exploit-kits, email, server vulnerabilities, etc.
Malvertising Vector

• Most websites on the Internet use one or more advertising networks to deliver advertising to its visitors.
• Smaller advertising networks may not have proper security in place to thwart targeted attacks.
• Infected ad networks distribute malicious content on well known sites such as CBS or Blogger.
Drive-by Downloads

- Generally advises user that they need an update to their system, or that their system is infected and requires immediate attention.
- Delivers many classes of malware, including ransomware.
- Malvertising threat actors can redirect visitors to malicious downloads on legitimate sites, increasing the chances of successful execution.
Exploit-Kit Vectors

- Highly specialized malware targets browser add-ons and their vulnerabilities.
- Many variants are highly polymorphic and employs sophisticated encryption / obfuscation techniques to evade detection by various security technologies.
- Examples: *Angler EK, Neutrino EK, RIG EK*.
- Serves as a conduit for malicious software to be installed on the victim’s computer.
Email Vector

- Uses deception in order to get the user to open an attachment or a link inside the email.
- Emails regarding tax forms, voicemails, and pending packages are very common.
- Emails can be targeted to the organization (e.g. healthcare forms, HR related activities, etc)
- Some types of ransomware specializes in email delivery (e.g. Locky)
Server Vulnerabilities Vectors

• Unlike other user initiated attack vectors, this vector is initiated by the attacker themselves.

• The vulnerable application is exploited over the Internet and ransomware is deployed on the affected servers.

• Infection may spread across the network using stolen credentials (e.g. SamSam).
Web-Based Ransomware

- Targets the website itself rather than the client machine / device.
- Generally targets out of date content management systems such as Drupal or Wordpress.
- Requires payment to unlock the content of the site.
- Less common than exploit-kit variants.
Web-Based Ransomware (EK Variant)

• No apparent signs of infection on the website.
• Infection can be difficult to locate once infected.
• Redirects visitors to exploit-kit landing pages in the background.
• Frequently occurs on publicly facing CMS sites that are not actively managed and updated.
What should we do?
Pay the Ransom?

- My answer: Never pay the ransom!
- Encourages the creation of more sophisticated variants and targeted attacks.
- Paying the ransomware does not guarantee decryption, as Kansas Heart Hospital has experienced.
  - You may become a repeat target for paying the ransom.
- Prevention is key!
Backups, backups, backups!

- Should be part of the business continuity plan (BCP).
- Do backups right!
  - Make sure all critical data is backed up and tested.
  - Backup targets shall not be directly accessible to the device (i.e. offline / air-gapped).
  - Versioning is important to prevent encrypted files from overwriting originals.
- Backup encrypted files before restoration if backups are not available.
Securing the human

• Users are generally the weakest link in the chain.
• User education can reduce the incidence of malware in the enterprise
  • Recognizing suspicious emails or links
  • Be cautious of opening attachments or providing information over email
  • Promptly reporting incidents to the enterprise security team
Securing the endpoint

• Limiting administrative access can improve odds of recovery via Volume Shadow Service (VSS).
• Group Policies can limit ransomware execution by targeting blocking executions in uncommon directories.
• Consider heuristics and specialized tools: Specialized anti-exploit and ransomware applications available (e.g. Malwarebytes Anti-Exploit / Anti-Ransomware)
• Endpoint agents such as Carbon Black or FireEye HX could provide insights to scope of ransomware infection and potentially block exploits on-the-fly.
Securing the network

• An up to date UTM / IP(D)S could provide some coverage for ransomware and exploit-kit attacks.
• Due to the polymorphic nature of many exploit kit vectors, not all vendors provide the same level of coverage (some vendors are not equipped to deal with these threats at all).
• Assume worst case scenarios – focus on detection as well as prevention.
Test, test, test...

• The best way to test your security defenses is by testing it against actual threats.

• Replaying traffic against IP(D)S systems can gauge effectiveness of protection.
  • *Proofpoint Emerging Threats* filters can be used to complement existing detection mechanisms.

• Malware blog sites can provide updates to the latest malware trends and/or actual samples for testing purposes.
  • *Malware Traffic Analysis*
  • *Malware Don’t Need Coffee*
Securing the enterprise / infrastructure

• Know your systems! Have an inventory of all of your critical assets.
• Know your risks! Do you have a Business Impact Analysis (BIA) or a incident response (IR) plan in place?
• Frequent vulnerability assessments and/or penetration testing of the enterprise can reveal missing patches / vulnerabilities.
  • External scanning from the Internet provides a “hacker’s view” into the enterprise.
• Ensure all content management systems are fully up to date with latest security patches.
For more information

- Ransomware Hostage Rescue Manual
- Department of Justice – Ransomware What It Is and What to Do About It
  - https://www.justice.gov/criminal-ccips/file/872766/download
- Malware Domain List
- Suricata IP(D)S / Emerging Threats Ruleset
  - https://suricata-ids.org/
  - https://rules.emergingthreats.net/
- Checkpoint: Inside Nuclear’s Core
- Malware Traffic Analysis
  - http://www.malware-traffic-analysis.net/blog-entries.html
- Malware Don’t Need Coffee
  - http://malware.dontneedcoffee.com
Questions?