Malware? What are They and How to Prevent

TRACK D – SUSAN MARTIN, DARREN LACEY

Three Main Security Threats

- Carelessness -- Still makes up a plurality of data breaches
  - Loss of documents
  - Stolen unencrypted laptops
  - Missing USB drives or backup tapes
  - Inadvertent message or publication on the internet
- Credential Theft – Most common enterprise security attack
  - Phishing attacks
  - Use password stores from other data breaches
  - Brute force
  - Administrator credentials
- Malware – breaking the computer first (the subject of our talk)

Why Malware?

- Technically interesting – for example, a lot of malware is not even software any more
- Complex – can involve multiple systems and techniques
- Ever changing – new variants are continuous
- Built on system and application vulnerabilities – involves patching
- Potentially most damaging – Stuxnet, WannaCry, ransomware
- Griping about phishing and locking file cabinets is tedious

Vectors

- Phishing messages with attachments
- Fake patching and update servers
- Web browsing – like phishing in that it requires some social engineering
- Lateral attacks inside a network – scanning and remote exploits
- Remote desktop tools – TeamViewer/ GoToMyPC
- Removable media – especially those with autoplay (like USB's)
- Web application exploits – including Cross-Site Scripting

How is Malware Different than a Virus?

- A virus or a worm is a species in the Kingdom of Malware
- Recent advances exploit systems tools like PowerShell, Command Tools, Python, JavaScript or Perl
- Virus permutations change so rapidly now (thousands of times per day) that traditional antivirus has become less effective against any attack
- Hurts more now – ransomware, keyboard loggers, botnets and the like
- Keep in mind – both often require regular communication with malicious sites on the internet
  - Exploit – vulnerability meet malicious code
  - Payload – do some real damage (e.g. keylogger, ransomware, email server)

What you can do?

- Basic security hygiene
  - Patch everything – OS, Java, Adobe
  - Antivirus helps some
  - Don’t run code automatically
    - Disable automatic loading of files from USB drives
    - Disable macros in Office
  - Use two factor authentication for Gmail, Facebook, banking sites
  - Be skeptical of attachments and web banners that require you to open something

How does Malware Impact Healthcare Organizations

Susan Martin, RN, JD, CIPP-G, CPHIMS

CC Privacy Office

NIH Clinical Center

Disclaimer – No conflicts of interest to disclose

How does Malware Impact Healthcare Organizations

What is the impact for the various practice settings?

- **Patient Safety –** When the templated orders, alerts and communications that clinicians rely upon in the EHR are unavailable, it delays patient care services and their safety (ER, ICU, OR examples)

- **Monetary Impacts** - It can be monetary (fines, expense of cybersecurity IT consultants, cost of providing identity fraud protection to those individuals affected, loss of revenue while systems are offline, potential litigation costs)
- **Reputational Impacts** - Equally important can be the loss of reputation and trust among patients, health plans and physician practice groups. Loss of trust may take time to earn back. Especially if patients, insurance providers and physicians have other options and choose to take their business to another hospital, lab or ambulatory care setting

Malware affecting Healthcare Organizations

2017

- Wanna Cry and NotPetya

2018 (so far) * source Feb. 2018 Healthcare IT News

- **Fresnia Medical Care** settled 5 suits for 3.5 million dollars for vulnerabilities resulting in breaches
- **Allscripts** hit by SamSam ransomware hackers
- **Oklahoma State University Center for Health Sciences** network hacked, Medicaid billing data for 279,000 patients exposed
- **Hancock Health** held hostage by ransomware attack
- **Florida's Agency of Healthcare Administration** fell for phishing attack exposing Medicaid enrollee data for 30,000 Florida Medicaid patients

Healthcare continues to be a Target

- No industry is immune
- Companies of all sizes are getting attacked
- Why are Hackers Targeting ePHI???
- Ransom
- Premium price for medical records ($70-100 each)
- Use for insurance fraud, medication fraud and financial fraud (355 healthcare breaches affect 15 million record in 2016)

How can healthcare organizations prepare?

Technical steps include:

- Scanning network and endpoints for malicious code
- Frequent and complete backups of PHI and sensitive business data
- Restricting access behind firewalls housing PHI
- Two-factor authentication
- Employ an account lockout policy

How can healthcare organizations prepare?

Administrative steps include education and planning

- IT security staff, system administrators and business associates processing organization's ePHI should establish Incident Response Plans for reporting, containing, mitigating the risks of cyber attacks
- Develop contingency and business continuity of operation plans (COOP)
- Practice plans with IT staff, end users and business associates
- Educate staff on manual processes when systems must be taken off-line to continue business operations

Other resources

- HITRUST Cybersecurity Framework Assurance Program and assessment scorecard for the NIST CSF Framework - hospitals and health systems can more effectively and efficiently ensure security compliance
- Join the HIMSS Healthcare Cybersecurity Community: a forum for the industry's leading security voices and education for advancing the state of cybersecurity in healthcare
- HIMSS members can monitor **Healthcare and Cross-Sector Cybersecurity Report** to learn about reported threats, vulnerabilities and mitigation information on medical products (Phillips IntelliSpace Cardiovascular System, BD Alaris and BD Pyxis products and more)

Educate staff about phishing attacks

HHS Office for Civil Rights (OCR) website provides tools to educate staff about phishing, a type of cyber-attack

https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-february-2018.pdf

Be wary of unsolicited third party messages seeking information

- Be wary of uncharacteristic messages even from recognized sources
- Be cautious when responding to messages sent by third parties
- Be wary of clicking on links or downloading attachments from unsolicited messages
- Be wary of even official looking messages and links
- Use multi-factor authentication
- Keep anti-malware software and system patches up to date
- Back up your data

Ransomware video

https://www.youtube.com/watch?v=FV-HW3NYdF8

Summary

Computer malware is a lucrative industry for hackers

Healthcare organizations need to be prepared

Organizations should monitor industry alerts and follow the mitigation steps shared by cybersecurity experts if their systems are affected

Organizations must continue to educate themselves as malware and virus evolve and educate their staff and C-suite.

Questions?