Cybersecurity Threats and Vulnerabilities in Healthcare

a presentation to the

Mid-Atlantic Society of Healthcare Materials Management

Kevin Crain, Sr. Director IT Security & CISO
23 February 2018

UNIVERSITY of MARYLAND MEDICAL SYSTEM

Objectives

Understanding of current security threat landscape…

Common cyberattack vectors impacting healthcare supply chain…

Value of partnership between security and supply chain…

Device and service risks treatable through procurement contractual controls…

Threat Spectrum Landscape

Healthcare under increased attack in 2016, growing further in 2017

- **Evolution in attacks: from primarily data theft, expanding to data destruction (ransomware)**
- **Value of Electronic Protected Health Information 10x value versus payment cards**
- **Complex IT system footprint with extensive integration presents large target**
- **Spectrum of threats: Ransomware disruption of clinical and administrative systems, theft of patient information, medical device compromise**
- **Healthcare service vendors also under attack, e.g. Nuance 2017, Allscripts 2018**
- **Evolving ransomware incorporated multiple capabilities: data encryption, reconnaissance, command & control communication, lateral movement**

Threat Spectrum Landscape

FBI: 172% increase in ransomware incidents in 1st half 2016

- **71% involved e-mail messages as delivery mechanism**
- **Variety of threat actors: large, organized, well-funded "Wolves" and small, opportunistic "Coyotes"**
- **$209M losses in 1st quarter 2016**
- **$8BN global cost of WannaCry ransomware attack 2017 (Barlyn, 2017)**
- **$850M economic cost of NotPetya cyberattack 2017 (Barlyn, 2017)**
  - **$300M losses at Maersk Shipping due to NotPetya cyberattack 2017 (Barlyn, 2017)**

Reference

Barlyn, S. (2017, July 17). Global cyber attack could spur $53 billion in losses: Lloyd's of London. Reuters. Retrieved from https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

Threat Spectrum Landscape

Nationwide surge in email malware attacks observed in June 2016

- **UMMS email malware detection volume jumped from ~250/day to >10,000/day on 6/22**
- **Primary malware: Ransomware including Dridex and Locky strains**
- **BotNet clusters of infected devices under central command & control sending emails**
- **Abruptly ceased on Wednesday Aug 31…reorganizing and improving again**

Threat Spectrum Landscape

2017 global cyberattacks conducted machine-to-machine

- **WannaCry exploited vulnerability in Windows operating system file sharing software (MS017-010)**
- **Servers running vulnerable file sharing service port exposed to Internet and/or vendors via private networks**
- **Interior devices with vulnerable file sharing service active**
- **Advanced malware designed to infect, encrypt, scan for new targets, repeat...**
- **NotPetya also machine-to-machine, but much more sophisticated**

E-Mail Attacks

Increase in attackers impersonating C-suite executives

- **"Whaling" variant of conventional Phishing attack**
- **Official-appearing personalized email messages including business signature, logo**
- **Worded to create sense of urgency, drive immediate action by target**
- **Motives include data theft, wire fraud, delivering malware via infected attached "invoice"**

From: Robert Chrencik [mailto:xxxx]
Sent: Thursday, January 26, 2017 12:10 PM
To: *redacted*
Subject: Need immediate attention

Hi *redacted*,

I need you to email me all copies of employees W2s in PDF file.

Thank you

Robert A. Chrencik, MBA, CPA
President and Chief Executive Officer
robert.chrencik@umm.edu

From: Suntha, Mohan [mailto:xxxx]
Sent: Tuesday, March 28, 2017 2:31 PM
To: *redacted*
Subject: CONFIRM

Kindly send list of W-2 (tax and wages) copy of all employees for 2016 in PDF now for review

Thanks.

Sent from my iPhone

E-Mail Attacks

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

February 21, 2018

Alert Number
I-022118-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

INCREASE IN W-2 PHISHING CAMPAIGNS

Beginning in January 2017, IRS's Online Fraud Detection & Prevention (OFDP), which monitors for suspected IRS-related phishing emails, observed an increase in reports of compromised or spoofed emails requesting W-2 information. Sometimes these requests were followed by or combined with a request for an unauthorized wire transfer.

The most popular method remains impersonating an executive, either through a compromised or spoofed email in order to obtain W-2 information from a Human Resource (HR) professional within the same organization.

Individual taxpayers may also be the targeted, but criminals have evolved their tactics to focus on mass data thefts.

This scam is just one of several new variations of IRS and tax-related phishing campaigns targeting W-2 information, indicating an increase in the interest of criminals in sensitive tax information.

HOW TO REPORT A DATA LOSS RELATED TO IRS RELATED TO A W-2 SCAM

If notified quickly after the loss, the IRS may be able to take steps that help protect your employees from tax-related identity theft. To contact the IRS about a W-2 loss, email IRS at dataloss@irs.gov and provide the information listed below so the IRS can contact you. In the subject line, type "W-2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information (PII) data.

Provide the following information in your email:

1. Business name
2. Business employer identification number (EIN) associated with the data loss
3. Contact name
4. Contact phone number
5. Summary of how the data loss occurred
6. Volume of employees impacted

Note: The IRS doesn't *initiate* contact with taxpayers by email, text messages or social media channels to request personal or financial information. Any contact from the IRS will be in response to a contact initiated by you. Criminals, when they learn of a new IRS process, often create false IRS web sites and IRS impersonation emails.

Procurement Security

Questions for discussion:

Is the product secure as purchased?

Will the product remain secure during life cycle?

Is the manufacturer secure?

Are your business partners secure?

Partner with security to assess and mitigate risks during procurement

Procurement Security

Defined security requirements in vendor/product selection phase

- Either field-installable software patching or SLA-based vendor patching
- Encryption of data storage to prevent confidentiality breach if lost/stolen
- No hard-coded passwords (can be found on the Internet)
- Wireless network security: current industry standard (WPA-2 Enterprise)
- ***Protection of data at rest, data in transit, and control interfaces***

Reference

AAMI. (2016, April). Mayo Clinic Emphasizes Security with Device Vendors. Association for the Advancement of Medical Instrumentation. Retrieved from http://www.aami.org/productspublications/articledetail.aspx?ItemNumber=3199

Procurement Security

Contractual controls

- Device vendor accountability for timely software vulnerability patches
- Vendor (NOT JUST BUSINESS ASSOCIATES) accountability for security practices, e.g. user awareness training, security policies, antivirus software, timely notification of security incidents
- Mayo Clinic technology and security requirement language for contracts with vendors of medical devices and healthcare technology (AAMI, 2016)
- **Specific contract language can be found in *Biomedical Instrumentation & Technology [January/February 2016]***

Reference

AAMI. (2016, April). Mayo Clinic Emphasizes Security with Device Vendors. Association for the Advancement of Medical Instrumentation. Retrieved from http://www.aami.org/productspublications/articledetail.aspx?ItemNumber=3199

Medical Device Security

RELATED CONTENT

Radiation oncology practice settles with HHS over data breach

Check your contract before you put your data on the cloud

Healthcare struggles to recruit cybersecurity pros

Lahey Clinic computer theft leads to $850,000 HIPAA settlement

By Joseph Conn | November 30, 2015

Lahey Hospital and Medical Center has agreed to pay $850,000 in a settlement with HHS' Office for Civil Rights to resolve alleged privacy and security violations stemming from the theft of a laptop computer with unencrypted patient records.

The Burlington, Mass.-based health system also entered into a corrective action plan to address other privacy and security issues raised during the breach investigation.

According to a 10-page settlement agreement, Lahey reported to the federal agency on Oct. 11, 2011, that an unencrypted laptop used with a computerized tomography scanner had been stolen from an unlocked treatment room in Lahey's radiology department.

Lahey "impermissibly disclosed" electronic medical records of 599 individuals "for a purpose not permitted by the privacy rule" under the Health Insurance Portability and Accountability Act, the agency alleges in the agreement. The Civil Rights Office is the primary federal enforcement agency for privacy, security and breach notification rules under HIPAA.

Discussion

Backup Materials

Ransomware

Ransomware:

- Malicious software encrypts files on desktop, laptop, and server storage
- Automated pop-up message demanding ransom payment in BitCoin or files deleted
- Moves laterally across network from initial victim computer, spreads infection and encryption impact
- Hollywood Presbyterian FEBRUARY-2016 (first widespread news coverage, paid ransom)
- MedStar MARCH-2016
- Similar attacks continuing in 2016
- Erie County NY APRIL-2017
- May 12, 2017: WannaCry ransomware global attack (North Korean government)
- June 28, 2017: NotPetya ransomware global attack (Russian government)
- Hancock Health, Indiana: JANUARY-2018 (paid ransom 4 BitCoin @ $55K value)
- Allscripts: JANUARY-2018

HHS guideline July 2016: ransomware infection involving EPHI <u>mandatory reportable</u>

Ransomware

How does Ransomware infect devices?

Common strains exploit vulnerabilities in software to infect devices, e.g. WannaCry

More sophisticated strains are multi-stage attacks, e.g. NotPetya 2017

- Ukrainian accounting software vendor MeDoc reportedly attacked and compromised
- Automated software updates to MeDoc client systems reportedly contained NotPetya
- Client systems then became launch platforms inside victim networks
- NotPetya used three automated attack vectors:
  - “Scrape” login credentials from device memory, then use common administrative command functions PowerShell Exec and/or Windows Management Interface Console to attack other target devices;
  - If these failed, the “EternalBlue” vulnerability exploited by WannaCry was attempted.

Targeted attacks use stolen login credentials to enter network and inject Ransomware, e.g. SamSam attack on Hancock Health 2018:

- "...the hacker gained access to the system by using the hospital’s remote-access portal, logging in with an outside vendor’s username and password.”