hfma
wisconsin chapter

Healthcare Under Attack

The Current Threat Landscape

Today's presenter

Christopher Gerg

Advisor – Security, Privacy, Risk Consulting - RSM

- Cybersecurity, risk and governance consultant
  - HIPAA, HITRUST, National Institute of Standards and Technology, International Organization for Standardization, Payment Card Industry Data Security Standard and Cybersecurity Maturity Model Certification
  - Information security maturity
  - Risk assessment and management
  - Incident response and preparation
- Experienced CISO
  - Payment card industry
  - Healthcare data industry
- Author of O'Reilly and Associates book "Managing Network Security with SNORT and IDS Tools"

The Current Threat Landscape

What should I be at least a little worried about? (Risk-based decision making is the goal, not fear.)

Business Email Compromise

Often the root cause

Compromise of the business' email can result in a loss of intellectual property and can lead to other forms of attack.

Wire Transfer Fraud

Tricked into sending money

Tricking someone in the organization into sending money to the wrong destination.

Ransomware

Often a lengthy process

Can result in complete business interruption due to all computing resources being unavailable.

Supply Chain Attacks

Who can you trust?

If the software purchased from another company is compromised, it can lead to compromise of your organization.

The Current Threat Landscape

- Business Email Compromise
  - Attackers can access business-critical information if they have unfettered access to email.
  - Specific roles are often targeted (Executives, finance, IT admins)
  - Can very often lead to other attacks (common root cause for wire transfer fraud and ransomware)
- Wire Transfer Fraud
  - Sometimes as simple as the “gift card” scam
  - Can divert funds for large infrastructure purchases
  - Can result in theft of customer funds that were meant for you
  - Often a procedural problem, not a technical problem

The Current Threat Landscape

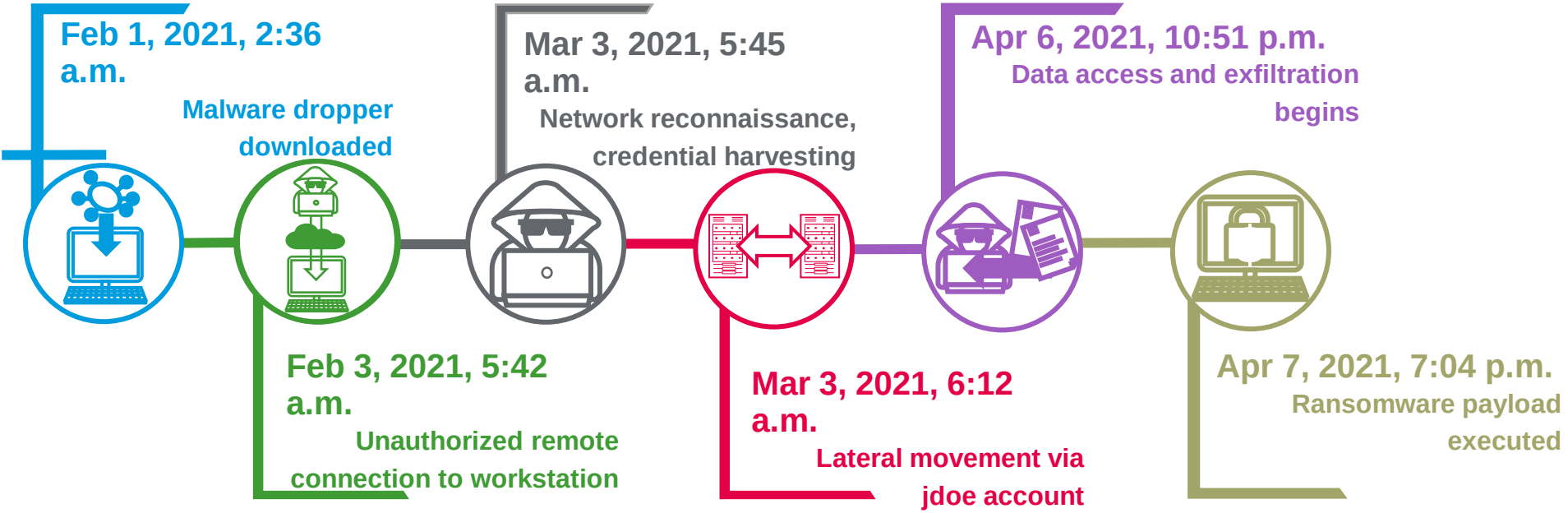
- Ransomware
  - Often a multi-month attack
  - Attackers are very organized
  - Multiple vectors of attack
  - Many attackers are state-sponsored
  - Backup archives and intellectual property are the main targets
  - “Ransomware as a Service”
- Supply Chain Attacks
  - Many recent examples: Target, Solar Winds, Kaseya, ASUS, Github
  - A successful attack can lead to the compromise of many other companies that use the compromised software/service
  - Many attackers are state-sponsored (Russia’s APT29 “Cozy Bear”)

Ransomware

Let’s dig into some details

hfma
wisconsin chapter

Ransomware Timeline Example



Who What Where When Why?

- Who is being targeted?
- Who is doing this?
- Why is it hard to catch them?
- When is it a breach?

Preventing Ransomware

There's not a single fix – it requires a program. But here are some foundational things that can help…

Foundational ransomware protections

- Implement multifactor authentication wherever possible.
- Limit and protect public-facing systems and services.
- Backups are and essential recovery mechanism
- Information security awareness training (The human firewall)
- Implement a robust endpoint detection and response tool (EDR).

There is not a “box of security” you an install to prevent ransomware. The goal is to make your exposure smaller and attacking you to be inconvenient so they move on to someone else!

Foundational ransomware protections

- Implement multifactor authentication wherever possible.
- Limit and protect public-facing systems and services.
- Backups are vital.
- The human firewall
- Implement a robust EDR.

- For all external access to email and other Software-as-a-Service solutions
- For all remote access (VPN)
- For all administrator-level access

MFA should be implemented everywhere possible—this has gotten a lot easier in recent years.

Foundational ransomware protections

- Implement multifactor authentication wherever possible.
- Limit and protect public-facing systems and services.
- Backups are vital.
- The human firewall
- Implement a robust EDR.

- Limit public-facing systems and services to the minimum necessary.
- Keep them separate from internal networks.
- Constantly update them to the latest code revision and patch level.

Foundational ransomware protections

- Implement multifactor authentication wherever possible.
- Limit and protect public-facing systems and services.
- Backups are vital.
- The human firewall
- Implement a robust EDR.

- Backup archives must be stored in a way that is inaccessible from the business network.
- Backup archives must use a different authentication mechanism than what is used on the business network (These authentication mechanisms should use MFA!).

hfma
wisconsin chapter

Foundational ransomware protections

- Implement multifactor authentication wherever possible.
- Limit and protect public-facing systems and services.
- Backups are vital.
- The human firewall
- Implement a robust EDR.

security program.

- Information security awareness training is a must at new hire.
- Periodic training refreshers are helpful for most users and frequent training is best for high-risk roles (e.g., executives, IT administrators, finance, HR and developers).
- Phishing testing is a very useful training and testing mechanism.

Foundational ransomware protections

- Implement multifactor authentication wherever possible.
- Limit and protect public-facing systems and services.
- Backups are vital.
- The human firewall
- Implement a robust EDR.

- EDR is more than just anti-virus (but includes that capability).
- EDR watches everything (the network, system calls, the file system and user activities).
- EDR is a very good candidate for a managed service because the initial rollout and interpretation of the output can be a daunting task, requiring highly qualified and informed experts.

QUESTIONS AND ANSWERS