The Wild West of Benefits

SWBA

43RD ANNUAL CONFERENCE

MAY 9-11, 2018

HYATT REGENCY
LOST PINES
AUSTIN, TX

Preventing a Stagecoach Robbery: The Next Level of Cybersecurity

Presented by:

Mark B. Bell, PMP, CISSP, CISA
EVP, Operations
Digital Defense, Inc

DIGITAL DEFENSE®
INCORPORATED

My Background

- Digital Defense, Inc.
  - Opened our doors on January 1, 2000
  - Headquartered in San Antonio, TX
  - Information security assessment services organization
    - Services include vulnerability scanning, ethical hacking, payment card industry security services, security awareness training and general security consulting
- Me
  - Digital Defense, Inc.
    - Senior Security Analyst / Director of Security Operations (2000-2003)
    - EVP, Operations (2007 – Current)
  - Retired Air Force Reserve
    - Active Duty: 1988-1998
    - Reserve: 1998-2009
  - Previously have worked for Fortune 500 companies working on contracts for the Air Force and Navy

Overview

- Definitions
- How do Stagecoach Robberies Happen?
- Stagecoach Robberies in the News
- Preventing a Stagecoach Robbery
- Conclusion

Definitions

- Incident vs Breach
  - **Incident**: A security event that compromises the integrity, confidentiality or availability of an information asset
  - **Breach**: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

  - Even if an incident does not become a breach, it can still be considered a "stagecoach robbery"
    - Costs associated with:
      - Data or services not being available
      - Redirecting internal personnel or hiring outside expertise to contain/clean up incident
      - Reputation loss

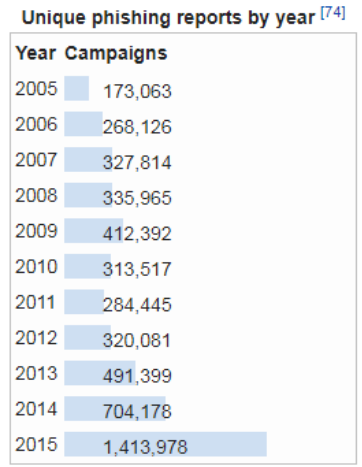
Definitions

- Malware vs Ransomware
  - **Malware**: An term to describe a wide range of software with malicious intent, including viruses, worms, spyware, etc.
  - **Ransomware**: A type of malware that blackmails victims by threatening to publish personal information or causing loss of availability of computing resources via means such as encryption and requiring the user to pay a ransom in order to prevent information release and/or return access to computing resources or files

Definitions

- Phishing vs Whaling
  - **Phishing**: A broad term describing various types of attacks utilized in an attempt to gain sensitive information from a target(s), including username & password, financial data, etc.
    - Phishing is itself part of a broader group of attacks known as Social Engineering
  - **Whaling**: A specific type of phishing attack targeting or appearing to come from senior management of a company. These types of attacks can be increasingly complex in attempting to convince employees to perform actions such as initiating a wire transfer.

  - Other types of phishing attacks include spear phishing, vishing, smishing
  - *Phishing attacks, alone or in coordination with other attacks, is increasingly one of the most popular ways the bad guys perform stagecoach robbery!*



Who is Behind Today's Stagecoach Robberies?

- 75% of threat actors are from outside the target organization
  - This means 25% are internal to the organization
    - Note that a breach can be intentional or unintentional!
- 51% are organized criminal groups
- 18% are state-affiliated actors
- 3% involved multiple parties
- 2% involved business partners

What Tactics Do They Use?

- 62% of breaches featured hacking
- 81% of hacking-related breaches leveraged stolen or weak passwords
  - *Have you checked https://haveibeenpwned.com to see if your passwords have been breached?*
- 51% of breaches included malware
- 8% of breaches included a physical security aspect

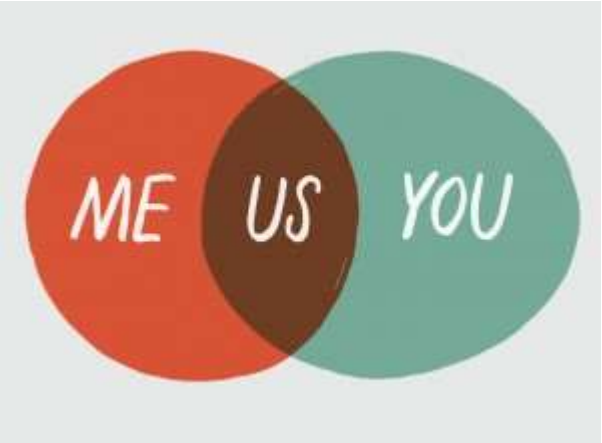
Who Are The Victims?

- 24% of breaches affected financial organizations
- 15% of breaches involved healthcare organizations
- 15% involved retail/accommodation organizations
- 12% were public sector entities

- The remaining 34% were everyone else!

Other Commonalities

- 73% of breaches were financially motivated
- 66% of malware was installed via malicious e-mail attachments
- 27% of breaches were discovered by third parties
- 21% of breaches were related to espionage



Stagecoach Robberies in the News

- Equifax Breach
  - Equifax failed to patch a known vulnerability they had on an external web server
    - Once breach occurred, were not very forthcoming about the damage
  - Estimated 147.9 million consumers were affected by this breach
    - Some were more significantly affected than others
  - Former CEO has to “resign” from his position
  - Overall cost at the end of 2017 was $439 million (and climbing)!
    - Only $125 million is covered by insurance

Stagecoach Robberies in the News

- Finger Lakes Health
  - E-mail, internet access, phone lines and several other electronic systems were shut down by a ransomware attack
    - Had to resort to paper-based record keeping
    - Eventually paid the ransom five days after the attack
      - Unknown exactly how much the ransom was
  - Apparently no health records or other sensitive data was accessed, just inaccessible
    - Therefore an incident, not a breach

Stagecoach Robberies in the News

- FACC Whaling Attack
  - Austrian aerospace manufacturer
    - Makes parts for Boeing, Airbus, etc.
- Attacker spoofed the CEO‘s e-mail (possibly with a fake, but realistic looking, domain)
  - Tricked a person within the finance department to wire money to an overseas account
    - Defrauded the company of @$55.8 million
    - The finance person, her immediate supervisor and eventually the CEO were all fired over the incident

Stagecoach Robberies in the News

- CarePlus Health Plans Privacy Breach
  - An error in mailing Explanation of Benefits letters
  - Due to programming and printing errors, letters were mailed to the incorrect CarePlus member
    - @11,200 members' information were exposed
    - Information disclosed included member name, plan identification number and name, provider of service, and services provided
      - No financial information or social security numbers were divulged
  - An example of an inadvertent data breach with a lack of an external or internal malicious actor
    - Still causes loss of trust and reputation

CarePlus HEALTH PLANS, INC.

The Wild West of Benefits

Preventing a Stagecoach Robbery

- **Physical Security Controls**
  - Ensure controls are implemented and followed in restricted areas
    - Don’t allow “piggy backing”
    - Trust, but verify
      - Verify badge, visitor access, etc.
  - Don’t leave sensitive information (i.e. printouts, computer, etc) left unprotected
    - The majority of physical security-related breaches actually involve lost documents (2017 VDBIR)
  - Don’t leave sensitive documents out unattended
  - Lock your computer screen when away
  - If you utilize point-of-sale terminals, ensure you have physical security protections as well as logical protection

Preventing a Stagecoach Robbery

- **Implement Technology to Detect and Prevent Breaches**
  - Most organizations block traffic coming into their network, but what is *leaving* your network?
    - Ensure you utilize egress filtering, i.e. only allow outbound services that are required for business
  - Is your staff utilizing mobile devices and/or laptops?
    - Ensure data is encrypted at rest
    - If employees are using mobile devices to access corporate resources (e-mail, files, etc), that you have the ability to remotely wipe those devices
  - Implement Intrusion Detection/Data Loss Prevention (DLP) technologies
  - Ensure anti-virus/anti-malware software is current and automatically updating

Preventing a Stagecoach Robbery

- **Partner/3rd Party Due Diligence**
  - Ensure your partners are following proper security processes in handling your data
    - The same can be said for you - are *you* following proper security processes in handling *your* client's data?
  - Hackers regularly attack partners of their target organization
    - Law firms that may hold sensitive patent data
    - Warehousing organizations that hold medical and/or financial data

Preventing a Stagecoach Robbery

- **Implement a Formal Vulnerability Management Program**
  - Ensure you have a program to detect vulnerabilities and ensure timely remediation of those vulnerabilities
    - Develop a service level agreement that states (for example) all critical and high severity vulnerabilities must be patched within 30 days of detection
  - Many organizations utilize vulnerability scanning and penetration testing but do not take action on findings
    - Equifax is a prime example
  - Organizations fail to run authenticated vulnerability scans
    - Hackers target the weakest link in the security chain – *your employees*
    - Many attacks start with a phishing e-mail, then exploit an unpatched vulnerability on your workstation
      - Microsoft Internet Explorer, MS Office and Adobe Flash/Acrobat are the most targeted pieces of software
    - Ensure patches are installed in a timely manner after release
      - Workstations should be patched immediately

Preventing a Stagecoach Robbery

- **Security Awareness**
  - This is your *most important and effective* line of defense in preventing a stagecoach robbery
    - One time a year and/or upon hire is not enough
      - Reinforcement of topics throughout the year as well as exercises to test effectiveness
    - Training should be memorable, engaging and fun
  - If training is ineffective, employees don't know how to identify and respond when faced with suspicious activity
    - *2017 VDBR:* Social engineering attacks were utilized in 43% of all breaches reported
      - Almost all phishing attacks that led to a breach were followed with some form of malware
      - Phishing is the most common social engineering tactic
        - Accounted for 93% of social engineering-related breaches
    - Be wary of realistic looking e-mails with attachments, links, etc.
      - Ransomware continues to be huge
      - Whaling continues to be a frequent tactic
    - *When in doubt, ask someone*

Preventing a Stagecoach Robbery

- **Social Media and Web Tricks**
  - Do the questions at the right look familiar?
    - Maybe because they are also common questions for secondary security questions!
      - Cambridge Analytica comes to mind…
    - Be wary of offers of ‘free’ stuff!
      - If something is too good to be true, it usually isn’t!
  - Typo squatting
    - There are more than 1,000 .cm typosquatting domains
      - espn.cm, cnn.cm, etc.
      - Sites like these were visited approximately *12 million times* during the first quarter of 2018.

Preventing a Stagecoach Robbery

- **Have a Plan**
  - No one is 100% immune from a security/data breach
    - An attacker with enough *time, resources and motivation* can breach even the best defenses
    - Have a plan ready for when things go wrong
  - Ensure you have effective policies and procedures in place
    - What should an employee do if they suspect a phishing attack?
    - How often should vulnerability patching take place?
    - What is you organization's Acceptable Use policy?
    - In absence of specific procedures, tell your manager or IT Security staff as soon as possible if you suspect a breach
      - Did you allow access to someone you shouldn't have?
      - Did you open an attachment or visit a strange URL?
      - Be careful using your corporate workstation/laptop for personal use

Conclusion

- Remember that the threat landscape is constantly evolving
- Reducing risk, increasing awareness and being prepared are keys to preventing, detecting and reducing the impact of an incident or breach
- Information security and breach prevention are *everyone's* responsibility

Conclusion

- Great links used as sources for my presentation and available for further information
  - Krebs on Security
    - https://krebsonsecurity.com
  - Verizon Data Breach Investigations Report
    - http://www.verizonenterprise.com/verizon-insights-lab/dbir/
  - Ponemon Institute Cost of a Data Breach Study
    - https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

Conclusion

My contact information:

mark.bell@digitaldefense.com

https://www.linkedin.com/in/bellmark/

Company Website

https://www.digitaldefense.com

THANK YOU!