UNDERSTANDING CYBER SECURITY, FOR FINANCE PROFESSIONALS

John Thomas

May 2019
AGENDA

- Hackers and Breaches
- Monetizing Breaches
- Incident Response and Forensics
- Password Considerations
- Indicators of Infosec Program Maturity
AGENDA

- HACKERS AND BREACHES
  - Monetizing Breaches
  - Incident Response and Forensics
  - Password Considerations
  - Indicators of Infosec Program Maturity
BREACHES - PAST

- Used to mainly target credit cards
  - TJ Maxx
  - Heartland Payment Systems
  - Ticketmaster
  - Target
  - Home Depot
BREACHES - TODAY

- Wider range of targets/data
- Equifax
- City of Atlanta
- Sony
- Ashley Madison
- National Bank of Blacksburg
TARGETS OF CHANCE

▪ Attacker casts a wide net

▪ May know how to exploit one website vulnerability in off-the-shelf website software
  ▪ Sets up a scan to try that exploit against every website

▪ Generalized phishing attacks
  ▪ Thousands or millions of recipients

▪ Brute-force password guessing

▪ Self-propagating viruses
  ▪ Some have built-in logic to test for something of interest – banking credentials or card payment applications
  ▪ Otherwise spread
TARGETS OF CHOICE

- Attacker has selected an organization as a target
- Automated and manual inspection of website for weaknesses
- **Spearphishing**
- Targeted password guessing
- Custom-built malware
COMMUNITY COLLEGES INCREASINGLY ARE TARGETS

- Lowest hanging fruit for attacks
  - Personal Information
  - Student Loans
  - SS Numbers used as identifiers
  - Cybersecurity “not a priority”

- Increasingly connected
  - Remote and mobile student body
  - Technology critical for education, operations, and service
  - Increasing use of cloud services

- Attackers have perfected multiple channels for monetizing community college breaches
AGENDA

- Hackers and Breaches
- MONETIZING BREACHES
- Incident Response and Forensics
- Password Considerations
- Indicators of Infosec Program Maturity
STUDENT LOAN FRAUD

- Thieves apply for loans using stolen personal information
- Federal funding goes to the school for tuition and fees, balance is remanded to the “student”
- Victim is left on the hook for the debt
ELECTRONIC PAYMENT FRAUD

- Sometimes called “email account takeover” since they are so intertwined
- ACH and wire fraud most common
- “Business” bank accounts don’t include the same consumer protections as personal accounts
- Victims usually take the loss
TAX RETURN FRAUD

- Relatively easy and low-risk form of identity theft
- Requires knowledge of name, DOB and SSN
CREDIT CARD FRAUD - INFECTED COMPUTERS
CREDIT CARD FRAUD - CARD SKIMMERS
DON’T CHIP-ENABLED CARDS STOP FRAUD?

- EMV-only cards make it harder to create a forged physical card
- Does not impact online/phone sales
- Does not prevent use of stolen cards
- Does not increase the security of networks or backend systems
- Why switch?
  - Otherwise your college can take the loss if someone pays with a forged card in hand
A BAD MONDAY MORNING
CYBER EXTORTION

- Harvest your data
- Demand Bitcoin payment or they will publicly disclose the breach or leak the data
CRYPTOCURRENCY MINING

- Increasingly sophisticated to avoid getting flagged
  - Slow down the speed of CPU fans
  - Switching off mining software during a users’ active hours
  - Artificially showing low computing power usage
SELLING DATA ON THE “DARK WEB”

- Credentials to sell
  - Student, professor, etc. usernames and passwords
  - Personal accounts
  - School accounts

![Image of card information](https://pastebin.com/1aw/)

---

Copyright © 2018 Sikich LLP. All rights reserved. Distribution or copying is strictly prohibited.
AGENDA

▪ Hackers and Breaches
▪ Monetizing Breaches
▪ INCIDENT RESPONSE AND FORENSICS
▪ Password Considerations
▪ Indicators of Infosec Program Maturity
RECENT TRENDS FROM FORENSIC INVESTIGATIONS

▪ Drastic changes in attacks in the past year
  ▪ Method
  ▪ Willingness to persist
▪ Attackers fighting to hold ground even after detection
▪ The professional criminals are handpicking their victims
  ▪ (No more just outrunning the bear)
WHAT HAPPENS WHEN A BREACH OCCURS

- Response activities may be driven by your bank or regulatory bodies
- Forensic investigations typically cost $20,000 and up
  - Collection and analysis of data
  - Attempt to determine how they got in and what they took
  - Seldom able to gather a complete record of the event
- Determine breach notification requirements
- Community college and media communications management
INCIDENT RESPONSE

- Identification
  - Is this a real incident

- Containment
  - Stop the bleeding

- Eradication
  - Remove the cause
  - Create indicators of compromise

- Recovery
  - Best route back to a trusted environment

- All the time balance these activities against facilitating day to day processes and maintaining evidence
FORENSIC INVESTIGATION

▪ Formal review/inspection of the event

▪ Disk and memory imaging of impacted systems

▪ Collection of log files

▪ Offline analysis of images
  ▪ Timeline analysis
  ▪ File integrity analysis

▪ Often the “smoking gun” and the whole picture cannot be identified
AGENDA

- Hackers and Breaches
- Monetizing Breaches
- Incident Response and Forensics
- PASSWORD CONSIDERATIONS
- Indicators of Infosec Program Maturity
JUST ONE PASSWORD

- From Outside
  - Email
  - Cloud file services
  - Registration, Payroll and Benefits sites

- From Inside
  - Query network for username list, who is admin
  - Unprotected/open network shares
  - Login to a workstation and run a keylogger
INCREASINGLY SOPHISTICATED PHISHING ATTACKS

- Spearphishing
- Tab nabbing
WEBSITE BREACH LISTS

- Many breaches result in theft of email/password pairings
- These lists are often leaked to the Internet
- Used in “credential stuffing” attacks
PASSWORD SPRAYING

- Guessing 500 passwords against one account → Lockout
- Guessing one password against 500 accounts → Often success
- Common password examples
  - Packers1
  - July2018
  - Summer18
  - Username as password
  - Welcome123
Offline brute-force guessing of passwords using a dictionary or character patterns

Used to recover plaintext passwords from encrypted files and network traffic
THE FIX: LONG PASSWORDS (PASSPHRASES)

- **UNCOMMON (NON-GIBBERISH) BASE WORD**
- **ORDER UNKNOWN**
- **~28 BITS OF ENTROPY**
  - $2^{28} = 3$ DAYS AT 1000 GUESSES/SEC
  - **Difficulty to guess:** EASY
- **Was it Trombone? No. Troubador. And one of the O’s was a zero?**
  - **Difficulty to remember:** HARD
- **Common Substitutions**
  - Numerical substitutions
  - **~44 BITS OF ENTROPY**
    - $2^{44} = 530$ YEARS AT 1000 GUESSES/SEC
    - **Difficulty to guess:** HARD
    - **Difficulty to remember:** YOU'VE ALREADY MEMORIZED IT

**Correct Horse Battery Staple**
- **Four random common words**
- **Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.**
MULTI-FACTOR AUTHENTICATION

- There are many cost-effective, non-invasive solutions available today

How does Google prevent phishing attacks on its 85K employees? It gives workers a key

Dive Brief:
- For the last year-and-a-half Google has prevented the successful execution of phishing attacks against its employees by simply introducing a key, a Google spokesperson told KrebsOnSecurity.
AGENDA

- Hackers and Breaches
- Monetizing Breaches
- Incident Response and Forensics
- Password Considerations
- INDICATORS OF INFOSEC PROGRAM MATURITY
AUTOMATED PATCHING

- Does your college have a centralized system for deploying and monitoring security patches?
- Does your college automate patching for third-party applications (such as Adobe Reader, Java, Firefox and Chrome?)
- This can be difficult with so many different systems!
CENTRALIZED ANTI-VIRUS

▪ Is there a central console to monitor anti-virus coverage and alerts?
▪ Does the College enable advanced anti-virus features?
  ▪ Behavioral detection
  ▪ Software firewall
  ▪ Host-based intrusion detection
  ▪ Device control/lockdown
▪ It is possible to provide free AV for students.
PASSWORD PRACTICES

- Are long or complex passwords enforced?
- Does the college train employees and students about the risks of weak password practices?
  - Guessable patterns
  - Password re-use on different systems
  - Formal training for faculty and staff
  - A simple newsletter for students.
BACKUPS AND DATA MANAGEMENT

- Does the college allow important data on laptops without backups?
  - Should not be done at all. Use a secure Cloud.

- Does the college’s IT department conduct periodic disaster recovery testing?

- Does the college have a network share that is a “dumping ground” to which all faculty and staff have rights?

- Are faculty and staff using cloud services (such as Google Docs) for work without IT oversight?
WEB FILTERING

- Does the college have web filtering in place?
- Effective web filtering provides numerous benefits
  - Can block phishing sites/drive-by malware downloads
  - Keeps employees on task
  - Helps reduce complaints of harassment or inappropriate use
  - Can block malware C&C channels
  - Freedom of speech vs safety
MULTI-FACTOR AUTHENTICATION FOR REMOTE ACCESS

- Does the college require multi-factor authentication for VPN and remote desktop access?
- Colleges are increasingly deploying multi-factor authentication for email, external application and cloud storage access as well
- Focus here on faculty and staff.
  - Can get bombarded with support calls if rolled out to students.
SYSTEM HARDENING

▪ Does your college run end-of-life systems, such as Windows XP and Windows 2003?
  ▪ Sometimes needed for research BUT they should be on their own network and have no access to file shares, etc.

▪ Does the college have a standard/automated build process for workstations?
  ▪ Does it reset when a student logs off a public computer?
SOCIAL ENGINEERING AND PHISHING

- Mistakes often lead to incidents
  - Phishing or pretext calling may lead to electronic payment fraud
  - Physical intrusions or “tailgating” can lead to keyloggers and rogue network devices

- Best defense is policies/procedures, education and enforcement
PHISHING EXERCISES

- There are a number of cloud service providers for periodic phishing exercises.
- These activities have been shown effective at reducing risky “click through” rates of employees.
THIRD-PARTY ASSESSMENT OF SECURITY POSTURE

- **IT Controls Audit**
  - List the organization’s control objectives and controls
  - Evaluate the appropriateness and execution of the controls

- **Framework Audit**
  - Assess the organizations controls against an industry or regulatory checklist

- **Risk Assessment**
  - “Thought exercise” type assessment considering threats, controls and control effectiveness

- **Network Security Assessment**
  - Automated and manual collection of vulnerability and configuration data to assess the organization’s posture

- **Penetration Test**
  - Simulation of a real-world attack
THANK YOU FOR YOUR TIME.

Are there any questions?

John Thomas
John.Thomas@sikich.com
877.403.5227