Cyber Security in State and Local Educational Agencies (SEAs and LEAs)

7/23/2018

Office of the Chief Information Officer
U.S. Department of Education

Agenda

Introduction

Overview of the present value trade-space

Threatscape

Best practices for data-focused missions

Federal resources that can help

Questions

Introduction

Steven Hernandez

MBA, CISSP, CISA, CNSS, CSSLP, SSCP, CAP, ITIL

Chief Information Security Officer (CISO)

US Department of Education

Prior Roles:

Vice Chairman Board of Directors $(ISC)^2$

CISO HHS OIG

Senior Official for Privacy, HHS OIG

Overview of Value

"**Brian Krebs** is an American journalist and investigative reporter. He is best known for his coverage of profit-seeking cybercriminals. His interest grew after a computer worm locked him out of his own computer in 2001.

From 1995 to 2009, Krebs was a reporter for *The Washington Post* and covered tech policy, privacy and computer security as well as authoring the *Security Fix* blog. He is also known for interviewing hacker 0x80.[2]

On March 14, 2013, Krebs became one of the first journalists to become a victim of swatting.[3] On December 18, 2013, Krebs broke the story that Target Corporation had been breached of 40 million credit cards. Six days later Krebs identified a Ukrainian man who Krebs said was behind a primary black market site selling Target customers' credit and debit card information for as much as US$100 apiece.[4] In 2014, Krebs published a book called *Spam Nation: The Inside Story of Organized Cybercrime - from Global Epidemic to Your Front Door*, which went on to win a 2015 PROSE Award.[5]" --Wikipedia

Overview of Value

Krebs is interesting because:

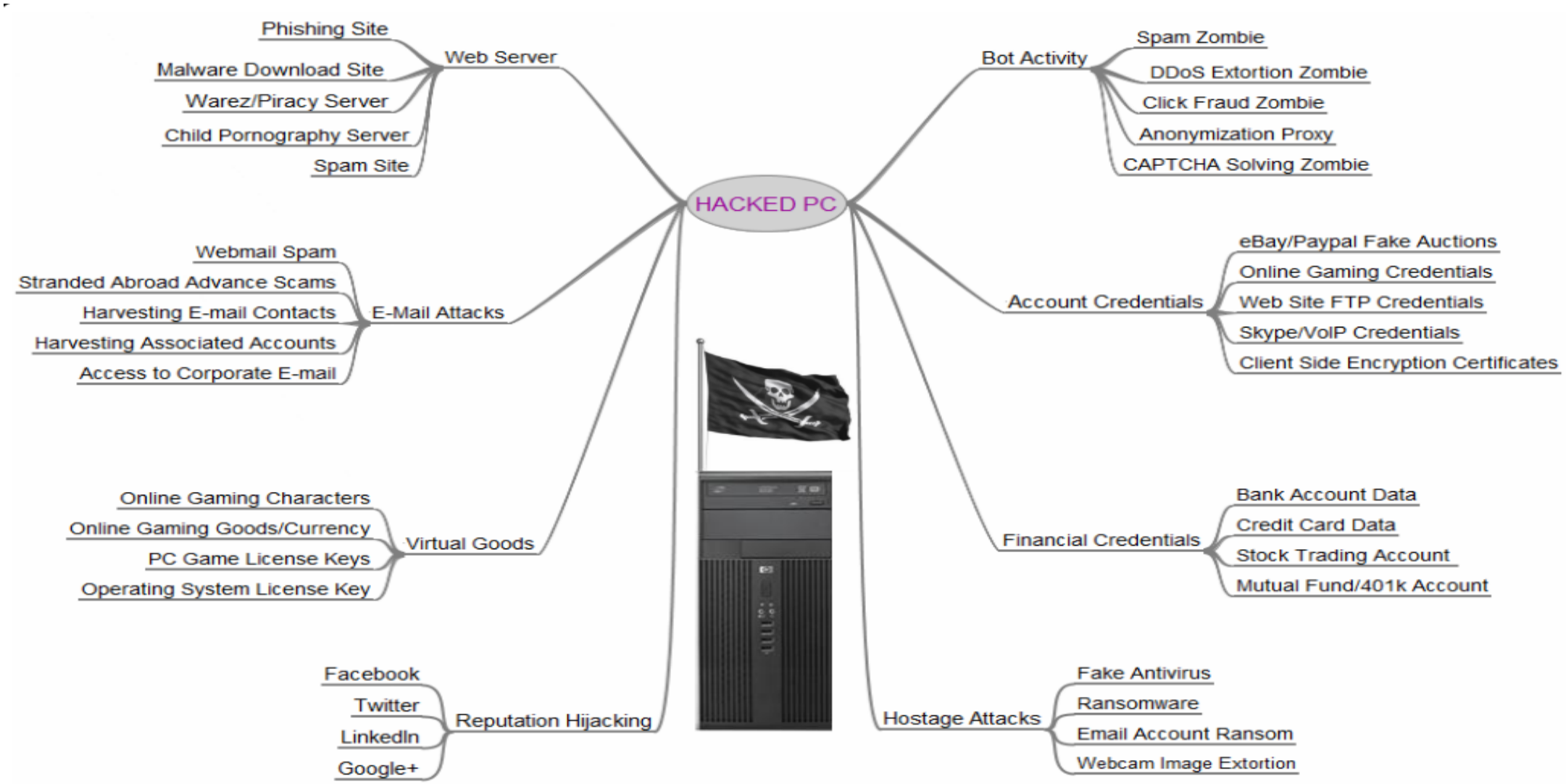
- Brings a journalists curiosity and rigor to cybersecurity
- Extensive research on the motivations of attackers (hackers)
- Has experienced the worst of the dark web (SWATing)
- Excellent research related to the value of cyber assets!
  - Value of a single computer
  - Value of email
  - Value of a hacked company or organization

Kreb's Value of a Hacked PC

How often have you heard?

- "My machine really doesn't have anything of value on it."
- "I only really do low value work on the machine like public information."
- "I really don't care of someone hacks my machine, if there's something they want they can have it."

Kreb's Value of a Hacked PC



https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

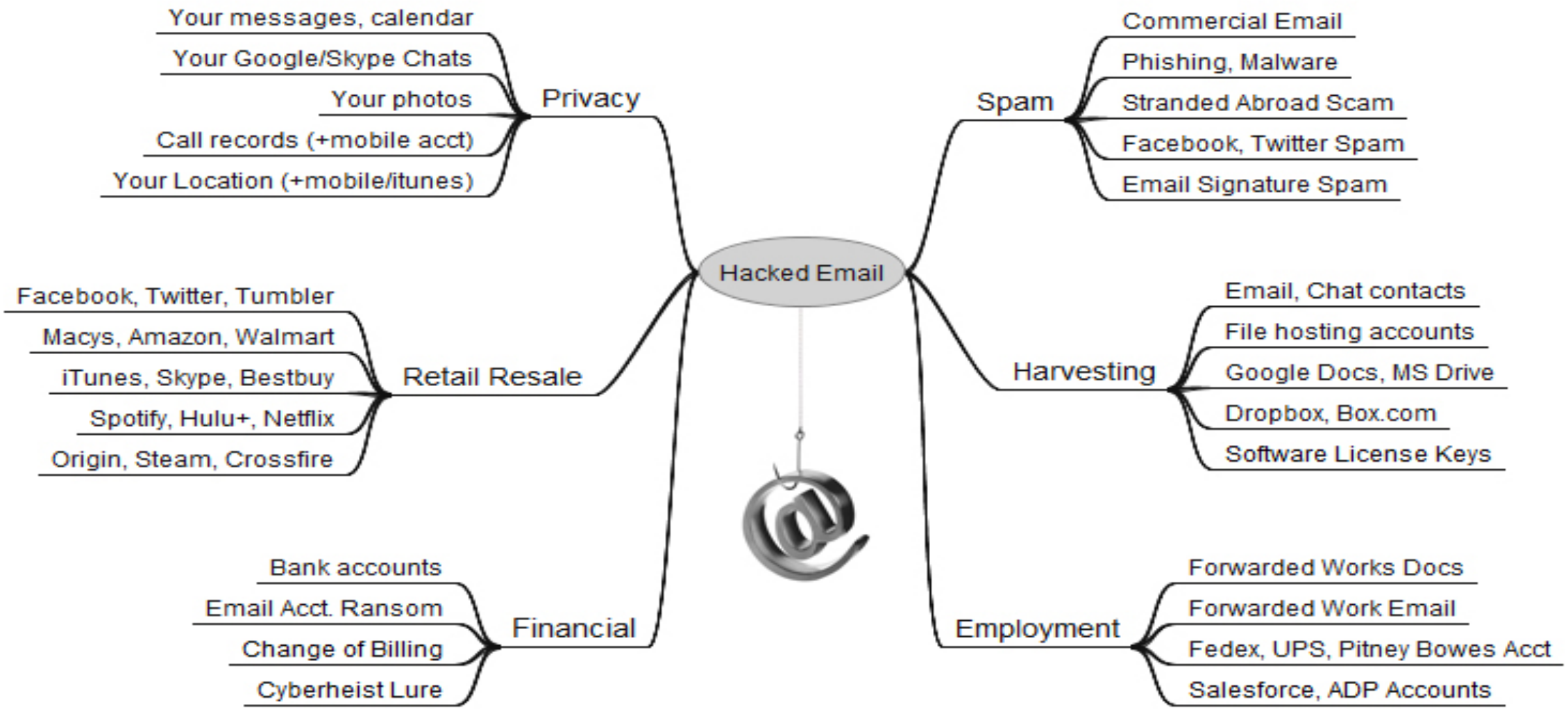
Kreb's Value of a Hacked PC

Bitcoin mining:

- Leveraging physical and cloud assets to mine cryptocurrency (cryptojacking)
- This turns any device or cloud infrastructure into a money mining machine
- The cost to you comes in terms of performance and in the cloud real cash.
- No real skill necessary, automated kits are available for ~$30

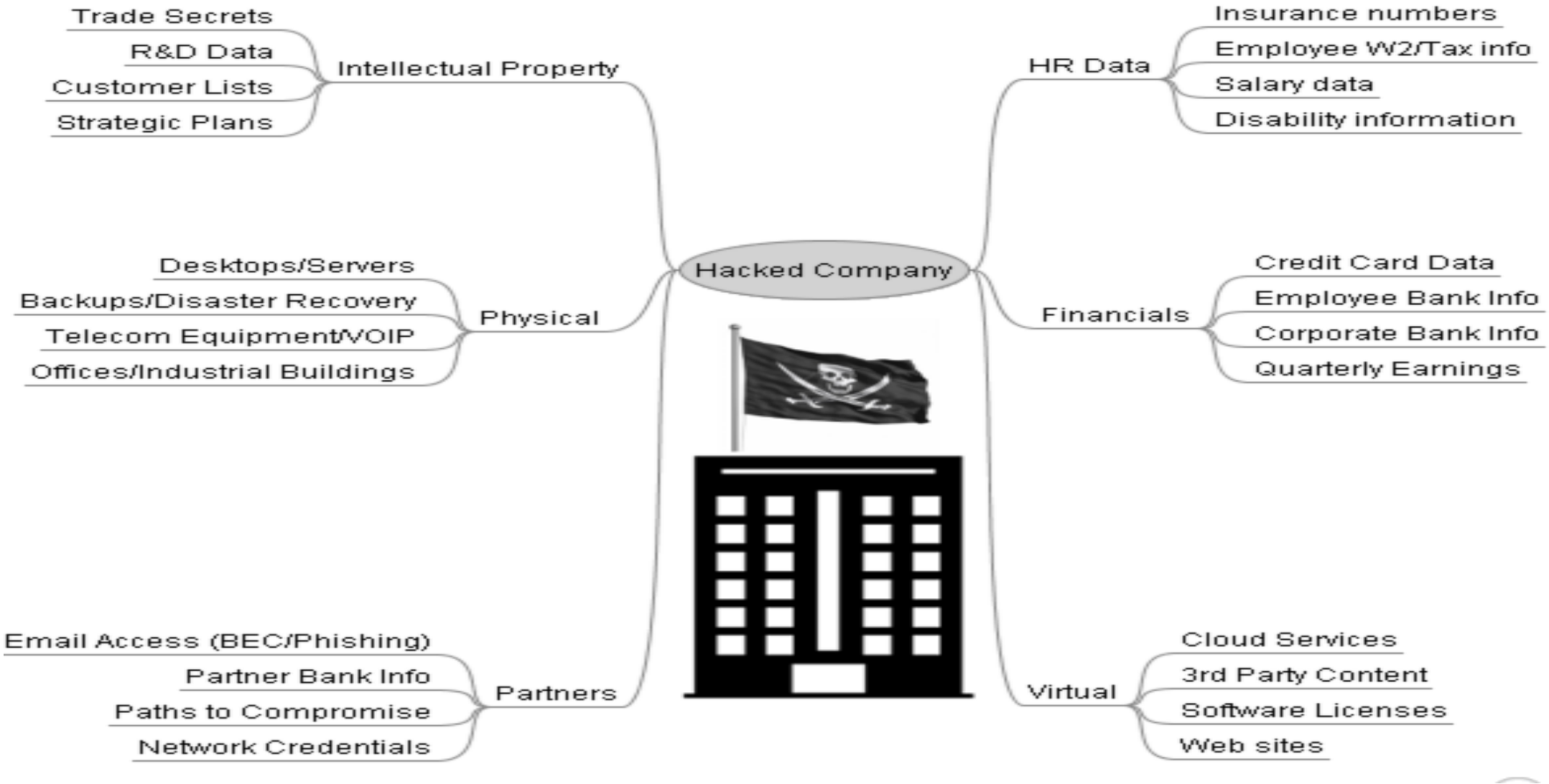
Unsecured AWS led to cryptojacking attack on LA Times, Tesla and Others. Insecure cloud resources, infested code and poor administrative control led to the attack.

Kreb's Value of Hacked Email (BEC)



https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Kreb's Value of a Hacked Company (Organization)



Value of the SEA/LEA information

Electronic Frontier Foundation did aa study titled "**Spying on Students: School-Issued Devices and Student Privacy"**

- In Summary the EFF concludes ed tech suffers from:
  - **Lack of transparency.** Schools issued devices to students without their parents' knowledge and consent. Parents were kept in the dark about what apps their kids were required to use and what data was being collected.
  - **Investigative burdens.** With no notice or help from schools, the investigative burden fell on parents and even students to understand the privacy implications of the technology they were using.
  - **Data concerns.** Parents had extensive concerns about student data collection, retention, and sharing. We investigated the 152 ed tech services that survey respondents reported were in use in classrooms in their community, and found that their privacy policies were lacking in encryption, data retention, and data sharing policies.
  - **Lack of choice.** Parents who sought to opt their children out of device or software use faced many hurdles, particularly those without the resources to provide their own alternatives.
  - **Overreliance on "privacy by policy."** School staff generally relied on the privacy policies of ed tech companies to ensure student data protection. Parents and students, on the other hand, wanted concrete evidence that student data was protected in practice as well as in policy.
  - **Need for digital privacy training and education.** Both students and teachers voiced a desire for better training in privacy-conscious technology use.

Value of the SEA/LEA information

The information, technology and access to students has tremendous value to an attacker:

- Student PII and PHI is often untouched in terms of prior breaches.
  - A ripe target for collection and maturing for use later
- Ed tech can provide a conduit for predators to profile, stalk or harass victims.

Value of the SEA/LEA information

- TheDarkLord:
  - "We Are Savage Creatures:
  - https://gizmodo.com/hackers-lock-down-entire-school-district-with-threats-1818542996
- https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html
- https://www.desmoinesregister.com/story/news/crime-and-courts/2017/10/05/dark-overlord-hacker-johnston-schools-threats/735950001/

Threatscape

- Ransomware
- Business E-mail Compromise
- Data Exfiltration/Breach

Ransomware

Ransomware is a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. Ransomware often infiltrates a PC as a computer worm or Trojan horse that takes advantage of open security vulnerabilities. Most ransomware attacks are the result of clicking on an infected email attachment or visiting hacked or malicious websites.

Upon compromising a computer, ransomware will typically either lock a user's system or encrypt files on the computer and then demand payment before the system or files will be restored. --Webopedia

Ransomware Examples

Financially-Motivated Ransomware

- **Locky** first appeared in February 2016 and is now one of the most distributed forms of ransomware. In late 2016 it became so proliferate that it was named one of the three most common forms of malware. There are distribution campaigns of Locky via email almost every day.
- **Troldesh** is mostly distributed in Russia and European countries. It is not prevalent in the U.S.
- **GlobeImposter, Philadelphia, and Cerber** are all ransomware threats using the "Ransomware as a Service" (RaaS) model. While some cyber criminals make and distribute their own ransomware, some have begun to provide a software package—complete with ransom note customization—to other cyber criminals for a fee.

  - https://www.bitsighttech.com/blog/ransomware-examples

Ransomware Examples

Disruption-Motivated Ransomware

- **WannaCry** is a wormable ransomware that spreads like a virus. Interestingly, it only collected a bit over $100,000 dollars total, quite a small sum considering its global spread. To that point, between May 12 and May 15, 2016, WannaCry was observed on over 160,000 unique IP addresses. (Read more about the global impact of WannaCry in this article.)
- **NotPetya** used a compromised accounting software provider as its initial point of distribution, and impacted many Ukrainian companies. But NotPetya didn't stop in Ukraine. Multinational companies with arms in Ukraine were compromised as well. While NotPetya was also not believed to be financially motivated, it did impact the bottom line of some large companies. According to this Insurance Journal article, "Package delivery company FedEx Corp. said on Tuesday a June [NotPetya] attack on its Dutch unit slashed $300 million from its quarterly profit, and the company lowered its full-year earnings forecast. The company said the cyber attack slashed 79 cents per share from its profit."
- **Bad Rabbit** is a variant of NotPetya that was also primarily distributed in Ukraine and Russia to a number of major corporations. NotPetya and Bad Rabbit share the same code, indicating that the same group is responsible for both ransomware examples. But unlike NotPetya, Bad Rabbit uses unique Bitcoin wallets for every victim. For this reason, the motivation behind these attacks is unclear.

  - https://www.bitsighttech.com/blog/ransomware-examples

Ransomware Countermeasures

Business Continuity Considerations

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up. Examples are securing backups in the cloud or physically storing backups offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

Ransomware Countermeasures

Business Continuity Considerations

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up. Examples are securing backups in the cloud or physically storing backups offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

Ransomware Countermeasures

What to Do If Infected with Ransomware

Should preventive measures fail, the USG recommends that organizations consider taking the following steps upon an infection with ransomware:

- **Isolate the infected computer immediately**. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- **Isolate or power-off affected devices that have not yet been completely corrupted.** This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.

Ransomware Countermeasures

- **Immediately secure backup data or systems by taking them offline.** Ensure backups are free of malware.
- **Contact law enforcement immediately.** We strongly encourage you to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance.
- **If available, collect and secure partial portions of the ransomed data that might exist**.
- **If possible, change all online account passwords and network passwords after removing the system from the network.** Furthermore, change all system passwords once the malware is removed from the system.
- **Delete Registry values and files to stop the program from loading.**

Ransomware Countermeasures

- **Immediately secure backup data or systems by taking them offline.** Ensure backups are free of malware.
- **Contact law enforcement immediately.** We strongly encourage you to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance.
- **If available, collect and secure partial portions of the ransomed data that might exist**.
- **If possible, change all online account passwords and network passwords after removing the system from the network.** Furthermore, change all system passwords once the malware is removed from the system.
- **Delete Registry values and files to stop the program from loading.**

Ransomware Countermeasures (Ransoms)

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom.
- Some victims who paid the demand were targeted again by cyber actors.
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

Business Email Compromise (BEC)

- Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.
- The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.[1]

https://www.ic3.gov/media/2018/180712.aspx

Business Email Compromise (BEC)

- The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses[2]. The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 115 countries.

- Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom, Mexico and Turkey have also been identified recently as prominent destinations.

Business Email Compromise (BEC)

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018:**

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	$12,536,948,299

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from **October 2013 to May 2018:**

Total U.S. victims:	41,058
Total U.S. victims:	$2,935,161,457
Total non-U.S. victims:	2,565
Total non-U.S. exposed dollar loss:	$671,915,009

Business Email Compromise (BEC)

Even the best get hit by this one:

"On Thursday, March 16, the CEO of **Defense Point Security, LLC** — a Virginia company that bills itself as "the choice provider of cyber security services to the federal government" — told all employees that their W-2 tax data was handed directly to fraudsters after someone inside the company got caught in a phisher's net."

"I want to alert you that a Defense Point Security (DPS) team member was the victim of a targeted spear phishing email that resulted in the external release of IRS W-2 Forms for individuals who DPS employed in 2016," Defense Point CEO George McKenzie wrote in the email alert to employees. "Unfortunately, your W-2 was among those released outside of DPS."

https://krebsonsecurity.com/2017/03/govt-cybersecurity-contractor-hit-in-w-2-phishing-scam/

Preventing BEC

Be mindful of phone conversations. Many victims have reported receiving phone calls from BEC/EAC actors requesting personal information for verification purposes. Financial institutions report phone calls acknowledging a change in payment type and/or location. Some victims report they were unable to distinguish the fraudulent phone conversation from legitimate conversations. One way to counter act this fraudulent activity, is to establish code phrases that would only be known to the two legitimate parties or call the business/requester back at a validated good number.

Preventing BEC

If you discover a fraudulent transfer, time is of the essence. First, contact your financial institution and request a recall of the funds. Different financial institutions have varying policies; it is important to know what assistance your financial institution will provide when attempting to recover funds. Second, contact your local FBI office and report the fraudulent transfer. Law enforcement may be able to assist the financial institution in recovering funds. Finally, regardless of dollar loss, file a complaint with www.ic3.gov or, for BEC/EAC victims, bec.ic3.gov. The IC3 will be able to assist both the financial institutions and law enforcement in the recovery efforts.

Best Practices for Data Focused Missions

- Identify Your “Crown Jewels”
  - Least Function
  - Least Privilege
  - De-Identification
  - Retention
- Have an Actionable Plan in Place Before an Intrusion Occurs
- Have Appropriate Technology and Services in Place Before An Intrusion Occurs
- Have Appropriate Authorization in Place to Permit Network Monitoring
- Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident
- Ensure Organization Policies Align with Your Cyber Incident Response Plan
- Engage with Law Enforcement Before an Incident
- Establish Relationships with Cyber Information Sharing Organizations

Best Practices for Data Focused Missions

- Building the Security in from the start
  - Consider leveraging cloud SaaS as much as possible
    - Review terms and SLA
    - Data Portability
  - Leverage FedRAMP systems
    - May not always be able to use GSA contracts
    - Federal Government Level of Security
    - You are still accountable for control configuration
    - State and local government representatives are encouraged to contact any FedRAMP Authorized CSP directly to determine their security package specifications.

Helpful Federal Resources

- US Department of Education
  - https://studentprivacy.ed.gov/
  - https://nces.ed.gov/programs/ptac/

- FBI
  - Internet Crime Compliant Center (https://www.ic3.gov/default.aspx)
  - Local Field Offices (Establish a relationship sooner than later!)
    - https://www.fbi.gov/contact-us/field-offices
  - Infraguard (https://www.infragard.org/)

- MS-ISAC (https://www.cisecurity.org/ms-isac/)
  - Connects back to the US Department of Homeland Security

- Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml)
  - Electronic Crimes Task Forces (ECTFs) (http://www.secretservice.gov/ectf.shtml)

Helpful Federal Resources

- DOJ Best Practices for Victim Response and Reporting of Cyber Incidents -
  - https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

- NSA's Top Ten Cybersecurity Mitigation Strategies
  - https://www.iad.gov/iad/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm

- DHS US-CERT National Cyber Awareness System
  - https://www.us-cert.gov/ncas

- United States General Services Administration FedRAMP Program
  - https://www.fedramp.gov/training/

THANKS!!!!

Questions??

Contact me:

Steven G Hernandez

Steven.Hernandez@ed.gov