Collection of Use of Electronic Evidence

NAME
Peter J. (PJ) Leiss, PE, CFEI, CVFI

EXPERT SPECIALTY
Vehicle Engineering and Accident Reconstruction Expert

DATE
May 2, 2019
AGENDA

Types of Evidence at the Scene
Methods of Collecting Scene Evidence
Types of Evidence at the Scene

Physical evidence such as:

• Skid and yaw marks from the involved vehicles
• Vehicle debris field at the scene
• Fluid trails
• Scrapes/gouges in the roadway
• Roadway characteristics (straight/intersection/condition/etc.)
• Presence of traffic control devices
Methods of Collecting Scene Evidence

• Camera – Still and Video
• Tape measure and/or measuring wheel
• Total Station
• Laser Scanner
Still Photography
Still Photography
Still Photography
Still Photography
Hand Measurements

Pros:
- Tools are inexpensive
- Ease of use
- Immediate data

Cons:
- Lacks precision
- Can be dangerous for operator
Total Station

Pros:
• Precise measurements
• Can take measurements from place of safety

Cons:
• May require a 2^{nd} operator (running the stick)
• Need to analyze the data for measurements
• Data points are not dense in number, creating denser data points takes time at the scene and in processing the data
Total Station

Total station data of yaw marks used to conduct a beta analysis for reconstruction
Laser Scanner

Pros:
- Precise measurements
- Requires 1 operator
- High point density allows for more accurate measurements
- Allows operation from a distance, increasing operator safety
- Scene scans port into simulation software such as PCCrash for more precise crash dynamics
- Scene scans port into an animation
- Vehicle scans can be 3D printed for demonstratives

Cons:
- Need to analyze the data for measurements
- Initial expense of the equipment ($30k-$80k)
Laser Scanner

Top view of a laser scanned scene
Laser Scanner

Closer view of the same laser scanned scene
Laser Scanner

3D printed vehicle from laser scan data
AGENDA

- Motivation: What do cyber criminals want?
  - Means: How do cyber criminals get what they want?
    - BEC cases
    - Intellectual property theft through phishing/spear-phishing
    - Ransomware
    - DDOS
  - Prevention: Basics of corporate cyber hygiene
MOTIVATION

- MONEY, MONEY, MONEY
  - Cash Transfers
  - Personal Identifying Information and tax information
  - Intellectual Property

- DISTRUPTION
  - Disgruntled employee/competitor
  - Cyber terrorism
  - Hacktivism
MEANS

- HUMAN BEINGS
  - Social engineering and spoofing emails
  - Spear-phishing and phishing to distribute malware
    - Don’t click “OK” for updates
    - Click “OK” without reading
    - Easy passwords/same password across infrastructure
- Technical vulnerabilities
- DDOS
Business Email Compromise (BEC) is a combination of a social engineering attack and a phishing attack. The fraudster hijacks an email account, or creates a similar/look-a-like email account, for an Executive, Client, or Vendor, and uses the email account to request a business transaction. Common incidents include a request for employee W-2 information, a request for payment (ACH, Wire), or a request to change Bank Account and Routing for future payments.
BUSINESS EMAIL COMPROMISES

• BEC attacks are the No. 1 reported cyber crime in CT
• The FBI (IC3) received 298,728 cyber crime and fraud complaints in 2016 with reported losses in excess of $1.4 billion - BEC was the No. 1 cause of loss.
• BEC Global Exposure - Over $5 billion (since 2013)
• BEC Reports - All 50 states & 131+ countries
• BEC From January 2016 - June 2017:
  • Attempted $222,890,660
  • Returned/Frozen $74,831,206 (34%)
  • Unrecovered $148,059,454 (66%)
• Real estate
• Legal services
• B2B commerce
• Database and W-2 theft
- Targeted Connecticut schools
- Spoofed the email address of the superintendent, asked for all W-2 information for approximately 1,300 school district employees
- Approximately 100 suspicious Forms 1040 were filed electronically with the IRS in the names of victims, claiming tax refunds totaling $491,737
Targeted CEOs, CFOs, controllers and others at U.S. businesses

Sent dozens of e-mails to controller a local company, posing as the real CEO of the victim company

Instructed the controller to send multiple wire transfers exceeding a total of $1 million

Sent e-mails and attachments containing malware to the intended recipients
BUSINESS EMAIL COMPROMISES

• Immediately contact the bank and initiate a recall
• Highest success for recall of funds is within 48 hours
• File a complaint with IC3.GOV – Specify “BEC attack”
• IC3 has a 24/7 response that will activate a Financial Fraud Kill Chain (FFKC) which attempts to stop foreign wire/ACH transfers
• Contact your local FBI, Secret Service, or IRS
• Change email passwords and check for changes to your mailbox rules, such as Mail Forward, Delete, CC, or BCC
• Change all e-banking and pertinent passwords
• Increase user awareness – Alert employees
Phishing is defined as “A scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly”

– Merriam Webster

The difference between Phishing and Spear-Phishing is that a Phishing attack is widely targeted, like a fishing net. Whereas a Spear-Phishing attack is highly targeted at specific people and/or industries.
MALWARE

- Key loggers
- Screen shots
- Search for and copying of specific data
- Ransomware
Chinese government targeted Westinghouse, SolarWorld, U.S. Steel, and Alcolac to obtain confidential and proprietary technical, legal and business information

- Phishing email with malware to exfiltrate data
- Hop Points and IP traffic
Ransomware is a type of malicious software (malware) that blocks access to a victim’s data or threatens to publish or delete files or data until a ransom is paid. Examples include:

- CryptoLocker
- WannaCry
- Cerber
- Jigsaw
- LeChiffre
- GrandCrab

- CryptoWall
- CTB-Locker
- CrySiS
- KeyRanger
- Locky

- TeslaCrypt
- TorrentLocker
- ZCryptor
- GPCode
- Petya
Denialware is a type of malicious software (malware), identical in function to ransomware, that blocks access to a victim’s data and causes a Denial of Access (DoA) attack. A request to pay a ransom is intended to obscure the true purpose of the attack.
DDoS

- A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.
In 2012 and 2013, hackers associated with the Government of Iran conducted widespread denial of service attacks on the websites of nearly 50 U.S. banks, week-in, week-out, for months.

At their peak, those attacks disrupted customers’ ability to access their accounts online and conduct transactions and cost tens of millions to remediate.
PREVENTION

- Intrusion detection systems, data loss prevention technology – monitor and act on event logs
- Encryption (don’t store encryption keys with the data!)
- System administrators: different computers for sysadmin vs. routine work
- Increasing contractual requirements for cybersecurity protocols and controls
PREVENTION

- Limit administrator privileges and employee/contractor departure practices and procedures
- Training, drilling, and hiring
- Backup off the network
- Consider cyber insurance
- Patch patch patch!
PREVENTION

- Federal Cyber Task Force
- Initiated in October 2017
- FBI, HSI, DEA, USPS, DOD, DOT, and USSS
- 14 Local and State Law Enforcement Agencies
- Goals
AUSA Vanessa Richards
Deputy Chief
National Security and Cyber Crime Unit
Vanessa.Richards@usdoj.gov
(203) 696-3016