Current Trends in Cybercrime

SPECIAL AGENT PAUL BINGHAM
FBI—SALT LAKE CITY
Current Trends in Cybercrime

- Who are the actors?
- What are they doing?
- Why are they doing it?
- Where are they?
- How are they doing it?
Who are the actors?

- Low Tech Attackers/Script Kiddies
- Professional Hackers
- Organized Crime
- State-sponsored Groups/Terrorists
What are they doing?

- Low Tech Attackers/Script Kiddies
  - Phishing
- Professional Hackers
  - Hacktivism
  - Data Breaches
- Organized Crime
  - Ransomware
  - BEC Scams
- State-sponsored Groups/Terrorists
  - Secrets
Why are they doing it?

- Low Tech Attackers/Script Kiddies
  - Phishing - $$$
- Professional Hackers
  - Hacktivism – Political/Social Change
  - Data Breaches – Notoriety and $$$
- Organized Crime
  - Ransomware – $$$
  - BEC Scams – $$$
- State-sponsored Groups/Terrorism
  - Secrets – Intelligence, Political Advantage, $$$, World Domination
Where are they?

- Low Tech Attackers/Script Kiddies
- Professional Hackers
- Organized Crime
- State-sponsored Groups/Terrorists
Where are they?

- Low Tech Attackers/Script Kiddies
- Professional Hackers
- Organized Crime
- State-sponsored Groups/Terrorists
Where are they?

- Low Tech Attackers/Script Kiddies
- Professional Hackers
- Organized Crime
- State-sponsored Groups/Terrorists
Where are they?

- Low Tech Attackers/Script Kiddies
- Professional Hackers
- Organized Crime
- State-sponsored Groups/Terrorists
Where are they?

- Low Tech Attackers/Script Kiddies
- Professional Hackers
- Organized Crime
- State-sponsored Groups/Terrorists
How are they doing it?

- Phishing
  - Phishing kits on compromised servers
  - Phishing emails
- Social Engineering
- Office 365, banks, PayPal,
- Use harvested credentials to buy goods or transfer money
- Credentials often go to personal email address
How can you stop it?

- Phishing
  - Relies on human error
  - EDUCATE YOUR EMPLOYEES
  - Keep browsers updated
  - www.ic3.gov
How are they doing it?

- Hacktivism/Data Breaches
  - Generally more sophisticated than phishing
  - BUT, still uses EMAIL as Attack Vector
  - May employ social engineering techniques
  - Exploit vulnerabilities in hardware and software
    - Web Server
    - Mail Server
How can you stop it?

- Hacktivism/Data Breaches
  - Patch, Patch, Patch
  - Enforce Aggressive Password Policies
  - Enhance Early Detection
    - Threat Hunting
    - Auditing
      - Outbound Traffic Analysis
      - Host-to-Host Connections
    - Intrusion Prevention/Detection Systems
- Report to law enforcement
  - www.ic3.gov
  - FBI

www.ic3.gov
FBI
How can you stop it?

- Hacktivism/Data Breaches
  - Ensure/Harden Physical Access
  - Jackpotting
    - Malware: Ploutus-D
    - Vulnerability: Kalignite Platform
      - XP, Vista, 2000, NT
How are they doing it?

- Ransomware
  - Primarily malicious email links/attachments
  - Automated replication
  - Encrypt files/drives
  - Demand payment through cryptocurrency
  - If payment is received
    - Request more money
    - Decrypt data
      - Sometimes it works
How can you stop it?

- Ransomware
  - One word: BACKUP
  - Separate, physical device
  - Location which requires distinct login
  - Report to law enforcement
    - www.ic3.gov
    - FBI

GOT BACKUP?
How are they doing it?

- **BEC Scams**
  - Stolen credentials/phishing/malware/spoofed or similar email domain
  - Scan of compromised systems for invoicing/financial practices
  - Social media snooping or surveillance
  - Executive impersonation through email (phone or fax possible)
  - Instructions for payment
    - Sense of urgency
    - From upper management
    - Reason for deviation from normal procedures
How are they doing it? (cont'd)

- **BEC Scams**
  - Real Estate (any B2B commerce)
  - Use of money mules to obfuscate trail and move money forward
  - Wire trends
    - Hong Kong
    - HSBC
  - Losses
    - Global: >$12 Billion
    - US – 2017: $675 Million
    - Utah – 2017: ~$2 Million
    - Utah – 2018: >$20 Million
How can you stop it?

- **BEC Scams**
  - **Before:**
    - Consider Two-Factor Authentication for Email
    - Check email forwarding rules
    - Educate Accounts Payable personnel
    - Examine payment policies
  - **During:**
    - **VERIFY!!**
    - Call whomever instructed payment
    - Call vendor*
    - Verify changes to invoices, payment instructions, or contact information
    - Consider two-level approval for rush payments
How can you stop it? (cont'd)

- BEC Scams
  - After:
    - IMMEDIATELY CALL BANK and INITIATE SWIFT RECALL
  - Retain logs and data
  - Contact law enforcement
    - FBI
    - www.ic3.gov
  - Conduct cybersecurity assessment
HACKING 101: A Review

USERS

INFO TECH/
INFO SEC
InfraGard
Partnership for Protection

- Partnership between the FBI and private sector to protect our nation's critical infrastructure
- Expedites timely exchange of information & promotes mutual learning opportunities
- Representation from all sectors of infrastructure
InfraGard
Partnership for Protection

www.infragard.org
Special Agent Paul Bingham

FBI Salt Lake City
801-579-1400
plbingham@fbi.gov