Hot Topics in Law Enforcement

April 20, 2016

Presented by: Beth Ferrell

©Bradley Arant Boult Cummings LLP Attorney-Client Privilege.

Speakers

- Beth Ferrell, Partner and member of BABC’s Privacy and Information Security Team
- Scott Augenbaum, Special Agent, Federal Bureau of Investigation, Computer Intrusion/Counterintelligence Squad

Agenda

- Trends in Cyber Threats
    - Ransomware
    - E-Mail Extortion
    - Business E-Mail Account Compromise
    - Accessing Privileged Corporate Information to Facilitate Securities Fraud

- Trends in Information Sharing/Reporting

RANSOMWARE

- Malware that restricts access to infected computer system or device (such as mobile phone)
- Malware downloaded from infected advertisement, email (or attachment) or infected website
- Ransom demanded for removal of malware
- Impact:
  - Ransom fee
  - costs of network mitigation and countermeasures
  - loss of productivity
  - Legal fees

FBI Recommended Precautionary Measures to Mitigate Ransomware Threats

- Ensure anti-virus software is up-to-date
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser

E-Mail Extortion

- E-mail threatening DDoS (Distributed Denial of Service) attack
- FBI suspects multiple individuals are involved in these extortion campaigns.
- FBI predicts that the attacks are likely to expand to online industries and other targeted sectors, especially those susceptible to suffering financial losses if taken offline.
- FBI Tips:
  - Do not open e-mail or attachments from unknown individuals.
  - Do not communicate with the subject.
  - If an attack occurs, utilize DDoS mitigation services

Business E-Mail Account Compromise

- FBI reports business e-mail compromise is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments
- The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds
- The scam continues to grow and evolve and it targets businesses of all sizes
- There has been a 270 percent increase in identified victims and exposed loss since January 2015
- The scam has been reported in all 50 states and in 79 countries.
- Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong

FBI Reports Following Measures Being Used for Protection

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of *abc_company.com would flag fraudulent e-mail of abc-company.com*
- Register all company domains that are slightly different than the actual company domain
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign- off by company personnel
- Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request
- Know the habits of your customers, including the details of, reasons behind, and amount of payments
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary

Accessing Privileged Corporate Information to Facilitate Securities Fraud

- FBI reports that criminal actors are relying on computer intrusion techniques to collect material, nonpublic information (MNPI) from publicly traded companies
  - MNPI is information not generally disseminated to the public that a reasonable investor would likely consider important in making an investment decision
- Such information allows criminals to accurately predict impending movements in stock, commodity, or other investment prices
- Allows criminal actors to potentially earn significant returns on their investments at little monetary risk
- Traders seeking MNPI may hire cyber criminals who offer “hacker-for-hire” services via the cyber underground

FBI Recommended Precautionary Measures to Mitigate Computer Intrusion Threats

- Ensure anti-virus software is up-to-date
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software - especially free software - from sites you know and trust
- Enable automated patches for your operating system, Web browser, and associated Web browser plug-ins
- Disable macros. Be careful of pop-ups from attachments that require you to enable them.
- Monitor employee logins that occur outside of normal business hours
- Do not use the same login and password for multiple platforms, servers, or networks.
- Use two-factor authentication for employee logins, especially remote logins
- Create a centralized Information Technology email account for employees to report suspicious emails
- Provide regular training to remind and inform employees about current social engineering threats.
- Monitor unusual traffic, especially over non-standard ports
- Monitor outgoing data, and be willing to block unknown IP addresses
- Close unused ports
- Utilize a Virtual Private Network (VPN) for remote login capability

Trends in Information Sharing/Reporting

- DHS
  - Automated Indicator Sharing initiative
    - Implements Cybersecurity Information Sharing Act of 2015
- FBI
  - The FBI encourages public to report information concerning suspicious or criminal activity to their local FBI field office or the FBI’s 24/7 Cyber Watch (CyWatch).

Questions?

Elizabeth A. Ferrell
202.719.8260
bferrell@babc.com

Bradley