CYBER SECURITY SUMMIT MIDWEST REGION

NIFA JOSHUA SENEY (CID) – DETROIT FIELD OFFICE

TOPICS

- Current Trends
  - Business Email Compromise
  - Ransomware
  - COVID-19
  - General Prevention

BUSINESS EMAIL COMPROMISE (BEC)

- Phishing / Spear Phishing Attacks
- Malicious Software
- Brute Force Password Attacks
- Wire Transfer Fraud
- Compromise Email Chain / Account

RANSOMWARE

- Phishing / Spear Phishing Attacks
- Remote Access Brute Force
- Malicious Email Attachment
- Vender Network Compromise (Access to Victim's Network)
- Malicious Websites / Website Advertisement
- Ransom / Covering Tracks of Exfil of Data

LEVERAGE CURRENT GLOBAL TRENDS

- COVID19
  - Generates More Anxiety / Urgency
  - Wire Transfer Fraud / Forgery
  - Remote Workforce

- Does not have to be COVID19…
- NO ENTITY IS TOO SMALL OR LARGE OF A TARGET!

COVID19

- Mass email campaigns posing as medical / health organizations
- Malicious malware attachments
- Malicious internet links
- Charity scams for fraudulent entities
- Fraudulent equipment / test kits to prevent /detect COVID19

INFRASTRUCTURE

- Reliable / Secure VPN solution for remote workers
- Updates / Upgrades continually monitored
- Are Enterprise security standards enforced on remote connections
  - Employee provided an employer owned / secured device
  - Employee using their own devices which may not be secured or updated
  - How secured is the remote worker's home network
- 3rd Party Vender security / accounts – temp accounts or constant access

INFRASTRUCTURE

- Multi-Factor Authentication put into place
- Complex password requirements enforced
- Continued network monitoring – to include access and failed access
- Proper backup solutions put into place and monitored
  - Breach months prior to incident is your backup clean of malware or are you installing it again?
- Don't just restore a backup and forget to plug the vulnerability

THE EMPLOYEE

- Continuous training on threat environment for ALL employees regardless of role
  - Such as malicious attachments
  - Social Engineering attacks
- Continuous evaluation of employee operational security
- Open lines of communication with management / I.T.

THE EMPLOYEE

- Protocols in place for financial transactions
  - Do not reveal financial account / transfer information in emails
  - Voice confirmations
- Cultivate the ownership of security with employees
  - Reward system for employees who identify / report threats
- Pause before a click

RESOURCES

- www.secretservice.gov/contact/field-offices/ (United States Secret Service)
  - Chicago Field Office – 312-353-5431
  - Cleveland Field Office – 216-750-2058
  - Detroit Field Office – 313-226-6400
  - Indianapolis Field Office – 317-635-6420
- www.dhs.gov/be-cyber-smart (Department of Homeland Security)
- www.us-cert.gov (Cybersecurity & Infrastructure Security Agency)
- www.cisa.gov (Cybersecurity & Infrastructure Security Agency)