CYBER SECURITY SUMMIT
POWER HOUR
DC METRO
JULY 16, 2020

R. MATTHEW CHEVRAUX

CYBER OUTREACH

CRIMINAL INVESTIGATIVE DIVISION

UNITED STATES SECRET SERVICE

TOPICS

- Current Threat Trends
  - Recent COVID-19 Fraud Schemes
  - Ransomware/Extortionware
  - Business Email Compromise
- Defending Against the Threat (COVID-19 and Beyond)
- Information Sharing and Resources

THREAT ACTORS (A.K.A. CRIMINALS) LEVERAGE CURRENT GLOBAL TRENDS

- COVID-19
  - Generates More Anxiety / Urgency
  - Wire Transfer Fraud / Forgery
  - Remote Workforce
- Does not have to be COVID-19…
- EVERYONE IS A TARGET! – NO ENTITY IS TOO SMALL OR TOO LARGE

COVID-19 THEMED FRAUD

- Phishing and "Smishing" (SMS-phishing)
  - Various Pretexts (PPE, Stimulus Payments, Charity, Non-Delivery, Testing Kits)
- Stimulus Check Fraud
- SBA Loan Fraud: Paycheck Protection Program (PPP) & Economic Injury Disaster Loan Fraud (EIDL)
- Unemployment Compensation Fraud
- Money Mule Scams (It's probably too good to be true!)

RANSOMWARE/EXTORTIONWARE

- 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

BUSINESS EMAIL COMPROMISE (BEC)

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

BACK TO NORMAL? – STAY VIGILANT

DEFENDING AGAINST COVID-19 CYBER SCHEMES (AND OTHERS)

- Use caution with email attachments and beware of social engineering and phishing; “Think before you click”
- Use trusted sources such as legitimate government websites for current, fact-based information about COVID-19.
- Do not reveal personal or financial information in email and do not respond to email or text solicitations for this information.
- Buyer/User beware – Trust your instincts

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

INFRASTRUCTURE

- Reliable / Secure VPN solution for remote workers
- Updates / Upgrades continually monitored (BYOD concerns)
- 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

CYBER FRAUD TASK FORCES (CFTF)

FORMERLY ELECTRONIC CRIMES TASK FORCES (ECTF)

- 44 Worldwide (42 Domestic / 2 International)
- Trusted Partnerships Between Law Enforcement, Private Sector & Academia
- 4,000 Private Sector Partners
- 2,500 Federal, State, & Local Law Enforcement Partners
- 350 Academic Partners
- Coordinated Investigations, Information Sharing, Technical Expertise, and Training

RESOURCES

- United States Secret Service/Cyber Fraud Task Forces
  - www.secretservice.gov/contact/field-offices/
- Department of Homeland Security
  - www.dhs.gov/be-cyber-smart
- Cybersecurity & Infrastructure Security Agency
  - www.cisa.gov
  - www.us-cert.gov
- Small Business Administration
  - www.sba.gov