Emergency Management Council
Cyber Preparedness for Small and Medium-sized Businesses
February 1, 2018
Scope: This product is designed to provide an overview of Cyber threats targeting small-to-medium sized businesses and the resources available to those businesses.

Note: This information is the property of the Washington State Fusion Center and may be distributed to law enforcement officials, as well as to public and private sector stakeholders with a legitimate need-to-know. Further dissemination to authorized recipients is permitted without prior approval. Precautions should be taken to ensure this information is stored or destroyed in a manner that precludes unauthorized access.
Agenda

➢ Threat Actors
➢ Motivations
➢ Techniques
➢ Information They Want
➢ Dark Web
➢ Preparedness and Response Resources
➢ Final Thoughts
Cyber Threat Actors

➢ State-Sponsored
  • China
  • Russia – APT 28 Cyber Espionage (Sandworm)
  • North Korea
  • Syrian Electric Army (Propaganda)

➢ Hacktivists – Conduct criminal activity to further agenda
  • Anonymous Collective (DDoS)
  • Islamic Cyber Army

➢ “Script Kiddies”

➢ Criminals
Motivations

➢ Defacement

➢ Espionage – Competitive advantage
  • Nation/Company advancement

➢ Disruption – Nuisance, DDoS, or financially motivated (hostage)

➢ Financial
  • Laundering; Credential Theft; Ransomware; Underground Market (TOR)

➢ Inflict Damage and/or Casualties
  • Stuxnet
  • Black Energy - Ukraine Power Grid
Techniques

➢ DDoS/TDoS
  • Mirai Botnet – East Coast Internet of Things
  • IoTroop

➢ Doxxing
  • Publicly Releasing Personal Information

➢ Phishing
  • Sale of Credentials on Dark Web

➢ Compromise/Deface websites
➢ Ransomware
Attempts to lure a user to provide private information via:
- Email
- Fraudulent Website
- Telephone
➢ Locks computer, files, file names, etc.

➢ Requires ransom be paid usually within hours or days; otherwise, threatens to permanently delete files.

➢ Infected by opening malicious emails or visiting infected websites.

➢ Angler Exploit Kit – An exploitation machine that seeks out vulnerabilities on a user’s system.

Ransomware Hostage Rescue Manual

UNCLASSIFIED // TLP: WHITE
Business Email Compromise

➢ Email Spoofing
➢ Requests immediate action from finance dept.

➢ +1,300% increase in exposed losses since 2015
➢ 50 States – Hundreds of millions of dollars

Step 1: Identify a Target
Organized crime groups target U.S. and European businesses exploiting information available online to develop a profile of the company and its executives.

Step 2: Grooming
Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).
Perpetrators use persuasion and pressure to manipulate and exploit human nature.
Grooming may occur over a few days or weeks.

Step 3: Exchange of Information
The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer
Upon transfer, the funds are steered to a bank account controlled by the organized crime group.

Note: Perpetrators may continue to groom the victim into transferring more funds.

Business E-Mail Compromise Timeline
An outline of how the business e-mail compromise is executed by some organized crime groups.
What do they want?

- Credentials
  - Log-in username and password

- Money...from you
  - Ransom
  - Pay for Service

- Information
  - Medical Data
  - Personal Data
  - Financial Data
Deep and Dark Web

- 0-Day kits for sale
- Malware readily available
- Sell financial/medical information
- Silk Road/Marketplace
- Sell PII
- Illegal goods
Resources

- WSFC
- MS-ISAC
- USSS
- FBI
  - Infragard
- IC3
- DHS
- NIST Framework
NIST Framework

Latest Updates

- RFC comments received on Draft 2 of Framework Version 1.1 and the Roadmap are now being reviewed. All responses will be published publicly in the coming weeks. NIST appreciates your feedback and as always, any additional comments can be directed to cyberframework@nist.gov.

- Two December 2017 webcasts about Framework basics and the proposed updates to Framework and Roadmap are now available for playback.

- A mapping of the Framework Core to NIST SP 800-171 Revision 1 has recently been published. This can be found in Appendix D of the publication.

- A blog entry on protecting critical infrastructure has been posted. A Framework for Protecting our Critical Infrastructure.

https://www.nist.gov/cyberframework/industry-resources
C³ Voluntary Program

Resources for Small and Midsize Businesses (SMB)

Cybersecurity is critical to any business enterprise, no matter how small. However, leaders of small and midsize businesses (SMB) often do not know where to begin, given the scope and complexity of the issue in the face of a small staff and limited resources.

To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks.

C³ Voluntary Program SMB Toolkit

This packet contains resources specially designed to help SMBs recognize and address their cybersecurity risks. Resources include talking points for CEOs, steps to start evaluating your cybersecurity program, and a list of hands-on resources available to SMB.

1. Toolkit for Small and Midsize Businesses (SMB) Table of Contents
2. Begin the Conversation: Understanding the Threat Environment
3. Getting Started: Top Resources for SMB
4. Cybersecurity for Startups
5. C³ Voluntary Program Outreach and Messaging Kit
6. SMB Leadership Agenda

Stop, Think, Connect, Toolkit

The Stop, Think, Connect™ campaign has an online Toolkit that includes information specific to SMBs. The Toolkit can be found at http://www.dhs.gov/stophinkconnect-toolkit or www.stctguide.com.

Small Business Administration (SBA) Training

https://www.us-cert.gov/ccubedvp/smb
Cybersecurity

Is your business prepared in the event of a cybersecurity breach? Now is the time to take stock of your cybersecurity health, including the importance of securing information through best cybersecurity practices; identifying your risk and the types of cyber threats; and learning best practices for guarding against cyber threats.

Introduction to Cybersecurity
Small employers often don’t consider themselves targets for cyberattacks due to their size or the perception that they don’t have anything worth stealing. However, small businesses have valuable...

Top Ten Cybersecurity Tips
Cybersecurity threats are real and small businesses are often an attractive target. As a small business owner, it’s critical to implement the best tools and tactics you can to protect your...

Protect Against Ransomware
Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered...

Top Tools and Resources for Small Business...
Where can you go to get trusted information about cybersecurity risk and mitigation that addresses the unique needs of small business owners? This targeted list of federal and local resources can...

Social Media Cyber-Vandalism Toolkit
Developed by the SBA in conjunction with the US General Services Administration’s SocialGov program, the Social Media Cyber-Vandalism Toolkit provides guidance and security practices to small...

Additional Cybersecurity Resources
Are you prepared for the shift to more secure card payments technology that took place on October 1st? Looking for trainings and professional certifications or other cybersecurity resources? Check...

https://www.sba.gov/managing-business/cybersecurity
Final Thoughts

➢ Threat actors will continue to seek vulnerabilities = PATCH!

➢ Employees will continue to click on links to get a “Free iPad”

➢ Have a policy in place to verify wire transfer requests

➢ Practice good cyber hygiene
  • Change default username and passwords
  • Use strong passwords and a password manager
  • Use multi-factor authentication

➢ Routinely backup data
QUESTIONS ?