CYBER THREAT TRENDS

KEVIN ANDERSON, CYBER SECURITY MANAGER
OCTOBER 31, 2019

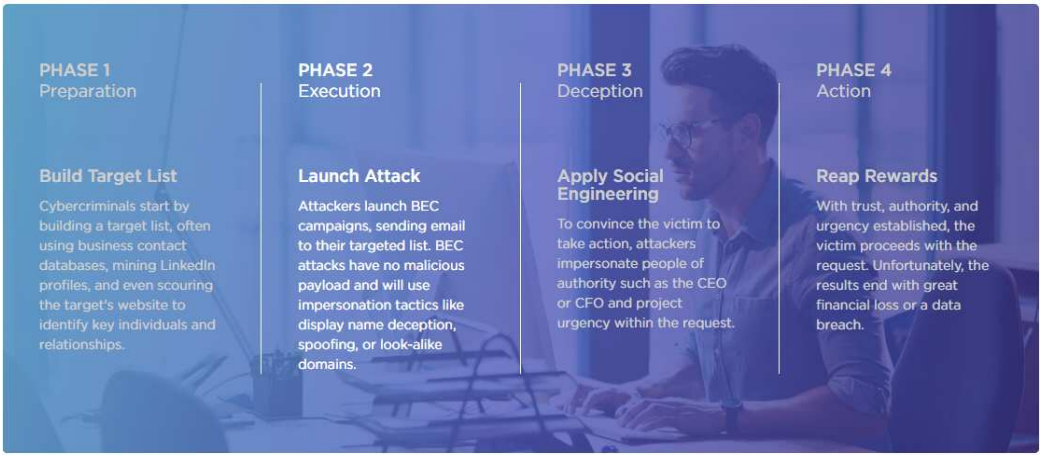
AssociatedBank

2019 THREATS

- Nation State
  - Focused on stealing intellectual data and creating collateral damage
  - Advanced Persistent Threat groups
- Organized Crime
  - Multiple organized groups working in unison for financial gain
  - Silence
    - Focused on attacking banks
  - Shadow brokers
    - Selling stolen cyber attack tools
- Data from past breaches being used for new scams.
  - Banking fraud
  - Credit fraud

2

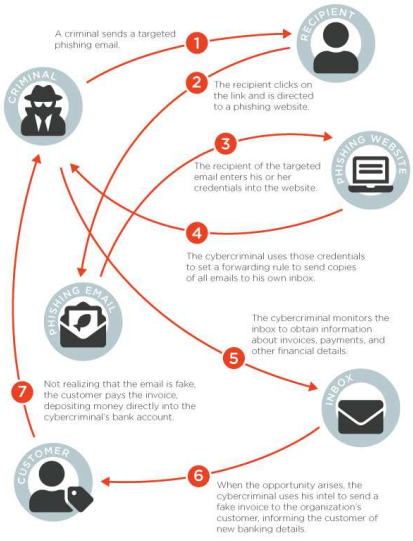
BUSINESS EMAIL COMPROMISE



https://www.agari.com/solutions/business-email-compromise/

3

VENDOR EMAIL COMPROMISES



https://www.agari.com/email-security-blog/silent-starling-vendor-email-compromise/

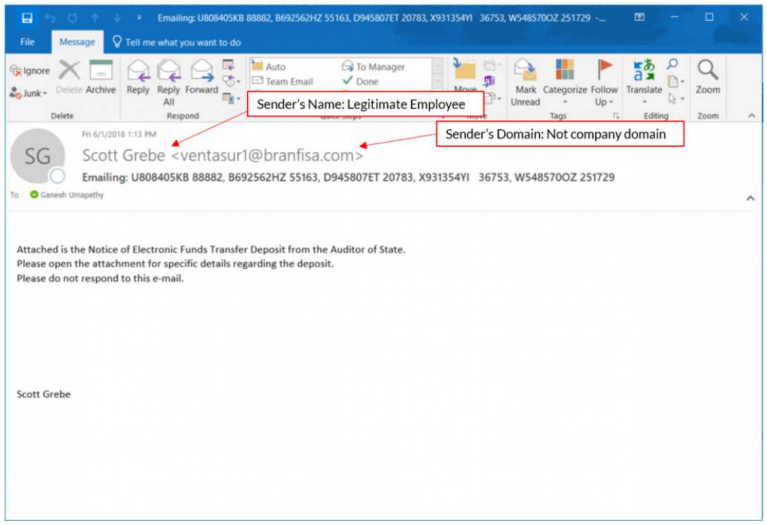
4

BEC\VEC BEST PRACTICES

- If something seems odd or out of place with an email you receive call the person who sent it.
- Disable any old or unused business or personal email accounts
- Routinely review email inbox settings for unauthorized installation of email rules to auto-forward or delete emails
- Enable Multi-Factor Authentication for all email accounts to defend against unwanted intrusion
- Call vendors if there is a request for change in bank account information
- Establish a user awareness program to educate users for cyber related attacks such as phishing.

5

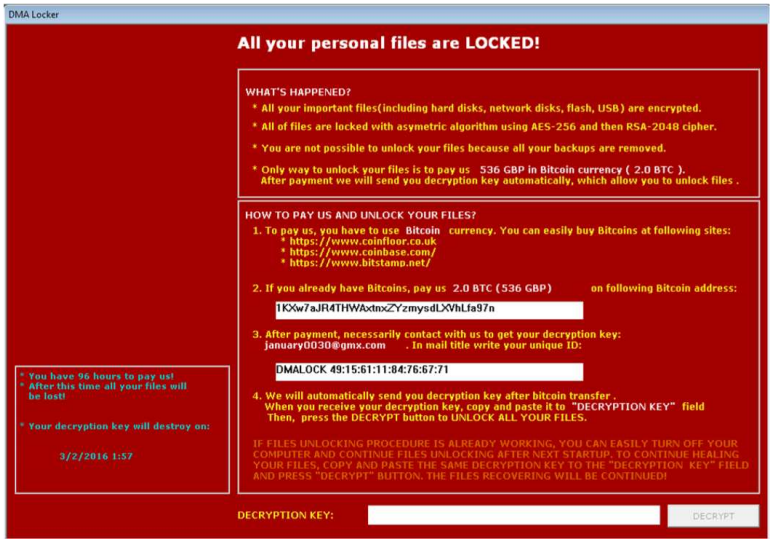
BEC EXAMPLE



https://blog.sonicwall.com/en-us/2018/08/report-business-email-compromise-bec-now-a-12-5-billion-scam/

6

RANSOMWARE



7

RANSOMWARE BEST PRACTICES

- Paying Ransom does guarantee the organization will regain access to their data.
  - Some organizations were never provided the decryption keys
  - Others were continually extorted
- Typically ransomware attacks are the results of gaps in security controls.
  - Backups are critical in regaining the data.
- Ensure software and windows patches have the latest applied.
- User awareness is crucial.
  - Majority of ransomware attacks are done by Phishing

8

CRITICAL TOP 20 CONTROLS

CIS Controls™ V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

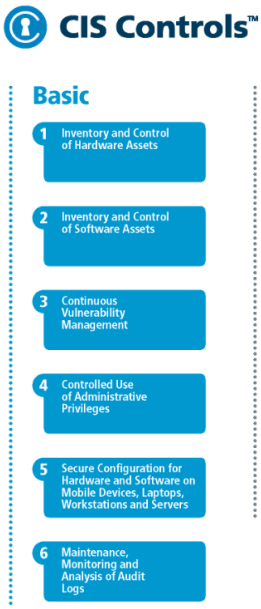
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/

9

CONTROLS 1-6

- Focus on the basics.
- Keep an asset inventory of hardware and software.
- Keep your operating systems up to date with patches.
- Have a vulnerability scan run on your network.
- Limit administrative access.to only those that truly need it.
- Remove unneeded software from company operating systems and mobile devices.
- Setup alerting for anti-virus software and other security applications you may have.



10

THANK YOU.

AssociatedBank

IMPORTANT DISCLOSURES

Investments, securities and insurance products:

NOT FDIC INSURED	NOT BANK GUARANTEED	MAY LOSE VALUE	NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY	NOT A DEPOSIT

SECURITIES AND ADVISORY SERVICES ARE OFFERED BY ASSOCIATED INVESTMENT SERVICES, INC. ("AIS"), member FINRA and SIPC, d/b/a Associated Investment Services Group in Minnesota. Insurance products are offered by licensed agents of Associated Financial Group, LLC (d/b/a Associated BRC Insurance Solutions in California). **The financial consultants at Associated Financial Group are registered representatives with, and securities and advisory services are offered through LPL Financial "LPL", a registered investment advisor and member FINRA/SIPC.** Associated Financial Group uses Associated Benefits and Risk Consulting ("ABRC") as a marketing name. Investment management, fiduciary, administrative and planning services are provided by Associated Trust Company, N.A. ("ATC"). Investment management services are also provided to ATC by Kellogg Asset Management, LLC® ("KAM"), a SEC-registered investment advisor. AIS is an affiliate of Associated Banc-Corp ("AB-C"). LPL is NOT an affiliate of either Associated Bank, N.A. ("AB") or AB-C. ABRC and ATC are wholly owned subsidiaries and affiliates of AB. AB is a wholly-owned subsidiary of AB-C. KAM is a wholly owned subsidiary and affiliate of ATC. AB-C and its affiliates do not provide tax, legal or accounting advice. Please consult with your tax, legal or accounting advisors regarding your individual situation. Associated Bank is a marketing name AB-C uses for products and services offered by its affiliates.