United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO BUSINESS EMAIL COMPROMISES

Business Email Compromise (BEC) is a sophisticated fraud scheme targeting businesses that use wire transfers as form of payment. The BEC scheme affects large global corporations, governments, and individuals, with current global daily losses estimated at approximately $8 million. Specific vulnerable sectors are real estate, finance, education, healthcare, and information technology.

Criminals compromise legitimate business email accounts through various hacking schemes, to include social engineering and the use of malware. Once a business email account is compromised, a fraudulent email is sent directing the recipient of the email to unwittingly transfer funds to an illicit account. Criminals obtain and use privileged information to convince BEC email recipients that the transfer instructions are legitimate.

PREVENT

Register all similar domain names that can be used for spoofing attacks.

Create rules that flag and delineate emails received from unknown domains.

Monitor and/or restrict the creation of new email rules within the email server environment.

Enable multi-factor authentication.

Conduct BEC drills, similar to anti-phishing exercises.

Educate employees, clients, and vendors to:

Authenticate all financial transactions through dual-factor authentication.

Confirm all payment method changes using trusted and authenticated information.

Learn the habits of those with whom they conduct financial transactions.

MAIL AUTO FORWARDING

A criminal logs in to a compromised email account just once to set up an auto forward inbox rule to forward emails to their own email address.

This rule will remain in effect even if a password is changed.

WARNING SIGNS

Urgency of Request: A request to transfer funds is sent with a pronounced sense of urgency.

Different Domains: Email communication originates from unknown or spoofed domain.

Out of Contact: Requestor is unreachable, but insists on the urgency of the transfer.

Language and Grammar: Syntax is different or erroneous.

Multiple Emails: Multiple recipients receive emails requesting transfer of funds.

Incorrect Context: Emails are not in the standard context normally encountered or for alternate business purposes while requesting a transfer of funds.

Secrecy: Email sender requests that information about transfer be kept secret.

RESPOND

Time is money! An immediate response is crucial, funds are moved within minutes of a BEC incident.

Contact your bank to reverse the wire, for hold harmless and indemnification.

Contact local law enforcement to request a report, which is needed to reverse a wire.

Contact a Secret Service field office Cyber Fraud Task Force.

Law enforcement can work with FinCEN to initiate Financial Fraud Kill Chain.

File a complaint with the Internet Crime Complaint Center (IC3).

Review email systems for unauthorized access or rule creation.

Conduct a cyber security analysis on your systems.

Change all login credentials.

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO RANSOMWARE

PREPARE

What is Ransomware:

Ransomware is a type of malicious software (malware), which denies access to systems or data and/or exfiltrates data.

How Ransomware Works:

Typically, the malware displays an on-screen alert advising the victim that their device is locked or their files are encrypted. In some cases, after an initial infection, ransomware attempts to spread to connected devices and systems.

Characteristics:

Non-encrypting ransomware locks the screen and restricts access to files.

Encrypting ransomware prevents computers from being booted up in a live environment by encrypting the Master Boot Record (MBR).

Leakage or "extortionware" exfiltrates data.

Mobile device ransomware infects cellphones through drive-by downloads or fake apps.

How Ransomware is Used:

Cyber actors hold systems or data hostage until a ransom is paid for a decryption key. Cyber actors also threaten to publish exfiltrated data, or sell it on the dark web. Increasingly, cyber actors request virtual currency transfers as a ransom payment method.

Incident Response (IR) Planning:

The U.S. Secret Service developed a Preparing for a Cyber Incident - Introductory Guide, which describes what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations.

Paying Ransom Demand:

Paying the ransom does not guarantee regaining access. In some cases, a decryption key was not provided in return to a paid ransom. In other cases additional ransom was demanded.

Contacting Law Enforcement:

Reach out to law enforcement before contacting the cyber actor. Include law enforcement in your response plan. Contact the local U.S. Secret Service Cyber Fraud Task Force.

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO RANSOMWARE

PREVENT

Patches
Update operating systems, software, and firmware on devices with the latest patches. Consider using a centralized patch management system.

User Permissions
Restrict user permissions for installing and running software applications. Apply the principle of least privilege to all systems and services.

Email Scanning
Scan all incoming and outgoing emails to detect and filter threats, such as phishing and spoofing emails, and executable files (used to perform various functions or operations on devices). This will prevent them from reaching end users.

Firewalls
Configure your firewalls to block access to known malicious IP addresses.

Application Whitelisting
Use application whitelisting to reduce the risk of execution of malware, and unlicensed and unauthorized software. An application whitelist is a list of applications and application components that are authorized to execute on a host.

Awareness
Implement a training and awareness program for all employees.

Controls
Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations (temporary folders supporting popular Internet browsers, compression/ decompression programs).

Remote Access
Consider disabling Remote Desktop Protocol (RDP) if it is not being used.

Virtualization and Separation
Execute operating system environments or specific programs in a virtualized environment (multiple simulated environments). Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

Backups
Have cold storage backups and test restoration of backup files regularly. This prevents the ransomware from infecting network-connected backup files.

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO RANSOMWARE

RESPOND

A. Do not power down or shutoff any systems affected by ransomware.

B. Isolate the infected device and the compromised portion of your network as soon as possible.

C. Secure backups by taking them offline and ensure they are free of malware.

D. Use out-of-band methods of communication, and do not trust the entire network system.

E. Collect and secure partial portions of the ransomed data that might exist.

F. Collect all available log information.

G. Change online account and network passwords after removing the system from the network.

H. Use the oldest back-up to restore the system, if you have multiple backups.

IDENTIFY AND RECORD THE FOLLOWING INFORMATION:

- ✓**Ransomware variant name.**
- ✓**What systems are affected.**
- ✓**Original emails with full headers and any attachments, if attack was executed by phishing.**
- ✓**Copies of executables or other files dropped onto the system after accessing malicious attachments, including a splash page.**
- ✓**Any domains or IP addresses communicated with just prior to or during infection.**
- ✓**Virtual currency addresses to which payment is requested, and the amount being requested.**
- ✓**Any forensic analysis or incident response reports completed.**
- ✓**Any memory captures taken during execution of the malware.**
- ✓**Status of the infection.**
- ✓**Provide network topology.**

Contact the local U.S. Secret Service

Cyber Fraud Task Force Network Intrusion Team

www.secretservice.gov

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

E-SKIMMING

Online shopping has steadily increased in recent years, which has led to an upsurge in e-Skimming. E-Skimming poses a threat to U.S. businesses, consumers, and the financial sector.

What is e-Skimming

Cybercriminals introduce malicious code on e-commerce payment card processing web pages with the intent to capture personally identifiable information (PII) and payment card industry (PCI) data. Cybercriminals then send the stolen data to network domains under their control.

How e-Skimming Works

Malicious code can be introduced through exploiting vulnerabilities on website e-commerce platforms, or by gaining access to networks. Malicious code signatures known to law enforcement are highly variable and are increasingly difficult to detect.

Who is at Risk

Businesses accepting online payments on their websites and third-party vendors who provide online advertisements and web analytics on payment processing platforms.

HOW TO PROTECT FROM E-SKIMMING

Software and Antivirus Updates: Install operating system and network software patches, firmware updates, and antivirus definitions as soon as they are available. Discontinue the use of outdated, unsupported operating systems.

Account Passwords: Immediately change factory preset passwords, change passwords regularly, and use different passwords for each system and account. Utilize multi-factor authentication and offer multi-factor authentication to customers.

Network Segmentation: Segregate payment system processing from other network applications, proper network segmentation and segregation lessens the network exposure.

Firewalls, Intrusion Prevention and Detection Systems: Use firewalls, properly configure and monitor intrusion prevention and detection systems for added defense.

Remote Access: Limit network remote access when and where possible. Always secure remote access and monitor for unusual activity to reduce risk. Identify a baseline of remote access activity for reference.

Backups: Have cold storage backups and test restoration of backup files regularly.

Online Payments: Utilize Payment Card Industry Data Security Standards (PCI DSS) for online transactions, to include encrypting (SSL encryption) customer PCI data being stored, processed, or transmitted. Verify card holder address and require Card Verification Value (CVV) code to help authenticate and validate card holder information.

Monitor: Implement software code integrity checks by scanning the payment website for irregularities within the software code (JavaScript). Monitor and analyze web logs.