SERIANU

Serianu Cyber Security Advisory

Business Email Compromise

Serianu SOC Advisory Number:
TA – 2020/024

Date(s) issued:
8th December, 2020

System Affected:

- Emails

Overview:

The COVID-19 pandemic prompted a mass shift to remote working among many businesses, resulting in increased usage of web-based email applications. Malicious attackers are taking advantage of the increased number of people working remotely by successfully compromising the business email.

This advisory contains an overview of the Business compromise email threat, recommended mitigations and is being issued to assist cybersecurity professionals, IT and managers guard against the persistent malicious actions of cyber-threat actors.

Threat Overview

Business Email Compromise (BCE) also known as Email Account Compromise (EAC) is a security exploit in which an attacker hacks into a corporate e-mail account and impersonates the real owner’s identity in order to defraud the company or an employee into sending money in accounts owned by the criminals. In most occasions, attackers will focus on the employees with access to company finances and attempt to trick them into performing wire transfers (electronic funds transfer from one bank to another) to bank accounts thought to be trusted, when in reality the money ends up in the attackers account. A cybercriminal initially compromises a business email account through social engineering or computer intrusion techniques.

According to our research, BEC scam starts with reconnaissance. An attacker gathers information about a target organisation through publicly available sources like website, press releases and social-media posts. They then look for names and official titles of company executive's, corporate hierarchy, emails and phone numbers. Using information gathered from the compromised accounts and reconnaissance efforts created by system access following the initial intrusion, the cybercriminal then impersonates an employee over email communications to redirect pending or future payments to fraudulent bank accounts.

BEC actors create auto-forwarding rules (forwarding messages to another account) within email accounts after they obtain employee credentials to decrease the victims' ability to observe fraudulent communications. After obtaining access to a victim's email account, cyber criminals update the auto-forwarding email rules in the web-based client. If administrators do not actively sync their web and desktop email clients, the auto-forwarding rules may only appear in the web client, limiting the rules' visibility to security administrators.

While IT personnel traditionally implement auto-alerts through security monitoring appliances to alert when rule updates appear on their networks, such alerts can miss updates on remote workstations using web-based email. If businesses do not configure their network to routinely sync their employees' web-based emails to the internal network, an intrusion may be left unidentified until the computer sends an update to the security appliance set up to monitor changes within the email application.

This leaves the employee and all connected networks vulnerable to cyber criminals. Even after a financial institution or law enforcement contact warns a victimized business of a potential BEC, a system audit may not identify the updated email rules if it does not audit both applications, increasing the time a cyber-criminal can retain email access and continue BEC activity. Cyber criminals may also use auto-forwarding rules to delete records from the recycle bin to further hide their activities.

Techniques of Business Email Compromise

1. **Spoofing email accounts and websites:** Creation of email messages with a forged sender address or forged website. Legitimate addresses vs fake email (aaa.bbb@abccompany.com vs. aaa.bb1@abccompany.com)

2. **Spear-phishing:** Email scam targeted towards a specific individual, organisation with an intention to steal data for malicious purposes or to install malware on a victim's computer.

3. **Malware:** Malicious software that could be used to gain access to internal data and systems, in order to view legitimate email regarding the finances of the company. That information is then used to avoid raising the suspicions of any financial officer when a falsified wire transfer is submitted.

Types of Business Email Compromise

1. **False Invoice Scheme:** Organisations with foreign suppliers are often targeted with this tactic, where attackers pretend to be the suppliers requesting fund transfers for payments to an account owned by fraudsters.
2. **CEO Fraud:** Attackers pose as the company CEO or any executive and send an email to employees in finance, requesting them to transfer money to the account they control.
3. **Account Compromise:** An executive or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.
4. **Attorney Impersonation:** An attacker will impersonate a lawyer or other representative from the law firm responsible for sensitive matters. These types of attack often occur through email or phone.
5. **Data Theft:** HR will be targeted in order to obtain personal or sensitive information about the employees or executives. This data can be very helpful for future attacks.

Recommendations

Serianu recommends organisations to:

1. Ensure both the desktop and web applications are running the same version to allow appropriate syncing and updates.
2. Be wary of last minute changes in established email account addresses.
3. Carefully check email addresses for slight changes that can make fraudulent addresses appear legitimate and resemble actual clients' names.
4. Enable multi-factor authentication for all email accounts.
5. Prohibit automatic forwarding of email to external addresses.
6. Frequently monitor the Email Exchange server for changes in configuration and custom rules for specific accounts.
7. Create a rule to flag email communications where the "reply" email address differs from the "from" email address.
8. Add an email banner to messages coming from outside your organization.
9. Consider the necessity of legacy email protocols such as POP, IMAP, and SMTP that can be used to deceive multi-factor authentication.
10. Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
11. Enable security features that block malicious email such as anti-phishing and anti-spoofing policies

12. Encourage employees to request clarification of suspicious payment requests to their management prior to authorizing transactions.

Conclusion

Corporate email security is an extremely important component. A compromised email can seriously damage business reputation and interests. Securing a company’s finances and privacy will not only empower employees but also ensure business to thrive.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to email related attacks to share it with us through our email info@serianu.com to allow us to analyze any indicators of compromise (IOC).