SEQURETEK

BEC SCAMMERS EXPLOITING EMAIL AUTO-FORWARDING RULES

OVERVIEW

Business Email Compromise (BEC) scammers are exploiting web-based email clients' auto-forwarding rules to intersect financial transactions.

The web-based client's forwarding rules often do not sync with the desktop client, limiting the rules' visibility to cyber security administrators. Cyber criminals then capitalize on this reduced visibility to increase the likelihood of a successful business email compromise (BEC).

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
8th Dec 2020	v 1.0	Vidhi Patel	Cdr. Subhash Dutta

OVERVIEW

- BEC (**Business Email Compromise)** scams are also known as Man-in-the-Email scams.
- In these scams, the attackers get unauthorised access to a legitimate business email account or create a spoof account with an almost identical corporate email address to conduct unauthorized fund transfers.
- This scam technique is also used to steal employee's personal information, salary and tax forms.

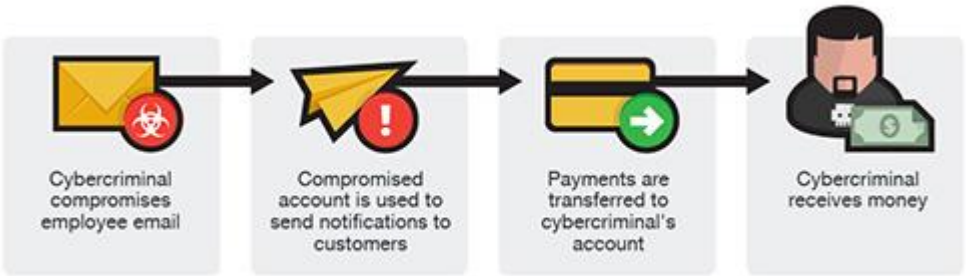

Figure 1: BEC scams

- The FBI has released a Private Industry Notification warning that cyber threat actors are **exploiting email forwarding rules** to **evade detection while conducting BEC attacks.**
- The attackers are setting email forwarding rules on web-based email clients. If the company admins have **not synced email settings for web-based email accounts and desktop clients, the forwarding rule changes could go unnoticed.** This leaves the employee and all connected networks vulnerable to attackers.

TECHNICAL DETAILS

- Attackers initially compromises a business email account and steals the username and password through social engineering or computer intrusion techniques. After initial access they try and establish a persistence mechanism to stay in or get back in after they are discovered and removed.
- To get compromised email account insight, attackers **alter the auto-forwarding rules of the victim's web-based client to send any inbound communications to their own attacker-controlled email addresses.**
- Attackers can also create email forwarding rule with an email containing keywords like "bank"," receipt", "payment", "wire", "check" and "invoice" are automatically sent onto the attacker's inbox. They can then monitor communications between that employee and other users, and delete certain emails to hide their activity.

- At last, attacker steps into conversations involving vendor payments and other financial transactions, pretending to be a legitimate contact such as a supplier, and sends a fake invoice or similar to be paid by the employee's company in order to perform a BEC scam.

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- Back-up data, store it outside of network connection.
- Update your Operating system and software to latest version.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Use strong email account password and change it at regular interval. Use multi-factor authentication.
- Do not open links and attachments from untrusted sources.
- Do not provide User ID and password on any page that appears when you click on some link received through email.
- Do not trust emails from untrusted source.
- Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
- Keep a check on bank transfer activity from own accounts regularly.
- Carefully check email addresses for slight changes that can make fraudulent addresses appear legitimate and resemble actual clients' names.
- Ensure the organization is running the same version of desktop and web applications for email to allow appropriate synching and updates.
- Be wary of last minute changes in established email account addresses.
- Prohibit automatic forwarding of email to external addresses.
- Frequently monitor the Email Exchange server for changes in configuration and custom rules for specific accounts.
- Configure Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent spoofing and to validate email.
- Consider the necessity of legacy email protocols, such as POP, IMAP, and SMTP, that can be used to circumvent multi-factor authentication.

- Create a rule to flag email communications where the "reply" email address differs from the "from" email address.
- Add an email banner to messages coming from outside your organization.
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Encourage employees to request clarification of suspicious payment requests to their management prior to authorizing transactions.
- Manually examine the rules for each mailbox.
- Look for rules that the user did not create, or any unexpected rules or rules with suspicious names.
- Look in the rule description for rule actions that start and application or refer to an .EXE, .ZIP file or to launching a URL.