United States Secret Service [INFO]

January 24, 2019

[INFO] Information Only Alert – GIOC Reference #19-001-I
TLP Green

Newest Trends in Business Email Compromise Matters

BEC attacks have evolved over the last couple of years from sending phishing emails to millions of targets, to sending spear phishing emails to a few hundred. The latest trend the USSS has identified is a focus on healthcare, professional services, higher education and real estate closing companies. The spear phishing is targeting individuals that are involved with a company's financial decisions with the intention of compromising that corporate officer's email account. The attackers are focusing specifically on Office 365 as many of the security features that product offers are turned off by default.

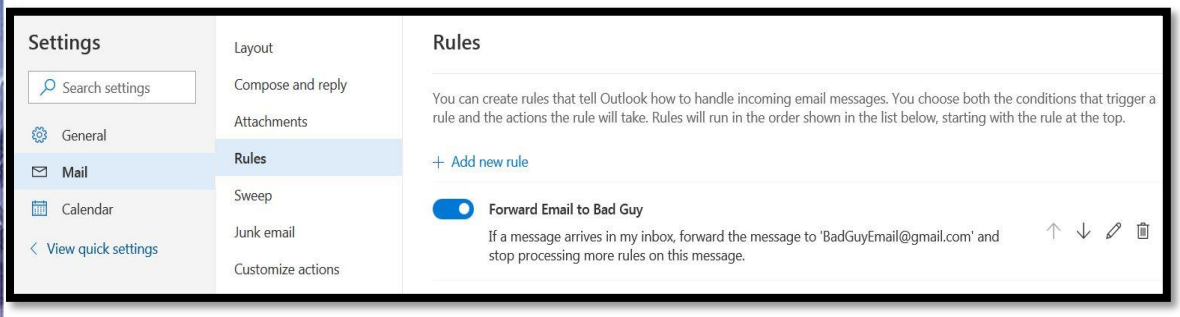
The spear phishing email will appear to be an email link to an encrypted document. Once the user clicks on that link, it will ask for their user credentials for Office 365 which is a cloud-based software service. Once the user enters their credentials, the attacker captures their user/password and will then have access to their Outlook email account without installing malware or remote software on their computer. Here is an example of the fake login request:

Once the account is compromised, the attacker views the inbox and sent messages, which may include invoice forms, to gather intelligence about the flow of money during legitimate business transactions.

The attacker will then change the mail rules associated with the victim's email account. Here are examples of some mail rules that are being changed:

[INFO] - Indicates informational or educational content.

- *Inbound/Outbound email forwarded:*
  - The attacker will have emails forwarded to their own email account to gain real time intelligence on the compromised user, customers, other employees, vendors, etc.
  - Alternatively, attackers are forwarding emails with key subject lines that they are interested in.
  - Once sufficient Intel is gathered, there are a few attack methodologies USSS has observed. For example:
    - Attacker logs into the compromised account and sends spear phishing emails to other victims to compromise or have them forward money to the attacker's bank account
    - The attacker creates an email account that appears to be from the compromised user (example: JohnDoeUSFinancial@gmail.com) and sends the BEC email having money transferred to another account



- *Move Emails:*
  - Similar to email forwarding, attackers will move emails to the Notes, Junk Email, or RSS Subscriptions folders.

- *Change Privileges:*
  - If the attacker compromises an admin account, they will elevate the privileges of a compromised user so they can read emails from an admin account.

- *Delete Emails:*
  - Attackers have also been known to create a rule to delete inbound emails from certain email accounts (other possible phishing victims, banks, etc.), so the user is not alerted that his/her email account has been compromised.

Remediation:[1]

Below are tips to follow once a company suspects or confirms that it has been a victim of a BEC:

[1] https://docs.microsoft.com/en-us/office365/securitycompliance/responding-to-a-compromised-email-account

1. ***Block the User/Attacker from Signing-in:***
    a. Open the "Office 365 Admin Center" -> "Users"
    b. Select the employee that you want to block, and then choose "Edit" next to "Sign-in Status" in the user pane
    c. On the "Sign-in status" pane, choose "Sign-in blocked" and then "Save"
    d. In the "Office 365 Admin Center", in the lower-left navigation pane, expand "Admin Centers" and select "Exchange"
    e. In the "Exchange Admin Center", navigate to "Recipients" -> "Mailboxes"
    f. Select the user, and on the user properties page, under "Mobile Devices", click "Disable Exchange ActiveSync" and "Disable OWA" for Devices and answer "Yes" to both
    g. Under "Email Connectivity", "Disable" and answer "Yes".

2. ***Remove the Compromised Account From All Admin Groups:***
    a. Sign in to the "Office 365 Admin Center" with a global administrator account and open "Active Users"
    b. Find the suspected compromised account and manually check to see if there are any administrative roles assigned to the account
    c. Open the "Security & Compliance Center"
    d. Click "Permissions"
    e. Manually review the role groups to see if the suspected compromised account is a member of any of them. If it is:
        i. a. Click the role group and click "Edit Role Group"
        ii. b. Click "Chose Members" and "Edit" to remove the user from the role group
    f. Open the "Exchange Admin Center"
    g. Click "Permissions"
    h. Manually review the role groups to see if the suspected compromised account is a member of any of them. If it is:
        i. a. Click the role group and click "Edit"
        ii. b. Use the "Members" section to remove the user from the role group

3. ***Reset Password:***
    a. Have the admin reset the password for the compromised user account.
    b. Make sure the admin does not email the new password to the user account.
    c. At this point, **Multi-Factor Authentication** is highly recommended.

4. ***Remove Email Rules:***
    a. Open the "Office 365 Admin Center" -> "Active Users"
    b. Review the compromised email account and expand "Mail Settings"
    c. Look for "Email Forwarding", click "Edit" and remove any suspicious forwarding addresses

5. ***Review Email Inbox Rules:***
    a. Log into the compromised account, click settings (the gear icon at the top) and then click "Mail"
    b. Click "Inbox and Sweep Rules" and review the rules
    c. Delete any suspicious rules

Once the compromised account is secured, the victim company should have the user of the compromised account perform a virus scan. Once the scan is complete, allow the user to log into their account.

Other Remediation Steps:

- As of October 2018, a security update patch for Office 365 now enables logs by default, but it is worth mentioning to the victims to check their logs – both global and account-based. Make sure that Audit Logging is turn on.
- The admin should disable automatic email forwarding. If the company is not able to disable email forwarding on all email accounts, then they should monitor the email forwarding rules by reviewing audit logs.
- The admin should fine tune the threat management policies in the Office 365 Security and Compliance Center. The Security and Compliance Center includes reports and dashboards that you can use to monitor users' settings.
- Companies that receive BEC emails should preserve the emails to provide to investigators for header information- even if the attack was unsuccessful.

Other Trends:

Attackers have been instructing victims to transfer money to bank accounts that have been opened by victims of romance schemes. Once the money reaches the romance scheme victim, the attacker requests that the money is used to purchase gift cards (Green Dot, Visa, Master Card, etc.) The gift card account numbers are then sent to the attacker.

Any questions relating to this alert can be directed to the GIOC at gioc@usss.dhs.gov or 202-406-6009.