Information Notice

Cybersecurity Alert: Cloud-Based Email Account Takeovers

October 2, 2019

Suggested Routing

- Compliance
- Information Technology
- Legal
- Operations
- Registered Representatives
- Risk
- Senior Management

Key Topics

- Cybersecurity
- Fraud
- Email Account Takeovers

Summary

Several member firms recently notified FINRA that they have experienced email account takeovers (ATOs) while using cloud-based email platforms, including Microsoft Office 365 (O365). Attackers used compromised email accounts to defraud member firms by requesting fraudulent wire requests or stealing confidential firm information or non-public personally identifiable information (PII).

This *Notice* outlines the attackers' tactics in executing ATOs, as well as steps taken by member firms to address ATO risks when using cloud-based email systems.

Questions concerning this *Notice* should be directed to:

- David Kelley, Surveillance Director, at (816) 802-4729 or *David.Kelley@finra.org*.

Background and Discussion

During the past six months, several member firms have notified FINRA staff that they have experienced ATOs, primarily on the O365 email platform. A large number of firms have migrated to cloud-based email platforms in the past 12 to 18 months, or plan to do so in the near future, so attackers may be intentionally targeting these firms to take advantage of weaknesses in their access and other controls.

FINRA reminds member firms that, under the U.S. Securities and Exchange Commission's Regulation S-P, they are required to have policies and procedures that address the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.

Attackers have executed email ATOs at member firms using techniques such as:

- phishing emails that impersonated support personnel requesting log-in credentials;
- credential stuffing, where the attackers automatically enter previously breached credentials into various websites and applications until they successfully match to an existing account;
- stolen passwords from a user's personal email account; and
- "brute-force attacks," where the attackers submit a large number of potential passwords until one of them works.

After gaining access to an email account, attackers typically monitor the account over several weeks or months to:

- observe email traffic;
- develop an understanding of the firm's processes for submitting financial transaction and wire requests to the back office;
- monitor communications with clients or other external parties; and
- identify possible opportune moments (*e.g.,* days when the email account owner will not be monitoring their email) to carry out the next step of their attack.

Following execution of the email ATO, the attacker may:

- email back-office personnel asking about wire transfers and other money movement procedures, or instructing them to transfer funds to a fraudulent external bank account;
- email firm clients instructing them to transfer funds to a fraudulent external bank account;
- install malware that creates a new avenue for attackers to access the users' accounts; or
- forward client information to another email account.

Whatever form the attack may take, the fraudsters typically hide their tracks by changing the compromised account's mailbox rules to hide or delete the emails they send from the account. As a result, the account owner may remain unaware of the sent emails until well after the fraudsters have achieved their intended effects, such as transmitting confidential information or causing a fraudulent money transfer.

Attackers have also successfully taken over accounts of firm staff with administrative privileges. This type of ATO creates heightened risks for firms and clients because accounts with administrative privileges may provide the attacker with a powerful platform to launch a larger-scale attack.

FINRA has observed that recovering from an ATO attack was particularly challenging for firms that had not configured their email systems to retain key data logs because they did not have sufficient information to analyze the full scope of the attackers' activities and determine the extent of the fraud. Notably, many firms could have prevented an ATO attack if they had implemented two-factor authentication (2FA).

Preventing ATOs

FINRA has observed that some firms have taken the following steps to configure their cloud-based email environments to help address possible ATO attacks:

- **2FA –** Implemented 2FA for all email account log-in activity outside of the firm's network for general users (*e.g.*, for registered representatives and internal administrators). On the O365 platform, some firms also implemented 2FA for Microsoft Partners and used the Microsoft Authenticator application on users' mobile devices or a dynamically generated personal identification number (PIN) sent via SMS text to provide the second factor.
- **Email Archiving –** Retained and archived all emails in a separate location from the email server to provide the firm with an additional copy of all inbound and outbound emails. In addition, some firms implemented alerts to appropriate firm personnel if there were interruptions in email archiving services.
- **Logs –** Maintained and retained logs of all email account access for an adequate period of time.
- **Administrator Accounts –** Carefully managed all firm administrator accounts by:
  - closely supervising which individuals received administrator accounts to limit access to specifically authorized individuals and minimize the number of individuals with such accounts;
  - reviewing the level of access granted to administrator accounts;
  - monitoring administrator accounts' activities, especially those of "global admin" accounts; and
  - on the O365 platform, confirming administrative privileges delegated to Microsoft Partners and evaluating whether Microsoft Partners should receive "full admin" rights or if "limited admin" privileges are sufficient.[1]

Firms also provided training on the appropriate configuration of cloud-based email services, as well as on phishing emails that could compromise email account security.

Responding to an Attack

FINRA has observed firms respond to ATOs by:

- immediately shutting down the email account by disabling access or resetting the compromised email account with a sufficiently complex password prior to reinstating the account;
- evaluating whether appropriate forensic expertise was available within the firm or whether a third-party service provider should be hired;
- making a copy of any affected email account, including all emails across all folders (such as those hosted by the record retention provider) to capture all information potentially accessed by the attacker at the time of the compromise;
- reviewing all of the email content in the compromised account, including attachments, to determine whether the attacker had access to sensitive or confidential information, such as PII;
- determining whether any client information was breached and notification required under federal or state law;
- confirming that any malware or viruses were deleted and unnecessary user accounts were closed;
- reviewing the overall cybersecurity environment to address any other potential impacts of the attack;
- implementing 2FA controls, if not already in use; and
- notifying appropriate law enforcement agencies (*e.g.*, the local Federal Bureau of Investigation field office) and their FINRA Regulatory Coordinator of the attack.

Endnotes

1. *See, e.g.* Microsoft Azure, About Admin Roles (providing additional information about access privileges for roles in O365).