Business E-mail Compromise TTP Changes

By Ken Dunham, 4D5A Security

Business E-mail Compromise (BEC) is on the rise globally according to the FBI in February 2017[1]. 4D5A Security (4D5ASecurity.com) has identified changes in TTPs (Tools, Tactics, & Procedures) known to exist in the wild since December 2017. These changes increase the trusted nature of attempted BEC fraud attempts that are commonly associated with large scale wire fraud of several hundred thousand dollars or more for each attempt made by remote threat actors. This article contains specific information that can be used to help identify these new BEC TTPs, with focus upon Outlook Web Access (OWA) cloud abuse, to proactively protect against such attacks. 4D5A gives thanks to Justin Vaicaro (XFIL Security Solutions) for his assistance in the authoring of this disclosure.

Introduction to BEC Fraud

The FBI has received thousands of complaints and incidents related to BEC fraud with losses in excess of 5 billion dollars to date. Victims of BEC fraud have been identified in 131 countries. BEC fraud begins with identification of a target. This may take place in a variety of means such as: Purchasing stolen credentials on the DarkNet or reconnaissance against a specific company to identify individual(s) of interest to support their targeted fraud operations.

Grooming then takes place to either build a relationship with the targeted individual or compromise their email or endpoint solution. Social engineering is a key element of the grooming phase where great care is taken by advanced BEC fraud threat actors to persuade or pressure a target as needed for the operation. If successful, BEC infrastructure is then created, configured, and deployed as part of an orchestrated attack against the specific target, related colleagues, or partners.

Advanced BEC operations are aware of roles and responsibilities of two companies that commonly work together, such as: A real-estate office and brokerage firm or a bank and one of their clients. This enables threat actors to properly orchestrate advanced social engineering tactics and leads into the setup of a robust BEC fraud mail infrastructure. The meticulous setup effort of the threat actors ensures maximum success against mail sender identification verification in the hopes of tricking the target into wiring substantial funds to a drop account.

Identifying Advanced BEC Operations

Earlier BEC fraud often took place with a simple spoofed email addresses or typo-squatting domains designed to trick a target. A more advanced threat actor operation, as of December 2017, now exists for BEC fraud due to increased levels of trust through Outlook 365 cloud-based email services. As a general overview, the following takes place when this type of fraud is orchestrated:

1. It is likely that a spam run is used to phish credentials from potential targets. In at least one BEC incident a spam run was performed through a compromised OWA account following detection and blocking of a wire fraud attempt. It appears likely that an exit strategy of this particular BEC campaign is to perform spam runs to new victims, abusing a compromised email from a financial to abuse trust.

2. Following compromise an Outlook 365 cloud-based solution is compromised and configured for reconnaissance or email message auto-filtering and customer email message rules are created for use in

[1] https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

BEC operations. In this campaign it appears likely that an endpoint is first compromised then resulting in OWA account manipulation.

3. Reconnaissance efforts take place on the endpoint/network (if compromised) and/or mailbox (sent items, archives), which is used to identify roles, responsibilities, and processes between the two companies abused in the BEC fraud attack. The threat actors will attempt to socially engineer the targeted organizations with a phish based wire transfer form or specially crafted emails as needed in order to groom the target for attack.

4. Emails are sent from a similar, yet rogue domain email account (e.g. *FinancialDomain* plus "lnc" to look like Incorporated when it is actually "LNC" (e.g. *FinancialDomainLnc*.com). This results in a rogue external email being sent to a legitimate internal financial email to the first target who never sees their own email due to OWA filtering rules. This email, originating from an Outlook 365 based email account, is then forwarded to the secondary internal target, such as a teller, who has the responsibility to perform the wire transfer. The overall objective is to socially engineer the teller to approve and request the wire transfer. A notification may be sent through the email system to the involved threat actors, via mailbox receipt and forwarding rules, of when the secondary target receives the email message or whether they are processing the wire transfer. When email headers are examined the targeted organization only see's IP addressing routing back through legitimate Microsoft email infrastructure.

5. A wire transfer is performed to a bank in Hong Kong or Japan (*other locations possible*) with all funds unlikely to be recovered.

The following TTPs have been identified that are much more sophisticated and mature than that of traditional spoofing type BEC fraud operations:

- **Rogue Domain**

  A rogue typo-squatting or punycode[2]-based domain is registered to look like a legitimate domain of a target. As aforementioned, the "lnc" domain registration took place in a recent attack. Research and response revealed that Wild West Domains was used as the registrar, a top ten abused registrar to date. Research also revealed additional domains registered using the legitimate financial name but punycode based domain names:

  - For example, the domain badthreatactors[.]com may result in a rogue domain such as badthreatactorsinc.com or xn--80agfjkc4abobjjq4i for a roughly translated Russian punycode domain representation. In the example below the financial name has been omitted in white:

- **Autodiscover Trust**

  An "autodiscover" sub-domain may be created with the rogue domain to orchestrate an internal Intermedia Autodiscover server[3] confirmation as part of rogue messaging orchestration.

[2] https://www.punycoder.com/
[3] https://kb.intermedia.net/article/1306

- **Rogue Email**

  A rogue email account may be created in association with the rogue domain and identity designed to look like that of a related partner or client to the targeted financial entity. For example, a bank that regularly performs business with a client may see an email account created using the rogue domain, but appearing to look like or be legitimate for the known trusted client with whom they work with regularly.

- **Auto-Forwarding Rule**

  A compromised Outlook 365 cloud-based email account may be configured to have auto-forwarding to the rogue email account for reconnaissance, which is unknown and invisible to the victimized targeted email account unless they have enabled mailbox audit settings.

- **Auto-Filtering Rule**

  A compromised Outlook 365 email account may be configured with rule(s) to auto-filter or notify based upon the orchestration of the BEC Fraud and monitoring of compromised accounts.

  An example of a rule that could be implemented as fraud:

  Being notified exactly when a secondary target receives and/or reads an email created by the threat actors. In at least one case, all rogue-based emails were automatically delivered to the "RSS Feeds" folder within the Outlook 365 mailbox as well as forwarded to a remote rogue monitoring email using the typo squatted domain name similar to that of the bank. RSS Feeds is a directory that exists by default and is likely never to be inspected manually.

- **Advanced Digital Editing & PDF Creation**

  Advanced digital graphics and manipulation of official wire transfer forms and signatures from formerly processed digital archives may be leveraged to create an official looking wire transfer PDF form. These PDF forms may appear to have been properly processed and signed by individuals trusted in such transactions between both organizations, including signatures, abused in the fraud operation. In at least one instance a wire transfer form was nearly identical to a legitimate form, but varied in the location and actual date of approval for the versioning of the official form template (not something an average user would normally recognize).

Proactive Protection Against BEC Fraud

A variety of proactive protective measures that can be implemented to lower the risk against current and future BEC fraud operations are listed below.

Email Lure

- User awareness training for any individuals related to wire transfer processing, handling, and approval. All identified users should all be trained regularly on BEC fraud operations and their respective TTPs.

  For example:

- Knowing to look for emails that may look legitimate, even "safe", based upon warnings and marks by IT Security, may still be fraudulent – careful inspection of the entire email and domain is required every time.

- Anti-phishing user awareness training that is tied to incentives and rewards for employees that are successful or who identify and report phishing attempts regularly.

- Mark all external emails as "external" and train users on how to handle external emails versus internal emails. Accentuate in training the complexities of how actors may attempt to leverage seemingly trusted internal communications so that context can be created for desired reporting outcomes to IT Security.

- Review policies and procedures to ensure the best possible two factor authentication measures are in place to mitigate future phishing attempts.

  For Example:

  - Having the individual that actually processes a wire transfer to call the requesting individual to confirm the validity of the wire transfer instead of relying upon an email confirmation from a manager who is responsible for the authorization of the requested action.

- Train employees to look for red flags, such as the transfer bank location existing in Hong Kong or Japan.

Outlook 365 (OWA) Monitoring & Hardening

Best practices exist online as a starting point[4].

- Use Multi-Factor Authentication (MFA)

- Use Cloud App Security

- Use Secure Mail Flow

- Enable Mailbox Audit Logging

  - Ensure that logging is enabled for all OWA accounts and configuration changes to where disabling of such settings results in notification to an administrator.

  - Regularly audit OWA accounts to ensure they do not have rogue rules, auto-forwarding, or activity potentially associated with compromise.

  - Limit administrative access to OWA accounts. Any administrator email account should only be used for administration of OWA accounts and have a unique password. Monitoring should be configured so that any rule changes or configurations to any accounts within OWA results in notification to the administrator.

- Configure Data Loss Protection (DLP)

[4] https://support.office.com/en-us/article/security-best-practices-for-office-365-9295e396-e53d-49b9-ae9b-0b5828cdedc3

- Use Customer Lockbox
- Use Secure Score
- Require unique robust passwords to be used for all email communications within an organization. Manage according to best practices and invest additional policies, technology, and training around any staff member with additional authority tied to wire transfer approvals and/or crown jewels of an organization.
- Implement robust spam filtering[5].
    - Connection Filtering
    - SPAM Filtering
    - Outbound Filtering
    - Email Flow Rules
    - Email Authentication

    SPAM Filtering Examples:

        - Use filtering for messages that match known patterns by flagging key words such as "payment", "urgent", "sensitive", or "secret".
        - Blocking any email coming from or going to the referenced phishing domain.

Encrypt Files

- Ensure that files, such as a wire transfer form, are encrypted and that passwords for such files are shared only through a second factor authentication mechanism, such as text to a trusted phone device. Even if an actor is able to acquire a copy of a wire transfer form contained within a sent email the form will be encrypted and not easily subverted. If files are stored on a centralized server and the data at-rest is encrypted it significantly reduces risk of an actor obtaining a copy of such trusted forms for BEC fraud.
- As part of policy, all pertinent staff members should regularly review and update internally used forms and participate in regularly scheduled user security awareness training. These critical measures should allow staff members to easily identify any forms that may vary slightly from the originals leading to possibilities of being fraudulent.
- Ensure traditional endpoint solutions exist such as, updated and hardened Anti-Virus solutions. For critical assets, one could deploy an Endpoint Detection and Response (EDR) solutions for critical assets.

Attack Scenarios

[5] https://support.office.com/en-us/article/office-365-email-anti-spam-protection-6a601501-a6a8-4559-b2e7-56b59c96a586

When considering the diversity and depth of BEC fraud operations a variety of attack vectors may be employed by remote threat actors.

A few key scenarios are identified below for user awareness and context:

Scenario #1

A password re-use scenario where an online social media account information may be harvested and cracked and then leveraged to compromise corporate mailboxes.

Scenario #2

A threat actor sends an email masquerading as a legitimate individual with a weaponized file attachment to a target, which is then downloaded and executed by the victim resulting in a compromise.

Scenario #3

A threat actor sends an email with an embedded hyperlink to a target to reset their password at customized phishing site resulting in a compromise.

For example:

A rogue phishing site may appear to the target as an Office 365 OWA login portal.

Scenario #4

Remote attack scenarios are employed to access an OWA email account using tools or code such as:

- https://silentbreaksecurity.com/malicious-outlook-rules/
- https://sensepost.com/blog/2016/mapi-over-http-and-mailrule-pwnage/
- https://www.blackhillsinfosec.com/abusing-exchange-mailbox-permissions-mailsniper/

Scenario #5

A Corporate insider shoulder surfs as password entry takes place or takes advantage of physical access in order to compromise a targeted device or account.

Closing Comments

The infrastructure required for this type of attack is sophisticated and easily operationalized for BEC fraud attacks to scale. Attackers have a myriad of tools and opportunities to perform such abuse against external facing and cloud-based email environments. If security controls do not exist, as aforementioned, it is trivial for such actors to manipulate and control all email communications. This activity will likely go unseen by the company or compromised email account holder. Sent emails, as part of BEC fraud, are not visible to an end user using a desktop email client. Based upon how the malicious forwarding rules are setup and then when the email headers are analyzed they will look as if they have come from a legitimate source based on the DNS mail infrastructure set up for such fraud. The cloud quickly becomes a dense fog where visibility into attacker operations is not seen unless one looks closely. Proactive user awareness training, security monitoring best

practices, and defense-in-depth hardening for control and visibility are the best methods of approach to lower overall risk against BEC fraud.

TTPs in this incident may suggest that a spam run was performed to acquire either credentials (phishing) or malware installations on multiple accounts or endpoints. Following initial compromise reconnaissance led to the construction of wire fraud media including the typosquatting and related domains, Autodiscover trusted solution for the rogue domain, fake signed wire transfer internal document, monitoring and manipulation of emails, and orchestration of the attack based upon known people, process, and technology between two organizations. Once the attack was discovered, attackers would know due to email monitoring, leading to the secondary attack on a different account within the financial resulting in spam to other external accounts abusing the financials legitimate email account. This may be a method used by attackers to then perpetuate the attack to the next round of possible victims as part of a staged plan.

Appendix A – IOCs

Sanitized IOCs for one advanced BEC fraud attack are as follows:

Domain * IP Data Linked to Remote Access/Abuse
Typo squatting domain created at Wild West Domains, LLC within 30-60 days of the attack registered via Domains by Proxy, LLC. Typo squatting is in the form of *legitimatedomain*lnc.com, where "LNC" in lowercase "lnc" has been added to make it appear as Inc or Incorporated. The legitimate financial domain does not use INC or LNC in the domain name, just the name of the financial, with typo-squatting appending LNC.

Domains hosted in the Philippines and Palau.

*autodiscover** sub-domain for rogue typo squatting domain used in attack to increase trust in the email chain framework for SPF, MX, and DNS records utilizing Microsoft email infrastructure.

Registration of Punycode (supporting non-ASCII characters) domain syntax for related typo squatting rogue domains using financials name.

69.16.152.176:20386
Arizona, AS12989, Highwinds ASN, SecuredConnectivity.net ISP, IPVanish.com domain,
https://cleantalk.org/blacklists/69.16.152.176

168.253.114.197
Nigeria, AS38347, NGCOM, NG ASN

Wire Transfer Details
Wire Transfer Request to Hang Seng Bank, ABA HASEHKHH, Hong Kong

Beneficiary Junghua Industrial Limited, 19th Floor Alexander House, 180 Charter Rd, Central Hong Kong, account 796-131985-883

Modified legitimate internal wire transfer approval form distributed as a PDF with date pagination offset and creation by Neevia Document Converter Pro v6.9

OWA Rules
Most organizations will not have a rule that exists to send received emails to the RSS Feeds directory. Existence of such a rule may be a strong indicator for this type of BEC fraud operations.

"It was received from…" rule for external email account sending items to "RSS Feeds" directory

"It was received from…" rule for internal email account tied to wire transfers processing sending items to "RSS Feeds" directory

AlwaysDeleteOutlookRulesBlob