Cyber Intel Advisory

June 2, 2017 - IA2017-0230

Business Email Compromise Scams Potentially Result In Data Breaches and Financial Losses

TLP: **GREEN** State, local, tribal, and territorial (SLTT) governments are frequently targeted by Business Email Compromise[1] (BEC) scams that attempt to deceive SLTT governments into sending money or personally identifiable information (PII), or that use the government's name to fraudulently obtain material goods. Successful attacks are highly likely to result in financial fraud or identity theft, and it is possible they will result in compromises or data breaches. Multi-State Information Sharing and Analysis Center (MS-ISAC) data indicates that BEC scams resulting in data breaches disproportionately affect educational entities and local governments, increasing the importance of local government awareness about BEC scams.

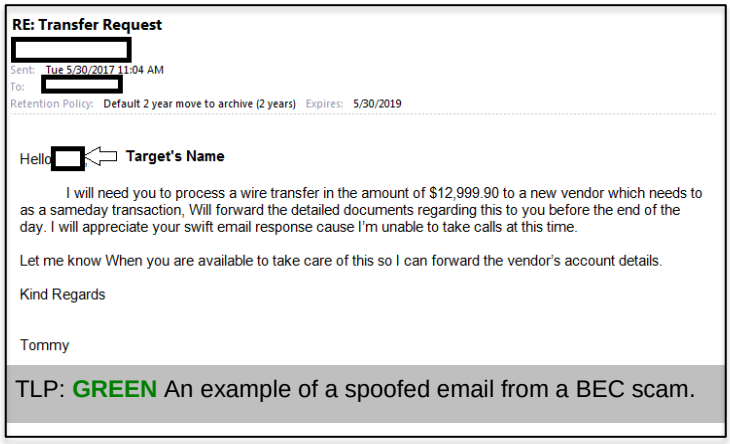
TLP: WHITE *Ransomware infections often receive more press coverage, although BEC scams can be more costly to organizations. In 2016 ransomware attacks were estimated to cost organizations $1 billion, while BEC scams have resulted in over $5 billion stolen since 2013, according to the Internet Crime Complaint Center (IC3). According to NTTSecurity, the average cost of a ransomware attack to an organization is $700, while the average cost of a BEC scam is $67,000.*

TLP: **GREEN** Although the Internet Crime Complaint Center (IC3) identifies five different BEC scam scenarios, the MS-ISAC has only identified three different variants amongst the scams targeting SLTT governments. All three of the below examples originate from compromised, spoofed, or fraudulent accounts, which are used to issue the request, and all three are associated with significant data or financial loss among SLTT governments.

- Purchase Order Fraud Variant: In early 2017, cybercriminals used the name of a local school district in Indiana to commit the purchase order variant of the BEC scam. In this scheme, cybercriminals obtain publically available purchase order forms, and change the contact details on the forms to include different telephone numbers and email addresses or copycat websites. They then submit the purchase order to a vendor, have the goods shipped, and sell them for profit while the bill goes to the affected entity. In the Indiana incident, the school district discovered the fraud when they received phone calls from multiple companies regarding bills for computers, radios, and other equipment. In this instance, the purchase orders included at least one correct name, but the contact information was changed and an associated tax exemption certificate used a combination of fictitious and outdated information.

[1] TLP: WHITE In 2017, the Internet Crime Complaint (IC3) merged the BEC and Email Account Compromise (EAC) scams together under the BEC name. They previously defined EAC scam as the same as the BEC scam, except that targets were individuals and not businesses.

- W-2 and PII Data Theft Variant: In early March 2017, a Texas school district announced that they were the victims of the W-2 variant of the BEC scam. In this variant, the cybercriminals pose as an administrator or senior official and send a targeted email to the human resource or finance departments requesting an email with all employees' W-2 information or PII. In the Texas incident, the cybercriminal crafted an email to appear as though they were the Superintendent of the school district, and requested W-2 information to be sent immediately. District employees complied, resulting in a data breach that compromised the W-2 information of 1700 employees. The MS-ISAC believes W-2 information and PII stolen in this manner are often used to commit tax fraud and identity theft.
- Financial Theft Variant: In late May 2017, cybercriminals targeted an Arizona county with a BEC scam by spoofing the email account of a senior official and asking for money to be transferred. In this variant, cybercriminals pose as an employee or senior official and request departments transfer funds immediately. The emails are typically directed toward the human resource or finance departments and contain a sense of urgency. In financial theft BEC emails, cybercriminals often use the name of the email target to establish trust and imply an existing relationship, which increases the likelihood of the target sending money to the cybercriminal. In the Arizona case, an attacker targeted the HR department and requested money be sent as a same-day transaction. In another late May example, the spoofed email did not directly reference a wire transfer, but rather specified that "transactions" needed to be "set up and processed."


RE: Transfer Request

[redacted]

Sent: Tue 5/30/2017 11:04 AM

To: [redacted]

Retention Policy: Default 2 year move to archive (2 years) Expires: 5/30/2019

Hello [redacted] ⇦ **Target's Name**

I will need you to process a wire transfer in the amount of $12,999.90 to a new vendor which needs to as a sameday transaction, Will forward the detailed documents regarding this to you before the end of the day. I will appreciate your swift email response cause I'm unable to take calls at this time.

Let me know When you are available to take care of this so I can forward the vendor's account details.

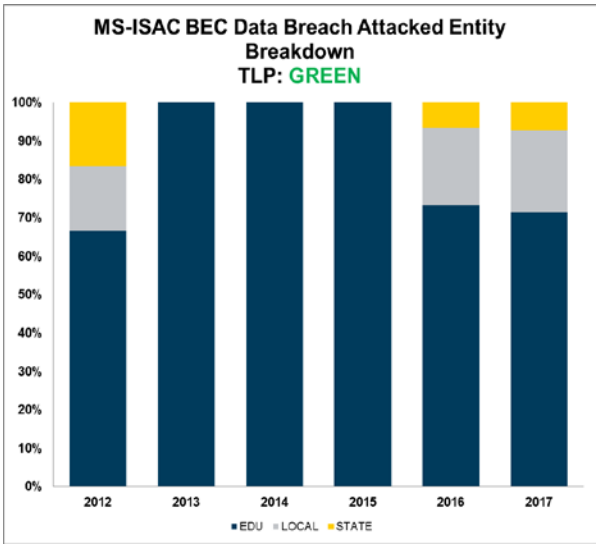
Kind Regards

Tommy

TLP: **GREEN** An example of a spoofed email from a BEC scam.

- Compromised Email Accounts: All variants of the BEC scam can involve compromising the email account of the senior official and using it to send the email request, rather than simply spoofing the account. When that occurs, the cybercriminal has full access to the account, and can setup auto forwarding or other rules, resulting in additional compromises.

TLP: **GREEN** Based on data identified by the MS-ISAC, it is highly likely education entities and local governments are and will continue to be disproportionately targeted by BEC scams in the future. As evidenced by the graph to the right, local governments and educational entities accounted for at least 80% of all identified BEC scams resulting in SLTT government data breaches.



TLP: **GREEN** Cybercriminals use traditional social engineering and phishing techniques to conduct BEC scams, which help increase the likelihood of successful attacks. Since the ultimate target of a BEC attack is the end-user, awareness of BEC scams and the indicators are key. The MS-ISAC recommends that SLTT governments:

- **Craft a policy** for identifying and reporting BEC/EAC and similar phishing email scams. Make sure to include the following:
    - When receiving unusual financial or sensitive data requests, users should **verify the identity** and authority of the email sender via standard (non-email) channels.
    - Users should **hover to discover**, to ensure that the email is going to the correct person. The true recipient of an email can often be verified by hovering the mouse over the address in the email header.
    - Users should **reply by forwarding**, and not by hitting the "reply" button, which helps to prevent successful spoofing attacks.
    - Users should **report** suspicious emails to security staff. The MS-ISAC also appreciates receiving notifications of all BEC scam attempts.
- **Train staff** in the finance and human resource departments to identify potential BEC scam emails and follow the suspicious email policy. Indicators of BEC spam emails can include:
    - Poorly crafted emails with spelling and grammar mistakes, that include a note indicating the email was sent from a mobile device (e.g. iPhone, iPad, Android, etc.) in order to convince the recipient the mistakes can be ignored.
    - The email may include the wrong or an abbreviated signature line for the supposed sender.
    - The email may use full names instead of nicknames (e.g. "Jennifer" instead of "Jen") and the language structure may not match how the supposed sender normally communicates.
    - The email specifies that the only way to contact the sender is through email. In some cases, the emails appear to be timed to correspond with times the senior official is out of the office.
    - The transactions are for a new vendor or new contract.
    - Internal warning banners to indicate the email is possibly spam, spoofed, or from an external source.
- **Implement filters** at your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall.
- **Flag** emails from external sources with a warning banner.
- **Reach out and warn** other departments, agencies, and schools of the BEC scam.
- **Report BEC scams** at https://bec.ic3.gov/. Tax-related suspicious emails should be reported to the IRS at https://www.irs.gov.
- Refer to the MS-ISAC's primer on Spear Phishing, which is available at: https://www.cisecurity.org/white-papers/cis-primer-phishing/.

(U) TLP: WHITE The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

(U) TLP: WHITE The information in this document is current as of May 31, 2017. Citations and more information regarding potential cyber threats are available by contacting:

OneNet
888-566-3638 · info@onenet.net
www.onenet.net

MS-ISAC
866-787-4722 · SOC@cisecurity.org
www.cisecurity.org