CONNECTICUT INTERLOCAL RISK MANAGEMENT AGENCY
Member Owned Member Governed

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

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

February 5, 2019 • IA2019-0109

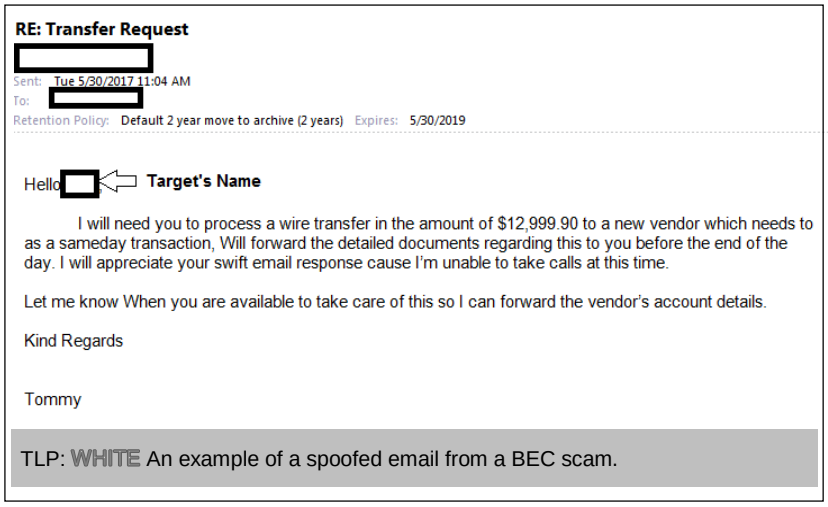
TLP: WHITE State, local, tribal, and territorial (SLTT) governments are frequently targeted by Business Email Compromise (BEC) scams that attempt to deceive victims into sending money, or personally identifiable information (PII), modifying direct deposit information, or use the government's name to 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 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.

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 $12 billion stolen since 2013 according to the Internet Crime Complaint Center (IC3). In 2018, BEC attacks cost U.S. victims $2.9 billion. 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: WHITE The MS-ISAC identifies four different variants among the BEC scams targeting SLTT governments. In these scams, cybercriminals often use the name of the email target to establish trust and imply an existing relationship, as well as a sense of urgency, which increases the likelihood of the targeted employee complying. Additionally, the emails often begin generically with questions asking if the employee is available to assist. The emails themselves can originate from webmail accounts spoofed to appear as though they are from other employees or from compromised accounts. Each of these types can originate from compromised, spoofed, or fraudulent email accounts and all three are associated with significant data or financial loss among SLTT governments.

- Direct Deposit Variant: In December 2018, cybercriminals updated their tactics to request direct deposit changes to executive accounts. In this variant, cybercriminals pose as a senior official and request finance or human resources departments change the direct deposit account details, resulting in the executive's paycheck being redirected.
- W-2 and PII Data Theft Variant: 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. These emails target schools and local governments, with the cybercriminal crafting an email to appear as though it was from a school superintendent or high level government official, and requesting all employees' W-2 information to be emailed immediately. If the target employee complies without encrypting the data or encrypts the data and provides the password, this variant results in a data breach. 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 this variant, cybercriminals pose as an employee or senior official and request departments transfer funds immediately. Attackers use this variant to request money be sent as a same-day transaction, such as a wire transfer. Occasionally, the spoofed email will 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: WHITE An example of a spoofed email from a BEC scam.

- Purchase Order Fraud Variant: 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. School districts are common targets and discover the fraud when they receive phone calls regarding overdue bills for computers, radios, and other equipment.

TLP: WHITE All variants of the BEC scam can involve compromising the email account of the 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 a compromise and if emails are forwarded outside the entity, in a data breach.

TLP: WHITE 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. In 2017, local governments and educational entities accounted for at least 80% of all identified BEC scams resulting in SLTT government data breaches according to MS-ISAC data.

RECOMMENDATIONS:

TLP: WHITE 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 someone within your organization, awareness of BEC scams and the indicators are key.

The MS-ISAC recommends that SLTT governments follow the below recommendations.

- Craft a policy for identifying and reporting BEC and similar phishing email scams. Make sure to include the following components.
  - When receiving unusual financial or sensitive data requests, users should verify the identity, authenticity, and authority of the email sender via non-email channels.
  - Users should 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.
- Train staff in the human resource and finance 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.
  - The wrong or an abbreviated signature line for the supposed sender.
  - The use full names instead of nicknames and a language structure may not match how the supposed sender normally communicates.
  - That the only way to contact the sender is through email.
  - The transactions are for a new vendor or new contact at a known vendor.
- Develop a BEC Incident Response Plan including emergency contacts with at the appropriate financial institutions in case it becomes necessary to stop a transfer.
- Ensure human resource and finance department employees are have a policy for out-of-band verifications (e.g. verbal confirmations, etc.) of direct deposit, account changes, or wire transfer requests. Collaborate with human resource and finance departments to ensure their policies are supported by technological solutions.
- Flag emails from external sources with a warning message in the subject line.
- Implement filters at your email gateway to filter out emails with known phishing attempt indicators and block suspicious IPs at your firewall.
- Refer to the MS-ISAC's primer on Spear Phishing for other recommendations.
- Report BEC scams to the MS-ISAC, local law enforcement, and the Internet Crime Complaint Center (IC3). Tax-related suspicious emails should be reported to the IRS. If there is a financial loss, notify the bank to stop payment and involve local law enforcement.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.

More information regarding potential threats is available by contacting:

Connecticut Interlocal Risk Management Agency
203-946-3700 • www.CIRMA.org

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