The Kansas City Terrorism Early Warning System (KCTEW) was established in 2007 by local, state and federal law enforcement and partner organizations to detect, deter and respond to terrorist threats in Greater Kansas City. The KCTEW Center collects information from a variety of sources. The data is evaluated in an effort to identify potential trends or patterns of terrorist or criminal operations within the region. The KCTEW provides regular bulletins to public and private partners to raise awareness and encourage actions that protect residents, businesses, organizations and assets in the metro area. The KCTEW Privacy Policy dictates that an individual’s privacy, civil rights and civil liberties be safeguarded. As such, the intent of this bulletin is to provide information only.

Who is the Bulletin for?
This bulletin is for local government officials, their agencies, and private industry managers. This document contains excerpts from unclassified FBI Press Releases and may be shared freely for information purposes. KCTEW encourages the bulletin to be shared as deemed useful.

What is the purpose of the bulletin?
KCTEW analysts have noted a significant increase in scam occurrences in the Metropolitan Kansas City area. Local governments, non-profit and public agencies and private business have been targeted by the scams. This bulletin is to provide situational awareness regarding these scams.

“FBI officials are warning potential victims of a dramatic rise in the business e-mail compromise scam or “B.E.C.,” a scheme that targets businesses and has resulted in massive financial losses in Phoenix and other cities.

The schemers go to great lengths to spoof company e-mail or use social engineering to assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money and use language specific to the company they are targeting, then they request a wire fraud transfer using dollar amounts that lend legitimacy.

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

- Law enforcement globally has received complaints from victims in every U.S. state and in at least 79 countries.
- From October 2013 through February 2016, law enforcement received reports from 17,642 victims.
- This amounted to more than $2.3 billion in losses.
- Since January 2015, the FBI has seen a 270 percent increase in identified victims and exposed loss.
In Arizona the average loss per scam is between $25,000 and $75,000.  

The B.E.C. Scheme:

“The main scheme is known as the business e-mail compromise scheme, or B.E.C. The scheme is also known as “CEO fraud” or the “man in the middle” scheme. B.E.C. is defined as a fraud targeting businesses that regularly perform wire transfer payments. The scam is carried out when perpetrators compromise e-mail accounts through social engineering or through computer intrusion techniques to fraudulently direct electronic fund transfers. There is no profile for victim businesses. Victims range from large corporations to tech companies, to small businesses, to non-profit organizations. The schemers conduct research to learn about the employees in a company who manage the money, as well as the protocol necessary to perform wire transfers within that business environment. In some cases, information is obtained through a phishing scheme. In others, businesses may be victims of ransomware or other cyber intrusion prior to the B.E.C attack.

Law enforcement globally has received complaints from victims in every U.S. state and in at least 79 countries. From October 2013 through February 2016, law enforcement received reports from 17,642 victims. This amounted to more than $2.3 billion in losses. The overwhelming majority of victims are located in the United States. Since January 2015, we have seen a 270 percent increase in identified victims and exposed loss.

In many cases, law enforcement cannot recover funds sent overseas and may not identify the perpetrator; therefore, education and prevention are stressed.

Versions of B.E.C. (also known as - Man in the Middle or CEO Fraud):

‘Version 1:
A business, which often has a long standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, fax, or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request. This particular version has also been referred to as “the bogus invoice scheme,” “the supplier swindle,” and “invoice modification scheme.”

Version 2:
The e-mail accounts of high-level business executives (CFO, CTO, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.” This particular version has also been referred to as “CEO fraud,” “business executive scam,” “masquerading,” and “financial industry wire frauds.”

Version 3:
An employee of a business has his/her personal e-mail hacked. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee’s personal e-mail to multiple vendors identified from this employee’s contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.

Version 4:
A fourth version of this scam has recently been identified based on victim complaints. Victims report being contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims

---

may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of B.E.C. scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.

Version 5:
Based on complaint data submitted to IC3, B.E.C. victims recently reported receiving fraudulent e-mails requesting either all Wage or Tax Statement (W-2) forms or a company list of Personally Identifiable Information prior to a traditional BEC incident. These fraudulent requests are usually sent utilizing a business executive’s spoofed e-mail. The entity in the business organization responsible for the W-2 and/or PII, HR, bookkeeping or auditing section, is the targeted recipient of the fraudulent request. Victims report they have fallen for the W2-PII twist even if they were able to successfully identify and avoid the traditional B.E.C. incident. The B.E.C. W2-PII twist appears to be timed for the tax season. This new twist, at this time, does not appear to link with other tax scams. \(^3\) (Note: IC3 is the acronym for Internet Crime Complaint Center)

According to the Federal Bureau of Investigation:

“If your company has been victimized by a BEC scam:
- Contact your financial institution immediately
- Request that they contact the financial institution where the fraudulent transfer was sent
- File a complaint—regardless of dollar loss—with the IC3.

Tips for Businesses:
- Be wary of e-mail-only wire transfer requests and requests involving urgency
- Pick up the phone and verify legitimate business partners.
- Be cautious of mimicked e-mail addresses
- Practice multi-level authentication.
- Resources:
  - FBI stats & tips on business e-mail scams
  - Public service announcement about the business e-mail compromise scam
  - More about IC3 \(^4\)

Kansas City Regional TEW Inter-Agency Analysis Center
Comments and questions regarding this product should be direct to:

KCTEW Staff
(816)413-3588
kctew@kcpd.org
