U.S. Secret Service

Business Email Compromise Scams

Warning: The Secret Service is currently observing a significant increase in the frequency, sophistication, and fraud losses associated with Business E-mail Compromise (BEC) scams, which are a form of Automated Clearing House (ACH) wire fraud. Organizations are encouraged to immediately implement additional authentication steps before performing wire transfer payments to non-U.S. financial institutions, and to report suspected criminal activity associated with these scams to their local Secret Service Electronic Crimes Task Force (ECTF) or field office.

About Business E-mail Compromise (BEC) Scams: BEC is a sophisticated scam commonly targeting businesses working with foreign suppliers or companies that regularly perform wire transfer payments. This scam uses social engineering techniques, often coupled with unauthorized access to corporate networks, to use business emails to initiate fraudulent wire transfer payments to non-U.S. financial institutions. These payments are often transferred several times before being quickly dispersed and "cashed-out" in a foreign jurisdiction. Banks located within Asia are the most commonly reported destinations for these fraudulent transfers. However, recent reports indicate banks in Eastern European countries are increasingly used as the ending destination for dispersal. Although the scam is not new, it has recently grown in popularity and increasingly sophisticated versions of the scheme are being employed.

In one version, the victim company's Chief Financial Officer (CFO) or business's accounts payable department are receiving spoofed e-mails from their Chief Executive Officer (CEO) requesting a wire transfer or from a regular vendor purportedly updating their bank account information with the target business. The fraudulent e-mails are highly deceptive and are usually not detected as fraudulent. The request is typically then forwarded to specific individuals responsible for initiating and completing wire transfers and contains specific language and wire amounts that are customary for the victim company. Victims report this version of the scam is usually not discovered until business executives contact each other during casual conversation, face to face, through e-mail, or by phone calls to verify or confirm the wire transfer request.

In another version, company's or employees' e-mail systems are being compromised through malware. Investigations indicate the malware was uploaded through "spear phishing" e-mails when employees opened email attachments verifying shipping documents or other normal business functions. Once the illicit actors have access to the systems, they initiate requests for payments from the compromised email accounts to multiple vendors identified from the compromised contact list that include fraudulent payment instructions. The emails are highly deceptive and avoid detection because the messages are specific to the business in the type and amount of the request. The victim business usually does not become aware of the multiple fraudulent requests until they are contacted by their vendors due to overdue invoices.

U.S. Secret Service

Business Email Compromise Scams

The illicit actors in both versions appear to have conducted extensive research, both open source and through access to private business records, to identify responsible parties as well as normal operating procedures used by the specific businesses and employees. In some cases, it appears the suspects have maintained illegal access to the business's computer systems or networks for extended periods of time. In all cases, the fraudulent wire transfer payments are sent to non-U.S. banks and are usually transferred several times before being quickly dispersed.

Losses associated with this scheme since October 2013, reported by U.S. businesses and international law enforcement, totaled over $1 billion.

This scheme is currently growing in popularity amongst organized cybercrime groups and techniques are rapidly evolving. **Implementing stronger authentication measures** before initiating wire transfers to non-U.S. financial institutions is strongly encouraged.

Reporting: Those who have been victims of this fraud scheme, or detect suspicious activity related to this scheme, should report this activity to their local U.S. Secret Service Electronic Crimes Task Force or field office. Early reporting of such incidents leads to the potential recovery of compromised funds.

A list of Secret Service field offices is available at: http://www.secretservice.gov/field_offices.shtml

JDL Technologies is a member of the U.S. Secret Service's Miami Electronic Crimes Task Force (MECTF) and periodically receives information regarding online fraud from the MECTF and Secret Service.