Methods of Business Email Compromise (BEC)

Author: eFraudPrevention

BankUnited

Business Email Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Methods of Business Email Compromise (BEC)

Spoof an Email Account or Website

Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic. The spoofed emails can be made to look like they are coming from anyone. Scammers target employees with transactional authority (accounts payable, check signers, authorized individuals) or access to systems managing personally identifiable information. Emails often display a sense of urgency culminating in a request for money transfers, data, or gift cards.

Phishing Emails

These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes. Emails attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate or clicks on malicious attachments. This is an attempt by attackers to solicit personal information, such as account usernames and passwords, these fraudulent websites may also contain malicious code.

Cloud-based Email Services

Cybercriminals are targeting organizations that use popular cloud-based email services to conduct Business Email Compromise (BEC) scams. The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds. Many phishing kits identify the email service associated with each set of compromised credentials, allowing the cybercriminal to target victims using cloud-based services. Upon compromising victim email accounts, cyber criminals analyze the content of compromised email accounts for evidence of financial transactions. Often, the actors configure the mailbox rules of a compromised account to delete key messages. They may also enable automatic forwarding to an outside email account. Using the information gathered from compromised accounts, cyber criminals impersonate email communications between compromised businesses and third parties, such as vendors or customers, to request pending or future payments are redirected to fraudulent bank accounts. Cybercriminals frequently access the address books of compromised accounts as a means to identify new targets to send phishing emails. As a result, a successful email account compromise at one business can pivot to multiple victims within an industry.

While most cloud-based email services have security features that can help prevent BEC, many of these features must be manually configured and enabled. Better protect yourself from BEC by taking advantage of the full spectrum of protections that are available. Depending upon the provider, cloud-based email services may provide security features such as advanced phishing protection and multi-factor authentication that is either not enabled by default or are only available at additional cost.

This often results in Trojans infecting a system without triggering any type of notification. There are several types of Trojans, each fulfilling a different purpose. Some Trojans are designed specifically to extract sensitive data from the infected system; these types of Trojans typically install keyloggers or take screenshots of the victim's computer and automatically transmit the information back to the attacker. Other, more dangerous "remote access Trojans" (RATs), will take control of the infected system, opening up a back door for an attacker to later access. Remote access Trojans are typically used in the creation of botnets.

Spyware/Adware

Like some types of Trojans, spyware is used to collect and relay sensitive information back to its distributor. Spyware typically is not malicious in nature. However, it is a major nuisance, typically infecting web browsers, and making them nearly inoperable. Spyware is often used for deceitful marketing purposes, such as monitoring user activity without their knowledge. At times, spyware may be disguised as a legitimate application, providing the user with some benefit while secretly recording behavior and usage patterns.

Like spyware, adware is a major nuisance for users. But it is usually not malicious in nature. Adware, as the name implies, is typically used to spread advertisements providing some type of financial benefit to the attacker. After becoming infected by adware, the victim becomes bombarded by pop-ups, toolbars, and other types of advertisements when attempting to access the Internet. Adware usually does not cause permanent damage to a computer. However, it can render the system inoperable if not removed properly.

Rootkits

Arguably the most dangerous type of malware is the rootkit. Like remote access Trojans, rootkits provide the attacker with control over an infected system. However, unlike Trojans, rootkits are exceptionally difficult to detect or remove. Rootkits are typically installed into low-level system resources (below the operating system). Because of this, rootkits often go undetected by conventional anti-virus software. Once infected with a rootkit, the target system may be accessible by an attacker providing unrestricted access to the rest of the network.

Knowing when you've got one Malware in network traffic or on a computer makes its presence known one of three ways:

- Signature" is a fingerprint or pattern in the file that can be recognized by a network security system like a firewall even before it gets to a computer. If such a file actually gets to a computer, the anti-virus/anti-malware software on the machine should catch it.
- A suspect file type appearing out of context, like an executable (.exe) or registry value hidden in a compressed file like a .zip.
- Behavior; even a rootkit may reveal itself when it "phones home" to the operator who controls it. If this behavior is abnormal—for instance, in volume or time of day—this can be an indicator of a compromised system.

All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.