THE THREAT
OF
CORPORATE ACCOUNT TAKE OVER
AND
BUSINESS E-MAIL COMPROMISE

Over the past several years the North Texas Electronic Crimes Task Force (N-TEC) has seen an alarming increase in the number of reported Corporate Account Take Over and Business E-Mail Compromise cases. The most recent cases involve area real estate, mortgage and title companies being led to believe they were sending money for established real estate transactions, when in reality, the malicious actors intercepted legitimate e-mails and diverted the settlement funds with losses exceeding $500,000.

The purpose of this advisory is to heighten the reader's awareness of the potential security risks associated with the two schemes, point out their similarities, as well as provide security measures for securing high-dollar financial transactions. Although there have been a number of previously published articles and advisories on Corporate Account Take Over and Business E- Mail Compromise, businesses are still getting hit at a disturbing rate.

CORPORATE ACCOUNT TAKEOVER (CATO) is a form of business identity theft causing huge financial losses for businesses, communities, and banks. This fraud typically occurs when malicious actors gain access to a victim's computer via malicious software (malware) downloaded through e-mail attachments, websites or malware disguised as legitimate software. The most common attack method of CATO is an attack (infection) against the computer(s) of the victim business.

THE BUSINESS E-MAIL COMPROMISE (BEC) scheme is very similar except, instead of gaining the business's on-line banking credentials and high-jacking the bank account, the attacker places himself in the middle of e-mail communications of a business or organization. Although there are various ways a malicious actor can gain access to a personal or business e-mail account, most BEC schemes involve hi-jacking free, web-based e-mail accounts or established company website domains resolved through a free web-based e-mail program. The level of social engineering associated with BEC scams has links and similarities to other email based internet fraud, which makes this type of fraud more of a network (internet) based attack.

CATO and BEC SIMILARITIES:

Although the types of organized criminals that normally commit CATO and BEC may be somewhat separately regionalized, both CATO and BEC share several very distinct similarities:

1. The attack vector involves placing the malicious actor or his malicious tools between the victim and a valuable resource, such as a person, company, website or e-mail account.
2. The goal of the attackers, regardless of the attack vector is to infiltrate a business or individual's computer, steal their data and monetize it.
3. Potential targets could be from any Critical Infrastructure and Key Resources (CIKR) sector that maintains large balances and performs electronic transfers.
4. Businesses or individuals are victims of high–dollar Wire or ACH transfers to domestic money mules or foreign banks located in the United Kingdom, Nigeria, Russia, China or Hong Kong, for example.
5. Both schemes affect the confidence and integrity of our banking system and exhibit a clear and present threat to our financial economy.

To combat these attacks, the utilization of a layered or defense in depth approach is needed to prevent malware from installing on your system while also protecting the integrity of your networked based email communication. If malware is the attack vector, its methods attempt to relay details of an infected user's online activity, intercept any financial transaction and view any user's email account. If email communications is the attack vector, it serves as the staging ground to exploit existing trusted relationships, impersonating the victim in an attempt to monetize financial activity.

For all high-dollar financial transactions, the only way to eliminate the threat is to employ multi- dimensional, preemptive strategies that verify transactions once they arrive at the originating communication channel's depository institution, and before they are released to the ACH or wire operator.

RECOMMENDATIONS TO BUSINESSES AND INDIVIDUALS:

Here are some of the ways businesses can reduce their chance of being victimized by CATO and BEC attacks:

- Restore a balance between security and usability. Establish other /second factor, Out of Band Verification (OOB) communication channels early in the relationship, such as smart phone authentication, token or ACH positive pay type of solution to verify significant transactions outside the e-mail/PC environment in order to avoid interception by a hacker.

- Try not to use free web-based e-mail platforms for high-dollar financial transactions. If free web-based e-mail is utilized, take advantage of providers offering multi-factor authentication to further secure your account and conduct your own self-assessment of your e-mail account by viewing "last Account Activity (Details)" to check for any unusual activities. Check all filters, forwarding addresses and recovery options to make sure nothing has been altered and avoid free Wi-Fi. Establish a company website domain and use it to establish company e-mail accounts.

- Require two people to sign off on every high–dollar transaction and beware of sudden changes in business practices.

- Conduct all banking on a dedicated machine used for no other task. Also, utilize a live CD–read-only, with bootable operating system, or create a dedicated virtual operating system (OS) for the sole purpose of providing a secure environment. Your network support company or staff can advise you more about these.

RECOMMENDATIONS FOR TECHNOLOGY AND SECURITY PRACTITIONERS:

- Protect against impersonation attacks by utilizing technologies such as sender policy framework (SPF), digital signatures, and Domain-based Message Authentication Reporting and Conformance (DMARC) in e-mail accounts. Be aware that this technology will not work with some web-based e-mail accounts and in some countries due to its limits on the use of encryption.

- Unfortunately, the convenience of remote access to systems has been embraced by both businesses and cyber criminals alike. If employees have the ability to access your company's system remotely from any device, from any location, at any time then so do the cyber-criminals, if security-measures are not taken and regularly updated.

- Third party remote access should not be permanently enabled; it should only be granted upon request from a known and trusted source, with an agreed end time. With shared risk comes shared responsibility. System integrators who setup and support remote access for a business that gets breached could also be held liable.

- In the era of mobile devices and Bring Your Own Device (BYOD) to work, many organizations have moved towards exposing their internal e-mail environment to the Internet and of course doing so opens a number of security risks. The Exchange client access server (CAS) is a component of Exchange Server that allows users access to their mailbox, using a web browser or mobile phone, which requires CAS to have full connectivity with the Exchange server. This is the main database in many corporate environments. Malicious actors could fingerprint an Exchange OWA server for version vulnerabilities or try a brute force hacking for administrative password. Tasks that should not be overlooked with the deployment of Outlook Web Access (OWA) are properly configured firewalls, routers and servers.

- OWA offers a means for ubiquitous access to Exchange email. Group policy settings allow utilization of an Account Lockout Threshold. Define strict access firewall rules with dynamic content filtering to detect and classify suspicious logon behavior. Utilize Exchange ActiveSync Mailbox Policy, to assign mobile device security policy to specific users, and decrease server and/or internal network exposure by deploying a virtual private network (VPN). Also, acknowledge that VPN access is only as secure as its connected device.

- Consider quarantine before authenticating any external devices utilizing OWA. While in quarantine, a device can be scanned to ensure it meets minimum security levels; verifying appropriate certificates, signatures and/or passcodes are supplied. Quarantined devices could also be provided the option to self-mitigate if a fail status is issued and they've properly authenticated.

NOTIFY LAW ENFORCEMENT:

Although law enforcement notification procedures may vary amongst Federal and State agencies, all notifications involving the United States Secret Service should be made by telephone or direct contact. There should be direct contact with the Secret Service so that the following steps can be immediately taken:

1. Provide a general description of this crime, how it occurred, losses experienced and Wiring/ACH instructions. Timing is critical in both CATO and BEC cases.

2. If notified immediately, financial institutions and law enforcement can work with you to increase the chance of recovering the stolen funds.

3. Law enforcement can also submit requests to Financial Crimes Enforcement Network (FinCEN) for information from its global partners, which can significantly expand their knowledge of the financial activity and reduce delays often associated with international investigative efforts.

Any questions regarding this advisory can be directed to the United States Secret Service North Texas Electronic Crimes Task Force at (972) 868-3200 or email us at Dallas.ECTF@usss.dhs.gov.

References and resources:

http://www.fbi.gov/seattle/press-releases/2013/man-in-the-e-mail-fraud-could-victimize-area-businesses

http://www.ic3.gov/media/2015/150122.aspx
http://www.ectf.dob.texas.gov/documents/bestpractices-catorisk_000.pdf
https://www.uscert.gov/sites/default/files/publications/money_mules.pdf
http://www.fincen.gov/law_enforcement/les/
http://www.procheckup.com/media/205152/pentesting_exchange_owa_final.pdf
http://www.gfi.com/blog/tips-for-better-outlook-web-app-security-exchange-_server/
http://www.fbi.gov/scams-safety/frauds-from-a-to-z
http://www.listcrime.com/
http://www.sans.org/reading-room/whitepapers/email/options-securely-deploying-outlook-web-access-873
http://www.bankandtechguide.com/mbcontent/GetImage.aspx?file=9c22027a-723d-4029-ae9a-62c701d8ab88.JPG&width=550&height=550
http://krebsonecurity.com/online-banking-best-practices-for-businesses/
http://kansasrealtor.com/scam-be-careful-with-your-clients-wiring-instructions/
http://krebsonsecurity.com/2014/04/phishers-divert-home-loan-earnest-money/#more-25690
http://blog.kaspersky.com/man-in-the-middle-attack/
http://www.bbb.org/datasecurity
http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-smallbusinesses-can-protect-and-secure-customer-information
http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html
http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf
http://www.fsisac.com/files/public/db/p265.pdf
http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm
https://technet.microsoft.com/en-us/library/bb125165(v=exchg.150).aspx
https://www.messagebus.com/site/docs/Fraud_Protection_DMARC.pdf