ADVISEN
Insurance Intelligence®

HACKED!

WHEN CYBER THIEVES CLEAN OUT A COMPANY'S BANK ACCOUNT

June 2014

Sponsored by:

OneBeacon
PROFESSIONAL INSURANCE®

HACKED!
WHEN CYBER THIEVES CLEAN OUT A COMPANY'S BANK ACCOUNT

Introduction

A Russian hacker was recently charged by US authorities with creating GameOver Zeus, a botnet based on code from the Zeus family of Trojans. These malicious programs are designed to steal a company's banking credentials and are responsible for losses of more than $100 million worldwide since 2011. GameOver Zeus is one of the best known and most successful strains of malware, but it is just one of many designed to assist in taking over a company's online bank accounts, a tactic known as a "corporate account takeover." In this form of business identity theft, a cybercriminal steals a company's online banking credentials and initiates fraudulent wire and/or automated clearinghouse (ACH) transactions to an account or accounts of his or her choosing.

Corporate account takeovers – typically committed via phishing, social engineering, or other schemes – have proven a challenge to both detect and prosecute.

Corporate account takeovers – typically committed via phishing, social engineering, or other schemes – have proven a challenge to both detect and prosecute. While no organization is immune, small and mid-size businesses are frequently targeted. Losses can be severe and can place a company and their financial institution in a precarious situation.

Problems generally arise when a financial institution's corporate customers assume that the same fraud protection offered on their personal bank accounts also applies to their corporate accounts. This assumption is false in most circumstances because a corporate customer will sign a "hold harmless" agreement with the bank. This agreement is in place to protect the bank from liability of unauthorized debits taken from a company's business account. Corporate customers are left in the unenviable position of either accepting the losses or relying on some form of insurance to mitigate their loss.

Unless the customer is properly insured, corporate account takeovers create a lose-lose situation for financial institutions and their customers. Both are potentially exposed to the risk of reimbursing the loss and face reputational risk from the discovery and potential disagreement of liability.

Many of today's bank thieves are anonymous, operate remotely from almost any place on the globe, and execute crimes that are difficult to detect and prosecute.

This paper aims to describe to financial institutions and their customers some of these risks and the potential options to attempt to minimize their risk in a situation where only the bad guy can come out on top. To do so, it will illustrate the methods used by cyber-criminals to perform a corporate account takeover, provide an examination of a financial institution's exposures and the current legal environment, and suggest potential risk mitigation strategies for both the bank and its customers.

Methods Used

Like most industries, financial institutions evolved to keep up with the customer demands of the 21st century. The interconnectedness of the global economy, and the ability to connect instantaneously from anywhere across the globe, has enabled financial institutions to meet customer demands by allowing individuals and businesses to more easily and efficiently conduct their financial activities online. While a necessity to maintain relevance and competitiveness, increased customer convenience also creates new security challenges for financial institutions.

Many of today's bank thieves are anonymous, operate remotely from almost any place on the globe, and execute crimes that are difficult to detect and prosecute. These crimes are constantly evolving as criminals attempt to stay a step ahead of network defenses while seeking paths of least resistance. Corporate account takeovers are increasingly the crime of choice due to their ease of execution and opportunity for large paydays. By targeting bank customers – often small businesses— who frequently lack even the most basic cyber defenses, cyber criminals can successfully obtain online banking credentials and quickly execute unauthorized transactions. Additionally, once a hacker has access, he also can transfer funds directly from the company, add fake employees to the payroll, or steal sensitive customer information.[1]

Malware

Attacks frequently occur quietly through the introduction of malicious software, known as malware, onto a corporate customer's system or network. This can be initiated in a variety of ways. Most commonly, a customer or employee of the targeted business is tricked into opening an email attachment or link within an email. This is known as a phishing scam. When this occurs the employee is redirected to an infected website where the malicious file is unknowingly installed onto their system. Once installed, the malware often remains on the system undetected for weeks or months.

While email scams are the most common approach of introducing a malicious file to a victim's computer or network, by no means is it the only way it can be introduced.

While email scams are the most common approach of introducing a malicious file to a victim's computer or network, by no means is it the only way it can be introduced. For example, a victim can click on a compromised link within social media or download data from an infected flash drive or other portable device.

In recent years, one of the most common and widely-spread malware used for account takeovers is the Zeus Trojan, or Zbot. These programs are created using a toolkit that is widely available in underground marketplaces for cybercriminals. The toolkit also allows a cybercriminal to modify the functionality of the malicious file, making it difficult to detect. The Zeus Trojan is primarily designed to steal confidential information from the computers it compromises. [2]

In 2012, the largest ever account takeover scam, known as Operation High Roller, was identified. This highly sophisticated cyber attack involved modified versions of the Zeus Trojan. It siphoned billions from bank accounts across Europe, Canada, the United States, and around the world. The scheme focused on high-value commercial accounts and extremely wealthy individuals by targeting their highest value bank accounts, transferring money onto prepaid debit cards, and modifying the statement balance to hide the transactions.

Another variant is GameOver Zeus, an extremely sophisticated malware designed to steal banking and other credentials from infected computers. It too is primarily spread through spam emails or phishing messages. What makes it unique is that the infected computers become part of a global network of compromised computers known as a botnet that can be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service attacks.[3] Its main purpose is to collect banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts controlled by criminals. Losses are estimated to be in excess of $100 million.

On June 2, 2014, the US Department of Justice and the FBI announced a multinational effort to disrupt the GameOver Zeus botnet.

Operation High Roller and GameOver Zeus are examples of widespread, well-organized, and highly sophisticated attacks conducted by organized crime rings scattered across the globe. However, the majority of corporate account takeovers are perpetrated by the everyday cybercriminal, a lone wolf or a small group of individuals, who possess a small degree of technological know-how but have very sinister intentions.

Among other things, the marketplace provides the ability to buy or sell stolen credit card numbers, purchase malware, and even offers hackers for hire.

The ability to pull off these attacks has become increasingly simple. This is thanks to a phenomenon referred to as "cybercrime as a service" (CaaS), an underground cybercrime marketplace that offers cyber criminals just about any product and/or service they would need to execute an attack. Among other things, the marketplace provides the ability to buy or sell stolen credit card numbers, purchase malware, and even offers hackers for hire.

Another trend in account takeover schemes is the use of distributed denial of service attacks (DDoS). In a DDoS attack, the targeted website is overwhelmed by messages, typically sent through a botnet. Traditionally used by hacktivist's as a method of making a political statement, DDoS attacks have increasingly been used to disguise account takeovers. The idea is that a DDoS attack will divert the attention of corporate IT departments allowing cyber criminals to simultaneously take over and transfer funds from a corporate online bank account without notice.

In one example, cyber criminals successfully wired $900,000 out of a construction company's bank account. In a creative scheme, the cybercriminals targeted the construction company's bank with a DDoS attack. The attack temporarily brought down the bank's website while the criminals concurrently transferred the money to 62 different accounts. Because the bank website was down, the company could not access their account and therefore were unaware of the activity.[4]

Although malware is often the cyber criminal's tool of choice in account takeovers, it is not the only method. Resourceful fraudsters have also been known to obtain banking credentials through deception and the use of publicly available information on the internet and social media websites such as Facebook.

Social Engineering

Social engineering is the art of manipulating people to give up confidential information. While this method can be used for a variety of purposes, criminals frequently try to trick the target into giving them passwords or other information that allows them to access the target's computer and install malicious software.

Manipulative and creative cyber criminals often prefer this tactic because they feel it is easier to take advantage of people's innate desire to trust than it is to find vulnerabilities in a target's cyber defenses. This approach has been aided in recent years by the popularity of social media where cybercriminals can find information about a person's interests and habits, as well as other personal information such as date of birth, phone number, or even

Corporate account takeovers are often executed by cybercriminals who dedicate their life to identifying vulnerabilities or designing malicious software.

their mother's maiden name. This is the exact type of information that a fraudster can use to execute a con and/or make changes to an online account.

In one example, a cybercriminal, through online research, learned that the CEO of a company had a family member that had battled cancer. The CEO had since been involved in cancer funding and research. The fraudster also learned about his favorite sports team and favorite restaurant through social media. Armed with this information, he called the CEO and posed as a fundraiser for a charity he had previously been involved with. The fraudster explained that the charity was offering a prize drawing in exchange for donations. Prizes included tickets to a game of the CEO's favorite sports team and gift certificates to his favorite restaurant. As a result, the CEO agreed to let the fraudster send him a PDF with more information on the fund drive. When the CEO opened the PDF, malware was installed on his computer that gave the fraudster access to his machine.[5]

Corporate account takeovers are often executed by cybercriminals who dedicate their life to identifying vulnerabilities or designing malicious software. The cards are often stacked against companies, especially small and mid-size organizations, who simply do not have the resources maintain a proper defense. Correct or not, these organizations frequently rely on their financial institutions to provide this security and feel betrayed if they sustain a loss and are not made whole.

The Legal Environment

According to legal experts, financial liability for fraud loss between a financial institution and a corporate banking client as a result of a corporate account takeover remains a legal gray area. Judgments have been mixed as courts' interpretations of responsibility have varied. Article 4A of The Uniform Commercial Code (UCC) states that the risk of loss for an unauthorized transaction lies with a customer as long as the financial institution provides reasonable and common sense security to recognize and prevent unauthorized payments. Where interpretations have varied is with what is considered to be commercially reasonable and common sense security measures.[6]

A case that illustrates the different views of what comprises a commercially reasonable security solution is PATCO Construction Inc. vs. Ocean Bank. In a series of six fraudulent ACH transfers in 2009, PATCO lost more than $500,000 from its commercial account with Ocean Bank using credentials stolen from a compromised PATCO computer. In the initial 2011 ruling, a district court in Maine ruled against PATCO stating that the bank did have commercially reasonable security in place. This ruling was based on a contract signed

Although, under the UCC, financial institutions are typically not legally obligated to reimburse businesses for losses, regulatory agencies such as the Federal Deposit Insurance Corporation (FDIC) and the Federal Financial Institutions Examinations Council (FFIEC) provide guidance on the matter.

by PATCO with Ocean Bank agreeing to the banks security solutions and procedures. This decision was reversed on appeal in 2012 where the appellate court focused more on the bank's actions in using security solutions and less on simply having the technology . This case is still under appeal.[7]

Missouri-based Choice Escrow sued its financial institution to recover $440,000 stolen by online thieves in 2009, the court ruled that fault lay with the business. This was because Choice had twice refused to use the bank's recommendation that a second authorized employee be required to sign off on all transfers. The judge ruled that this refusal shifted responsibility for the loss to the corporate client.

Although the bearer of the financial burden varies, the financial institution still is in a 'no win" situation in both cases: even if it proves no liability for a customer's loss, it may lose the customer and potentially tarnish its reputation with current and future customers. Therefore, reducing the risk of an account takeover is imperative.

Risk Mitigation

Although, under the UCC, financial institutions are typically not legally obligated to reimburse businesses for losses, regulatory agencies such as the Federal Deposit Insurance Corporation (FDIC) and the Federal Financial Institutions Examinations Council (FFIEC) provide guidance on the matter. The guidance provides financial institutions and their regulators a baseline they can draw upon for the development of industry expectations and security practices. As a result, most financial institutions have made online security investments in response to this guidance.

The FFIEC guidance, for example, suggests that institutions develop multiple layers of security, implement non-technical strategies such as more customer fraud education, and create policies for regular risk assessments. The guidelines are helpful, but they are not enough since the threat environment continues to evolve. Institutions should look beyond the regulatory recommendations.[8]

Security against corporate account takeovers should be a shared responsibility between the financial institution and its corporate clients. A strong partnership between the financial institution and its customers has proven the most effective prevention approach. If each

Financial Institutions should recommend layered security controls to create multi-level barriers. For example, they can recommend a multi-person approval processes for online banking transfers of a certain value in addition to their basic online security practices.

implements sound business practices, and work together when necessary, the risk of sustaining a loss can be greatly reduced.

The following are potential processes and controls that financial institutions and their corporate customers can implement to attempt to protect, detect, and respond to corporate account takeovers.[9]

- Financial institutions should expand on, or create, a risk assessment to include corporate account takeovers. The risk assessment should be reviewed annually to identify updates that should be made to existing controls.
- Financial Institutions should recommend basic online security practices to corporate online banking customers. Examples include not using unprotected internet connections, encrypting sensitive data, using complex passwords, not using public Wi-Fi for banking transactions, and keeping antivirus software up to date.[10]
- Financial Institutions should recommend layered security controls to create multi-level barriers. For example, they can recommend a multi-person approval processes for online banking transfers of a certain value in addition to their basic online security practices.
- Financial institutions should develop a security awareness education program for the employees of their corporate account holders.
- Financial institutions should recommend their corporate account clients create a secure environment by dedicating one computer to be used for the sole purpose of banking activities. The computer should not be connected to the corporate network, have email, or connect to the Internet for any reason other than banking.[11]
- Financial institutions should obtain legal counsel that is familiar with corporate account takeover risks.
- Financial Institutions should draft written agreements for corporate clients that address corporate account takeovers, identify roles and responsibilities, and includes disclaimers (hold harmless clauses).

As long as cyber criminals view corporate account takeovers as low risk/high reward, attempts will continue at a high frequency and the tools will only become more creative and sophisticated.

- Financial institutions should recommend that their corporate clients purchase fraud insurance that includes coverage for cybercrime and fraudulent bank transfers.
- Financial institutions and their corporate account clients should establish ongoing monitoring and timely reporting of suspicious activity.
- Financial institutions employees should be educated on identifying the signs that a theft may be in progress and immediately block the account and monitor activity.
- Financial institutions should educate their corporate account holders of signs that an account may be compromised.
- Financial institutions should immediately verify that a transaction was fraudulent and attempt to reverse all fraudulent transactions.
- Financial institutions should contact law enforcement and regulatory agencies.

Conclusion

As long as cyber criminals view corporate account takeovers as low risk/high reward, attempts will continue at a high frequency and the tools will only become more creative and sophisticated. Although financial institutions are not required by law to take responsibility for unauthorized debits from business accounts, they are generally required to provide commercially reasonable and common sense security measures. But what is considered commercially reasonable? In this gray area of the law, the courts have not come to a unified conclusion.

The best option for financial institutions is to partner with their clients and develop processes and controls that will reduce account takeovers, which also has the added benefit of creating stronger business relationships. They also should notify customers in writing of their liability in the event of a takeover, and recommend customers purchase adequate insurance protection. ■

[1] American Bankers Association, "The Small Business Guide to Corporate Account Takeover,"

[2] Symantec, Trojan.Zbot, http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

[3] United States Computer Emergency Readiness Team (US-CERT), "GameOver Zeus PFP Malware, http://www.us-cert.gov/ncas/alerts/TA14-150A

[4] Michelle Castelle, Retail Payments Risk Forum, "Mitigating Account Takeovers: The Case for Education," (April 2013), https://www.frbatlanta.org/documents/rprf/rprf_pubs/130408_survey_paper.pdf

[5] Joan Goodchild, CSO, "Social engineering: 3 examples of human hacking," (Feb 9, 2011), http://www.csoonline.com/article/2126983/social-engineering/social-engineering--3-examples-of-human-hacking.html6 Michelle Castelle, Retail Payments Risk Forum, "Mitigating Account Takeovers: The Case for Education," (April 2013), https://www.frbatlanta.org/documents/rprf/rprf_pubs/130408_survey_paper.pdf

[7] Tiffany Riley, Guardian Analytics, The Frontlines of Fraud Blog, "PATCO ACH Fraud Ruling – Lessons Learned," (Julty 16, 2012), http://guardiananalytics.com/blog/

[8] Tracy Kitten, CUInfoSecurity, "FFIEC Guidance: Has It Reduce Fraud?" (July 12, 2013), http://www.cuinfosecurity.com/ffiec-guidance-has-reduced-fraud-a-5905?webSyncID=8524a70a-ae3a-6911-e0eb-853be9430d1b&sessionGUID=e4215981-2c10-769b-3042-b653b0856906

[9] Texas Bankers Electronic Crimes Task Force, "Best Practices for Banks: Reducing the Risks of Corporate Account Takeovers," http://www.ectf.dob.texas.gov/documents/bestpractices-catorisk_000.pdf

[10] National Automated Clearing House Association, "Second Business Practices for Companies to Mitigate Corporate Account Takeover," (2011), https://www.nacha.org/system/files/resources/Sound%20Business%20Practices%20for%20TPSPs%20to%20Mitigate%20CAT.pdf

[11] National Automated Clearing House Association, "Second Business Practices for Companies to Mitigate Corporate Account Takeover," (2011), https://www.nacha.org/system/files/resources/Sound%20Business%20Practices%20for%20TPSPs%20to%20Mitigate%20CAT.pdf

This Report was written by Josh Bradford, Associate Editor, Advisen Ltd.