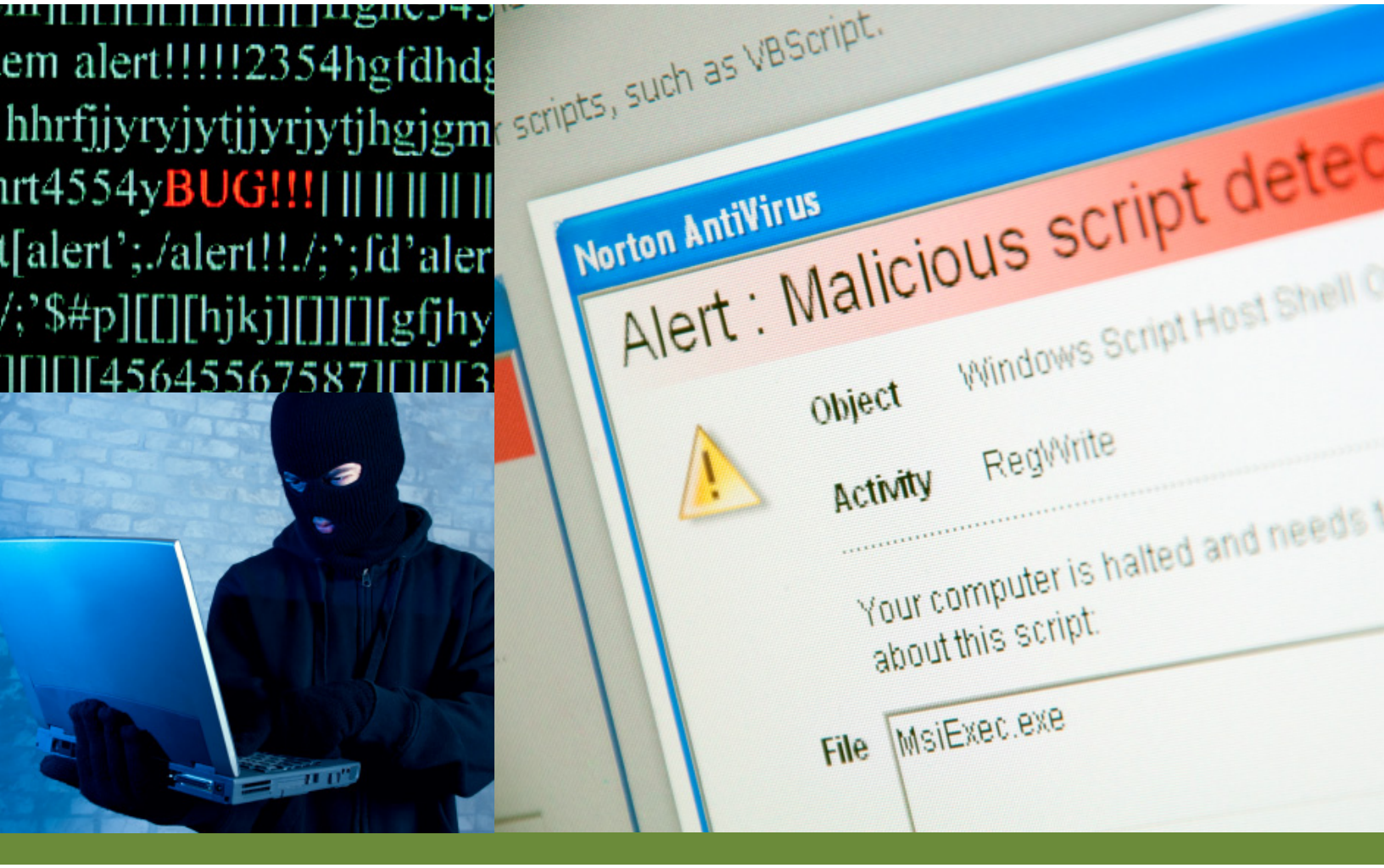
ADVISEN
Insurance Intelligence



Cyber-Threats and Financial Institutions:

Assume all networks are infected...Is this the new normal?

October 2012

Sponsored by: AIG

Cyber-Threats and Financial Institutions:
Assume all networks are infected...Is this the new normal?

Executive Summary

Financial Institutions, an already highly targeted industry by cyber criminals, should only expect the number and sophistication of malicious attacks to grow. The adoption of Internet-based commerce systems, while convenient for customers and financially beneficial for some institutions, provides criminals with more opportunities to steal both money and information. Cyber-thieves continue to introduce highly sophisticated malware strains to take advantage of vulnerabilities. Bank customers infected with the strains --which frequently go undetected by anti-virus software – expose financial institutions to computer network contamination. As a result, the recent consensus among banks has been to assume that all customer PCs are infected.

Introduction

Since America's first bank robbery in Philadelphia in 1798, financial institutions have been a favorite target of criminals. Some of the nation's most recognizable crooks such as Butch Cassidy, John Dillinger and Jesse James attained notoriety by robbing banks. In the 21st century, technology has changed the game. According to Professor Udo Helmbrecht, the Executive Director of the European Network and Information Security Agency (ENISA),"the old adage, 'criminals go where the money is', today means that 'bank robbers go online.'"[1] Many criminals now operate in anonymity from miles, or even oceans, away from their targets. These capable cyber-criminals are implementing increasingly sophisticated attacks, hitting many more targets and impacting many more people.

Despite increased efforts by the financial industry to protect systems and punish those perpetrating such attacks, top cyber experts agree that cyber-criminals show little sign of slowing down.

Despite increased efforts by the financial industry to protect systems and punish those perpetrating such attacks, top cyber experts agree that cyber-criminals show little sign of slowing down.[2] Instead, they are developing ever more sophisticated and targeted methods of breaching both banks' and bank customers' networks to obtain valuable information and execute fraudulent transactions. While financial institutions have recently done a better job of identifying and preventing these schemes, much more needs to be done.

Cybercrime is a global epidemic. According to a comment from ENISA in response to recent cyber-attacks on corporate bank accounts, the first step to securing the online banking environment is to "assume all customer PCs are infected."[3] This comment raises the question, should banks operating under this assumption consider this the new normal? While it may be too early to know for sure, staying informed and preparing for the worst seems prudent. To do this, financial institutions should understand the reasons behind this assumption, identify the cyber-threats plaguing the sector, recognize the potential consequences of those threats, and learn how best to secure against them.

Why assume all Customer Networks are infected?

"Many online banking systems dangerously rely on PCs being secure, but banks should instead presume all customer PCs are infected."[4] This ENISA advisory came in response to a recently published report by McAfee and Guardian Analytics detailing a sophisticated and highly automated malware strain dubbed "High Roller", which was designed to specifically target the PCs of bank customers with high account balances. High Roller, a customized version of already established malware, Zeus and SpyEye, aimed to transfer large sums of money into mule business accounts. The transfers occurred at the moment that the customer logged into his or her account. Attempted individual transfers were as high as $130,000.[5]

The sophistication of the malicious code, its execution speed and "the insider level of understanding of banking transaction systems" has led many to believe this is the work of organized crime.

The sophistication of the malicious code, its execution speed and "the insider level of understanding of banking transaction systems" has led many to believe this is the work of organized crime.[6] While High Roller may be one of the most sophisticated malwares to target the financial sector, it is by no means the first nor will it be the last. It is estimated that three quarters of the largest banks from around the world already are infected by malware such as Conficker, DNS Changer, Gameover Zeus, BlackHole Exploit Kit, and fake antivirus software.[7] Some of these programs use "man-in-the-middle" and "man-in-the-browser" technologies, which are highly effective and extremely difficult to detect, and have been called "the greatest threat to online banking today."[8]

High Roller infected approximately 5,000 PCs and was geographically confined to the Netherlands. Gameover Zeus, widely considered the largest banking Trojan today, has infected an estimated 678,000 Windows PCs around the world.[9] Regardless of their reach, both were designed to take advantage of the same vulnerability, one that is likely here to stay; online banking. This is the first reason why assuming all PCs are infected should be considered the new normal for the financial sector.

Cyber-Threats to the Financial Sector

"The number and sophistication of malicious incidents has increased dramatically over the past five years and is expected to continue to grow," according to Gordon Snow, Assistant Director of the Cyber Division of the Federal Bureau of Investigation (FBI), testifying before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit. "As businesses and financial institutions continue to adopt Internet-based commerce systems, the opportunities for cybercrime increase at retail and consumer levels."[10]

According to the FBI, eight cyber-threats expose both the finances and reputations of financial institutions:

- Account takeovers
- Third-party payment processor breaches
- Securities and market trading company breaches
- ATM skimming breaches
- Mobile banking breaches
- Insider access
- Supply chain infiltration
- Telecommunication network disruption

Of these, account takeovers, securities and market trading company breaches, mobile banking breaches, and supply chain infiltration all represent reasons why assuming all PCs are infected should be considered the new normal.

Account Takeovers: This is a leading concern for financial institutions. As mentioned above, cybercriminals are becoming more sophisticated in exploiting banking systems that connect to the Internet. Instead of targeting the financial institution directly, criminals have focused their attention to compromising the PCs of online banking customers to gain access to their accounts and execute fraudulent money transfers. The infection typically occurs through targeted phishing schemes via email or text messages and is designed to compromise the customer's online banking information.

According to Snow, the FBI is investigating 400 reported account takeover cases from the bank accounts of U.S. businesses. These cases total over $255 million in attempted fraudulent transfers and have resulted in $85 million in actual losses.[11] The scary part is that these figures only represent the reported cases; the actual losses are likely much higher. These numbers shed some light on a very profitable criminal undertaking, which is the second reason why assuming all PCs are infected should be considered the new normal.

According to the FBI, financial firms have become regular targets of supply chain attacks.

Securities and Market Trading Company Breaches: Financial institutions in the securities and brokerage business as well as their customers frequently find themselves the target of cybercriminals. According to the FBI, the schemes against these organizations include market manipulation and unauthorized stock trading. Cybercriminals are known to target both the companies trading the securities as well the exchanges that they are sold on.[12] Cybercriminals can access brokerage accounts in similar fashion to the account takeover examples above, which is a third reason why the assumption that all PCs are infected should be considered the new normal.

Mobile Banking Breaches: Smartphones and other mobile devices have become increasingly popular tools for conducting banking transactions. Customers appreciate the ease and flexibility that they provide. In turn, in the cutthroat financial sector, most banks believe that they must provide what their customers demand in order to remain competitive. This technology, however, has created a vulnerability that has become an increasingly popular target of cybercriminals. For example, by imbedding a variation of the Zeus malware via a malicious website, text message or mobile application, cybercriminals can gain access to the user's credentials and account information. This is another reason why the assumption that all PCs are infected should be considered the new normal.

Supply Chain Infiltration: According to the FBI, financial firms have become regular targets of supply chain attacks. Cybercriminals are infiltrating financial institution suppliers of technical, computer and security equipment, software, and hardware. When installing these devices banks could actually be installing malicious code. A fifth reason it is wise to assume that all PCs are infected.

What to do?

The sixth and final reason why assuming that all PCs are infected should be considered the new normal is that many of the banking viruses previously mentioned can be purchased relatively cheap via a do-it-yourself virus kit. Whether criminals are seeking only to cause trouble, or they have more sinister intentions, the ease by which banking viruses can be obtained and the simplicity by which they can be executed makes it all the more likely that this issue is here to stay. Assuming all PCs are infected spurs banks to be proactive and take the necessary protection measures to not only prevent an incident, but be prepared to respond if a problem were to occur.

Some suggestions for addressing the threats include:

Develop Alternate Approaches to Safeguarding Online and Mobile Banking Customers: Many customers have become accustomed to banking online, and mobile banking is also increasing in popularity. The broad appeal and demand for these services has made it such that eliminating them as a method of risk avoidance is no longer an option. As previously mentioned, many of the online banking systems operate under the assumption that the user's PC is not infected. By assuming that the user's PC is infected, banks can take an alternate approach to prevent fraudulent transactions. For example, according to ENISA, "a basic two factor authentication does not prevent man-in-the-middle or man-in-the-browser attacks on transactions. Therefore, it is important to cross check with the user the value and destination of certain transactions, via a trusted channel, on a trusted device (e.g. an SMS, a telephone call, a standalone smartcard reader with screen)."[13]

While most of the attention is focused on protecting financial institutions from external cyber threats, they also need to focus on preventing internal leaks.

Develop Strategies to Prevent Insider Access: While most of the attention is focused on protecting financial institutions from external cyber threats, they also need to focus on preventing internal leaks. Developing a risk management process that incorporates organizational checks and balances provides a first line of defense against the leakage of classified information. According to Deloitte's 2010 Global Financial Services Security Survey, 56 percent of senior IT executives surveyed are confident in their ability to prevent external breaches but only 34 percent are confident in their ability to handle internal threats.[14]

Share Information with other Institutions and Partner with Federal Law Enforcement Agencies: Deterring and punishing those behind cybercrime is not an isolated issue but a collective problem for the entire financial industry. Sharing information about threats with other institutions and with federal agencies is vital to successfully combating this escalating problem. The faster that information can be disseminated the quicker the response and the higher the likelihood of success.

Consult with an Insurance and Risk Management Consultant: Despite the proactive measures in place and the increasing awareness of cyber risk, data breaches do happen. Since the environment has shifted from "if a breach occurs" to "when a breach occurs," financial institutions should consider insurance for data breaches, network intrusions, and privacy violations. Consulting an insurance advisor is recommended since coverage terms can vary depending on the carrier. Policies with the most comprehensive coverage will provide protection not only for the direct costs associated with the breach but also third party costs such as public relations and breach notification expenses.

Conclusion

It takes only a brief review of the cyber-threats currently plaguing the financial industry to understand why ENISA would advise to "assume all customer PCs are infected". While the debate continues as to whether this is the new normal, it is fair to assume that new technology will continue to expose the sector to new threats. Financial firms must develop the flexibility and technical sophistication to identify emerging threats and address new data security challenges. Fortunately, they need not do it alone. Data security consultants – so-called white hats or ethical hackers – can help identify and fix vulnerabilities. Consulting a qualified insurance company and broker that understands the industry, coverage terms, and evolving threats should also be an early measure to proactively address the problem.

This Special Report was written by Josh Bradford, Associate Editor, Advisen Ltd.and sponsored by Chartis Inc.

NOTES:

[1] Press Release, European Network and Information Security Agency (ENISA), "Flash not: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps", (July 5, 2012), http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

[2] Fahmida Y. Rashid, eWeek.com," IT Security & Network Security News: Cyber-Threats Continue to Target the Financial Industry", (September 2011), http://www.eweek.com/c/a/Security/CyberThreats-Continue-to-Target-the-Financial-Industry-836311/

[3] Press Release, European Network and Information Security Agency (ENISA), "Flash not: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps", (July 5, 2012), http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

[4] Press Release, European Network and Information Security Agency (ENISA), "Flash not: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps", (July 5, 2012), http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

[5] Dave Marcus & Ryan Sherstobitoff, McAffee& Guardian Analytics, "Dissecting Operation High Roller", (2012), http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

[6] Dave Marcus & Ryan Sherstobitoff, McAffee& Guardian Analytics, "Dissecting Operation High Roller", (2012), http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

[7] Kelly Jackson Higgins, darkReading, "More Than Half of Major Banks Infected with Conficker, Zeus, Fake AV, Other Malware, (July 26 2012), http://www.darkreading.com/risk-management/167901115/security/news/240004457/more-than-half-of-major-banks-infected-with-conficker-zeus-fake-av-other-malware.html

[8] Ellen Messmer, ZeuS-style banking Trojans seen as greatest threat to online banking: Survey, Network World http://www.networkworld.com/news/2010/120810-trojan-bank.html

[9] Ellen Messmer, TechWorld, "'Gameover Zeus' P2P bank-theft botnet has infected 678,000 Windows PCS, (July 26 2012), http://news.techworld.com/security/3372250/gameover-zeus-p2p-bank-theft-botnet-has-infected-678000-windows-pcs/

[10] SECNAP Network Security, "FBI on Cybersecurity: Threats to the Financial Sector", http://www.secnap.com/support/whitepapers/fbi-cyberthreats-financial-industry.html

[11] SECNAP Network Security, "FBI on Cybersecurity: Threats to the Financial Sector", http://www.secnap.com/support/whitepapers/fbi-cyberthreats-financial-industry.html

[12] SECNAP Network Security, "FBI on Cybersecurity: Threats to the Financial Sector", http://www.secnap.com/support/whitepapers/fbi-cyberthreats-financial-industry.html

[13] Press Release, European Network and Information Security Agency (ENISA), "Flash not: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps", (July 5, 2012), http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

[14] Deloitte, "2010 TMT Global Security Study – Key Findings", http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/2010_TMT_Global_Security_study.pdf