Online Banking: Information Security vs. Hackers Research Paper

Paul Jeffery Marshall

Abstract— In this paper I will discuss four scenarios regarding cyber crimes specifically directed at financial institutions and give specific examples. Also, I will discuss the malicious Zeus and URLzone bank malware Trojans that is currently causing security issues and threats to some financial institutions. Expected results from study and research is to bring awareness of increased activity of cyber-attacks directed at financial institutions, call for a global alliance against cyber-pirates, and point out that financial institution's have a responsibility to protect and secure information as custodians of their customer's sensitive/legacy data online.

1 Introduction

Billions of financial data transactions occur online every day of the year 24 hours a day 7 days a week and bank cyber crimes take place every day when bank information is compromised. Skilled criminal hackers can manipulate a financial institution's online information system, spread malicious bank Trojan viruses that allow remote access to a computer, corrupt data, and impede the quality of an information system's performance. If sensitive information regarding commercial and personal banking accounts is not better protected, cyber-thieves will continue to illegally access online financial accounts to steal trillions of dollars plus sensitive customer information globally. Audit of bank information technology systems, ethics and policy requirements for bank information security systems, awareness of risk potential, continuity of financial institution information systems all should be high on the list of federal & state regulators and banking board of director'sagendameetings. One major real world cyber crime directed at any specific financial institution can severely take down a domestic and global financial network.

Banks and Savings & Loans is identified as financial institutions and both are custodians of not only their customer's money, but even more so a financial institution is responsible for their customer's personal and legacy data. Examples of information that financial institutions are the custodian of records for their commercial and personal banking customers is: day-to-day transactions including deposits, withdrawals, balance amount, social security number, birth date, loan information, partnership agreements related to a loan, year-to-date statements and a host of other extremely sensitive financial information. All the above mention records, transactions and sensitive information is events that occur online usually more than 50 percent of the time.

Cyber crooks, network hackers, cyber pirates, internet thieves is an emerging crime category of criminals and threat to online banking information security systems. According to reports $268 million dollars was stolen online from financial institutions, 2009 cyber-robbery of financial institutions escalated to $559 million dollars (Bankrate.com). The efforts used to hi-jack financial institutions was Banking Trojans that piggy-back legitimate customer bank accounts to steal passwords, fraudulent wire transfers, and hackers working from the inside to compromise the information security system of an financial institution, in other words; an inside job.

2 Methods

In age where technology has outpaced the law regarding banking cyber crimes many online pirates make it their full-time work to challenge bank information security systems to find a point of entry into an information system in order to access bank data and steal money. Customers can be clueless about cyber crimes until it is too late and all their money has disappeared from their account.

When a potential customer walks through the door of a financial institution to open a basic checking or saving account the customer is asked and required to provide all kinds of sensitive information like social security number, driver license number, and sign an affidavit that authorizes the financial institution to obtain a credit report to check the customer's current credit history and there after every six months before an account is open. Then on top of that requirement; the new customer is asked by the financial institution to trust them with all that sensitive information. Illustrated below are four scenarios and consequences of bank cyber crimes.

2.1 Scenario 1

Scenario 1, let's say that a cyber-pirate introduces to a silent and malicious bank Trojan to a financial institution's information system and domain that runs an agent or macro that extracts customer account information then text messages the information back to the hacker all in a nanosecond. When an online electronic process takes place where sensitive data is illegally accessed and manipulated a cyber crime has just transpired in the blink of an eye and should be treated. One, the bank's information security system has been compromised, two, the customer's sensitive information was stole. In a nutshell the financial institution was robbed just that quick.

2.2 Scenario 2

Scenario 2, let's say an undercover cyber pirate opens an account at a local branch office of a national bank or savings & loan financial intuition with the intent on committing an electronic robbery of money and any customer information that is not secure on any server in any state were the financial institution is doing business and custodian of electronic records. How does an information systems security team prevent cyber thief, perform application security intelligence and investigation a cyber crime waiting to happen when the cyber criminal is one of their own customers? Cyber crooks are opportunist. If a cyber crook sees an opportunity to steal they will steal. A cyber crook looking for an opportunity to commit a crime is like a homeowner leaving the door unlocked and a home burgular checks every door and window of the home and find that one door and window of the home that is not locked then access the home. Bingo, the burglar has gained access to valuable assets. The two scenarios are different but the concept is the same. In other words, never give a cyber crook a window of opportunity to compromise valuable information. Information system security teams responsible for securing information/data should create a cyber threat protection strategy, build layers of security to protect business process and data integrity (Abel, W.), SDLC security testing, build an information system security team that will keep each other aware of the latest cyber threat activity, information, trends, and frequent internal information system security audits.

2.3 Scenario 3

Scenario 3, let's say a crafty cyber thief conspires to bring down a bank information system domain by replicating malicious syntax embedded in attachments that navigates pass infrastructure security into a lockdown financial information system application; precious financial information is not only compromised but the entire network is at risk.

2.4 Scenario 4

Scenario 3, let's say a financial institution is seeking to generate new business by targeting an audience of customers that are highly attached to mobile phone connectivity. These specific customers prefer to receive monthly statements and access their account online by using the web browser tool enabled on their smart phone.

Customer access to financial accounts online using a smart phone is a great model and marketing idea but creates a whole new set of information system security concerns for the financial institution's CIO and the person responsible for information system security. For example, the smart phone creates another point of entry into the financial institution's information system that a criminal hacker can exploit the introduction of a silent but deadly bank Trojan to a financial institution's information system if the system is not fully updated with the latest internet security tools at all times.

3 Results

What is the global/domestic standard policy for information system security for financial institutions weigh heavy on the minds of chief information officers, regulators, internet security administrators. For financial institution; who writes the cyber crime laws? Who sets the cyber-security financial institution information system policy standards for private industry or federal government? Who is responsible for compliance, audit and assurance of internet information system security for bank and financial institutions? Who are the information system security police for financial institutions? What is the future of the internet and cyber security? (OECD Observer). Gone are days when a computer user can navigate the World Wide Web and not have computer security and be naive about hackers and cyber criminals. The internet is a beautiful world, but it can be joy and pain especially if your internet experience crash your computer; in addition to stealing sensitive financial and personal information.

H.R. 4061 is the Cyber Security Enhancement Act of 2010. February 9, 2010 H.R. 4061 legislation was sent to the 111th Congress 2nd session in the Senate of the United States of America (H.R. 4061—111th Congress: *Cybersecurity Enhancement Act of 2010*). H.R. 4061 legislation is to advance cyber security research, development, and technical standards. H.R. 4061 is currently being reviewed by the Committee on Commerce, Science, and Transportation. H.R. 4061 legislation focus on cyber security strategy, checklist to minimize security risk associated with hardware and software systems, consequences and best practices, and cyber security awareness and education.

FDIC - Federal Deposit Insurance Corporation is responsible for the solvency of bank institutions in the United States of America. FDIC has the federal regulatory responsibility for audit and compliance of bank information system security. FDIC should do compliance audits just like they do every bank that they insure and fall under FDIC regulatory jurisdiction. Example, let's say a cyber cartel loots a bank online of all the money in every customer account at the bank including required reserve cash; and all the account are below the $200,000 FDIC insured account limits. Results, FDIC pays each customer the verified deposit amount that was stolen by the cyber criminals. So it would be in the best interest of the FDIC - Federal Deposit Insurance Corporation to be proactive active about doing audit and compliance for security of bank information system s doing commercial and personal banking business online.

Every financial institution should have some type of information security policy or if they do not they should adopt one soon and have it signed by the CEO, CFO, CTO and each board member of the financial institution, ASAP before the bank regulators find out. Not having information system security policy and not performing information system due diligence spells one word RISK.

4 DISCUSSION

Bank Trojans steal online bank account information by exploiting security flaws in computer information systems. URLzone bank Trojan is extremely sophisticated and "the next generation of bank Trojans" said Yuval Ben-Itzak Finjan Software's Chief Technology Officer (McMillan, Robert).

What is the DNA of a Trojan? A Trojan is application-level rootkit data files that when improperly used seeks to modify an operating system, replace good system executables with bad Trojan executables that expose and exploit open ports, filenames, and system configurations in order to damage data located on servers, desktops, and workstations (Carrier, Brian D).

Digital forensic analysis is what cyber investigators are using to examine a cyber crime in progress or post cyber crime activity.

Ferocious and serious cyber invasions can cripple a financial institution if succumb by "backdoor" Trojan attacks from hackers by distorting information and content (Abdulla M.F., Ravikumar C.P).

Zeus and Clampi bank Trojans is the biggest and most well known bank Trojans infecting financial information systems today. URLZone bank Trojan exploits security holes in Internet Explorer 8, IE 7, IE 6, Opera, and FireFox using malicious JavaScript and Adobe PDF said Yuval Ben-Itzak Finjan Software (Mills, E).

The Washington Post reported in detail that cybercriminals located in the Ukraine with assistance of coconspirators in the United States unleashed the Zeus bank Trojan and stole $415,000 from Bullitt County, Kentucky (Krebs, T). Zeus is considered to a nasty bank Trojan because this bank Trojan is designed to use two steps of keystroke logging to access bank credentials online.

First, Zeus attacks the unsuspecting bank customer's own PC internet connection to validate access to the financial institution's information system and avoid detection of a cyber crime in progress.

Second, Zeus in a nanosecond creates a direct connection between an unsuspecting customer's computer that enables the cyber-pirate to falsely login into customers bank account using the customers stolen bank information (Krebs, T).

As technology advances, it is increasing important that information security stakeholders remain focus on the responsibility to protect the company's network, users, and software as well maintaining the integrity of information available online. Wireless peripherals play a major role in financial institution's business models and can be the focus of a cyber attack. Example, cyber criminals used precision-targeted hacking to attacked AT&T security then exposed more than 100,000 e-mail accounts of Apple Inc's iPad wireless peripheral users (Robertson, J). The hacker group that exposed the wireless vulnerability calls itself Goatse Security (Carlson, C). Personal e-mail and financial transactions on a wireless device should be a secure environment to exchange sensitive information.

5 CARDINAL RULES OF INFORMATION SECURITY

My research for this project paper lead me to the formation of what I believe to be a need for what I will call the CARDINAL RULES of Information Security related to all industries including financial institutions. CARDINAL RULES of Information Security is as follow:

1. Unprotected Information Systems is a Business Crime
2. Lack of Information Security Policy is Unacceptable
3. Audit and Compliance routinely to Identify Information Security Shortfalls
4. Risk Management Analysis Strengthens Information and System Security
5. Strong Virus Protection Policy help protect against Network Vulnerabilities and Threats

What is at stake when sensitive information is compromised online and all roads lead back to the custodian of the information?

In an age where hackers and online information bandits keep 24 hour vigilance as cyber intruders with intent on thief and crime; no information system is completely a safe zone. The best offence against cyber criminals who seek to compromise online system security is defense. Stakeholders who are responsible for online financial data must have a plan, policy, and protection related to information security.

In my opinion, CARDINAL RULES of Information Security should be adopted into the by-laws of all business models who expect to do online e-Commerce business in the future. Cyber threats and attacks are real, many go undetected, they occur every day, and will be on the rise in coming years. The facts are clear; the custodian of online information has the responsibility for the security of the data.

4 Conclusion

The four scenarios discussed regarding online crimes and malicious malware Trojans indicate that financial institutions face major challenges in the coming years defending against high tech robbery and attack by cyber thieves who purpose is to invent ways to infratrate data systems online to illegally access information, loot, embezzle, and steal money. What if the same minds that create bank malicious malware Trojans that successfully attack financial institution could be rehabilitated and trusted to use that same creative energy to reverse engineer counter attacks against financial cyber crimes. The best offense against cyber crimes is defense against cyber crimes. Financial institution manage security of their information system with great diligence, but it is a 365 days a year 24 hours a day 7 days a week responsibility. Just because your online network avoided a cyber attack one day will not insure a cyber attack will not happen the next day or occur in the future.

The negative impact and data integrity consequences of financial institutions without "Cardinal Rules" is infinity plus infinity; in other words there will be an endless degradation of sensitive commercial and personal financial information due to internet hackers access to unsecure financial systems online if cyber crimes using technology bombs like malicious code Trojans directed at financial institutions is not minimized.

Standard global and domestic policy regulation requirement for all financial institution's information system security along with legal enforcement for is non-compliance is needed. The security of a financial institution's information system is as strong as the weakest link in the chain. In other words, the security of an infrastructure needs to be strong; the enterprise scale virus protection software and engine should be updated and patched real time, and frequent information system security audits to identify risk and vulnerability to a financial institution should be mandatory. Criminal hackers do not care how they infiltrate an online information system, only that they are successful at getting pass layers of security check points to access accounts and financial data online.

It is the responsibility of every financial institution's stakeholder charged with the responsibility as the custodian of electronic information to redouble efforts to do all that can be done to combat cyber crimes.

Cyber attacks are escalating and internet criminals are using creative techniques to hack information systems; how financial institutions respond will determine who wins the data integrity prize daily.

An ambitious alliance effort against any and all who seek to cause unwanted risk to financial institutions is needed by financial institution decision makers, state and federal regulators, and all stakeholders responsible for bank and savings & loan industry information systems security.

The alliance will include all custodians of electronic commercial and personal banking legacy data. In addition, a secure global centralized database should be created as a watch list to identify cyber-criminals, their crimes, patterns and behavior of malicious and destructive banking Trojans, and any information regarding cyber-pirates and activity. If a known cyber criminal is identified and validated by intelligence as committing cyber crimes using malicious code Trojan cyber bombs their name, record, offense will automatically be posted in the secure global database and the maximum legal punishment will apply for the crime.

The goal of financial institution information system security stakeholders doing business online is not to lock down an information system so much that end users can not access the system and information online, but to create a secure environment, hacker free safe zone, and make the user experience the best it can be when banking online with a financial institution. The solution to financial internet crimes using malicious malware code cyber bombs is not simple it is complex, but to win the day to day online battle; stakeholders cannot become weak in online information security compliance effort or complacent.

Acknowledgment

The author wish to thank the UNIVERSAL GOD and Dr. Meledath Damodaran University of Houston-Victoria professor for this body of work.

References

1. Abel, W. (2009, March-July). *Agents, Trojans and tags: The next generation of investigators*. International Review of Law, Computers & Technology. Vol. 23 Issue 1/2, p99-108, 10p. Retrieved June 13, 2010, from http://search.ebscohost.com.ruby2.uhv.edu/login.aspx?direct=true&db=bth&AN=37362626&site=bsi-live&scope=site.

2. Abdulla M.F. and Ravikumar C.P. (2004). *A self-checking signature scheme for checking backdoor security attacks in internet*. Journal of High Speed Networks; 2004, Vol. 13 Issue 4, p309-317, 9p. Retrieved June 13, 2010, from http://search.ebscohost.com.ruby2.uhv.edu/login.aspx?direct=true&db=bth&AN=15285862&site=bsi-live&scope=site.

3. Bankrate.com. (2010, May 15). *Could Online Hackers Steal Your Cash*. Retrieved June 05, 2010, from http://finance.yahoo.com/banking-budgetingk/article/109549/could-online-hackers-steal-your-cash?mod=bb-checking_savings.

4. Carlson, C. FierceCIO. (2010, June, 11). *Lessons from AT&T/iPad user email address link*. Retrieved June 14,

2010, from http://www.fiercecio.com/story/lessons-t-ipad-user-email-address-leak/2010-06-11?utm_medium=nl&utm_source=internal

5. Carrier, Brian D. (2006, February). *Risk of LIVE DIGITAL FORENSIC ANALYSIS*. Vol. 49 Issue 2, p56-61, 5p, 3 Diagrams. July 2008, Issue 268, p10-11, 2p. Retrieved June 13, 2010, from http://search.ebscohost.com.ruby2.uhv.edu/login.aspx?direct=true&db=bth&AN=19568335&site=bsi-live&scope=site.

6. H.R. 4061—111 th Congress: *Cybersecurity Enhancement Act of 2010*. (2009). InGovTrack.us (database of federal legislation). Retrieved June 7, 2010, from http://www.govtrack.us/congress/bill.xpd?bill=h111-4061.

7. Krebs, T. (2009, July 02). *PC Invader Cost Ky*. County $415,000. Retrieved June 6, 2010, from http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html.

8. Mills, E. (2009, September 29). *Banking Trojan steal money from under your nose*. cnet news. Retrieved June 13, 2010 from http://news.cnet.com/8301-27080_3-10363836-245.html.

9. McMillan, Robert. (2009, September 29*). New Trojan Gives Criminals Full-service Bank Theft*. PC World; Sep 2009. Retrieved June 6, 2010 from http://www.pcworld.com/businesscenter/article/172859/new_trojan_gives_criminals_fullservice_bank_theft.html.

10. Robertson, J. (2010, June 10). *AT&T security hole exposes iPad users' e-mails.* Associated Press. www.washingtonexaminer.com. Retrieved June 13, 2010, from http://www.washingtonexaminer.com/local/ap/att-security-hole-exposes-ipad-users-e-mails-96016679.html.

11. OECD Observer. (2008, July). *Security and the Internet*. Issue 268, p10-11, 2p. Retrieved June 13, 2010, from http://search.ebscohost.com.ruby2.uhv.edu/login.aspx?direct=true&db=bth&AN=34045693&site=bsi-live&scope=site.