International Journal of Research
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

A Study And Research Is To Bring Awareness Of Increased Activity Of Cyber-Attacks Directed At Financial Institutions

(Online banking information security versus hackers)

T.LAKSHMI NARAYANAN
Assistant Professor, Department of Computer Science,
Government College of Arts and Science, Mettur Dam,
Salem Dist - 636 401.
lakshmitvr@rediffmail.com

ABSTRACT

In this article discuss four scenarios concerning cyber crimes exclusively bound for at financial institutions and give detailed examples. Also, I will converse the malevolent and URL zone bank malware Trojans that is at this time causing safety issues and threats to some financial institutions. Expected results from study and research is to bring awareness of improved movement of cyber-attacks aimed at at financial institutions, call for a global grouping against cyber-pirates, and point out that financial institution's have a accountability to defend and protected in sequence as custodians of their customer's responsive/heritage data online.

Keywords: cyber crimes, bank malware, online security issues and threats, cyber-attacks, cyber-pirates, network hackers.

Introduction

Billions of economic data communication occurs online every day of the year 24 hours a day 7 days week and bank cyber crimes take position each day when bank in turn is compromised. Expert unlawful hackers can operate an economic institution's online in turn system, spread malicious bank Trojan viruses that allow remote access to a computer, corrupt data, and hamper the superiority of an information system's act. If susceptible in turn regarding money-making and personal banking balance sheet is not better protected, cyber-thieves will prolong to dishonestly admission online monetary accounts to steal Trillions of dollars plus perceptive customer in turn globally. Audit of bank information technology systems, ethics and policy necessities for bank information sanctuary systems, responsiveness of threat potential, link of financial institution in turn systems all should be elevated on the list of federal & state regulators and banking board of director's schedule meetings. One major real world cyber crime bound for at any specific financial establishment can severely take down a domestic and global financial set-up.

Banks and Savings & Loans is acknowledged as economic institutions and both are custodians of not only their customer 's funds, but even more so a financial institution is answerable for their customer's individual and legacy data. Examples of information that financial institutions are the custodian of proceedings for their marketable and personal banking

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

customers is: day-to-day communication including deposits, withdrawals, balance amount, social sanctuary number, birth date, loan information, partnership agreements related to a loan, year-to-date statements and a host of other particularly sensitive financial in sequence. All the above declare records, transactions and susceptible in turn is events that take place online usually more than 50 percent of the time.

Cyber crooks, network hackers, cyber pirates, internet thieves is promising crime grouping of criminals and risk to online banking information protection systems. According to hearsay $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 genuine customer bank accounts to steal pass- words, fraudulent wire transfers, and hackers working from the surrounded by to negotiation the information security system of an financial institution, in other words; an inside job.

Method

In period where knowledge has outpaced the law concerning banking cyber crimes a lot of online pirates build it their full- time effort to challenge bank in turn security systems to find a summit of admission into an in turn system in organize to access bank data and steal money. Customers can be inexperienced about cyber crimes pending it is too late and all their money has moved out from their account.

When a possible customer walks from side to side the door of a financial institution to release a basic checking or saving account the customer is asked and necessary to make available all kinds of responsive in sequence like social safety number, driver license number, and sign an affidavit that authorizes the financial institution to obtain a recognition statement to check the customer's current credit account and there after each six months before an account is open. Then on top of that constraint; the new customer is asked by the financial institution to faith them with all that responsive in turn. Illustrated below are four scenarios and penalty of bank cyber crimes.

Scenarios

Scenario 1, let's say that a cyber-pirate introduces to a unvoiced and wicked bank Trojan to a financial institution's in turn system and domain that runs an agent or macro that extracts customer account in turn then text communication the information back to the hacker all in a nanosecond. When an online electronic procedure takes place where perceptive 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 safekeeping system has been compromised, two, the customer's sensitive information was stole. In a nutshell the financial institution was robbed just that quick.

Scenario 2, let's say an surreptitiously cyber pirate opens an account at a limited branch office of a national bank or reserves & loan financial intuition with the target on committing an electronic burglary of money and any customer information that is not protected on any server in any state were the financial institution is doing business and custodian of electronic records. How does an information systems safety measures team avoid cyber thief, execute application

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

safety intelligence and examination a cyber crime waiting to happen when the cyber criminal is one of their individual customers? Cyber crooks are opportunist. If a cyber crook sees an time to steal they will steal. A cyber crook looking for an opportunity to commit a crime is like a homeowner leaving the door not closed and a home robber checks every door and window of the home and fined that one door and window of the home that is not locked then access the home. The burglar has gained access to expensive assets. The two scenarios are unusual but the perception is the same. In other words, never give a cyber crook a window of occasion to negotiation expensive in turn.Information system security teams in charge for securing information/data should generate a cyber threat protection strategy, build layers of security to protect business process and data integrity and safety testing, build an information system safety team that will maintain each other aware of the newest cyber threat movement, information, trends, and frequent internal information system security audits.

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

Scenario 4, let's say a financial institution is looking for to create new business by targeting an audience of customers that are extremely attached to mobile phone connectivity. These detailed customers like better to receive monthly statements and access their account online by using the web browser tool enabled on their elegant receiver.

Customer entrance to financial accounts online using a neat phone is a large model and marketing idea but creates a whole new set of information system safety concerns for the financial institution's and the individual responsible for information system security. For example, the smart phone creates one more point of entry into the financial institution's information system that a criminal hacker can develop the prologue of a silent but fatal bank Trojan to a financial institution's information system if the system is not fully up- dated with the most recent internet security tackle at all times.

Result

What is the universal/familial standard rule for information system security for financial institutions evaluate heavy on the minds of chief information officers, regulators, internet safety administrators. For financial institution; who writes the cyber crime laws? Who sets the cyber-security financial institution information system strategy standards for private trade or federal government? Who is accountable for compliance, audit and guarantee of internet information system refuge for bank and financial institutions? Who are the in turn system safety police for financial institutions? What is the prospect of the internet and cyber security? (OECD Observer). Gone are days when a computer user can find the way the World Wide Web and not have computer safety and be naive about hackers and cyber criminals. The internet is a stunning world, but it can be joy and pain particularly if your internet practice collapse your computer; in addition to stealing sensitive economic and personal information.

FDIC – (Federal Deposit Insurance Corporation) is accountable for the solvency of bank institutions. FDIC has the federal regulatory accountability for audit and compliance of bank

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

information system security. FDIC should do fulfillment audits just like they do every bank that they cover and fall under FDIC narrow authority. Example, let's say a cyber cartel loots a bank online of all the money in every customer account at the bank including necessary reserve cash; and all the account are below the $200,000 FDIC insured account limits. Results, FDIC pays each customer the established deposit amount that was stolen by the cyber criminals. So it would be in the most excellent interest of the FDIC - Federal Deposit Insurance Corporation to be practical active about doing audit and fulfillment for security of bank information system s doing profitable and individual banking business online.

Every financial institution should have some type of in turn security policy or if they do not they should take on one soon and have it signed by the CEO, CFO, CTO and each panel member of the financial institution, ASAP before the bank regulators discover out. Not having information scheme safekeeping policy and not performing information system due attentiveness spells one word RISK.

Discussion

Bank Trojans appropriate online bank account information by exploiting security flaws in computer information systems. URL zone bank Trojan is extremely complicated and "the next production 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 root kit data files that when inappropriately used seeks to adjust an operating system, restore good system executables with bad Trojan executables that representation and develop open ports, filenames, and system configurations in order to break data positioned on servers, desktops, and workstations (Carrier, Brian D).

Digital forensic analysis is what cyber investigators are using to scrutinize a cyber crime in development or station cyber crime movement. Ferocious and serious cyber invasions can cripple a financial institution if give way by "backdoor" Trojan attacks from hackers by distorting information and content (Abdulla M.F., Ravikumar C.P).

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

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

Second, Zeus in a nanosecond creates a direct connection between an innocent customer's computers that facilitate the cyber-pirate to falsely login into customers bank justification using the customers stolen bank information.

As technology move forward, it is increasing significant that information security stakeholders remain focus on the responsibility to guard the company's network, users, and software as well maintaining the honesty of information available online. Wireless peripherals engage in activity a major role in financial institution's business models and can be the focal point of a cyber attack.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

Example, cyber criminals used precision-targeted hacking to attacked AT&T safety then uncovered more than 100,000 e-mail financial records of Apple Inc's iPad wireless tangential users (Robertson, J). The hacker collection that exposed the wireless vulnerability calls itself Goatse Security (Carl- son, C). Personal e-mail and financial transactions on a wire-less device should be a protected situation to exchange susceptible information.

Cardinal Rules Of Information Security

CARDINAL RULES of Information Security connected to all industries including financial institutions. CARDINAL RULES of Information Security is as follow:

1. Undefended Information Systems is a Business Crime
2. Require of Information Security Policy is Unacceptable
3. Audit and Compliance regularly to Identify Information Security Shortfalls
4. Threat Management Analysis Strengthens Information and System Security
5. Strong Virus Protection Policy help guard against Network Vulnerabilities and pressure

What is at stake when responsive information is compromised online and all roads go in front back to the custodian of the information? In an age where hackers and online information bandits keep 24 hour attention as cyber intruders with intent on thief and fault; no information system is absolutely a safe zone. The best offence aligned with cyber criminals who seek to com- promise online system security is security. Stakeholders who are answerable for online financial data must have a plan, policy, and protection related to information protection.

CARDINAL RULES of Information Security should be adopted into the by-laws of all production models who anticipate doing online e-Commerce business in the potential. Cyber pressure and attacks are real; many go unnoticed, they occur every day, and will be on the rise in approaching years. The facts are clear; the custodian of online in sequence has the responsibility for the defense of the data.

Conclusion

The four scenarios discussed regarding online crimes and malevolent malware Trojans point toward those financial institutions face most important challenges in the approaching years defensive touching high tech robbery and assault by cyber thieves who purpose is to formulate ways to right to use the data systems online to illegally admittance information, loot, embezzle, and steal money. What if the same minds that produce bank malicious malware Trojans that productively attack financial institution could be converted and trusted to use that same artistic energy to invalidate engineer contradict attacks against financial cyber crimes. The best offense touching cyber crimes is defense against cyber crimes. Financial institution supervise security of their information system with large 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 do violence to one day will not indemnify a cyber attack will not ensue the next day or occur in the potential.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

The unconstructive impact and data veracity penalty of financial institutions without "Cardinal Rules" is infinity plus infinity; in other words there will be continuous poverty of sensitive marketable and personal economic information due to internet hacker's right to use to unsecure financial systems online if cyber crimes using technology bombs like malevolent code Trojans bound for at financial institutions is not minimized.

Standard global and domestic policy parameter prerequisite for all financial institution's information system safekeeping along with legal enforcement for is non-compliance is desirable. The safety measures of a financial institution's information system are as well-built as the weakest link in the string. In other words, the safety of road and rail network needs to be strong; the enterprise level virus guard software and engine should be rationalized and patched real time, and every day information system safekeeping audits to identify risk and vulnerability to a financial institution should be compulsory. Criminal hackers do not care how they penetrate 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 stake- holder 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 increasing and internet criminals are using inventive techniques to hack information systems; how financial institutions take action will determine who wins the data truthfulness prize daily.

An ambitious association effort alongside any and all who try to find to cause not needed risk to financial institutions is desired by financial institution decision makers, position and federal regulators, and all stakeholders in charge for bank and savings & loan industry information systems safety.

The alliance will include all custodians of electronic profitable and personal banking bequest data. In addition, a locked global centralized database should be shaped as a watch list to identify cyber-criminals, their crimes, patterns and actions of malicious and critical banking Trojans, and any information regarding cyber-pirates and movement. 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 greatest legal penalty will apply for the crime.

The goal of financial institution information system safety stakeholders doing business online is not to lock down an information system so much that end users can not right of entry the system and information online, but to create a protected environment, hacker free safe zone, and make the user knowledge the best it can be when banking online with a financial institution. The explanation to financial internet crimes using malicious malware code cyber bombs is not trouble-free it is complex, but to win the day to day online battle; stakeholders cannot become weak in online information security observance attempt or satisfied

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,

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 08
August 2020

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,
3. Bankrate.com. (2010, May 15). *Could Online Hackers Steal Your Cash*. Retrieved June 05, 2010,
4. Carrier, Brian D. (2006, February). *Risk of LIVE DIG- ITAL FORENSIC ANALYSIS* . Vol. 49 Issue 2, p56-61, 5p, 3 Diagrams. July 2008, Issue 268, p10-11, 2p. Re- trieved June 13, 2010
5. H.R. 4061—111 th Congress: *Cybersecurity Enhance- ment Act of 2010*. (2009). InGovTrack.us (database of federal legislation). Retrieved June 7, 2010,
6. McMillan, Robert. (2009, September 29 *). New Trojan Gives Criminals Full-service Bank Theft* . PC World; Sep 2009. Retrieved June 6, 2010
7. Robertson, J. (2010, June 10). *AT&T security hole ex- poses iPad users' e-mails* . Associated Press. www.washingtonexaminer.com. Retrieved June 13, 2010
8. OECD Observer. (2008, July). *Security and the Inter- net*. Issue 268, p10-11, 2p. Retrieved June 13, 2010
9. Paul Jeffery Marshall (October 2010), international journal of scientific and engineering research, volume 1 , issue 1.