From Raids to Recovery:

An Analysis of the largest Retail Security Breaches in the United States

Ignatius I. Idio

George Mason University

Author Note

This research was conducted for the IT-103-011 “Intro to Computing” Lecture Course.

October 3rd, 2014.

GMU Honor Code Statement:

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/the-mason-honor-code/. I am fully aware of the following sections of the Honor Code: Understanding the Honor Code, Understanding the Consequences. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Abstract

This research paper analyzes wire feeds, weblogs, and trade journals that center on information related to two recent security breaches of retailers Home Depot and Target, and on-going investigations led by the U.S. government of the origination of the malware that infiltrated the databases of chains located in America, Canada, and Mexico, and its effects on customers who made purchases prior to and after the breach. The possibility of private information of consumers being stolen with the use of this virus is a primary concern addressed by these sources and the affected stores, whose managers are currently formulating and executing solutions to strengthen the defenses of the stores and the security of their patrons' credit card information. This paper will evaluate this recent development in IT Security and elaborate on its legal, ethical, security, and social aspects and issues, as well as suggest further research methods that are necessary to improving the safeguards of consumer databases for Target and Home Depot.

Keywords: security breaches, retailers, private information

From Raids to Recovery:

An Analysis of the largest Retail Security Breaches in the United States

Introduction

The days of both carefree and thoughtful shopping have come to a halt this past September of 2014. The early part of this month saw yet another breach in retail security in the United States, this time with Home Depot. The hacking incident takes place almost a year after Target stores were met with infiltration of their databases prior to Thanksgiving and Black Friday of November 2013. Recent investigations into both the Home Depot and Target incidents have yielded evidence of the malware stemming from hackers in foreign countries. Target and Home Depot are taking measures to compensate their customers, many of whom were affected

by the external pilfering of their credit card information, and restructure their security management in order to prevent intrusions from affecting their performance, but it may not be enough to extol the fear and possibility of a similar incident from occurring in the future. That is why it is important to discuss the legal actions that the United States government is taking to aide retailers, the ethical standpoints from which hacking and education of computer programming is viewed, the social effects of this security concern, and security tactics that are being implemented to combat these malicious external codes.

Background

Near the end of November of 2013, Target Corporation was hit with an alert of a fissure in their network of crucial transaction data caused by a virus known as BlackPOS, also known as Kaptoxa. According to Antone Gonsalves of ITworld.com (2014), "BlackPOS was designed by a Russian teenager to steal credit- and debit-card data from retailers' electronic payment systems." The young creator of BlackPOS was successful in stealing this valuable information from 40 million credit-debit card holders (D'innocenzio 2014), making it the largest breach in history to date. That is, until early this past September of 2014, in which Home Depot was targeted by a foreign intruder who managed to gain access to information from 56 million buyers in a majority of the Home Depot chains in the United States and in Canada (D'innocenzio 2014). Since these breaches were discovered, the United States Secret Service and other private IT companies have been investigating the matter, closely analyzing the structures of the databases of both retailers in order to pinpoint the exact areas where protection is necessary.

Legal Issues and Benefits

Not only is protection necessary for the cybernetic infrastructure of American shopper information, but it is also crucial to protecting the lives and ideals of American citizens who rely

on these retail stores for everyday living. Rhena Inocencio of Trend Micro states in an article from Progressive Digital Media Technology News (2014) that the BlackPOS malware "also contains links to media hostile to the US, including a cartoon of a matchbox emblazoned with the American flag stood alongside Molotov cocktails bearing the flags of Ukraine, Syria, Egypt and Libya" (*Alleged Home Depot*, 2014), which could prove to be dangerous for U.S. citizens who are affected by this virus since these terror groups are now in a position to potentially ruin the United States financially by tracing consumer credit card information to United States banks and possibly wiring deposits and savings of Americans back to their own countries, where they can use those funds to purchase weapons of mass destruction and terrorize their own governments if not the United States government. Fortunately, the data breaches have gotten the attention of Democratic senators "Jay Rockefeller (D-W.Va.) and Claire McCaskill (D-Mo.)…advocates for data security and breach notification legislation" (Sarkar 2014), who have written letters to Home Depot requesting more information about the matter. This close involvement of the U.S. government officials can prove to be helpful to the government itself and its people, as there are many citizens who still feel betrayed by the government in wake of Edward Snowden's leaking of the National Security Association's accumulation of private communications data from millions of citizens. The government can regain the trust of its people, but at the same time, it can also turn more people away since this attack was something the NSA might have been able to apprehend early on, especially with the advancements in American technology in which many people take pride.

Social Issues and Benefits

From the Space Race against Russia in 1958 (*Timeline of Space Exploration*, 2014) to the modern era with modifications of smartphone technology, the United States has prided itself on

its technological advancements and creations. But according to M2 Presswire (2014), "[the] Highest amount of fraud happens in U.S., and hardly a month goes by when there isn't a breach from some large U.S. retailer. U.S. lags in card security as compared to other countries."[6] Not only does this lower consumer and even citizen confidence in U.S. retailers, but it may also discourage consumers from purchasing from retailers as much as they have been doing before the discovery of offshore hacking activity within the web of safeguarded information. As a result, buyers will turn to making online transactions, which can be a better alternative to spending money and time on means of transportation to travel to retail stores, but it can prove to be a much more dangerous alternative because information entered on websites can never be erased once it is put out into cyberspace, which can provide ways for hackers to retrace that data back to the owner. In spite of this danger, people are slowly moving towards making online transactions more often nowadays, which leads to these online stores like Amazon, Netflix, and eBay gaining more popularity than ever before. Finally, now that other online stores like iTunes and Amazon are being used widely by teens and young adults, younger people will be able to appreciate using technology and learn more about making safer transactions both online and in their local shopping areas.

Ethical Issues and Benefits

Reviewing the evidence used earlier in the introduction to this paper will allow for a perspective on the morality of the data breach, and of computer science with youth as a whole. It is said by Antone Gonsalves (2014) that "BlackPOS was designed by a Russian teenager," which begs the question: how young is too young for children and teenagers to be given the freedom to program whatever codes and programs they desire? The potential that young people possess to do great and powerful things is often overlooked because of their inability to comprehend the

hardships, whether financial or technical, that can result from abusing that power. But if authoritative figures, whether they be parents or teachers, do not take the time to teach their children that controlling their potential is for their own good and the benefit of the people around them, then those children have the same if not greater chances of succumbing to the type of behavior that this Russian teenager is partaking in, the type of behavior that can get him into trouble not only with his own government, but the governments of other countries he targets, thus compromising any future relations of his with the United States and other countries based on his decision to commit a federal crime. Using this Russian teenager as an example of what could happen to children and teenagers who are skilled at programming but lack direction could lead children in the United States and in other countries to partner with organizations that teach them about ways the government uses people who work in the IT and Computer Science field, and can provide educational opportunities for these students to be certified by their governments and apply their knowledge under legal circumstances.

Security Concerns and Benefits

In light of Home Depot and Target's security breaches, there are solutions already being executed in order to assist buyers in defending their credit-debit information and other private information that was exposed during the infiltration. The Information Technology Business trade journal explains the new Masked Credit Cards created by the company Abine, which "protect consumers' existing credit cards by providing an alternative to giving out their real credit card for purchases. Masked Credit Cards have completely unique 16-digit card numbers, expiration dates, and security codes, so merchants never get consumers' real credit card info. These cards can be created with any existing debit or credit card, expire right after you use them" (*Abine's Masked Credit Cards*, 2014). This is a useful alternative for people who are wary about using their

personal credentials to make purchases. The only concerns that could arise from this type of security implementation is that customers will have to use their credit or debit cards to make this card, so they are still exposing their financial credentials to a company that could be securely unstable, a crucial factor that they may not contemplate until it is too late and Abine is hit with a breach of its own. A secondary issue could be that consumers may have to continue purchasing Masked Credit Cards since they are a one-time-only use for every purchase. Overall, while measures of defense against data breaches can be formulated and implemented, they must be done so enough time and consideration since one small flaw could prove fatal to the whole recovery process.

Further Required Research

Further research in this area will require detailed analysis of the institution of possible solutions and their strengths and weaknesses, especially if these solutions are meant to protecting databases against all types of malware. Types of malware and their effects on computer systems should also be considered as a component of research. Retail security breaches prior to the ones that have taken place in Home Depot and Target should be studied for the purpose of using past methods of recovery from successful foreign hacking attempts. International relations between the United States and Europe, especially those of the modern-day period and those that rely on the heavy use of network communication, should be another focal point in future studies.

Conclusion

On a final note, consumers of the western continent and the retailers that they depend on for everyday living, are entitled to their rights of being protected equally under U.S. federal authority and security, whose efforts should not be compromised by unwarranted identity and credit and debit card theft involving dangerous people from other nations.

References

"56 million payment cards compromised in Home Depot breach." (19 September, 2014). *Progressive Digital Media Technology News*. Retrieved from ProQuest Computer Science Collection on 01 October, 2014. http://search.proquest.com.mutex.gmu.edu/computerscience/docview/1563996184/F628E7F904FC4926PQ/1?accountid=14541

- This source provides details about the recent Home Depot security breach, including the number of people affected by the breach, as well as the time at which the malware used in the breach was present in Home Depot stores. This feed proves to be reliable because it is published in a medium that specializes in business news and other economic information. While the author is not listed in the publication information, the article has been published close to the time when Home Depot's breach occurred.

"Abine; Abine's Masked Credit Cards Stop Data Breaches Like Home Depot's - Unlike Apple Pay, They Work Everywhere Today." (30 September, 2014). Information Technology Business. p. 65. Retrieved from ProQuest Computer Science Collection on 01 October, 2014. http://search.proquest.com.mutex.gmu.edu/computerscience/docview/1564402598/A2E88120A4584818PQ/2?accountid=14541

- This source discusses a new development in credit-debit card information with the implementation of Masked Credit Cards, temporary credit cards that provide users and merchants with unique information that does not expose real private information of credit-debit card holders. This source is reliable because it provides links to Abine's website containing more information about the product. There is also a link in the article

that leads to a page where people specifically affected by the attack on Home Depot can subscribe to Abine's annual subscription plan.

"Alleged Home Depot breach may have involved Target malware." (08 September, 2014). *Progressive Digital Media Technology News*. Retrieved from ProQuest Computer Science Collection on 01 October, 2014. http://search.proquest.com.mutex.gmu.edu/computerscience/docview/1561118947/F628E7F904FC4926PQ/2?accountid=14541

- This wire feed provides details about the origin of the virus BlackPOS that was used to infiltrate Target retailer stores, linking it back to areas in the Middle East where anti-U.S. influence is present. The article also discusses the possibility of the Home Depot virus being the same virus that pilfered information from Target's stores. This cross reference to Target's breach incident strengthens the reliability of the article because it contains knowledge of other breaches that have recently affected U.S. retailers.

D'Innocenzio, A. "Home Depot Data Breach Far Exceeds Last Year's Target Hack." (18 September, 2014). *The Associated Press*. Retrieved from AOL Daily Finance on 02 October, 2014. http://www.dailyfinance.com/2014/09/18/home-depot-malware-hack-affected-56-million-payment-cards/

- This news article contains information about specific locations of Target and Home Depot stores in the U.S., Canada, and Mexico that have been affected by the breach, stating that Home Depot was affected more than Target. Profit and sales information of both stores is included. The article is posted on a site that covers specific business information and is supported by AOL.

Gonsalves, A. “Researcher disputes report BlackPOS used in Home Depot, Target attacks.” (15 September, 2014). *ITworld.com*. Retrieved from ProQuest Computer Science Collection on 02 October, 2014. http://search.proquest.com.mutex.gmu.edu/computerscience/docview/1562168162/9962277669E74863PQ/2?accountid=14541

- While the URL of the website may be professionally misleading, the article itself shares new information about the origin of the virus BlackPOS. The article disputes previous speculation about BlackPOS affecting both Target and Home Depot, and gives exact details about analyses have linked BlackPOS’ origin to a Russian teenager. This article comes from a blog that seems to specialize in IT security that is related to hacking.

Sakar, D. “Two Democratic Senators request more info from Apple, Home Depot about data breach incidents.” (11 September, 2014). *FierceGovernmentIT*. Retrieved from ProQuest Computer Science Collection on 02 October, 2014. http://search.proquest.com.mutex.gmu.edu/computerscience/docview/1561773699/9962277669E74863PQ/3?accountid=14541

- This article shares information about the involvement of the U.S. government, specifically Democratic senators Rockefeller and McCaskill, in investigations concerning the security breach of Home Depot and the leaking of private photographs from iCloud. The article also contains information about related articles and links to the letters written by the Democratic senators themselves. Therefore, this source is closely connected with the U.S. government because it provides primary source information.

“Timeline of Space Exploration.” (2009). *TheSpaceRace.com*. Retrieved from TheSpaceRace.com on 02 October, 2014. http://www.thespacerace.com/timeline/

- This website provides a timeline of the Space Race between the United States and Russia. According to the copyright information located at the bottom of the page, the website has not been updated since 2009, which may be crucial since this website is only eight years old. The copyright information also states that the website has no affiliation with NASA.

"U.S. Payments Authentication and Security Market Report 2014." (19 August, 2014). *M2 Presswire*. Retrieved from ProQuest Computer Science Collection on 01 October, 2014. http://search.proquest.com.mutex.gmu.edu/computerscience/docview/1554155121/F628E7F904FC4926PQ/3?accountid=14541

- This article provides reasons for why the U.S. is frequently targeted by hackers, as well as reasons for why the U.S. continues to be vulnerable to these cyber attacks. The article also discusses other U.S. retailers that have been affected by security breaches.

.