POS Attacks

Consumer and Retail Security Through the Lens
of the Target and Home Depot Breaches

Robert Lasell
Tufts University
Computer Security
12 December 2014

Abstract

It is nearly impossible to be a modern consumer without interacting with computers and databases at some point. This has inevitably led to computer security becoming increasingly relevant to consumers in all walks of life, as retailers and companies are given access to our private data (such as our credit card information) in the course of transactions. This paper will report on and discuss this issue, with a particular focus on the recent security breaches at major retailers including Home Depot and Target. Of particular interest is malware that targets point-of-sale systems to acquire consumer data as purchases are being made. The paper will also discuss the ramifications of companies apparently leaving bugs open even after those bugs have resulted in major breaches at other similar companies.

I. Introduction

Over the last two decades, computers have become completely ubiquitous, and nowhere is this fact more apparent than in retail. The role of computers and databases in online shopping is obvious, but, as modern consumers, we interact with computers constantly even when shopping offline in retail stores. While it is true that some businesses still rely exclusively on cold, hard cash, it has become impossible (or at least very inconvenient) to make major purchases without eventually using some form of electronic payment, usually a credit or debit card. This means that, at some point, a consumer's sensitive financial data will be fed into a retailer's computer system. Enter the point-of-sale system, or "POS". POS refers to the point at which a consumer's data is handed off to the network of a physical store; an example of a POS system would be the terminal through which a customer swipes his or her card, and possibly enters a PIN or signs their name. As they are simply the starting point for a customer's interaction with a retailer's computers, POS systems may seem relatively innocuous (indeed, many attacks on major retailers involve breaking into databases or other non-POS systems), but it is no

coincidence that many of the largest and most publicized computer security breaches in recent memory have been the direct result of poorly secured POS systems. This paper seeks to shed some light on these attacks and provide a starting point for retailer and consumer defense alike.

II. To the Community

Why study retail security? There are many reasons, but first and foremost is the fact that, as in many fields, the explosion of computer technology seems to have outstripped the focus on security; this phenomenon has far-reaching consequences. At a time when the average person's faith in the economy has been shaken time and time again, and data security is becoming an increasingly worrying subject, it is easy for consumers to lose their trust in retailers. Recent breaches have shown how quick customers are to withdraw their business if they feel a company is not capable of protecting their secure information – Target's profits supposedly fell 46% in the quarter following their massive POS breach in 2013[1]. Yet, across the board, retailers appear to be either unwilling or incapable of learning from their mistakes, and the mistakes of others, as evidenced by the continuing breaches resulting from POS attacks at numerous retailers. Notable among these is the 2014 months-long breach at Home Depot. This paper focuses on the breaches at Target and Home Depot, primarily due to their scale and similarity to one another.

III. POS Attacks

i. Why Attack POS Systems?

Point-of-sale systems represent a juicy target for attackers due to the fact that all information from the magnetic strip of a credit or debit card must pass through them at the beginning of a transaction before being passed on to other systems to be validated. If an attacker can extract this data as it passes through a POS system, or immediately afterwards, the data can be reproduced onto blank cards to create functional copies of the card in question. In practice, card data is typically sold in bulk by an attacker on underground internet marketplaces, after which buyers use the copied cards to make large purchases (such as expensive electronics) which can then be sold at a later date. Incredibly, attackers such as those involved in the Target breach even offer money-back guarantees to their customers if the credit cards are cancelled before their data can be sold on the black market[2][3][4].

ii. POS Attacks & Internal Networks

There are a few different ways in which an attacker can go about attacking a POS system, but the method used in most recent, large breaches is commonly referred to as "RAM-scraping." In order to perform a RAM-scraping attack, an attacker must first gain access to the internal network of the target retailer. The reason for this is at least three-fold. Firstly, the attacker must be able to install RAM-scraping malware onto the retailer's POS systems. As a safety measure, companies are required to adhere to certain security standards, overseen by the PCI Security Standards Council. One such standard requires that retailers keep POS systems (and, indeed, any systems that directly process

customer data) isolated from the outside network. However, these systems must be connected, at least to the retailer's internal network, for a multitude of reasons, including maintenance and updating, purchase data retrieval, and, of course, to pass customer card data on to banks and other such institutions so that the data can be validated. Unfortunately, this means that, if an attacker is able to gain access to a retailer's internal network, which can be accomplished via any of the hundreds of methods that exist to exploit web and other vulnerabilities, that attacker may be able to gain sufficient privileges to install their malware of choice onto POS systems in any of the retailer's physical locations[2][5].

The second reason that an attacker must gain access to a retailer's network is that, once their malware has performed its function and nabbed a consumer's card data, the attacker must be able to retrieve that data in order to sell it. Since POS systems are not connected to the public Internet, this means that the attacker must have the privileges necessary to transmit the stolen data internally to a staging area of their own creation, hidden within the target's internal network, from which the data can be sent out to a location of the attacker's choosing[2][4][7].

Finally, there is one more, potentially more subtle reason that an attacker might wish to gain high-level network privileges within a retailer's system. If an attacker is able to gain administrative privileges, they may be able to cover their tracks more easily within the internal network, whether by misleading security tools and officers, altering logs, or through other methods. This is critical, since, unlike other types of retail breaches where customer data is captured en-masse via database cracking or similar means, POS RAM-scraping requires that the attacker be able to keep their malware up-and-running

continuously for long periods of time; the longer the malware is running, the more customers will access compromised POS systems, and the more customer data can be harvested[2].

iii. POS Malware Anatomy

Once an attacker has access to the target's network, they will install various malware components onto POS systems and other parts of the target's network. The malware is typically disguised as harmless files; in some cases, including the Target breach, some pieces of the malware were even disguised as security software made by IT contractors servicing the retailer[6]. The main component of the malware, which is actually installed on the POS systems themselves, works by capturing card numbers and other data gleaned from a payment card's magnetic strip as the card is swiped and the data is stored briefly in the POS device's RAM. Although sensitive data is encrypted when it is sent around a retailer's internal network (for example, to be sent to a bank for validation), it is often in plain-text while still in the POS system. This allows an attacker's malware to simply store it in a file, where it will remain "safely" until the malware sends the data along, sometimes through a chain of computers and systems, to a hidden staging area set up by the attacker within the retailer's internal network. From there, the attacker sends bulk card information at his or her convenience from the staging area into the public Internet[2][4][7].

IV. Repercussions of the Target & Home Depot Breaches

i. Target

The 2013 breach at Target brought POS system vulnerability firmly into the public eye. It resulted in a massive business loss for Target, a persistent black eye to the company, the eventual resignation of Target's then-CEO, Gregg Steinhafel, as well as other senior executives[1]. According to Target and other sources, at least 40 million credit and debit cards were compromised[3]. This means 40 million people having to have new credit cards made, and 40 million potential opportunities for banks to take a hit due to fraud involving purchases made with stolen card data; no laughing matter!

ii. Home Depot

Almost a year after the Target breach, Home Depot discovered that it had been the ongoing victim of a similar attack. Because the Home Depot breach was discovered after months of under-the-radar activity by the attackers, it was responsible for even more damage than the Target attack – by Home Depot's own estimate, around 56 million cards[8]. In some ways, this breach was even less excusable than the Target breach in the eyes of many consumers, since it seemed to indicate that Home Depot had failed to update its security in the wake of Target's failings.

V. Defending Against Retail Attacks

i. Retailer Defenses

Target, Home Depot, Kmart, Dairy Queen, Neiman Marcus, UPS, P.F. Chang's – retailer after retailer has been hit by POS attacks in recent memory, and the list continues to grow. Fortunately, there are many ways in which a retailer can protect itself and its customers. Some of these are relatively straightforward, and it is likely that most companies already have staff members working on them. Companies should have staff focused on improving web security and strengthening defenses anywhere that a company's network might come directly into contact with outside attackers. For example, the Target breach allegedly began when an attacker was able to gain access to Target's network through a SQL injection attack on a Target web server. Other methods that seem simple but may be of help in detecting a POS attack include using up-to-date endpoint security software to secure every device. Although it is true that many modern instances of POS malware can be customized to deceive security programs, anything that might help detect an attack early is worth the money and effort, since – as noted earlier – POS attacks are ongoing, and worsen the longer they remain undetected. It could also be wise to encrypt card data as it enters a POS system ("point-to-point encryption"), thereby making it harder for an attacker to gain direct access to the information they hope to steal[2].

However, the most important step that any company can take to prevent the loss of business and face of a POS breach is simple: start taking security seriously. The Target

and Home Depot breaches involved a number of mistakes that should not have been allowed. In Target's case, a default username and password used by the manufacturer of a suite of IT software was implicated in the attack[6]; any security assessment worth its salt will advise that default usernames and passwords never be left unchanged, no matter how small or seemingly harmless the device in question[2][5]. Accessing a default account may give an attacker an in to the internal network, or grant them higher privileges within the network. At least one report contends that Home Depot management regularly ignored security suggestions and chose to optimize for low cost and downtime over careful security, including not updating security software and keeping costly features of software turned off[8]. In addition, some sources claimed that the POS malware used to attack Home Depot was a variant of the same malware that hit Target half a year earlier – something the Home Depot security team surely should have been looking out for[9]. These facts, and the fact that U.S. retailers continue to be hit by these same attacks, serve as evidence that companies are not yet treating computer security as the top-level priority that it is. Consumers trust their retailers with their data, and that data should be safe when inside of a retailer's internal systems.

ii. What Can YOU Do?

We have seen some steps that retailers might take in order to protect their customers from data breaches via POS attacks. However, the people most directly affected by the attacks at Target and Home Depot (and other similar attacks) are the consumers. So, what can you, the consumer, do to protect yourself? After all, it is <u>your</u> data that is at risk, and you have more of a stake in protecting it than any corporation or retailer does. The computer security side of POS defense falls to the retailers, so the

primary recourse of the consumer is financial care and awareness. This can manifest itself in numerous ways, many of which are things people already do or should do, such as monitoring bank accounts and credit cards closely, and quickly taking any steps necessary to protect oneself when breaches inevitably occur.

There is one more defensive tool that the consumer has at their disposal: the power to make retailers take security seriously. The sad truth is that data breaches are only an issue for companies because they affect a retailer's image, which may lead to fewer customers willing to shop at that retailer, which in turn would affect that company's bottom line. The only way to get retailers to make POS security (and computer security in general) a higher priority is to exercise your power as a consumer by voicing your concern to companies, and even refraining from shopping at retailers that suffer from lackluster security. Extreme? Perhaps, but necessary.

VI. Conclusion

Poor security continues to plague many industries and organizations where computers are used heavily. Nowadays, that list includes most major retailers. Until companies begin showing that they are willing to take the necessary steps to strengthen their internal security, POS attacks are a threat, and consumers and retailers alike should be aware of how they work, and how to defend against them.

References

[1] Harris *Faltering Target Parts Ways With Chief*
http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html?ref=technology&_r=0

[2] Symantec *Attacks on point-of-sales systems*
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf

[3] Krebs *Cards Stolen in Target Breach Flood Underground Markets*
http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

[4] Krebs *A First Look at the Target Intrusion Malware*
http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

[5] *Malware Targeting Point of Sale Systems*
https://www.us-cert.gov/ncas/alerts/TA14-002A

[6] Krebs *New Clues in the Target Breach*
http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/

[7] Cyphort Labs *POS Malware Revisited**
http://www.cyphort.com/wp-content/uploads/2014/11/POS-Malware-Report-WEB.pdf?utm_source=hs_automation&utm_medium=email&utm_content=12605277&_hsenc=p2ANqtz-8xt5-elbLpLqnN3P0Gvzl3tSRsADkHQmQc9YHir96g-GCokdvzvG2RhNOcNXaxx5skpwFo7r4ASlYw0AWMNr9tgIJquA&_hsmi=12605277
*Note: because this report requires registration with Cyphort to view, I have included a PDF of it in the GitHub repository that hosts this paper. I recommend this paper as a resource for those interested in reading a detailed, low-level, step-by-step analysis of the operation of a piece of POS malware.

[8] BusinessWeek *Home Depot Hacked After Months of Security Warnings*
http://www.businessweek.com/articles/2014-09-18/home-depot-hacked-wide-open

[9] Krebs *Home Depot Hit By Same Malware as Target*
http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/