IBM
MSS

INDUSTRY OVERVIEW: RETAIL

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: JANUARY 5, 2015

BY: DAVID MCMILLEN, SENIOR THREAT RESEARCHER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

Credit cards have been around for decades. They allow us to purchase items without having to carry large sums of cash. A small piece of plastic that offers so much convenience. Criminals target that convenience in many ways. Until recently, credit card fraud was mainly limited to a handful of methods;

- Physical theft of the card itself.
- Application fraud – an individual falsifies a credit card application.
- Intercept fraud – a credit card is applied for legitimately, but is stolen from the mail.

ATM skimmers have been around for a little more than a decade. They allow criminals to plant a card reading device covertly into a cash machine. The unknowing victims simply insert their card into the slot and the skimmer copies the data from the magnetic strip or the smart chip allowing the thief to reproduce the victim’s card.

As the world continued to progress into the Internet age, so followed the retail sector and the credit card once again became the target of criminal minds but with new focus. New theft strategies were developed specifically using the merchant’s own web site. Site cloning became very popular. A hacker copies the target web site and pushes it back up on their own web space after making a few minor edits to enable the transactions to follow a path back to them. A spam campaign is utilized to flood potential victims via email. The victims follow the link in the email to what appears to be a legitimate company. When they order goods or services via the web site, all of their personal information and credit card numbers are sent to the fraudster. To an unwary end user, this method is usually very successful.

In 2005, we witnessed the first attack targeting the retail Point of Sale (POS) systems that reside within the walls of the stores themselves. POS systems tie together payment processing, inventory and customer relationship management functions. One of the core weaknesses of these POS systems is they almost always use some variant of a Microsoft Windows environment. As a result, these systems are an extremely popular network entry point for criminals.

POS systems are being compromised by several different types of malware. The malware specifically intercepts the credit cards track 1 or track 2 data which is stored on the magnetic stripe. Criminals then re-encode the track data onto counterfeit cards. The main weakness of POS systems is that in order for a transaction authorization to take place, the data needs to be stored in the program memory in a decrypted state.

This report focuses on a few of the major data breaches, methods of data loss, and types of attacks targeting the retail industry. Additionally, this report highlights several types of malware utilized for POS attacks and how to mitigate the potential for sensitive customer data loss.

MAJOR RETAIL DATA BREACHES

According to the Privacy Rights Clearinghouse, more than 260 million retail records have been reported as leaked, lost, or stolen in the United States since 2005. This number would actually be much higher if data had been obtained for the 340 additional retail compromises documented since 2005 for which there is no total record loss listed.

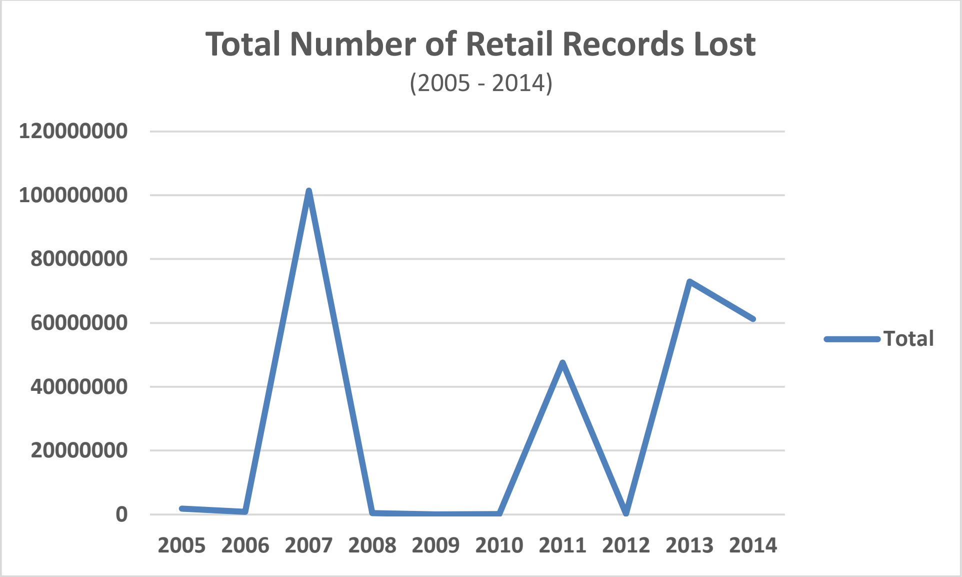

Figure 1. Timeline of number of retail records lost or stolen in the United States since 2005.[i]

The graph above certainly would have trended a little differently, if data had been captured for the additional breaches where no records were reported. However, it's unlikely that any of the breaches for which numbers were not reported would have exceeded the total number of records lost by the top three data breaches discussed below.

Review of Figure 1 above also may lead one to assume that there were many years where there were no breaches reported. However, this is not the case. Massive individual data breaches occurring at different times have skewed the scale so that years with less than 10 million records reported lost are not even a blip on the chart. Figure 2 below provides a view of the records lost, leaked, or stolen in the United States since 2005 with the following data breaches removed: The Home Depot (2014, 56 million); Target Corporation (2013, 70 million); Sony, PlayStation Network (PSN), Sony Online Entertainment (SOE) (2011; 12 million); Steam (The Valve Corporation) (2011, 35 million); and TJX Companies Inc. (2007; 100 million).

It's interesting that, despite removing the 2nd and 3rd largest data breaches from the data (Target Corporation (2013) and The Home Depot (2014), there remains a significant increase in the number of records reported compromised year over year since 2012. There is a 43% increase in records reported compromised over 2013. There is still time left in 2014 for more compromises, hence we expect that number to be slightly higher by the close of the year.

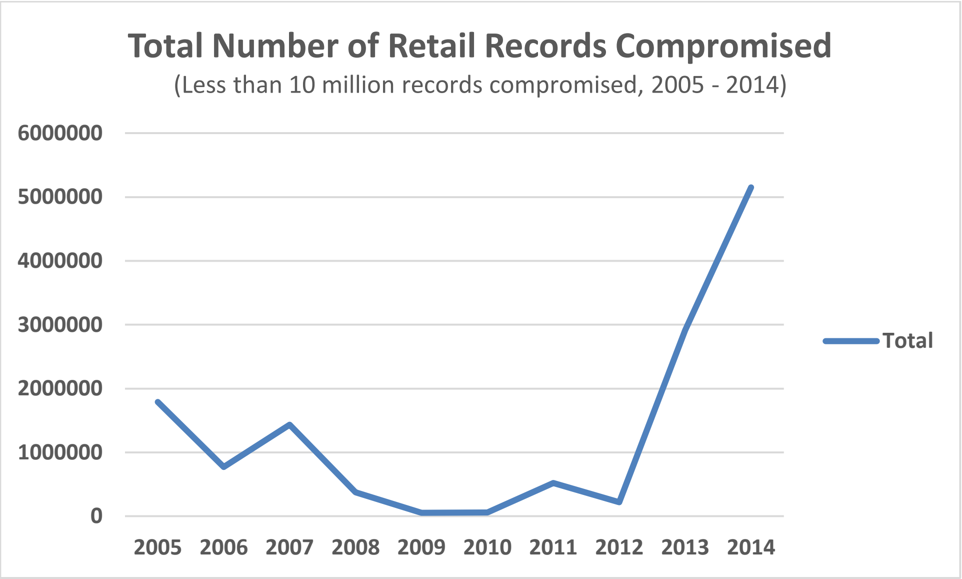

Figure 2. Total number of retail records lost in the United States since 2005 for breaches with less than 10 million records reported.[ii]

Ironically, while the number of records reported has increased, the number of total breaches reported has decreased since 2012. The number is down over 50% in 2014 from its peak in 2012. This means that, while we have seen fewer breaches reported in the last two years, these breaches were significant and wide-reaching in terms of victims affected.

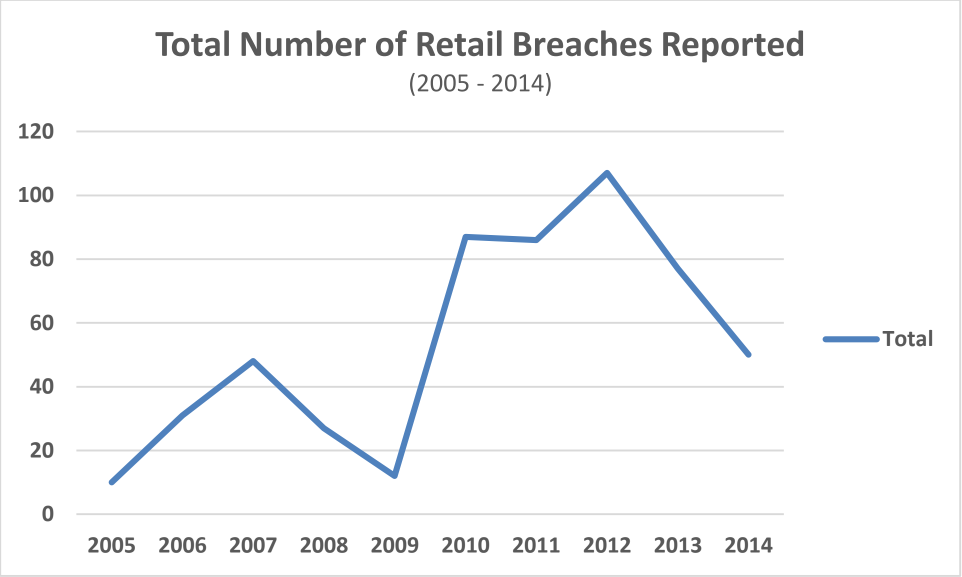

Figure 3. Total number of retail breaches reported in the United States since 2005.[iii]

The majority of the 260+ million retail records are the result of three data breaches from over 4400 reported by the Privacy Rights Clearinghouse since 2005.

In 2007, TJX Companies, Inc. was compromised resulting in over 100 million records stolen. The number was originally thought to be half of that however subsequent investigations have now revealed that this breach is in fact the largest of its type in history. Subsidiary stores including T.J.Maxx, Marshalls, Winners, HomeSense, AJWright, KMaxx and HomeGoods were all affected which resulted in the spike in Figure 1 above. All of these retailers were compromised by successful database attacks. Major factors that led to the breach included: outdated wireless encryption systems, failure to install firewalls and data encryption on computers using the wireless network, and failure to implement security software that was previously purchased. As a result, thieves were able to access data streaming between hand held price checking devices, cash registers and the stores' computers.

The Target Corporation breach is arguably the largest reported retail compromise, though it's difficult to determine total records reported based on official statements from the company. From their FAQ regarding the breach, "In mid-December 2013, we learned criminals forced their way into our system, gaining access to guest credit and debit card information. As the investigation continued, it was determined that certain guest information was also taken."[iv] They report that approximately 40 million credit and debit card accounts may have been impacted. Regarding the additional guest information, they report that 70 million individuals may be affected. What's not clear is if the 40 million credit and debit card records are part of the 70 million records. At a minimum, we know that 70 million records were compromised, therefore, we are listing this breach as the second largest reported breach. The compromise was traced back to a phishing attack targeting employees at Target's HVAC contractor, Fazio Mechanical, which contained a type of POS malware (Trojan.POSRAM).

The third largest major retail security breach was reported in September of 2014. The Home Depot also fell victim to a POS breach that affected over 2,200 stores. A significantly large amount of credit and debit card information immediately went up for sale on underground cybercrime sites. The number of breached cards exceeded 56 million. Specifically to blame for this breach was a type of POS malware called BlackPOS, addressed in the "Popular POS Malware" section of this report. The Home Depot uses Windows XPe on both the POS end point devices as well as the POS servers. This embedded O/S has many security holes and this breach demonstrates the importance of implementing a strong patch management process.

METHODS OF RETAIL DATA LOSS

Mining the public records for data loss reveals key insights into how exactly retail businesses are leaking customer data. There are many different methods in which data is stolen as indicated in Figure 4 below. In the data breach examples above, the methods used against the retail sector varied, however over 99% of these attacks had one thing in common - direct exploitation of an endpoint or successful deployment of malware.

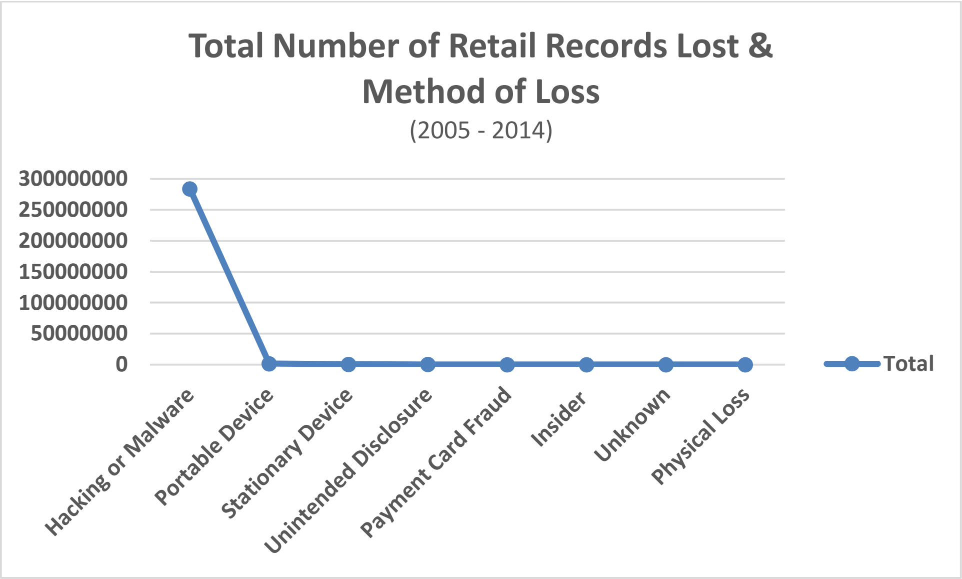

Figure 4. Breakdown of number of retail records lost and method of loss in the United States since 2005.[v]

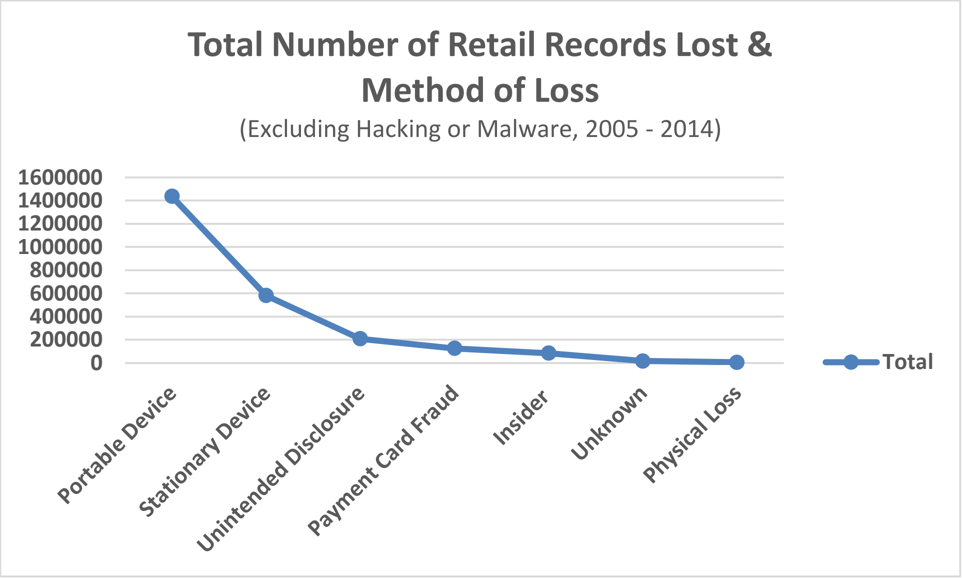

Figure 5. Breakdown of number of retail records lost and method of loss in the United States since 2005.[vi]

METHODS OF ATTACK

Managed Security Services has a wealth of information from our worldwide sensor network to see how attacks against any organization are being carried out. Let's take a look at the retail industry specifically.

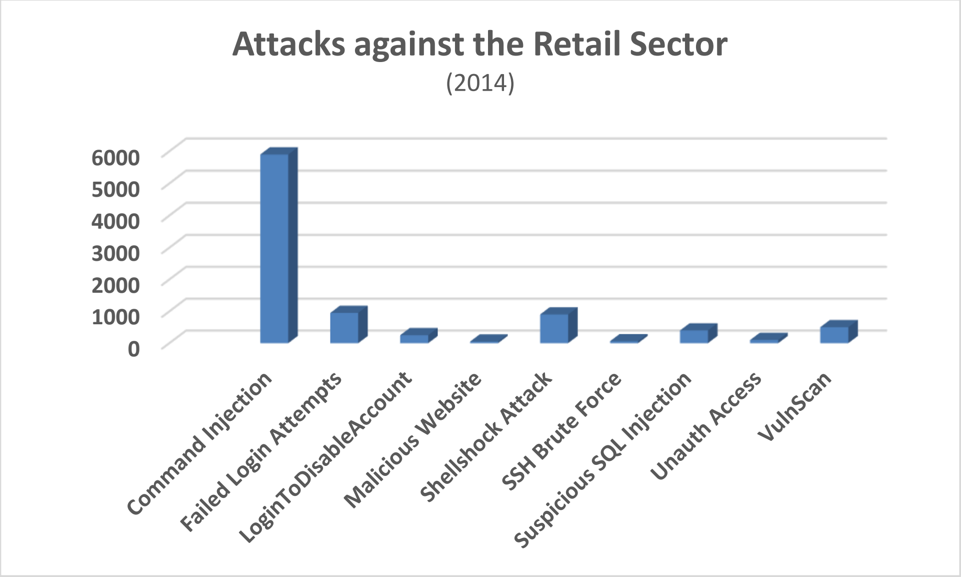

Figure 6. The majority of attacks seen against the retail sector via alerts in 2014.[vii]

COMMAND INJECTION

Although we have seen a rise in POS malware attacks, the majority of the attacks we have observed targeting the retail sector involve Command or SQL Injection. The complexity of SQL deployments and lack of data validation performed by security administrators make retail databases a primary target. Shellcode characters should never be allowed to enter an organization's network via HTTP. Deployment of security appliances that focus primarily on these attack vectors should be as routine as firewall deployments. IBM MSS Threat Research Group has published papers on the subject that help outline how attacks like these are carried out and how to help protect against them.

SHELLSHOCK

IBM MSS published the Command Injection paper three weeks prior to the Bash exploit disclosure. Those customers who took the time to implement the steps to mitigate shell code characters in their HTTP stream were virtually unaffected. Shellshock is not going away anytime soon much like SQL Slammer. Patching is of paramount importance for this specific attack vector.

POPULAR POS MALWARE

BLACKPOS: Responsible for The Home Depot breach, this POS malware was originally sold as "Dump Memory Grabber by Ree," and publicly disclosed by the Russian security firm Group-1B in March 2013. BlackPOS scans the memory of running processes for stored track 1 and 2 data. Once found, the data is then stored in a file called output.txt and is uploaded automatically to a predefined FTP server.

DEXTER: This is a Trojan horse which was publicly disclosed by Seculert in December 2012. Dexter scans the memory of processes looking for track 1 and 2 card data. Dexter utilizes HTTP communications with a command and control (C2) server to send stolen card data and receive updates. Included in this malware is an administration panel for browsing infected targets which is similar to the control panels in many banking Trojans.

VSKIMMER: This malware was disclosed my McAfee in March 2013. It utilizes the same mechanism as other POS malware however it only looks for track 2 formatted data. Vskimmer also utilizes HTTP to exfiltrate stolen card data to a C2 server. This malware can be configured to copy data to a specific USB device if it is not capable of connecting to the Internet.

ALINA: This Trojan was discovered by the SecureWorks Counter Threat Unit (CTU) in March 2013. Alina searches running processes for credit card track data. Alina also utilizes HHTP and a C2 server to upload its stolen card data as well as download and run updates.

CITADEL: Citadel is a well-known crimeware kit used to target online banking and credit card data strictly for fraudulent uses. This malware has the ability to track a user’s web browsing activity and embeds several features that allow it to identify and compromise POS devices. Citadel collects information about software installed on the infected host. Botnet operators can then harvest this information. This malware also has the capability to perform screenshots and keystroke logging.

RECOMMENDATIONS/MITIGATION TECHNIQUES

POS malware is a unique attack vector and its usage is expected to rise. Endpoint sales mechanisms must be hardened along with strict implementation of defensive appliances. At minimum, implementation of the following best practices are extremely important.

- **Use Strong Passwords:** During the installation of POS systems, installers often use the default passwords for simplicity on initial setup. Unfortunately, the default passwords can be easily obtained online by cybercriminals. It is highly recommended that business owners change passwords to their POS systems on a regular basis, using unique account names and complex passwords.

- **Update POS Software Applications:** Ensure that POS software applications are using the latest updated software applications and software application patches. POS systems, in the same way as computers, are vulnerable to malware attacks when required updates are not downloaded and installed on a timely basis.

- **Install a Firewall:** Firewalls should be utilized to protect POS systems from outside attacks. A firewall can prevent unauthorized access to, or from, a private network by screening out traffic from hackers, viruses, worms, or other types of malware specifically designed to compromise a POS system.
- **Use Antivirus:** Antivirus programs work to recognize software that fits its current definition of being malicious and attempts to restrict that malware's access to the systems. It is important to continually update the antivirus programs for them to be effective on a POS network.

- **Restrict Access to Internet:** Restrict access to POS system computers or terminals to prevent users from accidentally exposing the POS system to security threats existing on the Internet. POS systems should only be utilized online to conduct POS related activities and not for general Internet use.

- **Disallow Remote Access:** Remote access allows a user to log into a system as an authorized user without being physically present. Cyber Criminals can exploit remote access configurations on POS systems to gain access to these networks. To prevent unauthorized access, it is important to disallow remote access to the POS network at all times.

CONTRIBUTORS

Michelle Alvarez - Researcher/Editor, Threat Research Group
Nick Bradley – Practice Lead, Threat Research Group

REFERENCES

US-CERT Alert (TA14-002A) Malware Targeting Point of Sale Systems
https://www.us-cert.gov/ncas/alerts/TA14-002A

Privacy Rights Clearinghouse
http://privacyrights.org/data-breach

MSS Threat Research Papers
https://portal.sec.ibm.com/mss/html/en_US/support_resources/threat_papers.html

Researchers find new point-of-sale malware called BlackPOS
http://www.group-ib.com/?view=article&id=721

Dexter – Draining blood out of Point of Sales
http://www.seculert.com/blog/2012/12/dexter-draining-blood-out-of-point-of-sales.html

VSkimmer Botnet Targets Credit Card Payment Terminals
http://blogs.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals

Point-of-Sale Malware Threats
http://www.secureworks.com/cyber-threat-intelligence/threats/point-of-sale-malware-threats/

Citadel | Sophos Blog
http://blogs.sophos.com/tag/citadel/

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the benefit of IBM MSS clients only. This information is provided “AS IS,” and without warranty of any kind.

[i] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[ii] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[iii] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[iv] Payment card issue FAQ https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888

[v] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[vi] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[vii] 2014 IDS Data, IBM Managed Security Services.