The Low Cost and High Reward of POS Malware

By Adam Tyler, Chief Innovation Officer, CSID

CSID.COM

CSID®

A part of Experian

INTRODUCTION

Last year, Target and Neiman Marcus both experienced major breaches due to Point of Sale (POS) malware, bringing this type of security breach under intense scrutiny in 2014. Target's breach resulted in the loss of more than 40 million card numbers, including expiration dates, CVV codes and PIN numbers. Personal information for more than 70 million customers was also stolen including names, mailing addresses, email addresses and phone numbers.[1] Neiman Marcus' POS malware breach exposed data at more than 77 stores and resulted in 350,000 stolen credit and debit cards over an eight-month period.[2] Between the two retailers, more than 110 million customers were affected.[3]

The FBI has warned U.S. retailers to prepare for further cyber attacks on POS systems after linking malware used in the attack on Target to 20 other attacks in 2013.[4] To best guard against this growing threat, it is important to understand the ins and outs of POS malware. This paper will explore what it is, why the focus on POS systems now and what businesses can do to combat the threat.

The Lifecycle of POS Malware

POS malware naturally starts with a retailer's POS system. POS systems are designed in a way that makes it difficult for cyber criminals to steal information. The payment card industry has a set of standards, commonly referred to as PCI Data Security Standard (PCI DSS), which requires all companies that process, store or transmit credit card information to maintain a secure environment. PCI DSS requires the encryption of payment data when it is transmitted, received or stored.[5] However, at some point in the transaction process, the POS system has to host unencrypted data to process the payment. This is where POS malware comes in.

POS systems are not typically connected to the Internet, but are often connected with the company's internal network. This connection point is what makes them susceptible to malware. Any system that touches a network point can be infiltrated. All it takes is an employee clicking on a malware-ridden link or in the case of the Target breach, a third-party vendor with compromised credentials, for cyber criminals to gain access to the network and laterally work to access a company's POS system.

Once a hacker has access to the POS system, they can install a type of POS malware known as a RAM scraper. RAM scrapers are designed to extract payment data from a POS device's memory before the data is encrypted and transmitted. When a credit or debit card is run, data from the card is stored on the POS systems' random-access memory (RAM). PCI DSS requires sensitive data to be encrypted when it is being stored on a hard drive or transmitted through a network. This requirement is not applicable when the data sits on a POS systems' RAM. This opening gives cyber criminals the opportunity to steal the data by searching through the RAM of a POS machine for file names that are often associated with payment information and then scrapes that sensitive data and dumps it into a file or server that the criminal can access whenever and wherever.

While POS malware has made the news in 2014 due to the Target and Neiman Marcus breaches, it has actually been around for years. In 2007, TJX Companies lost more 45.6 million credit and debit card numbers after someone illegally accessed the company's payment system.[6] In 2009, Visa and Verizon published threat reports outlining a new type of malware called a RAM scraper.[7] Security and compliance standards evolve and the types of data that are valuable to cyber criminals shift. As these things change, cyber criminals will shift their focus to the type of crime that provides the most valuable data with the least amount of risk and effort. This is why we have seen the resurgence in POS malware. The

recent popularity of POS malware can be largely attributed to the following: increased availability of inexpensive, simple malware; more POS systems with increased complexity and connection points to the network; and the potential huge profits that can be made from a successful POS breach.

Evolution and Availability

In January 2014, RSA anti-fraud researchers identified a new strain of POS malware called ChewBacca. Researchers found that ChewBacca had been used to infect the POS systems of several dozen retailers beginning on October 25, 2013, resulting in stolen credit and debit card data in the U.S. and 10 other countries.[8] What is interesting about ChewBacca is its simplicity. The malware steals data in two ways – keylogging and memory-scraping. Both are simple functions and easily detectable by a good security system and yet ChewBacca managed to steal sensitive information from dozens of retailers around the world in a matter of months.

There has been a lot of speculation about the strain of malware used in the Target breach. IntelCrawler, a security research firm, reported that the mastermind behind the malware used in the Target attack is a 17-year-old boy. After creating the malware, called BlackPOS, he sold it to a number of hackers on the online black market for the relatively low price of $2,000.[9]

The simplicity of ChewBacca and the inexpensive availability of BlackPOS underlie the challenge that businesses are facing when it comes to POS malware. The community that creates and sells this type of malware is vast. It is knowledgeable and has seemingly limitless resources. POS malware is constantly being shared or sold on the online black market, and updated to outwit company security systems. All of these factors combined make it increasingly difficult for companies to protect against it.

POS Systems on the Rise

POS Systems can be incredibly complex. Not only do they read data off of debit and credit cards, but many also keep track of store and warehouse inventory, company promotions, and markdowns. As these systems are required to do more and track more, there are more connections to the POS system with outside networks and vendors. This makes the systems more vulnerable to malware and breach. The availability of POS systems is also putting businesses at risk. Historically, POS systems have been cost prohibitive for smaller businesses. Now that these systems are more widely available, their cost has decreased and more small businesses are adopting them. Unfortunately many of these small businesses don't have the security systems in place that larger corporations do, making them easy, profitable targets for cyber criminals.

Following the Money

According to the FBI, huge profits are being made off of POS malware both from hackers selling the code and cyber criminals using it to steal data from businesses.[10] Take, for example, Target's breach. Shortly after the breach was announced, CSID, a part of Experian started seeing bundles of the stolen cards appear for sale on the identity black market. Full debit and credit card numbers, including expiration dates and CVV codes were going for $20 to $100 each. A cyber criminal would have to sell just 100 stolen cards at $20 each to recoup the cost of the BlackPOS malware. Data for more than 40 million cards was stolen in the Target breach.

What Can Businesses Do?

The truth is, no POS system can be 100 percent secure but basic security measures can help. The following measures can be taken to reduce the risk and mitigate the impact of POS malware.

- **Use secure logins and passwords on all network systems and proactively monitor employee and vendor credentials.** In Target's case, a vendor's credentials provided access to the company's network, which ultimately led to access of the POS system. With proactive monitoring, employee and vendor credentials can be identified as soon as they are compromised, allowing the business to change the credentials before they can be used. Company IP addresses can also be monitored, giving businesses the opportunity to identify when sensitive data is leaving the company network and respond quickly.

- **Educate employees on security basics.** The basics include things like how to create secure passwords, not reusing passwords across multiple sites, how to identify malicious links, and what to do in the event a malicious link is clicked. Employees are often the weakest link in any security system. Education is an easy way to prevent costly mistakes.

- **Ensure that all POS software is up-to-date with the latest patches**. Updated versions can bring security and bug fixes that will keep card data safe.

- **Restrict POS system access to the Internet.** This will prevent users from accidentally exposing the POS system to security threats. This will not eliminate the threat of intrusions on a company's internal network.

- **Implement basic security measures like installing a firewall and encrypting sensitive information.** A firewall can prevent unauthorized access to and from a system. Encrypting sensitive information makes it more difficult for a cyber criminal to cash in on or use stolen data.

Looking to the Future

In the short-term, there is no sure solution to prevent POS system breaches. In the long-term, there are solutions that could be implemented that would reduce the impact of POS malware. One such solution is utilizing EMV-enabled credit cards. EMV stands for Europay, MasterCard and Visa. Traditional magnetic stripe cards store credit card numbers and expiration dates, which can easily be stolen and reused to make counterfeit cards. Conversely, EMV-enabled cards encrypt transaction data different each time the card is used, making counterfeiting incredibly difficult. It may be a while before EMV-enabled cards are widely available in the U.S.

For many retailers the cost of replacing their POS systems to be EMV-compatible outweighs the cost of a potential breach. But as the threat and cost of POS system breaches continue to increase, many retailers will likely look into speeding up the adoption EMV cards. Target's CFO announced in early February that the company is investing $100 million in order to be equipped to handle EMV technology by the first quarter of 2015. This is six months earlier than their previous implementation goal. [11]

As security measures are put into place that make POS system breaches more difficult and the data obtained from them less valuable, it is likely that the number of these breaches will decrease. Cyber criminals have proved that they follow the easy money. POS systems are just the latest in a long line of focused attacks and certainly won't be the last type of breach the security industry will have to deal with.

ABOUT CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

www.csid.com

ADDITIONAL SOURCES

[1] Data Breach FAQ, Target , 2013
[2] Neiman Marcus Downsizes Breach Estimate, *Bank Info Security,* 2014
[3] Who Should Pay for Data Theft?, *Bloomberg Businessweek*, 2014
[4] Target cyber attack not isolated, warns FBI, *ComputerWeekly.com,* 2014
[5] PCI FAQS, PCI Compliance Guide, 2014
[6] TJX data breach: At 45.6M card numbers, it's the biggest ever, *ComputerWorld,* 2007
[7] Understanding malware targeting Point of Sale Systems, Br Labs, 2014
[8] RSA Uncovers New POS Malware Operation Stealing Payment Card & Personal Information, RSA, 2014
[9] IntelCrawler: "The teenager is the author of BlackPOS/Kaptoxa malware, several other breaches may be revealed soon", IntelCrawler, 2014
[10] FBI Warns of More Cyber Attacks, *Financial Times,* 2014
[11] Are We Finally Ready for EMV Cards?, *Fox Business*, 2014