NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Point-of-Sale Malware: Continued Threat to Businesses and Consumers

July 27, 2015

TLP: **WHITE** | Point-of-Sale (PoS) malware breaches attracted wide media coverage throughout 2014 when at least thirteen major U.S. retailers suffered payment card data breaches, the largest affecting approximately 110 million customers. Although PoS incidents have largely remained out of the headlines thus far in 2015, payment card breaches have continued month to month and many new variations of PoS malware have been identified by law enforcement and security researchers. ***The NJCCIC assesses data breaches resulting from PoS malware will continue to occur at a steady pace throughout 2015 and pose a persistent threat to public and private sector organizations, particularly small to mid-size businesses that lack the cybersecurity resources to prevent, detect, and mitigate these threats.*** The industries most targeted by PoS malware include retail, food services, healthcare, education, and tourism. While the ongoing implementation of the more-secure Europay, MasterCard, & Visa (EMV) cards, also known as chip-and-PIN, is expected to mitigate PoS vulnerabilities and reduce fraud in the U.S., many retailers and cardholders will remain vulnerable until all EMV cards are issued and PoS terminals throughout the country are updated to accept EMV transactions.

Threat Overview

PoS malware is malicious software designed to steal credit and debit card data from retail payment processing systems. Since 2013, there has been a dramatic rise in the number of PoS malware variants, and the tools and knowledge to conduct these attacks are becoming more widely available through online criminal forums.[1] Ready-to-use PoS malware kits and the widely reported success of previous attacks have made PoS systems an attractive target and lucrative undertaking for criminals across the globe. Additionally, the 'swipe-and-sign' process used to complete transactions has been in place since the 1970s and is inherently insecure.

- Market research firms estimate that only 70 percent of U.S. credit cardholders will receive the new EMV cards by the end of 2015. Moreover, only 50 to 60 percent of PoS terminals throughout the U.S. are expected to be capable of accepting EMV transactions.[2]
- The new cards contain a microchip which authenticates transactions by generating a new digital signature each time the card is used. If criminals attempt to clone EMV cards, any transactions involving the use of the counterfeit cards would be denied due to the lack of a digital signature. However, until all PoS terminals are upgraded, even those with the new EMV-cards will continue to complete transactions with the traditional, and vulnerable, magnetic strip. A number of Western counties, including Canada, France, and the United Kingdom, have seen reductions in fraud since adopting the new EMV standard.[3]

How PoS Malware Works

PoS malware targets consumers' personal and financial data stored on one of up to three 'tracks' on the magnetic strip located on the back of a payment card. The majority of payment cards in the U.S. contain two tracks of data used by financial institutions to store a customer's information; some cards contain a third track.

- Track 1 stores 79 alphanumeric characters containing the customer's name, primary account number, card expiration date, and card verification value (CVV) code, along with additional characters to differentiate between data fields and identify endpoints.
- Track 2 stores 40 numeric characters and contains nearly the same information as the first track, except for the customer's name.
- Track 3 is not standardized among banks and therefore rarely used. If present, however, it may include an encrypted Personal Identification Number (PIN), country code, and currency units.[4]

When a payment card is swiped through a PoS system, unencrypted payment data from Track 1 and Track 2 of the card are briefly stored in the system's Random Access Memory (RAM) for authorization and processing before being encrypted for transmission and storage in the company's payment server. Although the payment card industry has uniformly adopted a strict set of data security standards which require end-to-end encryption of payment information, the RAM remains the one vulnerable location where PoS malware can exploit unencrypted payment information.
PoS malware uses RAM 'scrapers' to evaluate the clear-text RAM data by using regular expressions (regex) or the Luhn Algorithm to differentiate between Track 1 and Track 2 data versus other types of data. The malware then extracts the payment card data and transmits it back to the hackers via a command and control (C2) server.[5] That information can then be used to create fraudulent cards for physical use at retail stores and automated teller machines (ATMs), to make online purchases, or to sell for profit on black-market websites or forums.

The biggest challenge hackers face is gaining access to the targeted network to install the malware onto a PoS payment terminal. Some access vectors include:

1. exploiting weaknesses in a public-facing website
2. phishing campaigns to trick employees into clicking on a malicious link or attachment
3. accessing the network through a poorly secured device
4. using social engineering tactics to gain physical or remote access to the target's systems
5. compromising a third-party vendor with remote access to the targeted company's network

According to the Verizon's 2015 Data Breach Investigations Report, many PoS malware incidents that occurred in 2014 were the result of a company's employees being tricked into providing hackers with login credentials for remote access to the PoS system. Verizon reported a total of 198 PoS incidents in 2014.[6]

PoS Malware Variants

The following are examples of PoS malware variants that have impacted consumers, businesses, and organizations within the U.S. and worldwide [NOTE: all of these malware examples affect PoS systems running on a Windows OS platform]:

Dexter was first discovered in December 2012 by Seculert and continues to infect machines via phishing emails or by exploiting default system access credentials. After infecting the target PoS system, Dexter parses memory dumps for PoS processes that contain Track 1 and Track 2 card data. It simultaneously monitors changes in the system and maintains persistence by injecting itself into the Windows Explorer executable file and preventing session termination. It then communicates with a C2 server over HTTP (port 80) to transmit the card data back to the hacker. Variants of Dexter include 'Stardust', 'Millenium', and 'Revelation'.[7]

- Fortinet provides additional information about Dexter, including IOCs, here.

Alina was originally written in late 2012 but was not publicly disclosed until February 2013 and is believed to have come from the creator of the Dexter PoS malware strain. Organizations that have weak passwords for their remote access servers are vulnerable to this attack. Like other PoS malware variants, Alina contains a RAM scraper to harvest and transmit card data back to a C2 server over HTTP (port 80) using a C2 server. Other variants of Alina include 'Spark' and 'Eagle'. [8]

- Nuix offers a detailed breakdown of Alina and a signature to detect nearly all known versions here.
- Additional IOCs can be found on the Trustwave website here.

BlackPOS, also known as "Dump Memory Grabber by Ree," was first disclosed in March 2013 but continues to circulate and infect vulnerable PoS systems discovered by hackers conducting active network reconnaissance scanning. The malware uses a RAM scraper to find and extract the payment card data and then stores the data locally before it's uploaded to a remote server using File Transfer Protocol (FTP). BlackPOS has a variant known as KAPTOXA which is believed to have been used in some of the high profile retail breaches of 2014. KAPTOXA includes the ability to masquerade as a component of the antivirus software installed and running on the infected system.[9]

- IBM provides more information on BlackPOS/KAPTOXA, including IOCs, here.

vSkimmer, a successor to Dexter, was discovered by McAfee researchers in March 2013 in a Russian underground forum and demonstrates how PoS malware is evolving and adding new capabilities. The vSkimmer malware can connect to a C2 server to transmit card data but is also designed to transfer the data to a USB drive connected to the infected machine in the event an Internet connection is not available. According to McAfee Labs, USB drives are likely a primary method of infection for this variant and would require the hacker to have physical access to the machines.[10]

- McAfee Labs provides more information in vSkimmer, including IOCs, here.

Backoff is a PoS malware campaign that was determined to be active in October 2013 but the resulting attacks were not publicly disclosed until July 2014. The hackers use brute force techniques to gain access to victims' remote desktop servers in order to install the malware. Backoff uses its RAM scraper to harvest the payment card data and then transmits it back to the hacker over HTTP (port 80). Its C2 servers are connected to the same servers used to host other malware such as Zeus, SpyEye, and Citadel.[11] Three variants of the Backoff PoS malware include: 1.4, 1.55 (aka 'goo', 'MAY', and 'net'), and 1.56 (aka 'LAST'). Researchers have found that earlier variants included a malicious stub that is injected into the Windows explorer process to maintain persistence, but more recent variants dropped that capability in favor of a keylogging feature. Backoff also has the ability to uninstall prior versions of itself.

- The U.S. Computer Emergency Readiness Team (US-CERT) offers a detailed breakdown of each Backoff variant, including a list of the IOCs and mitigation strategies, here.

PoSeidon is a strain of PoS malware that Cisco discovered in March of 2015. The first step that this malware takes is to set and maintain persistence so that it can survive a system reboot. It then contacts a C2 server and retrieves a URL containing a piece of keylogger code to download and execute. Once the keylogger is successfully installed on the PoS terminal, PoSeidon checks the terminal's RAM for payment card data, searches for specific processes and number sequences, and then sends that information along with any recorded keystrokes back to the hacker. This variant also has the capability of updating itself and masks itself as Zeus malware in an attempt to evade further scrutiny by security researchers.[12]

- Cisco provides more information about PoSeidon, including IOCs, here.

LogPOS was first disclosed by Morphick in March 2015 and is the first PoS variant to use 'mailslots', a mechanism developed by Microsoft to allow system processes to communicate with each other to avoid detection.[13] LogPOS begins by attempting to create the string \\.\mailslot\LogCC and, if successful, compares host processes against a whitelist. It then injects shellcode into any processes not included on the whitelist, looks for payment card track data, and validates that data using the Luhn algorithm. Finally, it writes the data to the mailslot it first created and sends it to a C2 server via the HTTP GET request.

- Morphick provides more information about LogPOS, including IOCs, here.

FighterPOS, also known as BRFighter, was discovered by Trend Micro in April 2015 and labeled as a "one-man PoS malware campaign." This variant was used to steal more than 22,000 payment card numbers from Brazil, Canada, and the United States in just one month's time.[14] Designed and sold by a single threat actor, FighterPOS is written in Visual Basic 6 and collects both Track 1 and 2 payment card data by using a RAM scraper. It also contains a keylogger which allows the user to record additional sensitive information from infected systems. FighterPOS updates itself and copies itself to multiple locations to maintain persistence. Its control panel has a clean and well-structured interface that provides users with detailed information about their targets as well as a wide range of options for control and even includes a Distributed Denial-of-Service (DDoS) tool which can perform both Layer 4 (Transport Layer) and Layer 7 (Application Layer) attacks.

- Trend Micro provides more information on FighterPOS, including IOCs, in their report here.

Punkey was discovered and disclosed by Trustwave in April 2015 during a U.S. Secret Service investigation. Its name is a play on the 1980's children's TV show "Punky Brewster" and is believed to have evolved from the NewPOSThings malware family. Punkey works by injecting itself into the Windows OS Explorer process, creating registry start-up entries, and using a RAM scraper to look for any un-coded, plaintext credit card information. It then encrypts the data with AES and sends it to the hacker. Punkey also includes a keylogger to capture usernames and passwords that

employees use to log onto the system. It establishes a connection with a C2 server many times throughout a session to download code updates and additional malware.[15]

- Trustwave has more information about Punkey, including IOCs, here.

NitlovePOS, discovered by FireEye, began as a spam email campaign on 20 May 2015 and continues to circulate as it attempts to trick victims into opening infected attachments disguised as resumes and job or internship inquiries. The attachments, named *CV_[4 numbers].doc* or *My_Resume_[4 numbers].doc*, are embedded with a malicious macro. The spam email tries to trick the recipient into enabling the macro by stating that the attachment is "protected" and requires the editing option to be enabled in order to proceed. If the macro is enabled, it will immediately download the initial malicious executable which then downloads more malware from the hacker's server. It uses NTFS Alternate Data Streams to hide itself and evade detection, maintains persistence by monitoring for deletion attempts, and will restart itself if its processes are terminated. Similar to LogPOS, NitlovePOS also creates mailslots to store payment card data that it scrapes from the RAM before sending the data over SSL back to a C2 server located in St. Petersburg, Russia.[1]

- FireEye provides more information on NitlovePOS, including IOCs, here.

MalumPOS was discovered by Trend Micro in June 2015 and is distributed in various methods. MalumPOS specifically targets the Oracle MICROS Systems platform which is used by 330,000 customers in 180 countries.[17] MalumPOS is unique in that it disguises itself as the "NVIDIA Display Driver" (often stylized as NVIDIA Display Driv3r) in an attempt to avoid discovery. It monitors all running processes on the infected system and can target up to 100 processes for RAM scraping. After it finds the targeted Track 1 and Track 2 card data, MalumPOS extracts, encrypts, and saves the data in the following file path: C:\Windows\system32\nvsvc.dll. It also tries to avoid detection by modifying file time stamps and using dynamically loaded application program interfaces (APIs) to evade malware analysis tools.[18]

- Trend Micro provides more information on MalumPOS, including IOCs, in their technical brief here.

GamaPOS, discovered by Trend Micro in July 2015, is distributed through large spam campaigns containing malicious attachments or phishing links and uses the Andrometa botnet to infect PoS systems throughout the U.S. and Canada.[19] So far, GamaPOS has been seen targeting Visa, Discovery, and Maestro card data. Although closely related to NitlovePOS, GamaPOS distinguishes itself from other PoS malware as it is a .NET scraper which, up until now, has not been seen in prior PoS threats.[20] This variant has been targeting PoS systems in various industries including pet care, health care, consumer electronics, employment agencies, restaurants, software development, and industrial supply.

- Trend Micro provides more information on GamaPOS, including IOCs, here.

Common Characteristics of PoS Malware

- Brute-force password cracking on PoS terminals
- Targeting of tracks 1 and 2 of payment card data
- RAM scraping
- Keylogging
- Use of Remote Desktop to communicate with C2
- Use of HTTP POST request to check for updates
- C2 capabilities with bot masters
- Code injection for monitoring RAM processes
- Firewall evasion techniques
- Auto-run registry entries to maintain persistence
- Exfiltration of data via DNS requests
- Anti-virus (AV) evasion techniques

PoS Mitigation Recommendations

The following recommendations were derived from a joint product released by the Financial Services Information Sharing and Analysis Center (FS-ISAC), the United States Secret Service (USSS), and the Retail Cyber Intelligence Sharing Center (R-CISC), and represent a comprehensive strategy to mitigate the PoS threat. The full report is available here.

General Network and PoS Security

- Implement all recommended vendor patches and test to ensure the patch is successfully integrated. Refer to this best practices guide from Microsoft before implementing patches.
- Enforce up-to-date AV signatures, but do not only rely on AV signatures alone; criminals often customize PoS malware in order to bypass the targeted network's AV solution.
- Monitor firewalls for outbound traffic to unknown or suspicious IP addresses and domains.
- Mandate regular password changes, especially immediately before and after the holiday season, and enforce complex password rules for all network and remote access users.
- Implement multi-factor authentication wherever possible, especially for remote access applications and employees who manage customer data.
- Lock user accounts after multiple failed login attempts
- Implement malware detection software to identify anomalous and suspicious patterns of behavior.
- Implement software to detect key-loggers on PoS terminals.
- If possible, deploy a host-based intrusion prevention system (HIPS).

On the Network

- Ensure that your PoS systems have a firewall or proxy installed for protection.
- Deploy an appropriately configured intrusion prevention system (IPS).
- Employ proper network segmentation, such that PoS systems operate on a separate, protected subnet.
- All VPN access should be performed through the IPS and must use up-to-date authentication mechanisms.
- Segregate your PoS system from other network functions such as email and non-PoS related applications. If the PoS is attached to enterprise resource planning (ERP), inventory, or finance systems, use application gateways to ensure the PoS functionality is logically protected.

Encryption

- Confirm what data is at rest on PoS terminals and deploy endpoint encryption for those devices.
- Encrypting Card and PIN information before going into the payment terminal memory has been an effective technique to safeguard the payment data. There are several vendors who provide this technology.
- Some retailers have elected to replace in store payment terminals with new technology to encrypt card account numbers and other track data as it is swiped in the mag stripe reader or read by the chip reader.

Internet Access

- If the PoS is processed by software operating on a single terminal, consider not allowing that terminal Internet access, or restricting its internet access to only those destinations required for PoS functions (such as payment gateways).
- Do not use PoS terminals or other computers with access to PoS systems for Internet surfing, checking email, or accessing social media.
- Consider requiring two or more employees to approve any updates of the payment processing applications and, if possible, filter updates to terminals through a controlled server on the network.

Physical Access

- Ensure that there are no active USB ports or other media drives open on a PoS terminal. If running a Windows OS, ensure that auto-run is disabled to protect against insider threats.
- Inform employees to be on the lookout for skimmers, USB sticks, or other devices connected to PoS systems.
- Check all PoS systems, including card swipe equipment, for connected devices on a daily basis.
- Keep a detailed log of employees, vendors, and 3rd parties who access PoS terminals and servers.

White Listing

- Enforce a strict application whitelisting policy.
- Log and configure alerts triggered by any changes made to that whitelisting policy.
- Record and change default settings of any PoS hardware and software, including default passwords.

Application Security

- Perform Open Web Application Security Project (OWASP) audits on any web applications.
- Test databases and web login portals against brute force password attacks and SQL injections.
- Secure webservers that contain customer data, including payment gateways and e-commerce applications.
- Ensure that no unauthorized code has been introduced to the production environment.
- Run regular vulnerability scan against your approved applications and patch vulnerable software immediately. Re-run vulnerability scans whenever new or updated applications are introduced.

Remote Access Controls

- Segregate the payment processing systems from remote access applications when possible
- Restrict the network resources remote access users can access.
- Monitor remote user accounts for login abnormalities such as frequent failed login attempts, logins during non-normal working hours, and abnormal duration of logon.
- Enable and regularly review host-based security logs.
- Disable unused ports and services especially those that support remote access such as remote desktop protocol (RDP) and virtual network computing (VNC).

Third Party Vendors

- Conduct information security and risk assessments of all third party vendors with access to your network.
- Do not allow vendors to remote access your network with outdated and unsecure operating systems.
- Maintain an accurate list of third parties with remote access or physical access to the network perimeter.
- Require vendors to use multi-factor authentication (MFA) for remote access when possible. If MFA is not available, disable remote access except when specifically requested and scheduled by the vendor.
- Establish baselines for all 3rd party vendor network activity, including remote access and logins.
- Monitor 3rd party vendor activity for anomalous behavior such as frequent failed login attempts, logins during non-normal working hours, and abnormal duration of logon.
- Evaluate and limit third party network access privileges. For example, whitelist third party network addresses on a firewall provisioned to control remote access by third parties.
- Segment the network if possible through the use of secured VPNs with managed access control.[21]

Reporting

If your organization is the victim of a PoS malware attack, or would like to learn more about the NJCCIC, please contact a Cyber Liaison at njccic@cyber.nj.gov or visit www.cyber.nj.gov.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Sources

[1] Villeneuve, Nart. "Data Theft in Aisle 9: A FireEye Look at Threats to Retailers." FireEye. 6 October 2014. URL: https://www.fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html

[2] Xu, Kevin. "Three Critical Misconceptions About EMV". Payment Week. 21 July 2015. URL: https://paymentweek.com/2015-7-21-three-critical-misconceptions-about-emv-7748

[3] "EMV Cards are Proven to Reduce Fraud". Gemalto. URL: http://www.gemalto.com/emv/fraud

[4] "How Credit Cards Work." HowStuffWorks.com. 27 November 2006. URL: http://money.howstuffworks.com/personal-finance/debt-management/credit-card2.htm

[5] Huq, Numaan. "A Look at Point of Sale RAM Scraper Malware and How It Works." Naked Security. 16 July 2013. URL: https://nakedsecurity.sophos.com/2013/07/16/a-look-at-point-of-sale-ram-scraper-malware-and-how-it-works/

[6] "Verizon 2015 Data Breach Investigations Report". Verizon. April 2015. URL: http://www.verizonenterprise.com/DBIR/2015/

[7] Wilson, Curt. "Happy Holidays: Point of Sale Malware Campaigns Targeting Credit and Debit Cards." The Arbor Networks IT Security Blog. 3 December 2013. URL: https://asert.arbornetworks.com/happy-holidays-point-of-sale-malware-campaigns-targeting-credit-and-debit-cards/

[8] Grunzweig, Josh. "Aline Continues to Spread its Wings". Nuix. 9 January 2015. URL: http://www.nuix.com/blog/alina-continues-spread-its-wings

[9] Krebs, Brian. "Home Depot Hit By Same Malware as Target." Krebs on Security. 7 September 2014. URL: http://krebsonsecurity.com/tag/blackpos/

[10] Walker, Danielle. "VSkimmer Trojan Steals Card Data on Point-of-Sale Systems." SC Magazine. 22 March 2013. URL: http://www.scmagazine.com/vskimmer-trojan-steals-card-data-on-point-of-sale-systems/article/285725/

[11] Villeneuve, Nart. "Data Theft in Aisle 9: A FireEye Look at Threats to Retailers." FireEye. 6 October 2014. URL: https://www.fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html

[12] Chickowski, Erica. "Will POSeidon Preempt BlackPOS?" Dark Reading. 23 March 2015. URL: http://www.darkreading.com/attacks-breaches/will-poseidon-preempt-blackpos/d/d-id/1319585

[13] Vankempen, Mark. "A New Variant in POS Malware." LogRythm. 16 March 2015. URL: https://blog.logrhythm.com/security/new-pos-malware/

[14] Trend Micro Forward-Looking Threat Research Team. "FighterPOS, the Anatomy and Operation of a new One-Man PoS Malware Campaign." Trend Micro. April 2015. URL: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/wp-fighterpos.pdf

[15] Muncaster, Phil. "Punkey POS Malware Sets Sights on More Retailers." Infosecurity Magazine. 15 April 2015. URL: http://www.infosecurity-magazine.com/news/punkey-pos-malware-sets-sights-on/

[16] Villeneuve, Nart and Regalado, Daniel. "NitlovePOS: Another New POS Malware." FireEye. 23 May 2015. URL: https://www.fireeye.com/blog/threat-research/2015/05/nitlovepos_another.html

[17] Oracle Corporation. "Oracle and MICROS Systems." Oracle. 2014. URL: http://www.oracle.com/us/corporate/acquisitions/micros/index.html

[18] Yaneza, Jay. "MalumPOS History and Characteristics." Trend Micro. June 2015. URL: http://documents.trendmicro.com/images/tex/pdf/MalumPOS%20Technical%20Brief.pdf

[19] Xu, He. "A Good Look at the Andromeda Botnet." Fortinet. 16 April 2014. URL: https://blog.fortinet.com/post/a-good-look-at-the-andromeda-botnet

[20] Yaneza, Jay. "New GamaPoS Malware Piggybacks on Andromeda Botnet; Spreads in 13 States." Trend Micro. 16 July 2015. URL: http://blog.trendmicro.com/trendlabs-security-intelligence/new-gamapos-threat-spreads-in-the-us-via-andromeda-botnet/

[21] "Protecting Merchant Point of Sale Systems during the Holiday Season". Financial Services Information Sharing and Analysis Center (FS-ISAC), the United States Secret Service (USSS), and the Retail Cyber Intelligence Sharing Center (R-CISC). 7 November 2014. URL: http://www.secretservice.gov/HolidaySeason-2014.pdf