Point of Sale Security:

DEFENDING AGAINST POS MALWARE

www.alienvault.com

Point of Sale (POS) Security

This paper will take a look at PoS security and some of the common types of malware used to exploit these systems. Point of Sale (POS) systems are used to enable debit and credit card users to provide payment information to purchase goods or services. These systems include a range of hardware and software, including the ubiquitous POS terminals in retail locations as well as the applications used to process the payment data.

How does POS Malware Work?

POS malware has typically targeted Windows-based POS terminals.

Payment card data is most vulnerable when it is in memory as this is where it is least protected. This makes POS RAM scrapers very successful at stealing data. To keep data safe during transit, i.e. when it is passed between systems for processing a payment, it should be encrypted. If it is not, then attackers have yet another way to capture/steal card data.

However, POS terminals based on Apple's iOS and Google's Android OS have been gaining market share. The security models on these mobile operating systems have, thus far, raised the bar high enough that widespread attacks against those POS systems have not yet occurred. However, this may just be a matter of time, so when thinking about POS security it is important to understand how POS malware operates.

Common Attack Methods

- Vulnerable Software: When POS systems are configured with vulnerable versions of POS software, this opens the door to attack. When POS systems are purchased from vendors, they come with vendor-specific software that may have built-in vulnerabilities. Attackers can leverage these vulnerabilities to compromise the POS system and access credit card data.
- Abusing Remote Access Functionality: According to investigations of multiple breaches, attackers often obtain access to data by utilizing a remote administration utility using default credentials. These default credentials are added during the installation of POS software. Using a RAT and default credentials, an attacker can easily breach POS systems.
- Phishing: A very common & effective method of infection used to distribute a lot of POS malware. Phishing emails are sent to selected targets and malware is delivered either as malicious attachments or as embedded malicious links.
- Vulnerabilities in Host OS of POS Systems: Infecting the Operating System that powers ATMs/POS terminals with malware capable of stealing financial data is very efficient, as cyber crooks only need to compromise a few devices to collect credit card data and sell it in the underground market.
- Insider Threats: A malicious insider can cause quite a bit of damage to the enterprise as he/she has authorized access to POS systems and can infect the environment with POS malware. In some cases, malicious employees plug flash drives containing malware into servers containing sensitive data to compromise the payment systems.

Attackers utilize one or more of the various attack methods to compromise POS systems and infect them with POS malware to target and capture specific card data and exfiltrate the data to another system, possibly a CnC.

POS Malware:
COMMON METHODS & FEATURES

CARD DATA MINING

Credit card data (track 1 and track 2 information) is often stored in plain text in memory on the POS device. Several variants of POS malware leverage memory-scraping capabilities to capture the credit card data using regular expressions (RegEx), when searching through memory to find it. In fact, different families of POS malware sometimes share parts of RegEx or the entire RegEx. Regular expressions are an easy way to search for patterns that identify specific kinds of data; however, they can be computationally inefficient. Because of this, other malware variants use custom search algorithms to make their searches more efficient. Usually, these custom search algorithms will look for specific pieces of information: track delimiters, account number prefixes that correspond to major card issuers, primary account number (PAN) length, and some validate PANs using the Luhn algorithm. When the malware uses targeted custom searches, rather than scanning all data for patterns, the activity associated with the malware becomes more difficult to detect.

PROCESS INJECTION AND BLACKLISTING

Some POS malware reduce their footprint to avoid detection by injecting processes. In addition to this they increase performance by limiting the number of processes used in memory scraping. Some kinds of POS malware scrape memory from every process to increase the likelihood of obtaining useful information; however, this also increases the odds that someone will notice the malware. To avoid this, most POS malware has a blacklist of processes that are omitted from memory scraping and instead targets a few specific processes.

POS Malware:
COMMON METHODS & FEATURES

KEYLOGGING

A common feature of malware that usually accompanies memory scraping is key logging. Key logging allows attackers to capture PINs in addition to account numbers. PIN pads are usually recognized by an operating system as a keyboard device, so attackers don't need to write fancy new key logging codes to steal data from PIN pads.

DATA EXFILTRATION

Once POS malware has captured account details using the above techniques, attackers need to have some way of accessing this data. Some types of POS malware only store the data locally and don't have built-in exfiltration features. In such cases, attackers have to manually retrieve the data – typically via some kind of remote session, though manual recovery through physical access is also a possibility.

However, many variants of POS malware do have built-in exfiltration features that send stolen data to drop sites or command and control servers. Data exfiltration can take many forms. It can range from exfiltration via e-mail, FTP, HTTP, HTTPS, DNS, TOR or other protocols. Some transmit data in plaintext while others obfuscate or encrypt data before transmission.

POS Malware:
COMMON METHODS & FEATURES

ADDITIONAL FEATURES

Stealing credit card account details is not always the only objective of POS malware. Some variants can also incorporate other standard Trojan features such as:

- Credential harvesting (from browsers and remote access software)
- File download/upload capabilities
- File management
- Anti-debugging
- Anti-detection capabilities

Specific POS Malware Families

Now that we have a good understanding of the various capabilities of POS malware, we can look more closely at behaviors associated with some of the best-known malware families:

Rdasrv

Rdasrv was one of the earliest identified POS RAM scrapers, discovered in early 2011. Rdasrv functions in a manner that is distinct from all other POS RAM scrapers. Instead of looking at all of the processes, it only inspects processes that are hard coded into the malware itself. Patterns that match are written to a text file for manual exfiltration at a later date.

Dexter

Back in 2012 reports emerged on Dexter. Dexter has infected hundreds of point-of-sale computers at big name retailers, hotels, restaurants, and other businesses, according to a report issued by Aviv Raff, chief technology officer of Israel-based security firm Seculert[1].

Dexter steals payment card data from the POS system and sends it to a remote C&C server. The source code for Dexter was leaked sometime ago, leading to many variants being created even to this day as people improve upon the code base.

[1] http://arstechnica.com/security/2012/12/dexter-malware-steals-credit-card-data-from-point-of-sale-terminals/

Specific POS Malware Families

Alina

Alina is a fairly well known POS RAM scraper family, which was discovered in October 2012. As of the writing of this document, Alina variants are still being actively developed by the malware writing community. As a result, its methods of persistence, RAM scraping, and data exfiltration can vary from version to version. For example early versions sent data in plain text, while later ones utilized exclusive or XOR- based encryption, or established contact with multiple C&C servers, etc. Alina variants cast a wider net than other families because targeted processes are not hard-coded, making the malware more versatile and able to target a larger set of victims[2,3].

BlackPOS

BlackPOS rose to fame, or perhaps infamy, when it was discovered on the POS systems in retail giant Target, in December 2013. However, back in 2012, the source code of BlackPOS was leaked, which enabled many parties both malicious and non-malicious to examine and improve its codebase. It maintains persistence by masquerading as an AntiVirus program. The exfiltration methods used by the BlackPOS are fairly simple: track 1&2 payment card data is written to a file and offloaded to a FTP for later extraction[4,5].

[2] http://www.xylibox.com/2013/02/alina-34-pos-malware.html

[3] http://blog.spiderlabs.com/2013/05/alina-shedding-some-light-on-this-malware-family.html

[4] http://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/

[5] http://money.cnn.com/2014/02/11/news/companies/retail-breach-timeline/

Specific POS Malware Families

FrameworkPOS

Like BlackPOS, FrameworkPOS rose to infamy after it was found on the POS systems of another major retailer, The Home Depot. FrameworkPOS achieves persistence by installing a Windows Service, which starts at system boot and restarts. The service name is "McAfee Framework Management Instrumentation," a name likely chosen to allow it to further blend in. Like many malware families, FrameworkPOS has many variants, one of which stands out due to its method of data exfiltration. Another variant utilizes DNS requests to exfiltrate date, instead of the standard write file to a FTP (as seen during the Home Depot breach)[6,7].

Chewbacca

Chewbacca was discovered on the POS systems of several dozen different retailers around the world in late 2013. To maintain persistence, it installs itself as "spoolsv.exe" in the startup folder. After installation, the keylogger creates a file called "system.log" inside the system %temp% folder, logging keyboard events and window focus changes. Chewbacca also scrapes memory and utilizes regex to extract track 1 & 2 data of payment cards from the infected system. The extracted information is then transported via tor to a C&C server concealing the real IP address of the Command and Control (C&C) server(s), encrypting traffic, and avoiding network-level detection[8].

[6] https://blog.gdatasoftware.com/blog/article/new-frameworkpos-variant-exfiltrates-data-via-dns-requests.html

[7] http://www.cyphort.com/wp-content/uploads/2014/11/POS-Malware-Report-WEB.pdf

[8] https://securelist.com/blog/incidents/58192/chewbacca-a-new-episode-of-tor-based-malware/

Specific POS Malware Families

Backoff

Unlike many of the earlier malware families, Backoff was not built with a specific target in mind, which has allowed it to be used to cause a large number of data breaches. One of the larger ones targeted UPS stores between January and August, 2014. Backoff is also unique in that it uses a runtime packer to protect it from being detected. To maintain persistence Backoff will create an encrypted copy of itself. If the malware stops running for any reason, nsskrnl will be decrypted and executed to re-infect the system by utilizing a code that was injected into an explorer.exe process. Exfiltration and remote control is accomplished by communicating with a remote C&C via HTTP.

Cherrypicker POS

The malware dubbed Cherrypicker POS has been around undetected since roughly 2011. It avoids detection by the use of encryption, obfuscation and cleaning up after itself. It injects various based upon it's configuration and memory scrapes for track 1 and track 2 data, which is then logged. The logged file is then encrypted for communication back to the remote FTP.

Specific POS Malware Families

AbaddonPOS

AbaddonPOS is a simplistic piece of POS malware, coming in at around 5 KB in size. The malware implements several anti-analysis and obfuscation techniques to make manual and automated analysis difficult. To acquire track 1& 2 data the malware scraps all processes memory except it's own. The majority of the AbaddonPOS's code is not obfuscated with the exception of the code to encode and transmit payment card details. Which could be explained because unlike many POS malware families, which utilize existing prototols, such as HTTP/IRC/Tor to communicate with a c&c, Abaddon developers created their own binary encoded protocol to exfiltrate data.

New POS Security Techniques

October 1, 2015 marked the deadline set by credit card issuers to shift liability for fraudulent activity from card issuers or payment processors to the party that is the least Europay-MasterCard-Visa (EMV) compliant during a fraudulent transaction. In order to be EMV-compliant, retail merchants should, at a minimum, be switching to EMV card readers that are capable of accepting chipped credit cards.

However, switching to the new EMV standard does not eliminate the danger of POS malware. In addition, EMV itself might not make economic sense for all merchants.

As a POS security technique, the new, chipped cards are definitely more difficult to counterfeit than traditional cards (though a recent case showed that this is not impossible[9],[10].) However, since there is no requirement that new card readers encrypt card data before it reaches POS random access memory (RAM), it might still be possible for RAM scraping malware to extract account numbers and expiration dates even if merchants are using EMV card readers. These stolen account numbers can then be used by cybercriminals in card-not-present transactions (for example, e-commerce) or at locations that still use magnetic stripe readers (without CVV verification).

---

[9] http://www.cl.cam.ac.uk/research/security/projects/banking/nopin/oakland10chipbroken.pdf

[10] http://www.wired.com/2015/10/x-ray-scans-expose-an-ingenious-chip-and-pin-card-hack/

Tokenization

To better protect account numbers from such RAM scrapers, some payment solutions are utilizing tokenization and point-to-point encryption (P2PE). Payment tokenization is the process of replacing the account number with another non-sensitive value that can be mapped back to the actual payment details. However, the actual implementation of tokenization can vary from vendor to vendor, which can lead to weaknesses in specific implementations of tokenization.

In general, tokenization prevents (or at least reduces the likelihood of) account numbers being stored in the RAM of POS terminals. Tokens can be single use, short-lived or long-lived. However, tokens that can be used multiple times (potentially) leave the door open for attacks against weak implementations where an attacker might discover a way to reuse tokens. In that case, it might still be possible for malware to scrape for tokens.

Point-to-Point Encryption (P2PE)

P2PE makes it a lot more difficult for malware to scrape account numbers. Systems that use P2PE typically encrypt payment details directly on the card-reading device so that this information is not accessible to even the POS terminals themselves. In order to compromise encrypted card data, attackers would need to compromise the actual card-reading hardware device. Since different vendors use different hardware devices, attacks on the hardware would only yield returns on a small subset of the POS market. With non-encrypted data, RAM scrapping malware can target a broad swath of POS systems; however, hardware-specific attacks require a large time investment and typically yield limited returns.

Despite the October 1st deadline and vendors starting to use tokenization and P2PE, a recent report states that only 27% of merchants have upgraded to EMV card readers and only 60% of cardholders have received chipped cards. Even though there is movement toward more secure payment infrastructure, there is still a long way to go before even known POS malware is rendered ineffective.

Conclusion

For the security researcher, POS malware is an area of research that is of growing interest. Learning about the different families of POS malware is useful in this research, as it makes variants easier to identify and detect. Understanding the families with similar code base saves valuable time during research, especially when responding to the incident breaches – it is not necessary to view every new malware as something brand new. Lazy attackers are simply modifying existing malware to evade detection in many cases.

AlienVault Labs & Unified Security Management (USM)

AlienVault Unified Security Management (USM) combines 5 key security capabilities – asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and SIEM - with real-time threat intelligence from the Open Threat Exchange (OTX) and AlienVault Labs security research team to help customers identify threats like those described in this paper.

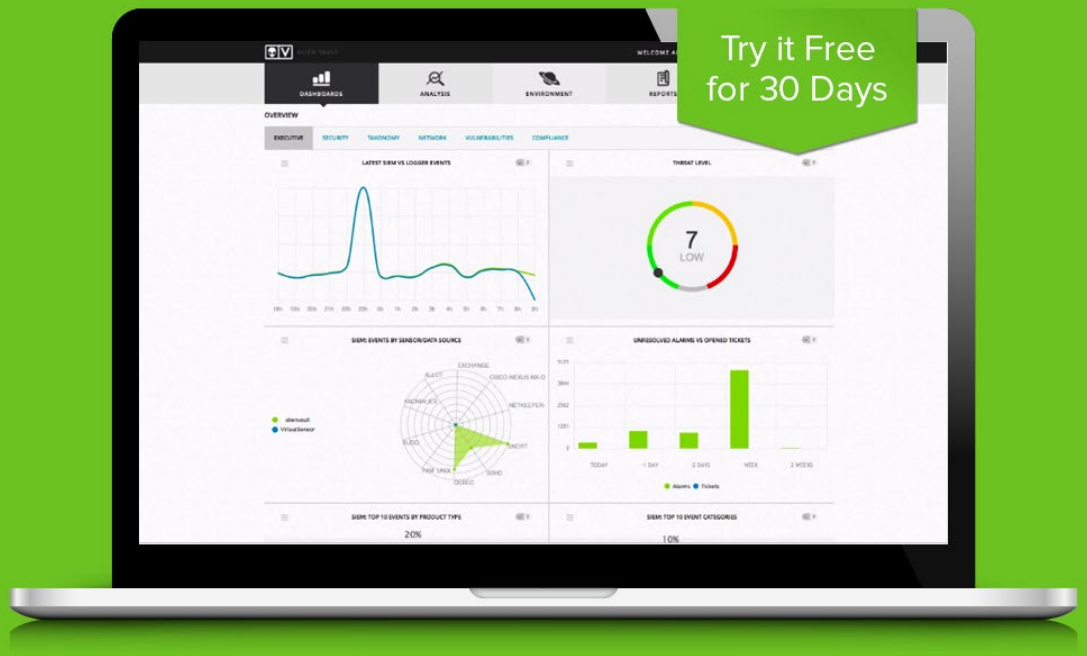
The AlienVault Labs team releases new and updated IDS signatures and correlation rules to the USM platform weekly so customers can identify and protect against the latest threats. All of the POS exploits described in this paper can be detected with USM, along with others such as:

- JackPOS
- vSkimmer
- FighterPOS
- BernhardPOS
- FindPOS
- Nitlove
- PunkeyPOS
- NewPosThings
- DecebalPOS
- POSCardStealer

AlienVault OTX, the world's first truly open threat intelligence community, enables collaborative defense with actionable, community-powered threat data to provide global insight into attack trends and bad actors. OTX pulses provide users with a summary of the threat, a view into the software targeted, and the related indicators of compromise (IoC) that they can use to detect the threats.

OTX pulses are integrated with USM so that threat detection capabilities stay up to date with the latest threats reported by the community, and vetted by the AlienVault Labs team.

Next Steps: Play, share, enjoy!



- Learn more about threat management with AlienVault USM
- Create a personalized demo
- Start detecting threats today with a free 30-day trial
- Join the Open Threat Exchange (OTX)

www.alienvault.com