This TLP White Alert was created as part of a joint effort between the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the Retail Cyber Intelligence Sharing Center (R-CISC) and the United States Secret Service (USSS).

Securing Merchant Terminals and Ecommerce Systems

December 2016

Executive Summary

This advisory was prepared in collaboration with the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Retail Cyber Intelligence Sharing Center (R-CISC), the United States Secret Service (USSS) and is directed to retailers or companies which are processing financial transactions and managing customer personally identifiable information. This advisory serves to provide information and recommendations for possible mitigations for common cyber-exploitation tactics, techniques and procedures (TTPs) consistently and successfully leveraged by attackers in the past year. Many of these TTPs have been observed by FS-ISAC and R-CISC, through their members and identified in Secret Service investigations. Some of the TTPs in this advisory have been reported in prior advisories. The repeat of the TTPs and risk mitigation suggestions is deliberate because attackers continue to be successful with these techniques.

The TTPs discussed in this report include:

- Trends on attacks against terminals using older technology;
- Unauthorized access via remote access;
- Attacks against online merchants that use open source shopping carts;
- Exploiting commercial application vulnerabilities;
- Email phishing; and
- Unsafe web browsing from computer systems used to collect, process, store or transmit customer information.

This document provides recommended security controls in observed areas to protect customer data and provides recommendations to smaller merchants who should work with their vendors to implement these recommendations (see Appendix A).

This advisory is not intended to be a robust, all-inclusive list of procedures as attackers will modify TTPs depending upon the target's network and vulnerabilities. This report does not contain detailed information about memory scraping Point of Sale (PoS) malware that has been used in recent high-profile data breaches. Secret Service investigations of many of the recent PoS data breaches have identified customized malware only being used once per target. A list of observed PoS malware families is provided in Appendix B.

These recommendations should be analyzed by cyber threat analysis and fraud investigation teams based on their operational requirements. The information contained in this advisory does not augment, replace or supersede requirements in the Payment Card Industry Data Security Standard (PCI DSS); however, the PCI DSS version 3.0 recommendations are cited when appropriate.[1]

[1] For the full PCI DSS v. 3.1 guide please see https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Table of Contents

PoS System Upgrade for EMV

Many companies have upgraded card payment processing hardware and equipment to read chips on payment cards as well as the magnetic stripe on the back of the card. The providers of these updated card payment hardware also provide an optional bundle of other security features that reduce the risk that the card payment data can be compromised. Companies, who have not upgraded, will be upgrading card payment processing hardware and equipment to avoid the shift in liability from the financial institution who issues the card to the merchant. Criminals are targeting the remaining merchants that have not upgraded including gas pumps.

Security features to consider when upgrading:

- End-to-end encryption. This feature encrypts the card account number and other data before it is temporally stored in the payment terminal. This encryption process is sustained during the balance of the payment processing, where the only entity capable of decrypting the sensitive data is the merchant acquirer/processor. In the past criminals, have not been able to monetize the encrypted payment data.
- Stronger encryption. The US National Institute of Standards and Technology (NIST) has scored SSL encryption and TLS encryption 1.0 as a weaker form of encryption. TLS 1.2 is recognized by NIST as strong encryption. NIST has also scored Secure Hashing Algorithm One (SHA1) to be a weaker encryption. SHA1 is being replaced with SHA256 for payment processing.
- Tokenization of the card account number. Merchants may need to store transaction information for a variety of business purposes. A tokenized account number is a replacement account number that is not valuable to anyone outside the merchant's own, protected environment.
- Physically attach the handheld credit card processing unit to a secure platform. Criminals have been known to replace existing handheld units with compromised units which capture card and PIN information.
- Criminals have been known to damage or disable the chips on the EMV cards so that they cannot be read and must be swiped instead. Retail staff should be aware of this practice.
- Risk mitigation for gas pump skimming:
  - For areas subject to high risk of theft, add special keys/locks to replace the standard locks.
  - Maintain employee views of the fueling islands because thieves don't like to be seen.
  - Inspect your site frequently, keeping watch for loose pump faces, doors, stray wires or other parts. Criminals can also install skimmers within the gas station stores by distracting the on-duty cashier even for a few seconds, so employees should be trained to check all PoS systems more than once during a shift.
  - Be alert for abnormal traffic patterns on the forecourt.
  - Periodically change the programming access (PIN) codes on the manager's keypad.
  - Remove the manager's keypads from the dispensers and store them in the station or other safe location.
  - There are mobile apps to detect and locate a WiFi signal. Gas pump skimmers may send the card information via WiFi. A pump that is sending WiFi signals needs to be examined.
  - Store managers can keep one another informed of skimmer activity in their geographic areas.
- Risk mitigation for gas pump fuel gorging:
  - Watch for multiple fueling of trucks taking on a high volume of diesel fuel. Criminals add fuel bladders in areas hidden in the truck. Some trucks are being filled with up to 500 gallons of fuel multiple times during one day.
  - High volume of diesel dispensed with multiple payment cards used. These cards may be counterfeit payment cards.

Remote Access Controls

Many retailers purchase a card payment processing system that is customized to their industry. The providers (managed service providers, MSPS) of these systems have methods to remotely access these systems to provide technical support and updates.

Criminals have successfully exploited databases and payment processing systems with remote access tools. There is a high probability that employees who have remote access to the company's network will be targeted especially if the attacker can steal virtual private network (VPN) logon credentials and leverage them to login during normal business hours.

Implementing multi-factor authentication on remote access devices reduces the risk of attackers gaining access to the network. Too often, this added layer of security is not configured in remote access platforms, making it a common target in past data breaches. Appendix C contains examples for enabling and configuring multi-factor authentication for the popular and widely deployed Citrix platform XenApp. Most other remote access platforms provide similar support for multi-factor authentication.

Organizations should evaluate their current policies and consider the potential elevation of risk as it relates to their individual environments. The below recommendations relate to techniques that can prove effective in limiting the success of observed attacks, or otherwise limit the potential for adverse impacts.

Recommendations

- Corporate users who typically access a network externally should be forced to periodically change their login credentials. Sophisticated criminal groups have likely already purchased stolen credentials to conduct an attack. Forcing password changes and enforcing complex password rules will help mitigate this risk.
- Group accounts and passwords should never be utilized. Often these group account passwords are never changed and may be compromised by a disgruntled employee after leaving their current employer.
- User accounts should be set to automatically disable if unused, typically after 90 days of inactivity. Administrative accounts should be set to automatically disable if unused within shorter timeframes, typically after 45 days of inactivity. All accounts should be reviewed on a scheduled basis to ensure all users are current and continue to require access.
- Multi-factor authentication should be required to mitigate risk for remote access. Many remote access appliances are provisioned to accept multi-factor authentication technology (see Appendix C).
- Require vendors to use multi-factor authentication for remote access when possible. If multi-factor authentication is not available to those vendors, then disable remote access services except when specifically requested and scheduled by the vendor. Force third-parties to change their login credentials before and after the holiday season. Sophisticated criminal groups have likely already purchased stolen credentials to conduct an attack this season. Forcing password changes and enforcing complex password rules will help mitigate this risk.
- Policies for vendors should be implemented and minimum levels of supported operating systems should be included. For example, vendors should not be permitted to remote access your network with an out-of-date operating systems like Windows XP.
- Identify third-parties with physical or remote access through the network perimeter. Monitor the remote user accounts for login abnormalities such as frequent failed login attempts, logins during non-normal working hours and abnormal duration of logon (i.e. very long or very short sessions). Additionally, host based security logs should be enabled and reviewed.
- Lock accounts after multiple failed login attempts. The industry standard is not more than six failed login attempts.[2]

[2] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

FINANCIAL SERVICES ISAC

- Disable unnecessary services especially those that support remote access such as remote desktop protocol (RDP) and virtual network computing (VNC) when not required.
- 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.
- Criminals are using social engineering to impersonate third-party support staff and install malware in the form of software updates. Establish a verbal code word or password that support staff must use and change it monthly or after an incident.
- Conduct information security and risk assessments of all third-party vendors that have access to your network.
- Segregate the payment processing systems from remote access applications when possible and restrict the network resources remote access users can access.
- Implement all recommended vendor patches and test to ensure the patch is successfully integrated.
- Enforce up-to-date anti-virus (AV) signatures, but do not only rely on AV signatures alone. Consider additional tools for the device being accessed such a host-based intrusion prevention system (HIPS) and host-based firewalls.
- Monitor firewalls for outbound traffic to suspicious IP addresses and domains.
- Ensure that all firewalls, intrusion detection systems, remote access and AV logging are enabled.
- All logs generated should be automatically ported off the PoS terminal onto a separate log system for centralized retention and analysis. This will prevent criminals from removing evidence of their activities from the compromised system.

Attacks Against Online Merchants That Use Open Source Shopping Carts

Some merchants use ecommerce payment processing system to support their online operations. Developers of these systems may use open source e-commerce software. There are reports that there are thousands of online merchants who are using older unpatched versions of the open source ecommerce solutions. Criminal have developed malware to successfully steal card account number, CVV, expiration date, customer name and address.

Retailers using certain ecommerce platforms should be aware of the newest web injection attacks for stealing customer credentials and card data. RiskIQ describes MageCart[3], which injects Javascript code into vulnerable websites and has been spotted targeting the Magento, Powerfront CMS and OpenCart platforms.

Recommendations

- Determine if your ecommerce system is using open source software, if so, has the system has been regularly patched?
- If the system has not been patched:
  - Install the latest patches.
  - Create a process to regularly patch the system.
  - Have a trained IT professional review:
    - Root directories for unauthorized code.
    - Server log files unauthorized access and connections to unknown IP addresses
    - Compromises of administrator credentials.
  - Adopt best practice security guidelines from the open source community (see Appendix D).
  - Review general recommendations in the next section of this advisory.

[3] https://www.riskiq.com/blog/labs/magecart-keylogger-injection/

Overall

- Inventory and conduct a review of how customer data is stored, moved and deleted. This should include the equipment and applications involved. It is likely that a sophisticated attacker will conduct reconnaissance on a target's network to identify where customer data is stored and how it is transmitted locally before being encrypted in a central database.

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.
- Do not use PoS terminals or other computers with access to PoS systems for Internet surfing, checking email or accessing social media.

Internet Access and Software Updates

- 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 (i.e. payment gateways).
- Consider requiring two or more employees' approval before any updates of the payment processing applications and, if possible, filter updates to that terminal's operating system (OS) though a controlled server on the network.

Physical Access and Multi-Factor Authentication

- 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. Insider threats, both intentional and unintentional, are a real danger.
- 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 regular basis (i.e. multiple times daily). Devices can be changed in as little as an hour after they were last inspected.
- Implement multi-factor authentication for the employees involved in managing the transactions of customer data and updating the applications protecting those transactions (see Appendix C).

Whitelisting

- If transactions are processed by a single software program operating on a single terminal, ensure that only that application is allowed to run on that terminal by enforcing a strict application whitelisting policy. If possible, log and configure alert updates for the security operations center for any changes made to that whitelisting policy by an individual user or business location.
- Record and change the default settings with any PoS hardware and software, including default passwords. Criminal groups have likely reviewed documentation and/or purchased the same software in order to exploit any default settings.

AV and Key Logging

- Do not rely on AV signatures to find memory scraping malware. Criminals have customized this type of malware in recent attacks and likely tested this against the target network's AV solution.

- Implement anti-malware detection software that looks for anomalous and suspicious patterns of behavior.
- Enforce up-to-date anti-virus signatures to find older malware that is being reused. This may be targeted at smaller or medium sized businesses or used by criminal elements with less resources and time. For a list of recently observed PoS malware families please see Appendix B.
- Implement software to detect key-loggers on PoS terminals.
- If possible, deploy a host based intrusion prevention system (HIPS).

Points of Contact

For law enforcement assistance, please contact your local U.S. Secret Service Field Office/Electronic Crimes Task Force (ECTF) or the USSS toll free number at (877) 242-3375. The US Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the US Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial, electronic and cybercrimes. As a component agency within the US Department of Homeland Security, the US Secret Service has established successful partnerships in both the law enforcement and business communities – across the country and around the world – in order to effectively combat financial crimes.

FS-ISAC encourages member institutions to report any observed fraudulent activity through FS-ISAC's submission process and login at fsisac.com. This reporting can be done with attribution or anonymously and will assist other members and their customer to prevent, detect and respond to similar activity. Non-members experiencing suspicious activity are encouraged to reach out to FS-ISAC SOC at soc@fsisac.us or to call (877) 612-2622 – prompt 2.

In addition to risks associated with merchant terminals, the R-CISC enables information sharing and threat intelligence exchanges for retail and consumer products, goods and services companies and provides resources for organizations within those industries that can be found at r-cisc.org. The R-CISC encourages its members to share any observed activities or suspicious behaviors through the secure portal located at portal.r-cisc.org, either anonymously or with attribution and the R-CISC ISAC staff will ensure that the appropriate distribution of necessary information will be performed. Non-members are encouraged to contact the R-CISC at isac@r-cisc.org to report suspicious activity.

Appendix A: Simple Network Controls for Small Merchants to Protect Customer Data

[NOTE: If you outsource your PoS solution, please work with your PoS or payment processor vendor to ensure that the following controls are implemented]

- Reset default passwords for vendor supplied equipment.
- Require regular password changes (at least every 90 days) and change all passwords if you observe any suspicious activity.[4]
- Enforce strong passwords (i.e. at least seven characters in length with both numeric and alpha characters).[5]
- Inform employees to be on the lookout for skimmers, USB sticks or other devices connected to PoS systems. Check all PoS systems for connected devices on a regular basis (multiple times daily is recommended), especially ahead of the holiday season.
- Segregate your PoS system from other computers on the network. Do not use PoS terminals for Internet surfing, checking email or accessing social media.
    - If a PoS terminal must be used for legitimate non-PoS functions, implement a commercial or open source web protection tool on the PoS terminal to limit access to harmful and inappropriate websites.
- If PoS services operate on an older operating system, update them immediately and configure auto-updates.
- Update all AV signatures and software on a PoS terminal daily.
- Implement multi-factor authentication for all remote access operations.
- Implement a unified threat management (UTM) device.
    - This is a device that "allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console."[6] This simplifies the cybersecurity management process for any small and medium-size business owner.
    - UTMs are typically purchased as cloud services or network appliances, provide firewall, intrusion detection, antimalware, spam and content filtering and VPN capabilities in one integrated package that can be installed and updated easily.[7]
- If possible, hire an independent third-party to assess your security needs.[8] After this inspection, consider hiring a monthly managed security service provider (MSSP) to manage based on the inspection results. MSSPs are out sourced services that manage network defenses such as firewalls and can typically be hired inexpensively. Below is a list of questions that the SANS cyber research institute has published for businesses evaluating a potential MSSP.[9]

MSSP Evaluation Questions[10]

Business managers should consider the following questions before deciding to hire an MSSP.

- Does the service provider offer an assortment of solutions that can readily address a variety of environments or do they specialize in a one-size-fits-all solution?
    - No service provider can be in expert in all possible solutions. They should, however, be able to offer a choice of products that can complement each other and provide a solution that offers an optimal amount of protection. [11]

---

[4] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
[5] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
[6] http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management
[7] http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management
[8] http://www.darkreading.com/risk/how-to-pick-the-best-mssp-for-your-smb/d/d-id/1138968?
[9] http://www.darkreading.com/risk/how-to-pick-the-best-mssp-for-your-smb/d/d-id/1138968?
[10] https://www.sans.org/security-resources/idfaq
[11] https://www.sans.org/security-resources/idfaq

    - Some MSSPs specialize in the applications and protocols used by particular sectors (i.e. gas stations). Ask whether the provider can monitor traffic for specialized software, not just well-known web and basic network traffic.
- Do not overlook physical security. How secure is the facility from which the service is being provided?
    - Does the service provider utilize proper access controls and is access to management consoles provided only to those who need it?[12]
- What provisions are in place with respect to fault tolerance? How often are the security devices being polled and what process is in place for notification should a problem occur?
    - While a device may appear to be "up," any number of problems could arise. Is logging being checked periodically and how? Are critical processes that run on the sensor being monitored to determine if they are functioning properly? What about routine maintenance of the device such as checking for disk space? Is there a centralized log server if the security device, itself, is compromised? How much activity is kept, that is, how far back is logging maintained? If a compromise is discovered well after the fact, can accurate data be pulled to help in the investigation?[13]
- Does the service provider have out-of-band access to managed devices?
    - Is there built-in redundancy or is the provider "blinded" and unable to access devices and receive alarms? If you run a high-profile site this is a potential point of attack.[14]
- Does the company specialize in security or is it merely and add-on to an existing business?
- How does the MSSP handle staff turnover? Are passwords routinely changed and do they utilize common passwords across multiple devices? Do they perform background checks on prospective employees and are they bonded?[15]
- What emphasis if any does the provider place on certifications?
    - While certifications do not in and of themselves guarantee expertise, they do provide a means of determining the level of knowledge that the staff has regarding intrusion detection. Look for non-vendor specific certifications, as well as vendor-specific certifications.[16]
- To what extent does the service provider provide continuing education or training for staff members?
    - Intrusion detection is a field that is rapidly advancing. The service provider should be able to readily address and provide information regarding new exploits. Part of the benefit of out-sourcing intrusion detection is that the service provider should be able to provide up-to-date information that would be beneficial in addressing new threats. By providing a proactive approach rather merely reactive, they can more readily determine "patterns of activity" that could pose a threat to an enterprise ahead of time.[17]
- Is the service provider capable of writing custom signatures that can address "zero-day exploits" or are they limited to the signatures that are provided by the manufacturer of the intrusion detection system? What assurance is there that the devices that are being maintained are continually updated with the latest signatures?
    - An intrusion detection system that is not updated is comparable to virus protection software that is out of date. It can provide a false sense of security that can fail when it is needed the most.[18]
    - How does the service provider staff keep current with threats? With whom do they exchange threat intelligence, and how do they notify customers about incidents?

[12] https://www.sans.org/security-resources/idfaq
[13] https://www.sans.org/security-resources/idfaq
[14] https://www.sans.org/security-resources/idfaq
[15] https://www.sans.org/security-resources/idfaq
[16] https://www.sans.org/security-resources/idfaq
[17] https://www.sans.org/security-resources/idfaq
[18] https://www.sans.org/security-resources/idfaq

Appendix B: List of Common PoS Malware Family Names

A list of common PoS malware family names that have been used in the past is available in Table 1 below. Sophisticated criminals will likely continue to use malware from one or more of these families, after testing a target's AV solution against their samples to evade detection.

[NOTE: Sophisticated criminals can make minor changes to existing families of malware, making it undetectable by signature-based AV solutions.]

Table 1 – List of Common PoS Malware Family Names

Family Name	Description
Alina[19]	A family of PoS malware that targets applications containing track data, applies basic encryption and exfiltrates the information. This malware has a command and control structure, which allows it to search for and install automatic updates when they are released.
Backoff PoS[20]	These variations have been seen as far back as October 2013 and continue to operate as of July 2014. In total, the malware typically consists of the following four capabilities. An exception is the earliest witnessed variant (1.4) which does not include keylogging functionality. Additionally, 1.55 'net' removed the explorer.exe injection component: • Scraping memory for track data • Logging keystrokes • Command and control (C2) communication • Injecting malicious stub into explorer.exe
BlackPoS/Kaptoxa[21]	BlackPOS infects computers running Windows that are part of PoS systems and have card readers attached to them. These computers are either infected by insiders or found during automated internet scans because they have unpatched vulnerabilities in the operating system or use weak remote administration credentials. Once installed on a PoS system, the malware identifies the running process associated with the credit card reader and steals payment card track one and track two data from its memory. BlackPoS is a RAM scraper, or memory-parsing software, which grabs encrypted data by capturing it when it travels through the live memory of a computer, where it appears in plain text. The captured information is uploaded to a remote server via File Transfer Protocol (FTP).
Chewbacca[22]	Chewbacca appears to have been a short-lived malware designed to attack PoS systems and exfiltrate data over TOR. The malware itself has been well documented.
Decebal[23]	Romanian PoS malware was released on January 3, 2014. It is written in Visual Basic Script and is capable of checking to see if the computer on which it is deployed is running any sandboxing or reverse engineering software. Decebal can also validate that the stolen payment card numbers are legitimate.
Dexter[24]	First discovered in December 2012, Dexter is a custom-made malware tool

[19] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.
[20] https://www.us-cert.gov/ncas/alerts/TA14-212A
[21] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.
[22] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[23] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.
[24] https://www.us-cert.gov/ncas/alerts/TA14-002A

	used to infect point of sale systems. Per Seculert, Dexter steals the process list from the infected machine, while parsing memory dumps of specific POS software related processes, looking for track one/track two credit card data.
FighterPoS	FighterPOS is a full-featured piece of malware, carefully developed using strong encryption. It supports multiple ways to talk with its C&C infrastructure. Its keylogging capabilities allow for DDoS attacks and gaining full control of victim machines. We currently estimate that each infected machine sends back ten new credit card numbers to the attackers.[25] This one-man operation has been able to steal more than 22,000 unique credit card numbers.[26]
JackPoS[27]	JackPoS was likely first developed in October 2014.[28] There are at least thirty-three distinct malware samples of JackPoS in this timeframe.[29] Some indicators suggest that JackPoS has evolved from, or was inspired by the Alina PoS malware.[30] JackPoS is distributed by cybercriminals through drive-by attacks.[31] The malware is sometimes disguised as the Java Update Scheduler.[32] "Several of the found loaders used in detected 'drive-by' download attack are written using obfuscated compiled AutoIt script, which became quite popular method to avoid AV detection in order to unpack additional binary malicious code and execute further instructions received from the command and control server."[33] "The bad actors have used some sophisticated scanning, loading, and propagating techniques to attack these vectors to look to get into the merchants system thru external perimeters and then move to card processing areas, which were possibly not separated in compliance with PCI polices."[34]
LogPoS	LogPOS avoids a traditional detection mechanism of scanning files for unencrypted credit card information by instead writing to a mailslot.[35]
NewPosThings	It operates similarly to other PoS malware by memory scraping processes looking for credit card track data and then exfiltrating the spoils to a command and control (C2) server. Based on compilation times, it has been in active development since at least October 20, 2013—with the latest timestamp being August 12, 2014.[36]
NitlovePOS	The NitlovePOS malware can capture and exfiltrate track one and track two payment card data by scanning the running processes of a compromised machine. It then sends this data to a webserver using SSL.[37] We believe the cybercriminals assess the hosts compromised via indiscriminate spam campaigns and instruct specific victims to download the POS malware.[38]
Find/Poisidon	Based on the earliest Virus Total submissions the First/PoSeidon malware family appears to date back to at least November 2014.[39] The malware

[25] http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/
[26] http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/
[27] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf and http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[28] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[29] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[30] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[31] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[32] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[33] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[34] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[35] http://morphick.com/blog/2015/2/27/mailslot-pos
[36] http://asert.arbornetworks.com/lets-talk-about-newposthings/
[37] https://www.fireeye.com/blog/threat-research/2015/05/nitlovepos_another.html
[38] https://www.fireeye.com/blog/threat-research/2015/05/nitlovepos_another.html
[39] First submitted on November 8 2014, source: https://www.virustotal.com/en/file/40680dbfb20fbb536bc04cffd886eb33481b655b978d213cd4c0b421cc8e245b/analysis/

	currently has a high anti-virus detection ratio (an average of 69 percent of AVs detect the file as malicious); however, most of these AV signatures are generic. According the Palo Alto Networks there are eight versions of the family and each variant was slightly modified. The malware is self-updatable and like many other POS families has a key logger component that was released with version 5.90.[40] When functioning, the malware searches memory for credit card track data and verifies any logged numbers through the Luhn algorithm; however, the memory scanning process is different in that samples use a variety of calls to identify and filter non-native Windows processes and then uses a common technique to scrape memory with VirtualQueryEx and ReadProcessMemory calls.[41]
PoSCard Stealer[42]	PoSCardStealer is a name used by ESET, which appears to cover several types of PoS malware. Where the malware does not have another name known to ASERT, we will use "PoSCardStealer". Other anti-malware vendors use different naming schemes such as Troj/Trackr-K.
Punkey	Punkey appears to have evolved from the NewPOSthings family of malware.[43] Punkey self-identifies its version. Three unique versions have been discovered.[44]
vSkimmer[45]	vSkimmer was disclosed by McAfee in March 2013. vSkimmer searches program memory for track data; however, it only looks for data matching Track 2 format. In addition to using HTTP to exfiltrate stolen data to a C2 server, vSkimmer can be configured to copy data to a specific USB device if it is unable to connect to the Internet. vSkimmer dumps its stolen data to a log file on a USB drive with a certain volume name.

[40] http://www.darkreading.com/attacks-breaches/will-poseidon-preempt-blackpos/d/d-id/1319585
[41] In 1954, Hans Luhn of IBM proposed an algorithm for validating credit card numbers. The algorithm is useful to determine whether a card number is entered correctly or whether a credit card is scanned correctly by a scanner. Credit card numbers are generated following this validity check, commonly known as the Luhn check or the Mod 10 check
Source: http://stackoverflow.com/questions/26642051/credit-card-number-validity-with-luhns-algorithm-java
http://blogs.cisco.com/security/talos/poseidon and http://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/
[42] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[43] https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges---Punkey/
[44] https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges---Punkey/
[45] http://www.secureworks.com/cyber-threat-intelligence/threats/point-of-sale-malware-threats/

Appendix C. Multi-Factor Authentication

This is an example of multi-factor authentication for a Citrix application.

[NOTE: Many Citrix remote access and virtualization solutions should support multi-factor authentication.]

Enable Two-Factor Authentication[46]

Use the Authentication Methods task in the Citrix Web Interface Management console to enable two-factor authentication for users, if required.

1. On the Windows start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit check box.
4. Click Properties and select Two-Factor Authentication.
5. Select the type of two-factor authentication you want to use from the two-factor setting list and configure any additional settings as appropriate.

Configuring Two-Factor Authentication

The following steps were recommended by the security firms ActivIdentify Channel and Duo Security for configuring Citrix XenApp.[47] These include the following steps: configure Citrix radius settings, configure RADIUS shared Secret and configure two-factor authentication settings.

For the XenApp:

1. Login to the Citrix Web Interface Management Console.
2. Navigate to XenApp Web Sites and click on Authentication Methods.
3. Confirm that only Explicit is checked and click properties.
4. Click on Two-Factor Authentication and select RADIUS for the two-factor setting.
5. Add a RADIUS server and enter the AuthProxy IP address as the server address and 1812 for the server port. Configure the Timeout to 60 seconds and save your configuration.
6. Create a new text file in the Citrix Web Interface \conf folder called radius_secret.txt. Type the radius_secret from the AuthProxy configuration in the radius_secret.txt file. The location for this file is given by the RADIUS_SECRET_PATH configuration value in the web.config file (for sites hosted on IIS) or web.xml file (for sites hosted on Java application servers). The location given is relative to the \conf folder for sites hosted on IIS and relative to the /WEB_INF directory for sites hosted on Java application servers.) Typically, the location will be similar to: C:\inetpub\wwwroot\Citrix\Xenapp\conf.
7. On the Citrix Web Interface server open the web.config (IIS Hosted) or web.xml (Java Apps) file and add the Citrix Web Interface IP address as the "RADIUS_NAS_IP_ADDRESS".

[46] http://support.citrix.com/proddocs/topic/web-interface-hardwick/wi-enable-two-factor-authentication-gransden.html
[47] http://www.youtube.com/watch?v=ZRbi88JujO0 and https://www.duosecurity.com/docs/citrix_web_interface

Two-Factor Authentication Tokens Authentication Methods for XenApp Web Sites[48]

- **Aladdin SafeWord for Citrix.** An authentication method that uses alphanumeric codes generated by SafeWord tokens and, optionally, PIN numbers to create a passcode. Users enter their domain credentials and SafeWord passcodes on the logon screen before they can access applications on the server.
- **RSA SecurID.** An authentication method that uses numbers generated by RSA SecurID tokens (*tokencodes*) and PIN numbers to create a *PASSCODE*. Users enter their user names, domains, passwords, and RSA SecurID PASSCODES on the Logon screen before they can access resources on the server. When creating users on the RSA ACE/Server, user logon names must be the same as their domain user names. **Note:** When using RSA SecurID authentication, the system can generate and display a new PIN to the user. This PIN appears for 10 seconds or until the user clicks OK or Cancel to ensure that the PIN cannot be viewed by others. This feature is not available on PDAs.
- **RADIUS server.** An authentication method that uses the Remote Authentication Dial-in User Service (RADIUS) authentication protocol (as opposed to proprietary agent software). Both SafeWord and SecurID can be installed and configured to be presented as a RADIUS server. For Web Interface for Java Application Servers, RADIUS authentication is the only two-factor authentication option available.

Appendix D: Security Patch and Best Practices Magento Community Ecommerce System

- https://magento.com/search/gss/security%20patches
- https://magento.com/security/best-practices

[48] http://support.citrix.com/proddocs/topic/web-interface-hardwick/wi-configure-two-factor-authentication-gransden.html

