ASEE's 123rd Annual • Conference & Exposition • New Orleans, LA • June 26-29, 2016

New Orleans JAZZED about Engineering Education

Paper ID #17151

A Call to Arms: Defending Against Point of Sale Malware

Ms. Sarah A. Cunha

Sarah Cunha is a student at Brigham Young University studying Information Technology with an emphasis in Cyber Security. She is originally from Dos Palos, California. She has participated in multiple Collegiate Cyber Defense Competitions and Capture the Flag events and currently is employed as a Research Assistant in the BYU Cyber Security Research Laboratory. Sarah is an active member of the BYU Red Team which has participated in several penetration tests for departments on campus, and businesses in the local area. Sarah has come to love both offensive and defensive cyber security and is currently planning on pursuing a Masters degree emphasizing Cyber Security.

Dr. Dale C. Rowe, Brigham Young University

Dr. Rowe has worked for nearly two decades in security and network architecture with a variety of industries in international companies. He has provided secure enterprise architecture on both military and commercial satellite communications systems. He has also advised and trained both national and international governments on cyber-security. Since joining Brigham Young University in 2010, he has designed a variety of courses on Information Assurance, Cyber Security, Penetration Testing, Cyber Forensics and Systems Administration and published over a dozen papers in cyber-security.

A Call to Arms:
Defending Against Point of Sale Malware

Abstract - Point of Sale (PoS) malware has been alarmingly successful over the past year and is estimated to have cost businesses billions of dollars. While PoS malware does not represent any major technical evolution, it suggests that cybercrime is shifting focus from the consumer to the retailer. Rather than relying on infecting relatively small groups of users with specific vulnerabilities who may conduct e-commerce a few times per month, PoS malware is able to take advantage of standardized point-of-sale deployments in the retail sector to affect thousands of systems, each reading credit-card information hundreds or even thousands of time per day.

In this paper we discuss the trends and evolution of point of sale malware. Case studies of three specific malware families are examined and recommendations are made to harden systems against similar attacks in the future. We conclude with a list of general recommendations which, if implemented, would significantly reduce both the likelihood and impact of a PoS malware attack.

Introduction

Computer viruses have been a growing security concern for over four decades. First instances of code that functioned as viruses were often accidents or jokes written for the fun of the author. *Elk Cloner,* a prank written by a 15-year-old became one of the first uncontained computer viruses [1] to be found in the wild. Some were created as proof of concept, showing what theoretically can be done by outside software. The use of viruses gradually developed to read, destroy, or even steal data. These functions have become a key part of cyber-crime, and are continually on the rise today. The malicious intent of these programs gave rise to the term malicious software, otherwise known as malware.

According to Verizon's 2014 Data Breach Investigations Report, 63,437 security incidents were reported in the year 2013, and 1,367 of those incidents resulted in a confirmed data breach [2]. The 2014 US State of Cybercrime Survey claims that an average of 135 security incidents per organization were detected in the same year and that 77% of respondents detected a security event in the past 12 months [3]. This rise in cyber-crime has led to both small and highly organized attacks, not to mention terrorism and cyber-warfare.

Not only has the rate of cyber-crime risen in the country, but the economic cost of cyber-crime has also increased. According to McAfee, the estimated global cost of cyber-crime in 2014 will exceed $445 billion dollars. This same report states that the 2013 hack against the US retailer Target alone cost banks more than $200 million.

The Target attack represents a new form of retail targeted malware designed to specifically attack the method of transaction from customer to provider, with the ability to steal debit or credit card information. These breaches, taking place at Point of Sale terminals (PoS), can cause huge damage to companies, customers, and the global economy at large. PoS malware has hit many other large retailers recently, including Home Depot, Staples, and Dairy Queen.

This paper will analyze how PoS attacks are realized. Specifically, what have been the delivery mechanisms of Point of Sale malware and how they collect and exfiltrate stolen data. We show that by understanding the methods employed by malware, existing best practices can be tailored to provide a comprehensive and effective defensive strategy to minimize the risks posed by PoS malware.

Methodology

To understand the methods by which Point of Sale malware establish themselves and operate within retail systems, current technical literature and case studies previously conducted on this type of malware have been studied and compared. While there are many different versions of PoS malware, for the purposes of this study only those directed against high profile targets are considered. These are summarized as follows:

The **BlackPOS**, or **Kaptoxa** malware, is best known for its usage in the 2013 Target breach [4]. This was perhaps the largest profile and most significant breach to date. This malware has been used as a basis to develop more advanced strands, for example BrutPOS [5]. Two detailed reports on this malware facilitate the study of its functions and exfiltration methods: “KAPTOXA Point-of-Sale Compromise” [4] and “PoS RAM Scraper Malware - Past, Present, and Future” [5].

Alina is a highly developed malware family that is now in its sixth version. It is highly advanced in its capabilities and exfiltration methods [5] [6]. Several other PoS malware samples have been discovered that are built on Alina’s feature set, including Backoff and JackPOS [7]. The principal two reports found that detail the operation of the Alina malware family are “PoS RAM Scraper Malware - Past, Present, and Future” [5] and “Special Report - Point-of-Sale Malware” [6].

Dexter is a well-developed virus which contains many variants, the most popular being Dexter Revelation [8–10]. As one of the older PoS malware families, there has been significant research into Dexter’s operation and development. Dexter was used in a series of attacks in South Africa, specifically targeting hotels and restaurants. “PoS RAM Scraper Malware - Past, Present, and Future” [5] includes in-depth specifics on Dexter’s operations. Three additional reports demonstrate the impact Dexter has had, as well as some specifics to its character. These reports are “ASERT Threat Intelligence Brief 2014-3 Dexter and Project Hook Point of Sale Malware Activity Update Point of Sale Malware Overview PoS Malware Activity : Dexter and Project Hook” [8], “Visa Data Security Alert - Dexter Malware Targeting Point-of-Sale (POS) Systems” [9], and “Dexter and Project Hook Break the Bank - Inside Recent Point-of-Sale Malware Campaign Activities” [10].

The research methodology will consist of a comparative study of the articles listed above, focusing on both malware delivery and post-infection methods used to extract data. For BlackPOS, Alina, and Dexter, this will take the approach of a literature survey based on existing research.

Comparative Study

Delivery

A given malware sample may be delivered by a variety of different means for each infection. For malware capable of self-replication, the delivery can refer both to the initial infection, and then secondary infections of connected systems – otherwise known as self-propagation. While secondary infection and exfiltration methods are determined by the malware sample, the initial infection may vary significantly and often requires additional steps by the attacker.

Initial infection methods can be grouped into three categories as shown in TABLE *1*. This grouping is based on exploitation methods described by several security experts [5], [11], [12].

In service attacks, the attacker targets a network application or service that is listening for network data. Exploits are generally found on systems that have not been updated with current security patches or have lost security support. Once found, a security hole can allow cyber-criminals to enter a system, gain root access, and deploy their malware infection.

Where client side attacks are in scope, compromise is almost always successful. A client side attack relies on a vulnerable application that is run by the user, such as a web browser, PDF viewer or office application. By tricking the user into opening a malicious file, an attacker can deliver a malware payload on their victim's computer without even arousing suspicion. These attack vectors in particular, benefit from social engineering efforts.

TABLE 1 – INITIAL INFECTION METHODS

Category	**Examples of Attacks**
Service attack	Remote service exploitation, weak access control lists, sanitized user input.
Client side attack	Cross-site scripting, code execution, browser vulnerabilities, e-mail attachment.
Manual delivery	Infected USB thumb drive, physical access, supply-chain infection.

Manual delivery is an attack performed by someone with either direct physical or virtual access to the targeted system, such as a dissatisfied employee who has been given credentials to the network. This person can either drop a virus physically using a USB, or they can use their employee credentials to access the network and download the virus to a local computer or server. This type of attack is difficult to secure against, and a certain level of trust in employees and business interactions is required.

Many infection methods are supplemented with social-engineering efforts employed by the attacker to gain and abuse a basis of trust. For example, many cyber-crime organizations will use user credentials (usernames and passwords) gathered from hacking attacks to send malware from a 'trusted source' such as a work colleague or acquaintance. This can lull the victim into a false sense of security as the attachment is coming from a known person. Such attacks are extremely effective and relatively simple to execute [13,14].

BlackPOS

BlackPOS, or the Kaptoxa virus, is best known for its use in the Target breach between 27 November and 15 December in 2013, and has been cited to have aided cyber-criminals in stealing the card data of 70 million American consumers [5]. When BlackPOS was discovered it had a zero percent anti-virus detection rate, meaning that of the tested anti-virus software, none of them were capable of detecting an infection. It has since become one of the more popular viruses because much of its base code has been leaked, making it freely accessible to all cyber-criminals [4]. In the target attack, attackers were able to leverage a stolen username and password from a HVAC contractor to deploy the malware within the PoS systems.

In a report earlier this year by ThreatScape, BlackPOS operations and exfiltration methods are explained in detail. Like most point-of-sale malware, BlackPOS is a RAM scraper, meaning that it collects sensitive credit card data while the data is stored in the RAM (Random Access Memory) of a point-of-sale system's running processes. In order to authenticate credit card data, PoS systems must store the data unencrypted in the RAM, leaving it vulnerable to this type of attack. BlackPOS identifies the running processes and searches through each process's RAM for data synonymous with the format of credit card track data. When it finds information that fits the search description, BlackPOS saves it to a local file %windir%\system32\winxml.dll.

To exfiltrate the data back to the original attackers, BlackPOS checks that the local time on the infected system is between 10am and 5pm every seven hours. If it is between those times, the virus will send the winxml.dll file to an internal host within the compromised network, eliminating the need for a direct external internet connection from the PoS system. Using various hacking tools, the attackers access and send the file to their own network over File Transfer Protocol, or FTP, to use and exploit the data on their local machines [4]. Although the ThreatScape report only highlights an internal host sending the sensitive information over FTP, Trend Micro research claims that BlackPOS is also capable of exfiltrating data via email through an email client using Transport Layer Security (TLS) for encryption [5].

According to the Trend Micro research, the main identifying characteristics of BlackPOS are as follows:

1. Uses socially engineered filenames
2. Uses multiple components
3. Attacks systems with weak or default passwords
4. Uses multiple exfiltration methods

BlackPOS is somewhat unique in that it has multiple exfiltration methods. Most PoS malware viruses have one exfiltration method hardcoded into them. The flexibility and accessibility of BlackPOS has aided in its popularity, and make it one of the most threatening viruses in point-of-sale malware.

Alina

Alina was discovered in October of 2012. It is one of the older and more developed PoS viruses, is actively developed, regularly updated, and is currently in its 6th version, as well as being the base for many other break-off viruses [5]. Like BlackPOS, Alina searches for credit card track data inside of the RAM in processes running on a PoS system. It applies basic encryption and exfiltrates the stolen data using a Command and Control (C&C) server structure, which also gives Alina the ability to search for and install updates automatically as they are distributed [6].

Trend Micro has extensive research on the methods Alina uses to execute its operations [5]. Alina takes extra precautions to remain hidden and persistent in a system once it has deployed. Once executed it installs itself onto the PoS system, copies itself to a pre-coded inconspicuous filename, and deletes all original Alina files. Not only does the virus run under a fake filename, but the binary file of the virus reinstalls itself on each reboot of the PoS system, making the actual malware process persistent.

Alina is also known for its efficiency. Unlike BlackPOS, which scrapes the RAM of every process running on a PoS system, Alina has a blacklist of processes to skip if seen operating. This allows Alina to skip the complex computations needed to scrape high-memory processes such as web browsers that would be unlikely to hold any credit card track data.

For exfiltration, Alina stores the data it collects in a file and uses HTTP POST (a request method protocol for sending data over the internet) to securly tranfer the file to a C&C server with addresses that were previously hard-coded in the Alina binary.

The characteristics of Alina are described as follows:

1. Collects system information
2. Uses a single component
3. Uses socially engineered filenames
4. Updates itself

Alina is known as a “general-purpose” RAM scraper for its ability to attack all kinds of targets. Overall, Alina is one of the most sophistocated and dangerous PoS viruses because of its high quality persistence, efficency, and flexibility.

Dexter

Dexter was discovered operating in December of 2012. According to a Visa Data Security Alert, Dexter steals the full magnetic strip of credit card data from memory and, like Alina, exfiltrates the data using a Command and Control server. This malware is particularly malicious because it not only target credit card information, but also collects and steals information about the PoS system it infects, potentially compromising even more of the network it has infiltrated [9]. Instances of Dexter have been reported world-wide [10].

The Dexter virus does more than either the BlackPOS or the Alina malware in order to maintain persistence on a compromised system or network. On execution, Dexter opens a process of Internet Explorer, injects itself into the process, copies itself to a file, changes auto start runkeys, modifies the registry keys for low risk files types, changes permissions on the machine, and drops a keylogger (a piece of software that runs on a system and logs all key presses into a file), all in order to maintain control [5].

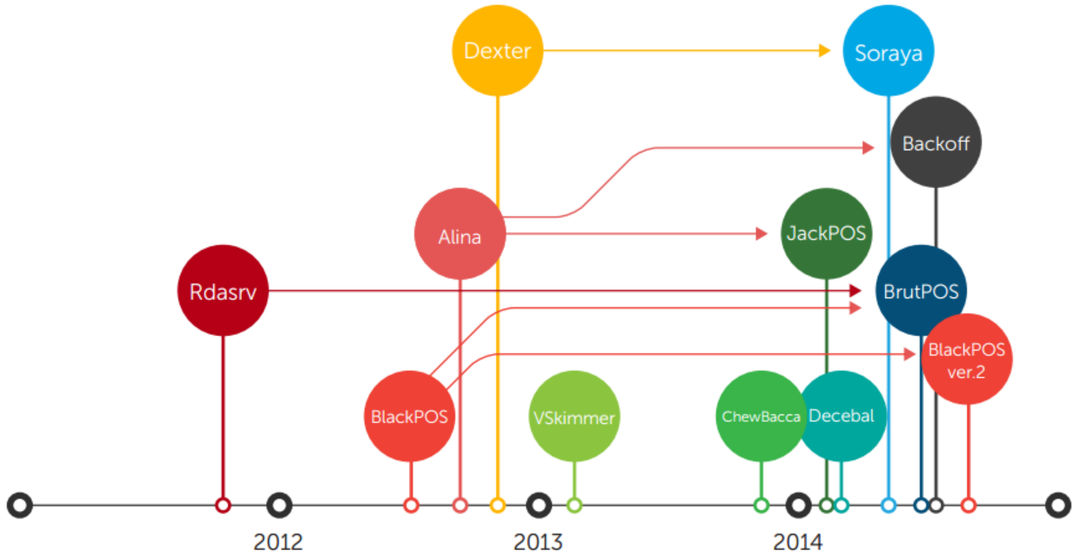

Figure 1 - PoS RAM Scraper Family Tree [5]

Dexter's data collecting method is similar to that of BlackPOS in that it uses custom searches on the PoS process RAM [10]. In contrast, Alina uses pre-determined functions to search for credit card data. As custom searches are more dynamic in their nature, they are harder to spot by anti-virus applications that watch for suspicious activity. This type of approach is often referred to as a stealth characteristic and is commonly found in more advanced malware.

Dexter's exfiltration method is comparable to Alina. Dexter uses the same HTTP POST and C&C server with FTP methods to transfer data externally to the cyber-criminals who infected the system [8,10]. While static methods to exfiltrate information can make malware easier to detect on a network, they have the advantage of being completely autonomous (requiring minimal intervention by the attacker).

According to Trend Micro [5], Dexter's main characteristics are as follows:

1. Collects system info
2. Uses a single component
3. Uses socially engineered filenames
4. Updates itself
5. Has bot functionality
6. Pretends to be java
7. Has a kill switch
8. Hooks APIs
9. Injects code

Three different threat briefs and alerts have been produced to explain and warn of the security danger that Dexter is to PoS systems [8–10].

Recommendations

A thorough risk-management strategy that incorporates the threat posed by PoS malware should be implemented as part of regular business practices in all retail businesses. This will help organizations to foster a defense-in-depth approach to their security posture. Business continuity and incident response plans should include preventative, detective and responsive strategies.

Host-Based Approaches

A popular technique in PoS malware is to search process memory for arrays of decimal characters that conform to credit-card patterns. Thus an effective strategy would involve the obfuscation or encryption of credit-card numbers. Generally, encryption would be the preferred approach using industry-grade encryption such as Advanced Encryption Standard (AES). The encryption key should be stored in a randomized memory location to impede attempts to retrieve this from known addresses. Better still would involve the use of the Trusted Platform Module (TPM) to hold crypto-keys. If this approach is employed, care should be taken to not store pre-encrypted numbers in memory. A stream cipher should be utilized to minimize the window of opportunity for malware to obtain numbers prior to their encryption. Care should be taken to overwrite memory locations in the heap and stack that may have been used to temporarily hold all, or part of credit-card numbers.

Most PoS terminals are based upon standard embedded versions of operating systems such as Microsoft Windows. This leaves them open to the same vulnerabilities to common desktop platforms. However, unlike their desktop counterparts, PoS terminals use general purpose software to perform a limited set of specific activities, such as process retail payments. This allows for more restrictive hardening approaches to be used in minimizing the attack surface area. Popular techniques that should be considered include the removal or disabling of all unused services; disabling unused applications such as text editors, games and web-browsers; application white-listing; host-based firewalls; locking down external media and USB ports; and enabling hardware and OS built-in protections such as code signing, User Access Control (UAC), Data Execution Protection (DEP) or No Execute Protect (NX Protect).

Care should be taken to follow vendor recommendations when deploying systems. For example, where baseline images are used to create PoS terminals, organizations should ensure that public/private key pairs are not reused. Where used, base images should be analyzed as part of a penetration test to ensure that the information within an image could not lead to compromise. The risk of an attacker using information in a deployment image may be significant for larger organizations. Patch management should include sandbox stability testing, followed by organization-wide deployment with rollback capabilities.

User accounts where possible should employ multi-factor authentication (such as an ID card and PIN number). Where passwords are used, passphrases can provide an effective way for employees to memorize a password while avoiding easily guessable dictionary words. Accounts should have the minimum privileges required to operate and should never be shared between users. Contractor, maintenance and other temporary accounts should be disabled when not in use. Where shared accounts are unavoidable, passwords should be changed on a regular basis.

User input devices such as keyboards should be located out of the direct line of sight of customers.

Client logs should regularly be inspected for unauthorized login attempts, application crashes and host configuration changes. Such analysis can be automated using open-source tools such as logstash or proprietary tools like Splunk.

Network-Based Approaches

Network defenses for retailer PoS networks should include forced segregation of PoS systems from other traffic by using both physical and logical methods. Effective methods to separate traffic include encrypted Virtual Private Connections (VPN), and enforced firewall isolation (preventing peer-to-peer communications between PoS terminals). As well as separating PoS traffic from business traffic, a VPN will impede attempts to eavesdrop on sensitive network traffic. By restricting PoS terminals to communications with associated servers, the risk of malware propagation can be significantly reduced. More involved hardening would include using a different operating system such as Linux for PoS servers. The restricting of all PoS communications to PoS servers of a different operating system would severely impede the ability of malware to propagate through systems.

Additionally, network defenses should include both signature and behavioral detection systems must require regular log inspection. Typically, advanced application-layer network security appliances can be costly. Organizations should perform regular risk assessments to determine the potential Return-On-Investment (ROI) for such appliances. Once installed, they should be monitored regularly to avoid missed detections. In the 2013 Target breach, multiple reports indicated that threat indicators were reported from a FireEye device but not given sufficient attention [15]. In light of the severity of PoS malware threats, organizations must ensure that policies are enforced to investigate, and respond to attacks. In a recent report commissioned by IBM, malicious attacks can cost organizations $246 per card number lost [16]. Given that Target is reported to have lost 40M card numbers in an 18-day window, it is not difficult to infer that a rapid response to detected events can minimize losses.

Employee Training Approaches

Staff training is a critical part of any defense-in-depth strategy and must be properly implemented in order to be effective. Up-to-date threat awareness training, best practices and standard-operating-procedure training can increase employee vigilance and awareness to a variety of cyberattacks. While host and network hardening should minimize the potential of a widespread attack, significant damage may be done on a more local basis by a careless employee. Employees should be provided with ongoing training to help develop ongoing awareness.

A minimum standard for employee training should include password complexity, PIN code entry shielding, reporting lost ID cards, checking for unusual attachments or devices to PoS terminals and correct reporting suspicious or unusual activity. Training should be expanded to include log inspection, audit logging and system monitoring for specific employee rolls that include any technical aspect such as networking, systems maintenance or technical support.

Discussion

PoS malware is a new and evolving threat that specifically targets retailers using computer systems to handle large numbers of credit-card data. By stealing data in large quantities, cyber-criminals have a new and highly lucrative means to gain access to sensitive information. Traditional approaches to credit-card data theft typically rely on ATM and other physical skimmers, physical card theft and dumpster diving to retrieve sensitive information. The target in each of these is either an individual card, or small collection of card-users at a specific geographical location. The development of PoS malware has made it possible to steal millions of numbers with very little risk due to the high-level of attacker anonymity.

In the past two years, Dexter, Alina and BlackPOS have led the development of several other PoS malware strands with increasing levels of complexity (see Figure 1) [5]. For example: one of the newest strands, known as Chewbacca uses the Onion Router (TOR) network to exfiltrate data in a way that makes it virtually impossible to detect the origins of the attack, or where the exfiltrated data is being sent [17]. There is no indication that PoS malware has reached maturity and we should expect to see more varied and sophisticated attacks in the near future.

The continual mutations of PoS malware increases the difficulty for security professionals to protect their systems. However, given the similarities in their modes of delivery, operation, and exfiltration, we believe that effective risk mitigation is possible. We have discussed several approaches to systems defense based on a combination of policy, technology and training [18] and specified simple, yet effective strategies to disable currently known malware payload attacks, propagation and delivery vectors.

References

1. Dwan B. The Computer Virus — From There to Here. Computer Fraud & Security. 2000 [accessed 2014 Dec 1];2000(12):13–16. http://www.sciencedirect.com/science/article/pii/S1361372300120263

2. Verizon. 2014 DATA BREACH. USA; 2014.

3. McAfee. Net Losses : Estimating the Global Cost of Cybercrime. USA; 2014.

4. ThreatScape. KAPTOXA Point-of-Sale Compromise. USA; 2014.

5. Huq N. PoS RAM Scraper Malware - Past, Present, and Future. USA; 2014.

6. HackSurfer. Special Report - Point-of-Sale Malware. 2014.

7. Mcgrew W. Instrumenting Point-of-Sale Malware. In: DEFCON 22 Archives. Las Vegas, Nevada, USA: DEFCON; 2014.

8. Hook P. ASERT Threat Intelligence Brief 2014-3 Dexter and Project Hook Point of Sale Malware Activity Update Point of Sale Malware Overview PoS Malware Activity : Dexter and Project Hook. USA; 2014.

9. VISA. Visa Data Security Alert - Dexter Malware Targeting Point-of-Sale (POS) Systems. USA; 2012.

10. Wilson C, Loftus D, Bing M. Dexter and Project Hook Break the Bank - Inside Recent Point-of-Sale Malware Campaign Activities. USA; 2013.

11. Skoudis E. Counter Hack Reloaded. 2e ed. Prentice Hall; 2006. 748 p.

12. Faulhaber J, Felstead D, Henry P, Jones J, Kowalczyk EC, Kuo J, Lambert J, Lauricella M, Margosis A, Meyer M, et al. Zeroing in on Malware Propogation Methods. Redmond, WA; 2011.

13. Lieu CD. Social Engineering - Attacking the Weakest Link. GIAC Certification Papers. 2002;(Security 401).

14. Gulati R. The Threat of Social Engineering and Your Defense Against It. GIAC Security Essentials. 2003.

15. United States Senate. A “Kill Chain” Analysis of the 2013 Target Data Breach. 2014.

16. Ponemon Institute. 2014 Cost of Data Breach Study: Global Analysis. 2014.

17. VISA. VISA Security Alert - “Chewbacca” POS Malware. USA; 2014.

18. Maconachy VW, Schou CD, Ragsdale D, Welch D. A Model for Information Assurance: An Integrated Approach. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. US Military Academy, West Point, NY; 2001. p. 11–15.