GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Understanding and Preventing Threats to Point of Sale Systems

GIAC (GSEC) Gold Certification

Author: Richard Hummel, rhummel@mastersprogram.sans.edu
Advisor: Dr. Kees Leune
Accepted:

October 2015

Abstract

Data breaches have become a systemic problem in the retail, financial, and healthcare sectors, resulting in mass exfiltration of sensitive customer and/or patient data. These breaches continue to be a major problem for all sectors, but primarily that of the retail sector. It has seen many different Point-of-Sale systems compromised, databases stolen, and customer data sold in underground forums. Many studies and white papers describe and analyze these breaches in detail, but fail to address all aspects of a single breach in one succinct article. As such, practitioners are only educated in part on the threats and the methods to mitigate these threats. This paper will cover three of the more prominent breaches, how the breaches occurred, how data was stolen, and actions organizations need to take to mitigate or, hopefully, eliminate the threats altogether.

© 2015 The SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Retail data breaches have reached a tipping point and credit card vendors are adopting a "conform, or be left behind strategy." Visa and MasterCard are just two vendors that have set the date of October 2015 to transition over to microchip-embedded credit cards (Gara, 2014). The United States is one of the last to switch over and embrace this new technology and this shift in technology is long overdue. The goal of the new technology is to prevent attackers from compromising users' credit cards by capturing the Magnetic Stripe Reader (MSR) data from Point-of-Sale (POS) systems. Attackers accomplish this data theft by gaining privileged access to the systems and installing malware on the devices that facilitate credit card transactions. The attacker often gains this access by a well-planned, methodical approach of reconnaissance, scanning, and exploitation (Engebretson, 2013). The aforementioned steps are a standard approach an attacker will use for attacking. Because the approach is often the same, it is important for security researchers, network defenders, network security architects, CISO's, and anyone authorized to work on an organizations network to be fully informed of the different threats and gain the ability to prevent these attacks.

1.1. Understanding the Threat

"If you know your enemy and you know yourself you need not fear the results of a hundred battles. If you know yourself but not the enemy for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself you will succumb in every battle" (Tzu, 40). Sun Tzu may have been speaking about tactical warfare, but the same holds true when dealing with any type of threat. If you know the enemy, attacker, and you know yourself, organization (network, security, and vulnerabilities), then one need not fear the vast majority of attacks. Looking at some of the recent breaches, the attackers gained access through means that should not have been an issue such as: Third-party vendors (Dayhoff & Holmes, 2014), RDP ports (Villeneuve, Wilhoit, & Homan, 2014), or social engineering (Trend Micro, 2014). These would not be considered major issues if proper steps are taken to use segmentation, system hardening, and general education of personnel. Organizations should follow the Critical Security Controls

© 2015 The SANS Institute Author retains full rights.

(CSC), which is a list of key controls based on real-world attack scenarios. The Council on Cyber Security manages the list of controls. These controls cover items such as: "Controlled Access Based on the Need to Know" (possible reduction in threat from third-party vendors), "Secure Configuration for Hardware and Software…" (Useful in securing the aforementioned RDP ports), and "Security Skills Assessment with Appropriate Training to Fill Gaps" (educate personnel on the effectiveness of social engineering and how to spot it). (Council on CyberSecurity, 2015)

In order to successfully defend an organization from cyber threats, one first needs to understand the threat, recognize the threat, and prevent the threat. Understanding the threat revolves around being able to know the attacker and understand how they may attack an organization. The next step involves being able to recognize the threat, the anomalies, malicious activity, logs, suspicious behavior, etc. Finally, one needs to take proactive steps in shoring up defenses using a "Defense-In-Depth" approach, as seen in figure 1, and the CSCs. (Defense in Depth, 2015). The following research will present three different retail breaches, show the evidence from the actual attack, as well as provide a list of solutions or recommendations to help organizations establish defenses from these threats.

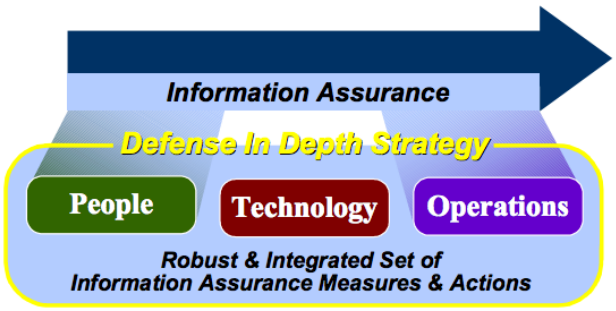


Figure 1 Retrieved from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

2. Recognizing the Threat

2.1. The Home Depot Breach

Perhaps one of the bigger data breaches as it pertains to retailers in the last couple of years is that of The Home Depot, hereinafter referred to as HD. This breach has been notorious because the attackers used a similar tactic to gain access to their systems as seen in the 2013 Target breach. According to a press release by HD, "Criminals used a third-party vendor's user name and password to enter the perimeter of HD's network." (Dayhoff & Holmes, 2014). From there the attackers were able to elevate the privileges

© 2015 The SANS Institute Author retains full rights.

on the infected machine and subsequently install malware on the self-checkout devices. This malware has been coined as "MozartPOS" based on specific strings in the malware itself, which will be discussed later (Hoffman, 2015). The Department of Homeland Security (DHS) based on findings from the U.S. Secret Service announced these findings. Further, authorities stated that the malware was tailored to mimic actual running applications in the infected environment (Banjo & Yadron, 2014). Based on the above scenario there are a few security measures that would have negated this attack vector and subsequent compromise: isolation of POS systems and 3rd-party vendor access relegated to non-critical systems or use of a segmented authentication step (i.e. Two-factor authentication).

2.1.1. MozartPOS

Before digging further into what could have prevented the above attack and compromise, one needs to first learn more about the threat, how it works, how to recognize it, and ultimately prevent and/or eradicate it. As noted in the DHS report, the MozartPOS malware was used in the targeted attack. This malware uses several different techniques to stay hidden such as naming that reflects the infected environment and deleting traces of original files used for the infection. For the purpose of this analysis, only one variant of the malware will be discussed.

NCR SelfServ Platform. The malware that has been dubbed MozartPOS is a customized Random Access Memory (RAM) scraper designed to run on the HD network. The malware, upon execution, creates a Windows Service called *NCR SelfServ Platform* (Hoffman, 2015). This technology is software used for self-checkout terminals (Smith, 2000) that were targeted in the HD breach. The fact that the malware was named to mimic running applications in the HD environment indicates that the attackers had access to the network with sufficient time to customize the malware to hide and operate effectively in the targeted environment.

Upon execution, the malware creates a Windows Service to manage the startup function of the malware in the event of a computer reboot. A notable indicator that the malware has been installed on the system is that a Windows "command prompt" will be displayed on the console with the following text:

© 2015 The SANS Institute Author retains full rights.

- The NCR SelfServ Platform Remote Monitor service is starting.
- The NCR SelfServ Platform Remote Monitor service was started successfully.

The above service names can be used for detecting an infection on the POS terminal using a signature with a Host Intrusion Prevention System (HIPS). Additionally, one could use application whitelisting (a measure addressed in the CSCs), which will be discussed in the preventative measures further in this paper.

In addition to creating a Windows Service for persistence, the malware will also create artifacts on the infected system such as "garbage.tmp", which is used to store the captured credit card information retrieved from memory. It is important to note here that Payment Card Information (PCI) compliance does not necessarily account for "data in memory". Thus, RAM scrapers are hugely successful at capturing credit card data before encryption can occur. Slava Gomzin, in his book entitled *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*, states, "Neither Track 1 nor 2 are protected, so the data is stored in clear text" (Gomzin, 2014). It is this scenario that has caused so much trouble in the retail sector; however it is not the ultimate cause of the data theft. By the time an attacker gains access to a POS terminal, they will have already bypassed multiple measures of security, albeit incomplete security measures that allowed the breach in the first place.

Getting back to the artifacts created on the system, there are a few additional ways to detect this particular threat running on an infected system. The garbage.tmp file, for instance, is only a temporary placeholder for the malware. The data in garbage.tmp will be copied to a file called "Athena.dll" (other names for the .dll file have been observed). It is important to note that the DLL is stored in what appears to be an internal HD server based on the following folder path: "\STWISM\DeviceUpdates\500\athena.dll". This file then sits at rest until a secondary payload exfiltrates the data to the attackers Command and Control (C&C) server. MozartPOS does not inherently contain the ability to connect back to the attackers C&C server. This is quite possibly a result of the POS environment not allowing direct access to the Internet. In fact, many of the POS malware families currently being used by malicious operator have no built-in exfiltration mechanism and instead rely on secondary payloads.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Finally, the last thing to examine for this malware family is some unique indicators or strings within the malware itself. These strings can be used to detect if the malware is running on an infected system using a tool such as Yara. Yara allows the creation of custom signatures to do pattern matching on strings or binary data (YARA, 2015). Creating a signature to match the strings contained within MozartPOS is relatively easy, but it should be noted that this would be a counter-measure to detect and eradicate an already present infection. Yara is a good way to perform post-infection memory scanning to detect the malicious applications. Some appliances will also use Yara to scan new files looking for malicious applications. However, this isn't always successful because some malware will only be revealed after it is installed and running in memory. Creation of a signature to detect the following strings contained within MozartPOS would help with the detection:

- http://www.the-philosopher.co.uk/whocares/popups/warcrimes.htm
- http://academic.evergreen.edu/g/grossmaz/interventions.html
- z:\Slender\mozart\mozart\Release\mozart.pdb
    - NOTE: This last string is how the malware received it's naming and is the attackers development or "working" folder for the malware.

The Yara rules are very easy to create, are able to scan very quickly, and deployable in many hardware solutions including IDS and IPS.

2.2. Goodwill Breach

The Goodwill breach is a sore point for many security researchers as the 3rd party POS vendor has not yet revealed how the attackers compromised their environment. Unfortunately, this is the case in many data breaches over the past several years. Rather than sharing details with the community, organizations instead conceal critical details of the breaches whether out of embarrassment or fear of brand damage. There are also some legal reasons to consider such as protecting customer data and confidentiality of ongoing investigations by law enforcement. Ultimately organizations should offer details about the breach, when able or authorized to do so, so that others can learn from the security breaches and

© 2015 The SANS Institute Author retains full rights.

prevent a similar attack. Another factor to keep in mind as Brian Krebs, KrebsOnSecurity, points out is that many organizations do not report breaches since they are not obligated to "unless the data that is lost or stolen includes the customer's name" (Krebs, 2014). It is unfortunate that in many cases retailers would rather "save face" than help others who may face a similar situation. An attacker already holds the upper hand, yet is repeatedly given more advantages.

2.2.1. rawPOS

Even though Goodwill or C&K Systems, Inc. have yet to release details on the avenue the attackers used to breach the company they did report that the particular malware used in the breach was a highly customized POS malware called "rawPOS" (Sarmiento, 2014). Digging into rawPOS it is immediately clear that similar tactics, as seen in MozartPOS, are used for this malware. Similar to MozartPOS, it does not have its own exfiltration mechanism, stores data in a temporary file, and then moves it to a separate storage location. Additionally, rawPOS uses a simple Regular Expression (REGEX), frequently used in many of RAM scrapers, to detect credit card Track data. The following analysis will walk through the malware and how it interacts on the infected system.

Also similar to MozartPOS, rawPOS is run using a Windows service. In the example provided by Josh Grunzweig, the service is installed as "Microsoft Support" as seen in figure 2.

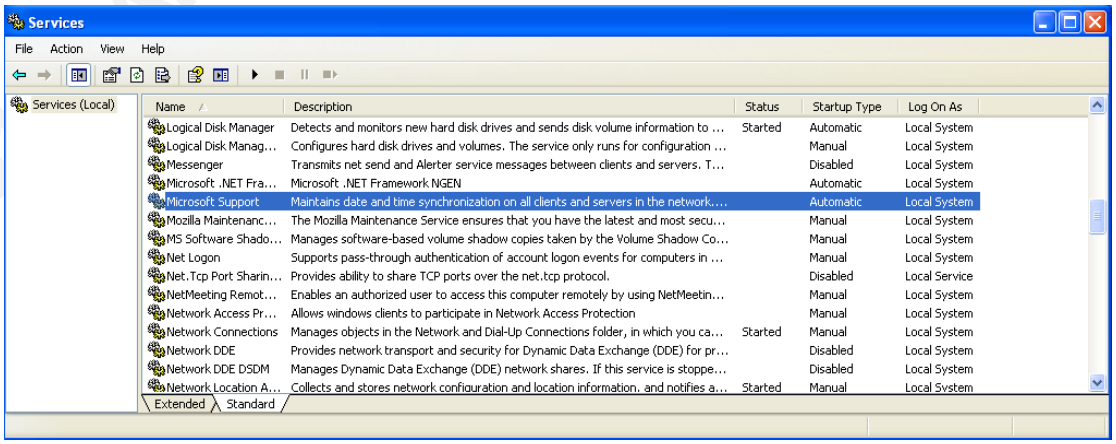


Figure 2: rawPOS service (Grunzweig, 2014)

© 2015 The SANS Institute Author retains full rights.

Unlike MozartPOS, this malware family relies on a separate component to create the service and maintain the persistence of rawPOS. In addition to rawPOS and the service installer, the payload includes a third binary compiled using Perl2Exe. This Third binary is primarily used to encrypt the captured credit card data and store it in a file for eventual exfiltration. The following steps describe this process:

1. Payload drops three binaries
2. Service installer creates persistence for rawPOS and Perl2Exe binary
3. rawPOS scans list of pre-identified processes for credit card data
4. Credit card data is matched based on hard-coded REGEX
5. Credit card data is stored in ".dmp" file in custom directory
6. Perl2Exe encrypts captured data using XOR with hard-coded key
7. Encrypted card data stored in alternate file for manual exfiltration

It is very easy to see that many of these POS malware families share common Tactics, Techniques, and Procedures (TTP) with each other. Although there are many different families of POS malware, it is easier to model new ones after their predecessors than it is to create a completely novel family with a new code base. To re-iterate the need for tighter security controls, application whitelisting again would have gone a long way to preventing the installation of this malware family and may have prevented the theft of any credit card data. Previously in this paper, PCI compliance was lightly broached in regards to data at rest and data in memory; and although this compliance doesn't fully address the need for data to be encrypted it does set high expectations for data at rest. As such, if an attacker were to gain access to the servers housing the credit card data "at rest" on a system, it would be encrypted. Therefor, regardless of the breach consumers would have been safe. However, because this RAM scraper steals the data before encryption can occur, it is highly successful on systems that allow rogue applications to run.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

2.3. NEXTEP & Bevo POS

The first two scenarios reviewed discussed larger retailers and unfortunately the same attacker vector of a 3rd party vendor compromised both. Perhaps if the investigators with HD had released details sooner others could have learned from the incident and taken precautions to prevent the vulnerability in the vector. Even though these larger breaches hold a higher spotlight in the media, it is equally important to address smaller scale breaches as attackers broaden the net of targets and larger organizations begin to implement stronger security measures. Being in the spotlight of a breach debacle enormously degrades brand image and can cost a large organization millions of dollars in damage. However, large organizations can often recover and recoup losses with a marginal impact on the bottom line. On the contrary, smaller organizations, food chains, or what some refer to as "ma and pa stores", do not fare as well and often result in severe impact to the affected entity to the point of crippling a business.

The last of the incidents to be examined in this research is that of NEXTEP Systems and Bevo POS. These two have been combined into one incident for the purpose of this report as the same malware was used in the breaches. NEXTEP Systems was deemed to be the culprit in this breach because the main affected business was a soup restaurant called Zoup. The CEO of NEXTEP, Tommy Woycik, hints that more entities than just Zoup were affected, but that many of the businesses did not have any indications of compromise (reason unknown) and some POS management firms, who ran POS systems for potential victims, refused to cooperate in the investigation (Krebs, 2015). Woycik further stated that some of the involved parties would not provide NEXTEP with critical data to aid in the investigation. Ultimately, this impacts more than just NEXTEP, their clients, and customers of the infected organizations; it affects all organizations that run any type of POS system because security researchers are unable to learn from these incidents to prevent them in the future.

© 2015 The SANS Institute Author retains full rights.

According to Krebs, the malware that was used is called PoSeidon (Krebs, 2015). However, this is actually just another name given to the Backoff POS malware family. There have always been issues in the community about naming malware families when new strains or versions are brought to light, which often confuses some into thinking a new malware family has emerged. Before diving into the malware used in these two incidents, it should be noted that many of these POS management firms use remote desktop software to manage the POS environments. Thus, several potential vulnerable ports are left open, credentials are susceptible to compromise, and POS terminals are left unsecure in a non-segmented environment. Some tools that the management firms use include "pcAnywhere or LogMeIn", says Krebs, and often are configured with simple or easy-to-guess passwords (Krebs, 2015). If an attacker were to gain access to this remote login, they could then login with authentication and upload any malware to the systems with elevated privileges. Some potential remedies to this situation will be addressed in later sections.

2.3.1. Backoff POS

"Over the past year, the U.S. Secret Service has responded to network intrusions at numerous businesses throughout the United States that have been impacted by the "Backoff" malware. Seven PoS system providers/vendors have confirmed that they have had multiple clients affected. Reporting continues on additional compromised locations, involving private sector entities of all sizes, and the [U.S.] Secret Service currently estimates that over 1,000 U.S. businesses are affected." (US-Cert, 2014)

Over 1,000 business affected by Backoff POS malware is a huge number that took many by surprise. The reality is frightening and the threat is likely a lot broader than estimated. In previous statements, this researcher has already addressed that many businesses do not come forward to report breaches due to several different reasons and as such there is a much wider number of breaches than is reported. Backoff POS malware has been one of the more prominent

© 2015 The SANS Institute Author retains full rights.

malware families in the POS environment over the past couple years with thousands of infections, both large and small.

A key differentiator in this malware from MozartPOS and rawPOS, is the ability to exfiltrate data without the use of a secondary binary. The C&C aspects of this malware family will be discussed along with its behavior and capabilities. One of the more startling, and the first thing to look at with this malware family, is the number of variations that have been observed since U.S. CERT first released their report on the malware. The following table is a list of the variants this researcher has observed while analyzing the malware (NOTE: Some versions do not have names and some variants do not have version numbers):

Variant Version	Variant Name
1.2	
1.4	
1.55	backoff, goo, MAY, net, thu, THU, DEC, DEFAULT, AERO3, SOUTH, NET, NO_GOOGLE, MONDAY, JAN
1.56	LAST, WED, NETX,
1.57	NEWGRUP, LAST, MARY
2.1	
2.2	
4.0	
5.57	
5.8	
5.9	
6	
6.02	

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 The SANS Institute Author retains full rights.

6.03	
6.04	
6.05	
7.1	
7.3	
7.5	
8.3	
9.2	
N/A	BIG, ROM, BEER, GR110, GRBIG, grpfix

Table 1: Backoff POS Malware Versions/Variants

NOTE: The analysis above is supplemented in part by Loucif Kharouni's research at Damballa. (Kharouni, 2015)

Over the course of one year the authors have gone through 42 "known" different strains of this one malware family. What is even more astounding is that there is no evidence pointing to multiple groups using this malware family or of it being sold in underground forums. Evidence points to a single group/organization using this malware to infect many thousands of entities. This is a large-scale operation and the attackers have been wildly successful in getting their malware on POS terminals.

As with the previous malware samples we've looked at, Backoff POS also attempts to disguise itself by installing as a legitimate seeming file name like the following:

- C:\Documents and Settings\Application\Data\Media Player Classic\mplayerc.exe

Also of note with this family, is that it incorporates a "service" installer/downloader similar to what was observed above in the rawPOS samples.

© 2015 The SANS Institute Author retains full rights.

Because of the addition of this component some gave it a new name, PoSeidon, but in fact it is still just Backoff POS malware with a secondary component (Allievi, Baker, Biasini, Cummings, Goddard, Largent, Zidouemba, 2015). This downloader is slightly more complicated, but essentially functions the same. Upon first launch/installation, the downloader saves a configuration file in the system folder (%System32%). This configuration file contains the C&C URLs for the malware. The malware will also create a Windows registry key to run at system reboot if certain conditions are met; this registry key looks like the following:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Winhost

If a Windows service is created like in figure 3, it will also have parameters to "Auto Start" and point to the copy of the malicious downloader. See the image below for an example:

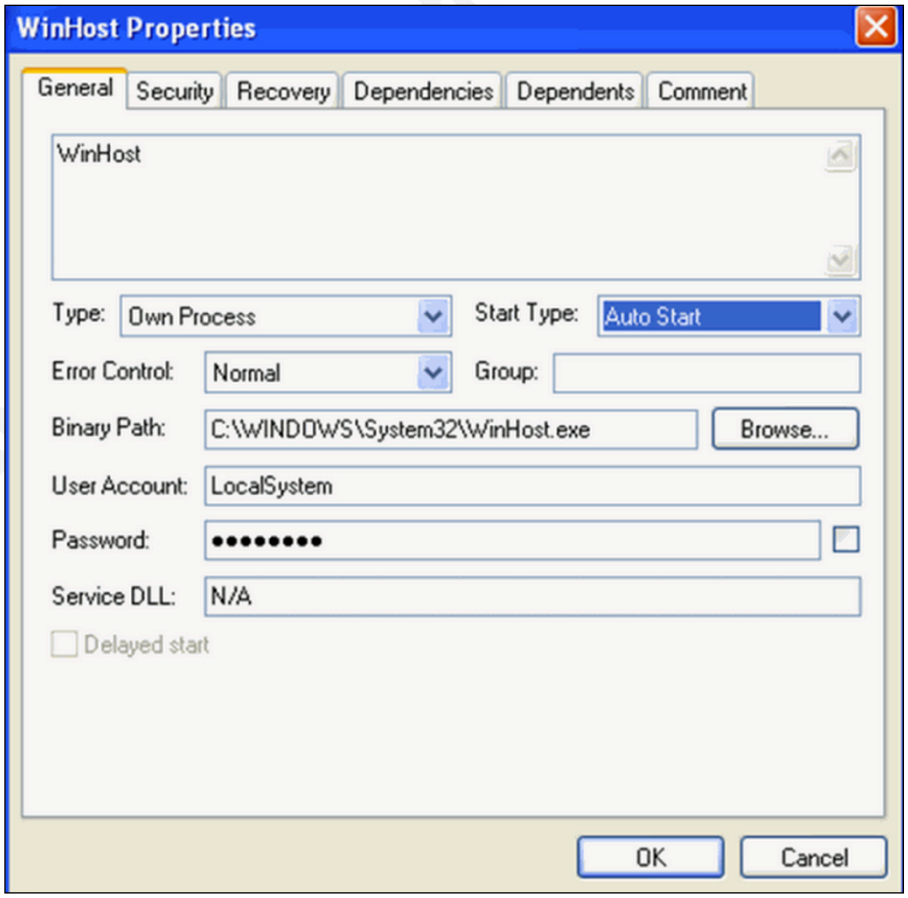


Figure 3: Backoff POS Service Creation

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 The SANS Institute Author retains full rights.

The final capability of backoff to look at, before discussing its exfiltration method, is that in addition to the RAM scraping capabilities, many of the versions have a keylogger component. The keylogger provides an added benefit of potentially capturing manually added credit card data, CVVs, PINs, and even credentials for users on the system. Thus, backoff POS malware is a two-edged sword that will capture the data using either method.

Backoff POS has used a few different methods of communicating with their C&C servers, but notably all of them involve Hyper Text Transfer Protocol (HTTP). Many of the original variants uses simple HTTP POST requests to the C&C in order to exfiltrate data about the infected machine such as the following (Kerner, 2014):

- Operating System (later versions)
- Computer Name
- Unique ID
- User Name
- Backoff Version Number
- Backoff Version Name

Not all of the above data types are consistent across different versions, but for the most part the data remains the same. However, the way the data is reported back to the C&C server is altered slightly across versions. The attackers can issue certain "commands" to the malware to control it, as seen below:

- Update
- Terminate
- Uninstall
- Download and Run
- Upload Keylogs

© 2015 The SANS Institute Author retains full rights.

- Thanks! (Do nothing, just a check-in response)

The important information to realize about the above outlined threat is that there are many more attacks than are being openly reported. The malware is constantly in flux and identification of all the variants is improbable. As such, it is very important to have a layered defense that can help prevent the threat from entering the network, compromising critical assets, and ultimately stealing sensitive customer data that will be used to perpetrate fraud.

3. Preventing the Threat

Defense In Depth. Media reports continue to poor in on what seems like a recurring theme, "Data Breach". The threat is not going away and will only grow as an organization grows and increases their presence. The bigger an organization, the more potential vectors for an attacker to get into said organization. This is why a measured, layered defense is necessary in order to minimize the risks. According to Jeorg Hirschmann, CEO for NCP Secure Communications, "defense in depth does not create an impenetrable cyber shield. Rather, it minimizes risk and keeps organizations one step ahead of the criminals" (Hirschmen, 2014). The ultimate goal of a defense in depth approach or a layered defense is to protect the most critical part of the organization. Jerry Shenk, in his paper *Layered Security: Why It Works*, (Shenk, 2013) says it best with the following: "To assess your defense-in-depth strategy, it's important to start with identifying the type of data you have that might be of interest to attackers, then determining where that data resides and evaluating what your level of vulnerability is."

For retailers, this data begins with their customers. Therefore, it is critical that retailers put their customers' data in the most protected environment possible. By using a layered defense and some practical application of the CSCs this can be accomplished. Larger organizations will take longer to roll out new security measure due to the volume of devices, employees, and potential 3rd party participants that work on their critical systems. Before digging into some specifics

© 2015 The SANS Institute Author retains full rights.

for retailers, let's first take a look at the CSCs as seen in figure 4. These will be the basis for determining a layered defense. The Council on CyberSecurity (CoSC) has the following to say about the CSCs:

> "The Critical Controls for Effective Cyber Defense (the Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses." (Council on CyberSecurity, 2015)

Figure 4: Critical Security Controls (http://www.counciloncybersecurity.org/critical-controls/)

© 2015 The SANS Institute Author retains full rights.

Organizations should seek to adhere to all of these controls. Because this research mostly focuses on POS systems and protecting the data on POS systems, this paper will primarily focus on key controls that will help to mitigate, or at the very least, help to prevent the theft of customer data.

© 2015 SANS Institute, Author retains full rights.

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 The SANS Institute Author retains full rights.

3.1. Inventory of Authorized & Unauthorized Devices

Starting at the top of the CSC list and with the most critical of the controls is that of inventory for all devices on a network. Knowing what assets are on a network will help to target key devices that need to be hardened, segmented, or even removed for security concerns. Each control is further broken down into sub-categories. One specific category stands out that will help to inventory devices that may seem trivial, but that an attacker can leverage as a foothold into an organization; one such device may be security cameras via RDP brute force attack (a documented attack vector preceding POS breaches) (Kerner, 2014). The Sub-control 1-4 is outlined by the CoSC as follows:

> Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

These instructions are very practical in getting the current state of a network and being able to pinpoint each device in a network for quick remediation. It will also make it very easy to automate alerts based on new devices that are introduced into a network as well as auto-allow authorized/trusted devices.

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 The SANS Institute Author retains full rights.

In addition to sub-control 1-4, 1-6 can also be applied as an added layer in a layered defense approach. This sub-control involves deployment of Network Access Control (NAC). If a system is compromised, it can immediately be segregated to a Virtual Local Area Network (VLAN) with limited or no access to critical systems. Therefore, if an attack were to occur by an attacker brute forcing access via RDP on a device and it was detected prior to attackers gaining access and moving laterally, then the device could then be isolated before any lasting damage is done to more critical systems.

3.2. Inventory of Authorized & Unauthorized Software

Although second on the list of CSCs, it could be argued that this single control would make RAM scrapers (POS malware) obsolete. Attackers can often find ways around security measures, but one of the key elements of data theft in retail environments is an attacker being allowed to execute hostile, or unauthorized, software on a POS terminal. Some malware families run solely in memory and disk artifacts are never installed. However, malware that runs in memory would still rely on code injection into a legitimate process. As a result of that code injection, the integrity of the legitimate application would be compromised and a system employing application whitelisting would be able to detect the change and remediate. In fact sub-control 2-1 suggests this "quick win" of application whitelisting:

> Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (isolating the custom software in a virtual operating system that does not retain infections.). (CoCS, 2015)

© 2015 The SANS Institute Author retains full rights.

With application whitelisting, all of the applications on a system are pre-approved and hashed. Hashing is used for checking the integrity of an entity. In the case of application whitelisting, this would be the integrity of the application running. With this security measure in place all applications will be hashed and that hash stored in a list of approved applications. Then, when an attacker attempts to install a rogue application it will be denied as the hash does not exist in the list of approved applications. If the attacker attempts to inject code into a legitimate application, that applications hash would change, breaking its integrity. A recursive scan of all systems, sub-control 2-3, for valid applications would easily catch this intrusion. Instead of individual application updates, any changes should be done using a strict change-control process. Although there have been instances of circumventing application whitelisting it is much harder and the chances of an attacker being discovered before they succeeded are much greater.

A POS terminal only needs minimal software to run making application whitelisting ideal for preventing installation of RAM scrapers. If an attacker cannot get to the data in memory on a POS terminal, the chances of a data breach is minimal since the Payment Card Industry Data Security Standard (**PCI** DSS) policy is enforced on any "data at rest" and as such the data is encrypted and safe from compromise. The PCI DSS policy is designed around many different types of payment systems and covers many scenarios, but data in memory, which is targeted by RAM scrapers, does not have a clear-cut solution for prevention of data existing for a brief moment unencrypted. Application whitelisting will help solve the issue of hostile applications being installed on POS terminals and thereby protect sensitive data in memory.

3.3. Secure Configuration for Hardware and Software on Mobile, Laptops, Workstations, and Servers

© 2015 The SANS Institute Author retains full rights.

"Establish and ensure the use of standard secure configurations of your operating systems." (CoSC, 2015). Secure configuration and hardening of systems is a must in any organization. It involves doing the following:

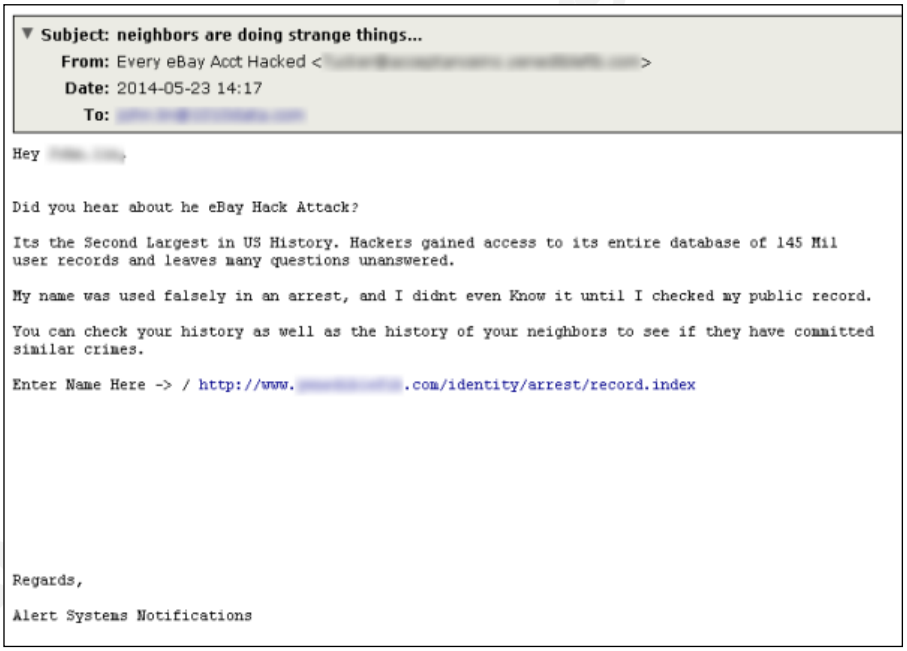
- Standard, hardened images of systems
- Remove unnecessary accounts
- Disable and/or remove unnecessary services
- Configure non-executable stacks and heaps
- Apply patches
- Close open and unused network ports (This will effectively stop RDP brute forcing if it is not needed on a system.)
- Implement intrusion detection and/or intrusion prevention systems
- Use of host-based firewalls

Although not an all-inclusive list, the aforementioned items will help secure systems to prevent unauthorized activity. Many of these activities can also be automated to help ensure the security at all times. One of the first stages in an attackers' playbook is to "scan" an organization looking for vulnerabilities. Scanning in this context means the mapping of a network about to be attacked. Part of the scanning techniques will be to acquire any knowledge of the Operating Systems (OS), hardware, network addresses, any "open ports", and many other items. By pro-actively scanning one's own network and systematically shutting down unneeded services, removing identifiable information about systems, and keeping systems up to date the attackers job becomes significantly harder to find a vulnerable attacking point.

3.4. Security Skills Assessment and Appropriate Training to Fill Gaps

© 2015 The SANS Institute Author retains full rights.

"…Human[s] remains the weakest link in the information security chain." (Schmidt, 2011). A SANS student, Chan Lieu, said it well with the following, "Social engineering is so effective simply because they [attackers] target the weakest link in the information security universe: humans." One particular breach that comes to mind in recent years is that of eBay. Although some speculation still exists around how the attackers gained access to several employees' credentials, the most obvious is that of spear phishing and social engineering. It is ironic, that right after the reveal of the breach, attackers immediately began crafting new spear-phishing emails using the breach topic as a subject. See figure 5 for an example of the spear-phishing message:



Subject: neighbors are doing strange things...
From: Every eBay Acct Hacked <[redacted]>
Date: 2014-05-23 14:17
To: [redacted]

Hey [redacted],

Did you hear about he eBay Hack Attack?

Its the Second Largest in US History. Hackers gained access to its entire database of 145 Mil user records and leaves many questions unanswered.

My name was used falsely in an arrest, and I didnt even Know it until I checked my public record.

You can check your history as well as the history of your neighbors to see if they have committed similar crimes.

Enter Name Here -> / http://www.[redacted].com/identity/arrest/record.index

Regards,

Alert Systems Notifications

Figure 5: Spear phishing message following eBay breach (Retrieved from http://blog.appriver.com/2014/05/ebay-breach-used-as-a-spam-lure/)

© 2015 The SANS Institute Author retains full rights.

After most major events, hackers take advantage of public interest by crafting unique spear phishing with subjects that boast of a specific topic, or an attachment "you don't want to miss". It is much easier for an attacker to craft a specialized spear phish than it is to recover from an employee incidentally clicking that malicious link or downloading a weaponized Microsoft Word document. Because it is so easy for an attacker to exploit the weakest link, humans, it is highly important that everyone in an organization be educated to recognize potentially misleading spear phishing or other forms of social engineering. Physical threats are just as real as cyber threats; therefore a robust policy for maintaining security for an organization needs to be implemented at all levels and for every facet of the organization.

3.5. Controlled Access Based on the Need to Know & Secure Network Engineering

The final CSCs to examine in the course of this research are the "need to know" and "secure networking". These two have been combined as some of the setup and configuration should go hand-in-hand. Specifically for the "secure network engineering" portion, this paper is focusing on sub-control 19-4: "Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses." (CoCS, 2015). In addition to setting up these trust zones, it is important to have segmentation of critical systems based on a "need to know". The sub-control 15-1 addresses this action with the following: "Segment the network based on the trust levels of the information stored on the servers…" (CoCS, 2015).

Combining both of these controls into one, it can be summarized that systems should be segmented based on a "need to know" as well as data restriction. What this means is that systems that have sensitive data should be behind multiple layers of security. The control further divides the segmentation into three categories (sub-control 19-1):

© 2015 The SANS Institute Author retains full rights.

- DMZ
- Middleware
- Private Network

Sensitive information should not be directly accessible to the Internet, but should rather be on a private network, which requires additional authentication steps, such as an application proxy, to access and only on a "need to know" basis. Further, for the objective of this research, POS terminals should not have direct access to the Internet, but rather should be routed through an internal system over an encrypted channel. As seen in multiple recent breaches, many POS terminals have direct access to the Internet allowing for the exiltration of credit card data to an external C&C server. Some organizations disallow HTTP traffic, which would prevent some malicious traffic. However, in the case of FrameworkPOS, POS malware used in some recent breaches, the credit card information is exfiltrated through DNS requests. It is possible that using sub-control 19-3 with Domain Name System (DNS) deployed in a hierarchical fashion, that this type of traffic could also be prevented. In this type of setup, the POS terminal would instead query an internal DNS server for resolution of the destination address. If the internal system could not resolve it, the request would then go to a DNS server on a protected DMZ. Although not a definite preventative measure for this type of exfiltration, it would be much easier to detect and prevent the malicious traffic from leaving the network, if the POS terminal was infected with malware.

4. Reflecting on Threats and Security Measures

© 2015 The SANS Institute Author retains full rights.

Cyber Security is a very difficult task for any organization and as the organization gets larger, the threat of attack becomes more likely. It is for this reason that it is essential that anyone working on these systems and networks become familiar with the types of threats in existence and what can be done to fight the threat. Often, the task is daunting and sometimes it is impossible to secure every aspect of a network. However, if a layered defense or "defense-in-depth" approach is taken, the probability of preventing an attack soars exponentially.

Some of the threats observed in the above research include spear-phishing attacks against personnel and 3rd party vendors, remote access attacks by brute forcing RDP on devices with open ports, installation of rogue software on POS terminals, and the possibility of physical attack vectors. All of these threats are a possibility and real-world examples exist for each of them. Therefore it is imperative for any organization in the retail sector running POS terminals implement the CSCs to protect their organization and customers.

There are too many possible security measures that can be implemented to begin setting up a layered defense and this paper addresses many key areas including six of the high-level CSCs as well as many sub-controls. The areas to consider involve inventorying hardware and software within the organization, secure configuration for all devices connecting to the network, appropriate training for personnel within the organization, controlling access based on "need to know", and finally using secure network engineering.

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

Alert (TA14-212A). (2014, July 31). Retrieved September 3, 2015, from https://www.us-cert.gov/ncas/alerts/TA14-212A

Allievi, A., Baker, B., Biasini, N., Cummings, J., Goddard, D., Largent, W., . . . Zidouemba, A. (2015, March 20). Threat Spotlight: PoSeidon, A Deep Dive Into Point of Sale Malware. Retrieved September 4, 2015, from http://blogs.cisco.com/security/talos/poseidon

Banjo, S., & Yadron, D. (2014, September 24). Home Depot Was Hacked by Previously Unseen 'Mozart' Malware. Retrieved August 30, 2015, from http://www.wsj.com/articles/home-depot-was-hacked-by-previously-unseen-mozart-malware-1411605219

Council on CyberSecurity Critical Security Controls for Effective Cyber Defense. (n.d.). Retrieved September 6, 2015, from http://www.counciloncybersecurity.org/critical-controls/

Dayhoff, D., & Holmes, S. (2014, November 1). The Home Depot Reports Findings in Payment Data Breach Investigation. Retrieved August 30, 2015, from https://corporate.homedepot.com/MediaCenter/Documents/Press Release.pdf

Defense in Depth. (n.d.). Retrieved October 2, 2015, from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Engebretson, P. (2013). What is Penetration Testing? In The basics of hacking and penetration testing ethical hacking and penetration testing made easy (2nd ed., p. 18). Amsterdam: Syngress, an imprint of Elsevier.

French, J. (2014, May 29). EBay Breach Used as a Spam Lure - AppRiver. Retrieved September 7, 2015, from http://blog.appriver.com/2014/05/ebay-breach-used-as-a-spam-lure/

Gara, T. (2014, February 6). October 2015: The End of the Swipe-and-Sign Credit Card. Retrieved August 29, 2015, from http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Gomzin, S. (2014). Turning 40 Digits into Gold. In Hacking point of sale: Payment application secrets, threats, and solutions (p. 99). Indianapolis, Indiana: John Wiley & Sons.

Grunzweig, J. (2014, October 8). Taking a Look at Rawpos. Retrieved September 2, 2015, from http://www.nuix.com/2014/10/09/taking-a-look-at-rawpos

Hirschmann, J. (2014, September 1). Defense in Depth: A Layered Approach to Network Security. Retrieved September 6, 2015, from http://www.securitymagazine.com/articles/85788-defense-in-depth-a-layered-approach-to-network-security

Hoffman, N. (2015, January 11). The Mozart RAM Scraper. Retrieved August 31, 2015, from http://securitykitten.github.io/the-mozart-ram-scraper/

Kerner, R. (2014, December 1). Https://blogs.rsa.com/wp-content/uploads/2014/12/point-of-sale-malware-backoff.pdf. Retrieved October 2, 2015, from https://blogs.rsa.com/wp-content/uploads/2014/12/point-of-sale-malware-backoff.pdf

Kharouni, L. (2015, May 22). New Variant of PoSeidon malware. Retrieved October 2, 2015, from https://www.damballa.com/new-poseidon-spotted/

Krebs, B. (2014, September 16). Krebs on Security. Retrieved September 2, 2015, from http://krebsonsecurity.com/2014/09/breach-at-goodwill-vendor-lasted-18-months/#more-27835

Krebs, B. (2015, April 15). Krebs on Security. Retrieved September 3, 2015, from http://krebsonsecurity.com/2015/04/pos-providers-feel-brunt-of-poseidon-malware/#more-30585

Lieu, C. (2002, March 1). Social Engineering – Attacking the Weakest Link. Retrieved September 7, 2015, from http://www.giac.org/paper/gsec/2082/social-engineering-attacking-weakest-link/103563

Sarmiento, C. (2014, September 2). Goodwill Provides Update on Data Security Issue | Goodwill Industries International, Inc. Retrieved September 16, 2015, from

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

http://www.goodwill.org/press-releases/goodwill-provides-update-on-data-security-issue/

Schmidt, J. (2011, November 3). Humans: The Weakest Link In Information Security. Retrieved September 7, 2015, from http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/

Shenk, J. (2013, December 1). Layered Security: Why It Works. Retrieved October 2, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805

Smith, C. (2000, December 16). Enterprise management software for self-checkout terminals. Retrieved August 31, 2015, from http://www.ncr.com/news/news-releases/retail/ncr-introduces-enterprise-management-software-for-self-checkout-terminals

Social engineering attacks on the rise, part 1: EBay breach. (2014, June 26). Retrieved September 16, 2015, from http://blog.trendmicro.com/social-engineering-attacks-rise-part-1-ebay-breach/

Tzu, S., & Giles, L. (2011). Terrain. In The art of war (p. 40). Place of publication not identified: Vigo Books.

Villeneuve, N., Wilhoit, K., & Homan, J. (2014, July 9). BrutPOS: RDP Bruteforcing Botnet Targeting POS Systems « Threat Research. Retrieved September 16, 2015, from https://www.fireeye.com/blog/threat-research/2014/07/brutpos-rdp-bruteforcing-botnet-targeting-pos-systems.html

YARA - The pattern matching swiss knife for malware researchers. (n.d.). Retrieved September 16, 2015, from http://plusvic.github.io/yara/

Richard Hummel, rhummel@mastersprogram.sans.edu

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.