COMBATTING POINT-OF-SALE MALWARE

WHITE PAPER

Trustwave®
Smart security on demand
Cybercriminals continue to maintain their lead in the malware race. As security technology advances in an effort to detect or protect against malware, so too does the malware itself. Attackers are dedicated, persistent and clever. Criminals follow their own software development lifecycle (SDLC) and test and retest their malware against anti-virus solutions to ensure it evades detection. They incorporate usernames, passwords and network addresses for their specific targets into their code. And as long as money can be made from the spoils of their conquests, they won’t let up.

One especially lucrative target for attackers is retail point-of-sale (POS) systems. If report after report of breached retailer after breached retailer hasn’t already provoked concern, it’s time for businesses to get informed about POS malware and develop a strategy to address it. Traditional security controls are not enough. Not only is a defense-in-depth strategy imperative, but businesses also need to prepare to detect and respond to a breach of their systems.

In this document, we describe the POS malware we’ve encountered in our forensics investigations and security research, explain how it’s installed on POS systems, discuss why anti-virus (AV) solutions are not enough to detect such malware and provide recommendations to address the problem. However, this paper won’t provide all of the answers. Operating under the assumption that you will be compromised is one of the better ways to increase the chances that you detect a breach when it occurs and respond appropriately to contain and mitigate it.

**WHAT IS POINT-OF-SALE (POS) MALWARE?**

Point-of-sale (POS) malware is highly customized malicious software written to identify, aggregate and exfiltrate cardholder data (CHD). According to estimates, cybercrime and data breaches involving POS malware have driven organized crime profits into the billions of dollars.
HOW DOES POS MALWARE WORK?

Legitimate Payment Card Transactions

To understand how POS malware functions, one must first understand how a legitimate credit card transaction takes place.

When a cashier or customer swipes a card, the POS system reads the account data from the magnetic stripe on the back of the card. This data is referred to as Track 1 or Track 2 data, and each contains slightly different data elements.

Below is a diagram of each track:

**Track 1**

```
<table>
<thead>
<tr>
<th>SS</th>
<th>FC</th>
<th>PAN</th>
<th>NAME</th>
<th>EXPIRY</th>
<th>SC</th>
<th>PVV</th>
<th>CVV</th>
<th>ES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8401249576443652</td>
<td>Smith  JR/JOE S M R</td>
<td>120810</td>
<td>565204</td>
<td>4738 ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIN</td>
<td>DISCRETIONARY DATA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Track 2**

```
<table>
<thead>
<tr>
<th>SS</th>
<th>FC</th>
<th>PAN</th>
<th>EXPIRY</th>
<th>SC</th>
<th>PVV</th>
<th>CVV</th>
<th>ES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4012449576443652</td>
<td>120810</td>
<td>565204</td>
<td>4738 ?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIN</td>
<td>DISCRETIONARY DATA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Merchants frequently use a software-based POS system to facilitate payment processing. Since information security is not their core competency, neither merchants nor their POS integrators (vendors that install and maintain the POS software and systems) have a solid understanding of how data breaches occur or how to prevent them. As a result, retailers are frequently the weakest link in the protection of CHD.

When this data is read by the input device (card reader) one of three scenarios plays out:

1. The data is sent directly from the POS system to the merchant’s acquiring bank. Authorization is then sent from the bank directly to the POS system.
2. The data is sent to a back-of-house (BOH) server that acts as a central aggregation point for all of the POS systems in that physical location. The BOH server then transfers the data to the merchant’s acquiring bank for authorization. Authorization is then sent back to the BOH server, which then relays that message to the appropriate POS terminal.

3. The data is sent from the POS system to a BOH server and then to a central payment switch via an MPLS network. The data is sent to the merchant’s acquiring bank for authorization. Authorization is then sent back to the central payment switch, relayed to the appropriate BOH server via the MPLS and then sent to the appropriate POS system.
The Purpose of POS Malware

POS malware has just one objective: to steal cardholder data. To accomplish this, the attackers must first identify a point or points at which the CHD is unencrypted (i.e., in clear text). Once this area of opportunity has been pinpointed, the attackers will typically deploy one of three types of malware. These types of malware—key loggers, memory dumpers and network sniffers—are described below.

Keyloggers

Keyloggers monitor the input devices on the target system. As the name indicates, this is normally the keyboard, but it can be any input device including card readers. Once data has been entered into the targeted input device, the keylogger records that data and sends it to an output file. Many keyloggers can also take screenshots of the infected machine. Screenshots give context to the captured data and might help an attacker determine which information might be a password, username or payment card number.

Once the data has been sent to the output file, it can be encrypted, encoded or left to remain as clear text. This data is then exfiltrated to a system controlled by the attackers by an automated exfiltration mechanism. In other cases, the attacker manually retrieves it. Keyloggers are normally installed on the POS terminal.

Throughout the many POS-related cases Trustwave has encountered, two main types of keyloggers have been witnessed. Homemade, or customized, keyloggers are sometimes discovered in a POS breach. These sometimes may be packaged with other malicious components, such as memory dumpers. Additionally, attackers will often use commercial, off-the-shelf keyloggers, such as Ardamax Keylogger or Perfect Keylogger. While providing a rich feature set, they enable the attackers to accomplish their goal without writing any code.
Memory Dumpers
When a credit card is swiped, the track data lives in memory for a split second before being whisked away by the payment application. Many POS vendors may claim that their application encrypts CHD at the point of swipe, and they probably believe the claim to be true. However, before the CHD can be encrypted by an application, it resides in a buffer in memory before it passes to the portion of the payment application performing the encryption. The memory dumper—which can be installed on either the POS or BOH system or on the payment switch—strikes at this split second by copying the contents of that buffer into an output file.

Memory dumpers have evolved throughout the years. The most notable trend in the past year has been the focus on command-and-control (C&C) capabilities. Prior to 2013, this feature was almost non-existent with regard to memory dumpers. However, as we’ve seen with a number of major malware families (Dexter, Alina, vSkimmer, etc.), C&C has become a popular feature. This allows attackers to control multiple instances of their malware, execute additional malware, and update their memory dumpers from a single location. Most notably, this has allowed attackers to create a botnet of memory dumpers.
Network Sniffers
Network sniffers can be installed on either the POS or BOH system. By placing the network interface card (NIC) into what’s called “promiscuous mode,” a network sniffer can monitor all traffic on its specific portion of the network. When the POS systems pass CHD to the BOH server for aggregation and transmission to the acquiring bank for authorization, the CHD is copied from the data packets and sent to an output file. While we have not witnessed the use of network sniffers in POS-related forensic cases in recent years, they remain a threat.
How is Malware Planted on POS Systems?

To deploy their malware, an attacker must first gain access to the target environment. This could include compromising POS systems prior to their installation at the retailer site or by physically tampering with the systems, but in our investigations we most often find attackers obtaining access by utilizing a remote administration utility. Examples of these utilities include Remote Desktop (RDP or Termserv), Logmein, pcAnywhere or RealVNC. IT support teams and POS system integrators use these utilities to perform legitimate remote administrative functions on POS systems and software. If remote access channels are not secured, however, an attacker can use them to gain access to the target as well.

Achieving access to the target environment is only the first step. An attacker also needs a username and password, preferably for an account with administrative authority. All too frequently an attacker can just use the default credentials added during installation of the POS software. Below is a table containing the most popular POS vendors and their respective default username and password.

<table>
<thead>
<tr>
<th>POS Vendor</th>
<th>Username:Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radiant/Aloha</td>
<td>aloha:hello</td>
</tr>
<tr>
<td>Micros</td>
<td>micros:micros or M1cr0s9700</td>
</tr>
<tr>
<td>PosiTouch</td>
<td>posi:posi</td>
</tr>
<tr>
<td>Xpient</td>
<td>support:suppport</td>
</tr>
<tr>
<td>Digital Dining</td>
<td>ddpos:ddpos</td>
</tr>
<tr>
<td>Grandbury/Firefly</td>
<td>term1:term1 or pos:pos</td>
</tr>
</tbody>
</table>

With an open remote administration utility and the default administrative username and password in place, an attacker can breach the POS systems in a matter of seconds. We encounter such a scenario in more than 80 percent of the POS-related compromises we investigate. In addition, many organizations or POS integrators that maintain systems at multiple locations will use a common username and password for all of their systems. Such re-use of credentials can rapidly lead to a widespread breach of geographically dispersed locations.

It is important to note that POS malware does not have what is referred to as a “propagation mechanism.” It is not capable of moving from one system to another like a worm. POS systems are not infected through common malware entry points, such as web browsing, visiting an infected site or using social media sites like Facebook. An attacker intentionally must place POS malware on the target system(s) and needs administrative privileges in order to do so.
WHY DON’T ANTI-VIRUS SOLUTIONS DETECT POS MALWARE?

In the past, anti-virus engines relied heavily on the identification of hash values belonging to known malicious files. Hash values are generated by taking a file and processing it with a mathematical algorithm that yields an alpha-numeric string. This string serves as a “fingerprint” for that file, and like a human fingerprint, it is wholly unique to that file. Today, most reputable anti-virus products use a cocktail of heuristic, behavioral and generic detection rules. For example, an anti-virus engine might look for calls to suspicious application programming interfaces (APIs), signs of process injections, or substrings typical to certain malware types. Detecting on heuristics allows anti-virus engines to protect against variations of known malware, even if it isn’t an exact match, and potentially prevent infection from previously unknown malware. The typical anti-virus engine itself is aware of many generic activities that, alone or in combination, are highly suspicious or overtly malicious. So, why do anti-virus products normally fail to detect POS malware? Primarily, that’s because of POS malware’s targeted nature.

Cybercriminals modify malware in their labs until they manage to create a sample that is not detected by the anti-virus that is used by the organization they are targeting. They use underground anti-virus scan sites that, unlike VirusTotal (a free service that analyzes suspicious files and URLs), do not share samples with security vendors. Samples shared by VirusTotal allow vendors to incorporate detection capabilities into their products. Because it’s restricted to POS systems, POS malware is only a small fraction of the malware that exists. Further, POS malware is not distributed in the same fashion as more conventional malware. It doesn’t spread via worm-able exploits, exploit kit delivery mechanisms or social engineering. And with the limited distribution of any given POS malware family, anti-virus vendors do not regularly encounter and gain visibility into the authors’ obfuscation techniques to improve their generic and heuristic detections.

Illustrating the relatively small percentage of malware that is specific to POS systems, in our investigations of 450 compromises in 2012, we identified 40 malware variants. The majority of these samples fell within the same “family,” was in some way related in functionality, re-used code, or exhibited linguistic patterns similar to another sample or samples. Based on analysis performed by our threat and research team, these samples were written by six different malware authors or attacker groups.

Additionally, POS malware victims face significant hurdles in sharing that malware with anti-virus vendors and others in the information security industry. In many cases, the malware itself may be customized for a specific target’s network or POS environment. Usernames, passwords, and network addresses may be hard-coded into the malware. Making that malware public could result in the exposure of credentials and poses substantial additional risk. Sharing malware with third parties can also negatively impact criminal investigations and alert the attacker to the fact that their malware has been identified. These and other challenges make vetting and submitting malware files to anti-virus companies a low priority in most organization’s incident response procedures.
Considering all of these factors, it is easy to understand why POS malware authors are able to stay a step (or two) ahead in the anti-virus arms race. Unfortunately, a negative feedback loop also contributes to the effectiveness gap—anti-virus is not very successful at detecting POS malware, so POS owners tend to avoid the expense.

In addition, we have to face an unfortunate truth about anti-virus adoption in the POS ecosystem. Payment terminals are designed to require minimal maintenance and operate reliably for years or even decades. Windows XP Embedded (XPe) is among the most common POS operating systems, and while it is similar to the desktop version of Windows XP, it is also stripped of many features and may not be compatible with many commercial anti-virus products. POS platforms based on Linux fare similarly and add the challenge of a limited selection of products. Even if a suitable product is found, maintaining POS vendor support for the anti-virus, dealing with performance issues due to anti-virus overhead and managing the updates in logically disjointed environments (e.g., environments using XP and XPe or XP and Linux) across an entire retail organization is complex. As a result, fewer and fewer POS terminals have anti-virus installed. The situation is less dire on backend systems, yet Trustwave has found that even these sensitive, full-featured systems are left to run without anti-virus in over 30 percent of incident response cases.

Another problem is the proper implementation and configuration of anti-virus products. In many of our investigations, we find that while anti-virus may have been installed on a device, it was not turned on, was considerably out of date or had expired.

We have also encountered cases where anti-virus was running and up to date, and actually identified the malware. However, because the anti-virus was only configured to alert on the identified malware, the malware was not quarantined or deleted. Typically in these cases, the organization did not have a full-time IT staff, so nobody reviewed the alerts or logs on a daily basis. If a security technology alerts on malware but takes no action on it—and no human takes notice or action either—the malware will infect and remain on the system. For example, a server at a restaurant may see an anti-virus alert on the POS but merely close it out so that they can enter a customer’s order and continue on with their duties.

In spite of the limited effectiveness of anti-virus products in detecting targeted malware, we still recommend that a company install, maintain and update a reputable anti-virus on all POS systems and other systems within the customer environment. The anti-virus product must also be configured to quarantine and/or delete any detected file. An anti-virus product alone will not protect a POS from targeted malware, but it is one (but again, only one) aspect of a defense-in-depth strategy.
How Can a Business Detect POS Malware or Know Whether They’ve Been Breached?

Identifying a POS breach is extraordinarily difficult. Even seasoned IT security professionals and cybercrime investigators have a difficult time identifying indications of these types of compromises if they are not intimately familiar with them. And of course, as explained in detail earlier, the malware is designed to make detection difficult.

Attackers don’t label their malware as “malware.exe” or “creditcardsniffer.dll.” That would be too easy. Instead they use a process referred to as “malware steganography” to hide the malicious binaries in plain sight. Windows File Protection (WFP) prevents the user from creating a binary with the same name as a legitimate Windows binary running from its legitimate directory. To circumvent WFP, attackers will give the malware a legitimate Windows process name (such as “dllhost.exe”, or “1sass.exe”) and instead of it running from the default directory (C:\Windows\System32), it will run from a non-standard location (such as C:\Windows\System32\config or anywhere within C:\Windows except the legitimate directory). Or, attackers will run the binary from the legitimate directory (like System32) but alter the name slightly using names such as “1sass.exe”, “svqhost.exe” or “office.exe.” This is only one example of how attackers avoid detection.

As an end user, you cannot conduct an anti-virus scan or run MalwareBytes (an anti-malware solution) alone and expect to identify POS malware on your systems. The best and most effective way to identify whether you have been breached is to have a POS malware expert review your payment systems. However, if retaining a PCI forensics investigator is not an immediate option, the following steps can be taken:

1. Review all accounts with administrative access for password complexity. Change any weak or default passwords to something more complex (at least seven characters including at least with one number, one capital letter and one special character).

2. Check your remote connection logs, firewall logs, or Windows Security Event Logs for successful logins from foreign IP addresses. If there is not a legitimate business reason for remote access from such IP addresses, consider the activity to be an attack.

3. Review all running processes for potential malware by identifying the process name and path from which each process has been executed. Look for slightly misspelled names running from a legitimate directory (like C:\Windows\System32), as well as for legitimate Windows binary names running from a non-standard directory (like C:\Windows\System32\config).

4. The method by which POS malware transmits stolen data could potentially be detected. In some cases, POS malware uses HTTP or HTTPS protocols. A data loss prevention (DLP) or secure web gateway (SWG) solution that scans outgoing HTTP and HTTPS traffic could potentially identify attempts to send sensitive information such as cardholder data to remote servers—and block the transmission. For instance, version 11.5 of Trustwave Secure Web Gateway includes this capability within its TextCensor2 DLP engine.

5. Segment the POS system from the network and only allow it to communicate with a handful (at most) of systems outside of that segment. The firewall should restrict those communications. You might also add network protection that detects any unexpected traffic coming to or leaving the POS—for example, traffic that is unencrypted, from an unexpected host, through an unexpected port or using an unexpected protocol.

6. Regularly check POS systems for physical tampering.
WHAT DO YOU DO WHEN YOU FIND IT?

If you identify POS malware on your systems, take the following actions immediately:

1. Inform your merchant bank. The sooner the bank can report the incident to the card associations, the better.

2. Request a dial-up terminal from your merchant bank. The bank can usually get a terminal to you and up and running within 24 hours.

3. Stop all payment-card processing on the affected systems.
   a. If the malware is found on the POS terminals, stop processing payment-card transactions on those terminals.
   b. If the malware is found on the BOH server, stop payment-card transactions on all POS terminals.
   c. You can continue to input orders into the system for purposes of inventory tracking and business analytics, but process payment card transactions on stand-alone, dial-up terminals. While temporarily inconvenient, the dial-up terminal with a phone-line connection to the bank is a secure method to process payments.

4. Contact your local U.S. Secret Service (USSS) field office and ask to speak to the Electronic Crimes Special Agent Program (ECSAP). Payment card compromises fall within the ECSAP’s jurisdiction.

5. Call a PCI forensic investigator (PFI) such as Trustwave.

6. Take notes regarding exactly what occurred, when the malware was identified, how the malware was identified and any actions that have taken place since the initial discovery. This information will be valuable to the Secret Service and PFI.
CONCLUSION

Attacks involving POS malware are financially motivated. As long as a criminal enterprise can profit from targeting POS systems, they will continue to develop malware to do so. Just like a legitimate software enterprise, a malware author follows a software development lifecycle (SDLC). Malware is tested and re-tested in underground labs to ensure it avoids anti-virus detection and other security controls before the author brings that malware to market.

Cybercriminals have professionalized, and you must respond by professionalizing your approach to data security.

Research cyber security best practices, assess your environment, evaluate the security measures you have in place and implement processes for maintaining and updating your security controls and systems. Operate under the assumption that not only is a compromise possible, it may well be imminent (if it hasn’t already occurred). Make your employees aware of the malware problem and other data security issues. Enforce strong passwords and change default passwords. Implement two-factor authentication to strengthen the security of any remote access channels. Undergo regular penetration testing to identify vulnerabilities before they lead to catastrophes. Scan and secure data where it resides, in the database. Use a secure web gateway (SWG) and secure e-mail gateway (SEG) to prevent phishing, spear-phishing and other web-based attacks. Separate assets that handle valuable data from publically accessible assets that don’t. Develop a plan for responding to an incident.

If you feel overwhelmed or underqualified, you also don’t have to do it alone. Consider partnering with a data security expert to assess, implement, manage and monitor your systems and security technologies. Just don’t put your faith in a single solution. No silver bullet will slay malware.