A Trend Micro Research Paper

Point-of-Sale System Breaches

Threats to the Retail and Hospitality Industries

Trend Micro Incorporated

Contents

PoS Systems in Retail/Hospitality Industry Networks

Point-of-sale (PoS) systems have been around in one form or another for decades. Businesses in the retail and hospitality industries use these systems not only to accept payment, but to provide other operational information such as accounting, sales tracking, and inventory management. These systems are also used to improve the customer experience through customer loyalty programs and suggestions.

From a security perspective, the most immediate risk to businesses and customers lies in accepting payments. The information customers hand over, if captured, can be used by cybercriminals to commit credit card fraud. Risk of exposure is the primary reason why the Payment Card Industry Security Standards Council (PCISCC) has established data security standards for organizations that handle the information of credit, debit, and ATM cardholders.[1]

PoS systems require some sort of connection to a network in order to contact external credit card processors. This is necessary in order to validate credit card transactions. How this connection is provided may depend on the store in question. For small businesses, this may be provided via a cellular data connection.

However, larger businesses that wish to tie their PoS with other back-end systems may connect the former to their own internal networks. In addition, in order to reduce costs and simplify administration and maintenance, PoS machines may be remotely managed over these internal networks.

Many PoS terminals are built using embedded versions of Microsoft™ Windows®. This means that it is trivial for an attacker to create and develop malware that would run on a PoS terminal, if he can gain access to that terminal and bypass or defeat any running security solutions present.

Sufficiently skilled and determined attackers can thus go after a business's PoS terminals on a large scale and compromise the credit cards of thousands of users at a time. The same network connectivity can also be leveraged to help exfiltrate any stolen information. This is not just a theoretical risk, as we have observed multiple PoS malware families in the wild.

1 PCI Security Standards Council, LLC. (2014). *PCI Security Standards Council.* "PCI SSC Data Security Standards Overview." Last accessed February 13, 2014, https://www.pcisecuritystandards.org/security_standards/.

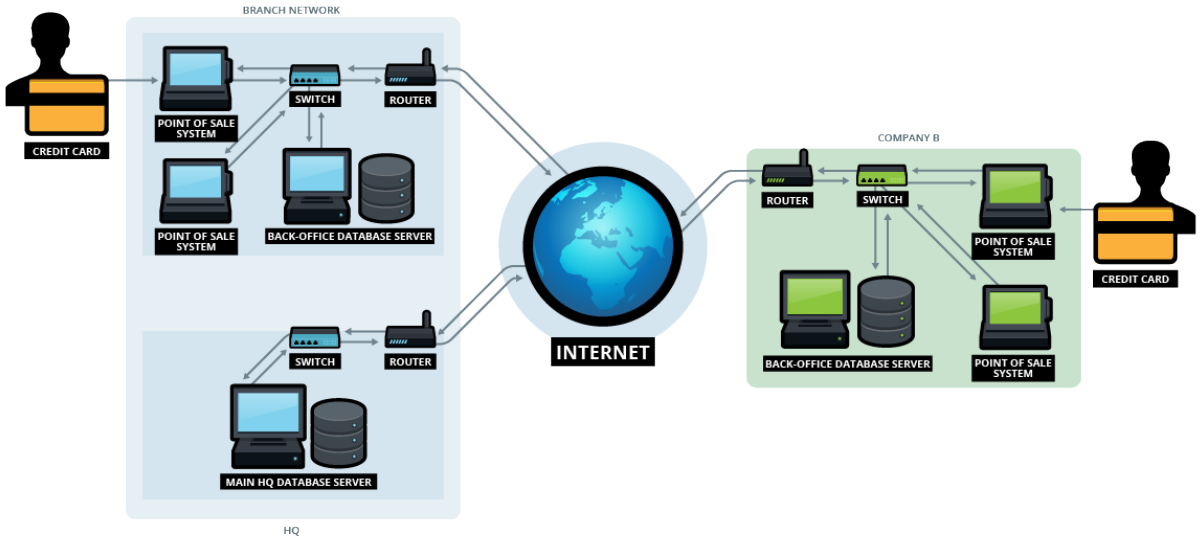


Figure 1: Basic network setup for PoS systems

PoS Device and Network Setup Weaknesses

PoS systems are difficult to secure, mostly because of their role and exposed location in the network. They handle critical information and at the same time require being managed from remote locations, a scenario typical of corporate environments that implement software package management solutions.

Industry-established standards such as the PCI Data Security Standard (DSS) are set up to ensure that the systems—and the information they handle—remain safe from unauthorized access. However, as the whole computing industry has learned through the years—it only takes one weakness to infiltrate a network.

Hacking PoS Devices

A PoS device can be considered the most important landmark in any retail location, as it is where all purchases are finalized. An attacker can find a way to infect a PoS device even before deployment, for instance, in the vendor's factory shop floor. While there have been no specific reports for PoS devices, there have been cases of newly purchased devices such as digital frames, navigation devices, smartphones, and even MP3 players found to contain malware.[2]

2 Bernadette Irinco. (December 26, 2008). *TrendLabs Security Intelligence Blog.* "Yet Another Digital Picture Frame Malware Incident." Last accessed February 13, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/yet-another-digital-picture-frame-malware-incident/; Eric Avena. (January 29, 2007). *TrendLabs Security Intelligence Blog.* "Trojans Loose on Navigation Devices." Last accessed February 13, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/trojans-loose-on-navigation-devices/; Danielle Veluz. (March 12, 2010). *TrendLabs Security Intelligence Blog.* "Malware Gets Smart with Vodafone Smartphone." Last accessed February 13, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/malware-gets-smart-with-vodafone-smartphone/; Ryan Flores. (October 18, 2006). *TrendLabs Security Intelligence Blog.* "McDonald's Japan Recalls Promotional MP3 Players." Last accessed February 13, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/mcdonald27s-japan-recalls-promotional-mp3-players/.

PoS devices are normally "guarded" by an employee during operating hours so getting to a PoS device and infecting it with malware can prove difficult for an attacker though still very doable. All it takes is a disgruntled employee or a well-disguised attacker to gain access to a system and manually install an information-stealing malware into it. Attackers may also take advantage of "self-service" terminals and PoS locations that are not as closely monitored as other stations.

Several years ago, we also reported about the sale of fake PoS devices in the cybercriminal underground.[3] These fake devices were designed to print out default receipts that inform the counterfeiter's victim that an error has prevented the transaction from proceeding when in fact the device has already skimmed the data from his credit and debit cards.

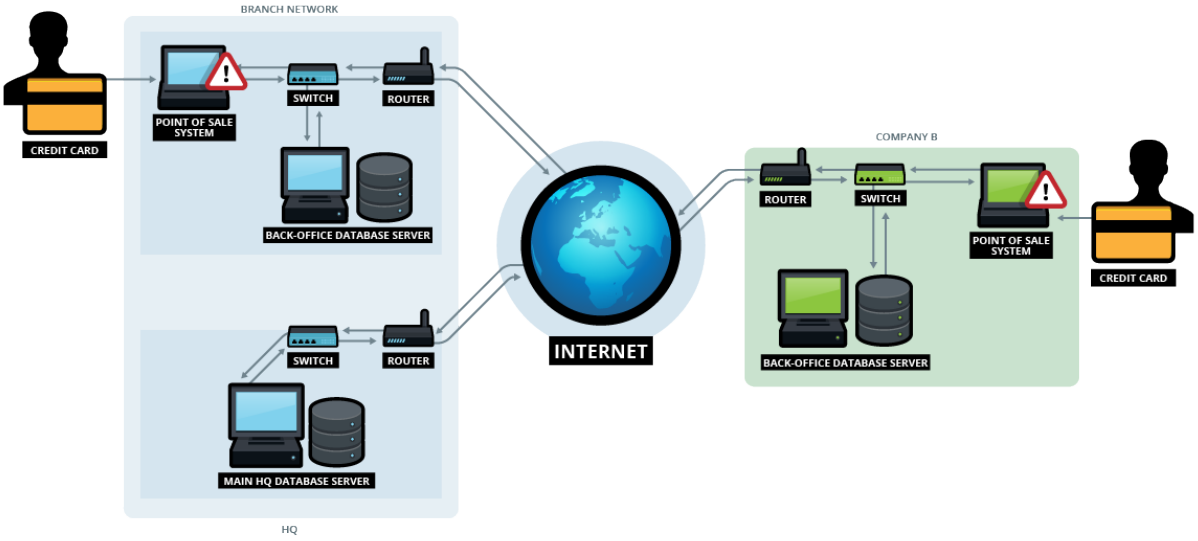


Figure 2: PoS device weaknesses

Hacking Network Communications

Network-level hacking is another technique seen used in the past wherein attackers may try to check for access to the PoS system through the network that the systems belong to. For example, in a hacking case that affected U.S. merchants between 2009 and 2011, attackers were able to conduct a port scan of the systems and identify those with remote desktop access software installed, thus gaining access to them.[4]

3 Maxim Goncharov. (June 23, 2010). *TrendLabs Security Intelligence Blog.* "For Sale: Fake PoS Devices." Last accessed February 13, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/for-sale-fake-pos-devices/.

4 U.S. Department of Justice. (September 17, 2012). *The United States Department of Justice.* "Two Romanian Nationals Plead Guilty to Participating in Multimillion Dollar Scheme to Remotely Hack into and Steal Payment Card Data from Hundreds of U.S. Merchants' Computers." Last accessed February 13, 2014, http://www.justice.gov/opa/pr/2012/September/12-crm-1124.html.

Network-level hacking can also be made possible through different methods. One can be through shared connections between systems in an establishment such as PoS systems that share the same connection with the Wi-Fi hot spot provided to customers. These PoS systems can be using Wi-Fi such as in a “back-office” area to communicate with servers. The PoS systems can also be using a closed Wi-Fi network but attackers can still be able to crack its passphrase. Attackers can also find an open port on a switch and add their own Wi-Fi access point.

Such security holes are products of noncompliance. The security standard for payment card processing requires a secure connection for the PoS system, encryption of card data, authentication for remote access to and from PoS machines, and many other methods that ensure that transactions remain safe from unauthorized access.

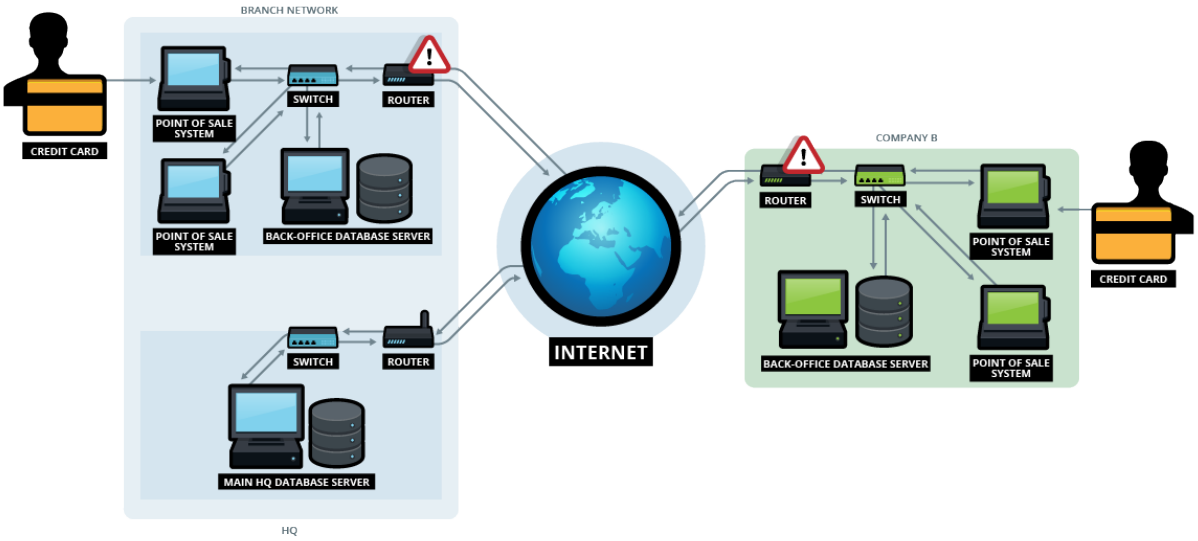


Figure 3: Network-level hacking

Targeting Specific Servers

Infiltrating networks is possibly the most sophisticated method an attacker can use in order to get in to a PoS device but it also promises the biggest payout. Unlike device- and network-level infiltration, a successful server breach will give attackers access to not just a single PoS system or a network of PoS systems in a single location, but, depending on the architecture, possibly all PoS systems controlled by the retailer in multiple locations. This is not without additional difficulties, however, as they need to gain network access before they can reach the servers. It may also take some work for attackers to know the available software on the server and the means to exploit it.

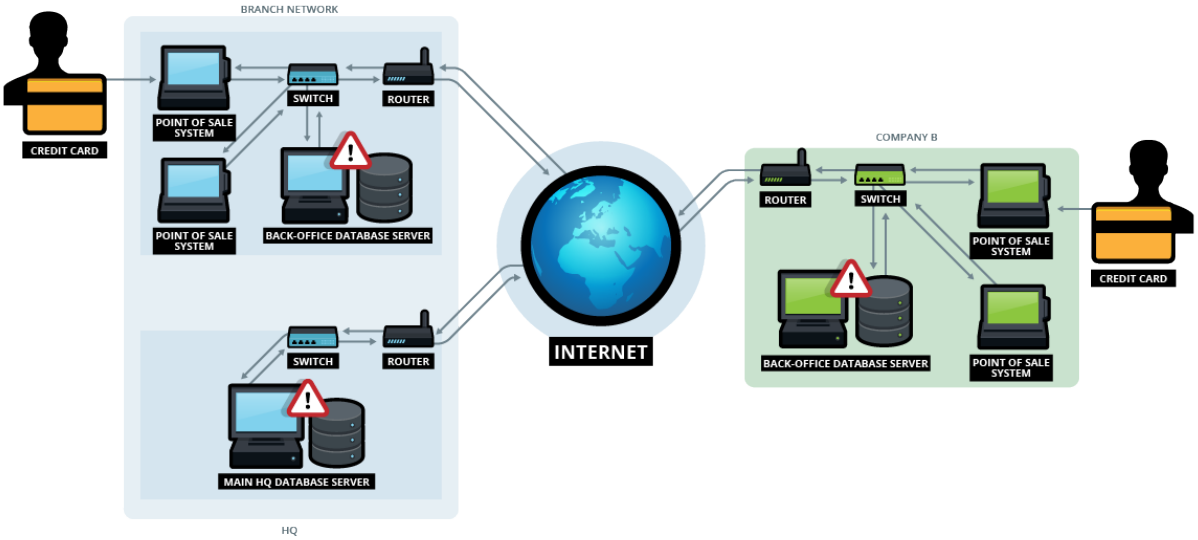


Figure 4: Hacking in to back-end office systems

Point of Entry and Lateral Movement in a Network

In a typical attack, a target receives a socially engineered message such as an email or an instant message that encourages him to click a link or open a file. The links and files sent by attackers contain a piece of malware that exploits vulnerabilities in popular software such as Adobe® Reader® (e.g., .PDF files) and Microsoft Office® (e.g., .DOC files). They may also send .EXE files that come with false icons and file name extensions. The payload of these exploits is a piece of malware that is silently executed on the target's computer. This allows the attackers to take control of and obtain data from the compromised computer, ultimately establishing the beachhead.

The attackers use this beachhead to laterally move throughout the network and finally infiltrate their ultimate target—database servers, computers with important documents, or PoS systems in this case. They typically download remote access Trojans (RATs) or tools that allow them to execute shell commands in real time on the compromised host. In addition, they may seek to elevate their privileges that they could then use in techniques such as "pass-the-hash" and seek out key targets.[5] In this particular scenario, the key target may be a system that will allow the attacker to deploy malware to all PoS systems within the network.

5 Trend Micro Incorporated. (2013). "Lateral Movement: How Do Threat Actors Move Deeper into Your Network?" Last accessed February 13, 2014, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf.

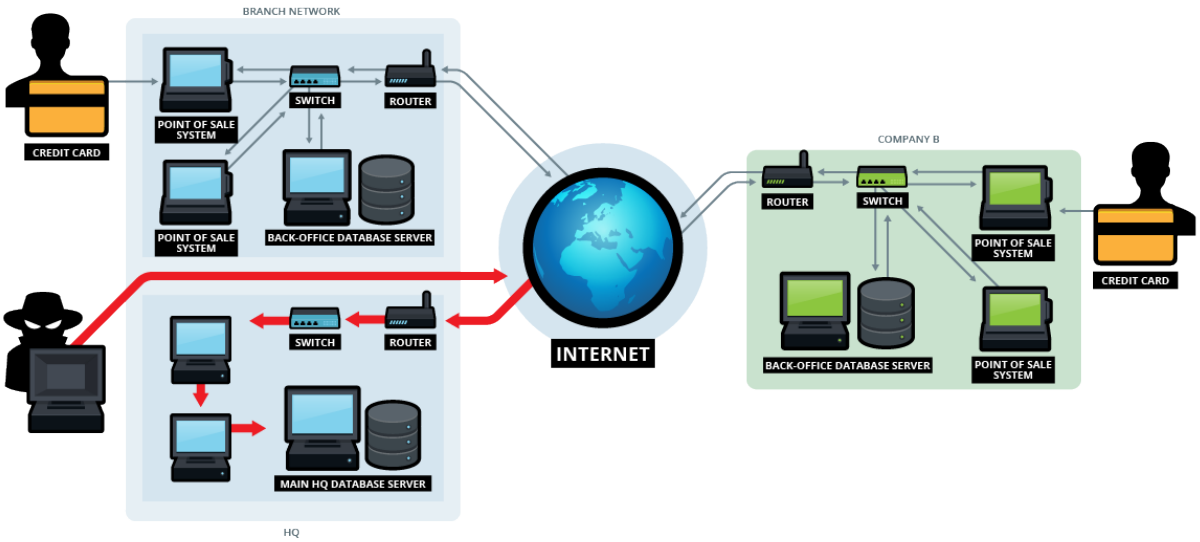


Figure 5: Point of entry and lateral movement

As the attackers move throughout the target's network, they explore and collect information that can be used in future attacks or prepared for exfiltration. They may also set up additional back doors in case the others are discovered.

Find an Update Mechanism or Another Way to Deploy Malware on a Large Scale

A server-level attack may involve the misuse of any management system used by the retailer to monitor or maintain all PoS systems. It may be one to manage system updates, collect accounting data from branches, or even one that monitors the man-hours employees put in. Any system that has control or access to all PoS systems is a potential target for attackers that aim for a server-level infiltration.

Once attackers gain access to this system, they gain access to the entire network of PoS systems, and are enabled to deploy malware that will steal customer information.

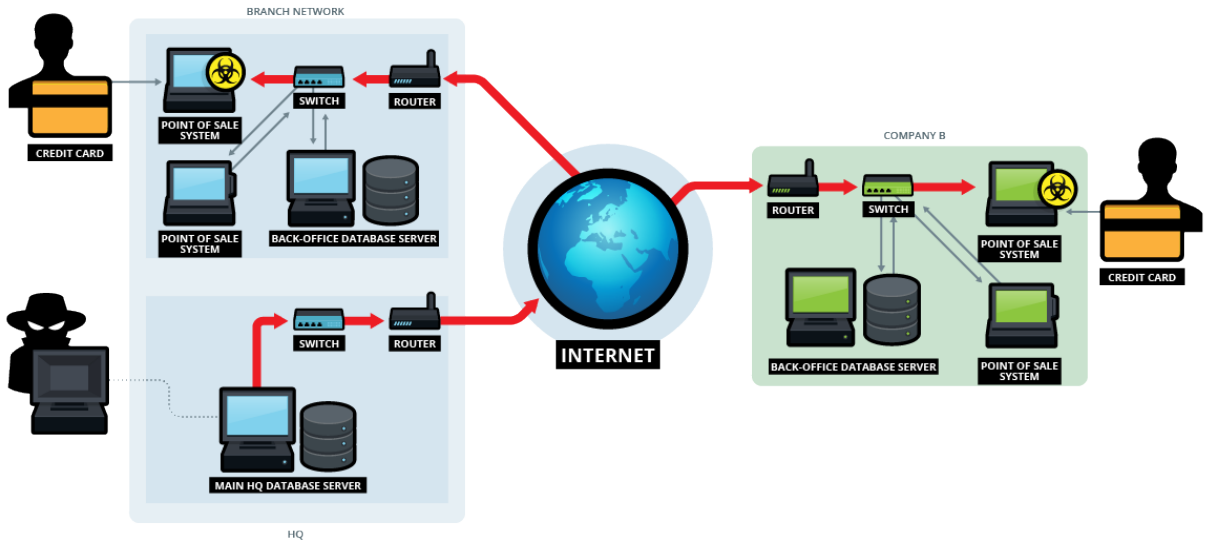


Figure 6: Spreading PoS malware to devices

Data Exfiltration

After the malware is installed on the PoS systems and the information is stolen, the next critical step for attackers is to get the stolen data from the target's infrastructure and under their control. In order to accomplish this objective without getting caught, the attackers will use a variety of techniques to obfuscate their activities. They can, for instance, collect and compress the desired data then split the compressed file into chunks that can be transmitted to locations under their control. A variety of transmission methods are used such as File Transfer Protocol (FTP) and HTTP. Attackers can, however, also use methods such as exfiltrating data by using and abusing the Tor anonymity network.

Alternatively, threat actors may use the built-in file transfer functionality that comes with some remote management tools in order to pass off their outside communications as legitimate. Some remote access tools are legitimately used to provide remote technical support assistance. Because such tools are already available in the system, solutions such as white-listing may not detect the activity, suspicious or otherwise.

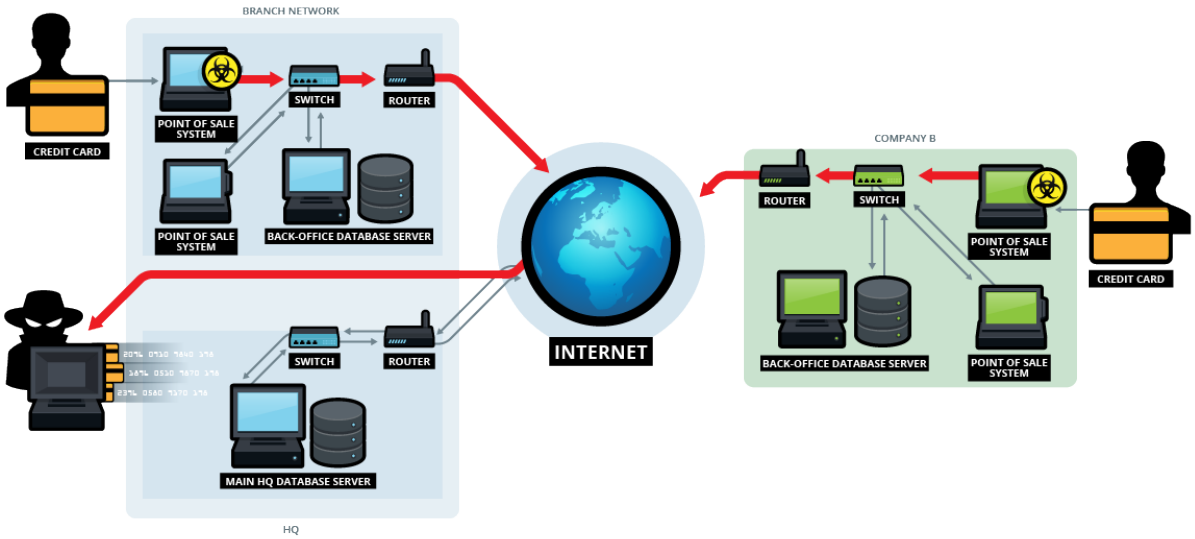
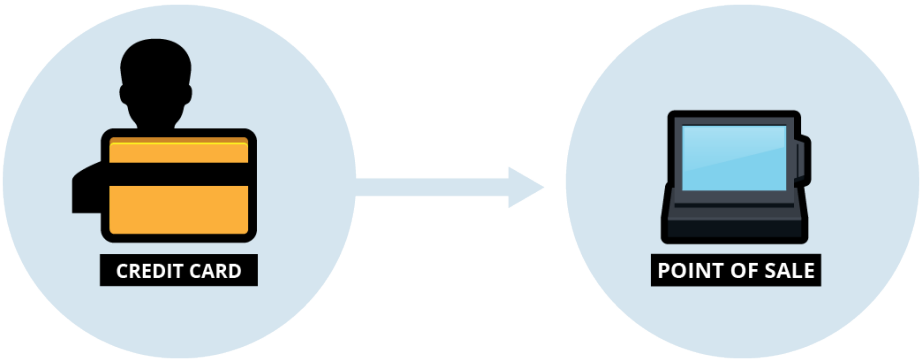


Figure 7: Data aggregation and exfiltration

Common PoS Device Malware and How They Scrape and Send Credit Card Information Back to Attackers

To comply with PCI DSS requirements, the payment card industry uses a set of security standards that enforce end-to-end encryption of sensitive payment data captured from payment cards when this data is transmitted, received, or stored. However, when the information is first read from the card, it can be found inside the PoS device's memory in unencrypted form. PoS malware exploit this by capturing the payment card information directly from the memory; this behavior is known as "RAM scraping."



Several malware families that target PoS devices are known to exist in the wild. These families are all widely available in underground marketplaces and have been used in various attacks.

ALINA

One of the more basic PoS families known is the ALINA malware family, also known as "Trackr."[6] This malware scans the system's memory to check if the contents match regular expressions, which indicate the presence of card information that can be stolen. These are sent to the command-and-control (C&C) server via an HTTP POST command.

vSkimmer

The vSkimmer malware family is easy to obtain for cybercriminals, as a cracked builder and control panel is readily available. As is the case with most information-stealing malware, it uploads any data it captures to its own C&C server. However, if it does not find its server, it has another data exfiltration method. It checks for the presence of a removable drive with the label "KARTOXA007." If this drive is found, it drops a file that contains any stolen information into it, allowing a method of offline data exfiltration.

We detect vSkimmer malware under the HESETOX family.[7]

Dexter

Dexter is one of the most potent PoS malware families in use today, in part because its information theft activities are not limited to just stealing card information. It also steals various system information and installs a keylogger onto affected systems.

In a corporate environment, this is particularly dangerous, as this could mean that even corporate information entered into PoS systems can be stolen by Dexter. Some Dexter versions are known in the underground as "Stardust" and detected under the DEXTR family.[8]

FYSNA

The FYSNA malware family, also known as "ChewBacca," is in many respects, fairly typical.[9] However, it adds a new wrinkle to PoS malware by using the Tor network to communicate with its C&C server in a secure manner. This can make detection and investigation of any breach more difficult by making all of the network traffic made by the malware extremely difficult to thoroughly analyze.

6 Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_ALINA.NG." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/bkdr_alina.ng.

7 Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_HESETOX.CC." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/bkdr_hesetox.cc; Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_HESETOX.A." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/bkdr_hesetox.a.

8 Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_DEXTR.A." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/bkdr_dextr.a; Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_DEXTR.C." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/bkdr_dextr.c; Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_DEXTR.D." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/bkdr_dextr.d; Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "TSPY_DEXTR.A." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/tspy_dextr.a.

9 Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "TSPY_FYSNA.A." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/TSPY_FYSNA.A.

Decebel

The Decebel malware family adds well-defined evasion techniques to PoS malware. Cybercriminals are aware that researchers are looking into this emerging threat and so are accordingly designing their wares. Decebel checks if sandboxing or analysis tools are present on a machine before running. This aims to make detection and analysis more difficult, buying attackers more time before their scheme is eventually discovered and shut down.

As is the case with other PoS malware families, Decebel uploads stolen information to its C&C server via HTTP POST. This family is detected as DECBAL.[10]

BlackPOS

BlackPOS, also known as the "Memory Form Grabber," is the most well-known PoS malware family. It is easily available as its source code has previously been leaked online. Like all PoS malware, BlackPOS checks the PoS terminal's memory for sensitive information to steal. However, even here, BlackPOS shows some sophistication, as some variants are only set to carry out information theft between 10 a.m. and 5 p.m. Any stolen information is stored in a .TXT or .DLL file, depending on the variant.

Unlike other malware families that directly upload stolen information to a C&C server, BlackPOS uses FTP to upload information to a server of the attackers' choosing. This allows attackers to consolidate stolen data from multiple PoS terminals on a single server, allowing for more control over data exfiltration.

Associated Threats

PoS malware are rarely, if ever, used without other malware to help carry out attacks. It is worth noting that PoS malware are almost never used on their own. Other malware components are frequently used to carry out PoS attacks. One example are Internet Control Messaging Protocol (ICMP) listening malware—PoS malware will rarely directly transmit any stolen data to a malicious or compromised server, as this would be too obvious and easily blocked. Frequently, the information is sent to a compromised server within the target organization. This "aggregator" of stolen information will then be the one that exfiltrates the data out of the network, making detection of the malicious traffic more difficult.

Shellcode-loading malware may also be used in a PoS attack. Command and control for PoS malware is difficult, as again communications to an external server may not be possible. Instead, a compromised server inside the network acts as a C&C server.

This C&C server sends shellcode across the network to PoS machines where they are loaded and executed on affected machines. This allows for covert command-and-control and renders forensic investigation of any attack more difficult.

10 Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "TSPY_DECBAL.A." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/TSPY_DECBAL.A.

Impact of PoS Hacks to Industry and Consumer Public

A major effect of PoS hacks would be the possibility of identity theft. Personal and sensitive information stolen from credit and debit cards can be used to impersonate unsuspecting consumers. These victims may soon encounter problems such as fraudulent purchases, financial loss, and damaged credit standing. Trend Micro research into different cybercriminal underground forums has revealed an ongoing, thriving, organized economy of buyers and sellers of stolen information.

Furthermore, the time, money, and effort to repair such damage can be significant—the average amount of time spent addressing fraud ranged from 11 to 37 hours in 2012. Victims may not immediately receive replacement cards, as reissuing cards can be a costly process for banks, ranging from US$3 to US$5 per card.

Compromised banks and retailers may experience backlash from PoS hacks. The public may opt to turn to other banks and retailers. A report from Javelin Strategy & Research shows that 15% of fraud victims change behaviors and avoid smaller online merchants.[11] Such breaches may also lead to class-action lawsuits. Compromised organizations may also find their value drop, if they are publicly traded.

What Should Consumers Do?

While consumers cannot control whether or not their favorite business establishments are secure against PoS malware, they can take some steps to ensure that their accounts are not put at unnecessary risk.

Reputable merchants will inform users about any potential breaches as well as absorb any financial losses as a direct result of the fraud. However, users may be defrauded even before merchants become aware of any problem so they should be on guard in any case.

Check Your Bank and Credit/Debit Card Statements

It is a good idea for users to regularly check their bank statements for any anomalous transaction. Online banking sites allow users to check recent transactions. Going over this list on a regular basis should allow users to spot and dispute fraudulent transactions made on their cards.

If users spot any fraudulent transaction, they should immediately report this to their banks and ask that the credit card in question be suspended and replaced.

Ask for a Chip-and-PIN Card

In many countries, both banks and retailers have shifted to using "chip-and-personal identification number (PIN)" or Europay, MasterCard, and Visa (EMV) cards, which primarily use an embedded chip to hold the information on the credit card instead of a magnetic strip.

11 Javelin Strategy & Research. (February 20, 2013). *Javelin Strategy & Research: Strategic Insights into Customer Transactions.* "More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report." Last accessed February 13, 2014, https://www.javelinstrategy.com/news/1387/92/1.

EMV cards offer improved security over conventional magnetic strip cards. However, not all banks offer EMV cards to all of their customers. In these cases, users should check with their banks if EMV cards are available; many banks will issue these cards upon request.

How to Secure Networks Against PoS System Breaches

How to Secure PoS Devices

- Implement hardware-based point-to-point encryption
- Limit access to the Internet
- Disallow remote access
- Routinely delete cardholder data
- Deploy the latest version of OS with updated patches
- Employ white-listing in order to lock PoS systems down only to its intended uses
- Limit internal access to the physical PoS device
- Enforce policies regarding the physical repair and/or upgrade of the PoS device
- Deploy security software and keep it updated with the latest signatures

How to Secure Networks

Cloud and Data Center Security Solutions for the Retail and Hospitality Industries

In a retail/hospitality environment, there are many potential attack vectors to consider with the increasing number of interaction channels for customers such as websites, PoS systems, mobile apps, and social media. There are multiple security controls required in order to cover attack vectors, including controls for your applications, servers, and networks. These include Web applications and servers.

At Trend Micro, we recommend the following controls in your data center:

- Restrict communication in and out of your environment to only what is required.
- Ensure that you are constantly protected against vulnerabilities in both systems and applications, even in-between patch cycles.
- Identify when a system component has changed.
- Protect against malware and malicious URLs.
- Encrypt communication between applications and data.

- Continuously scan Web applications for potential vulnerabilities.

To address risks within your evolving data center, Trend Micro provides a security solution that is open, automated, and highly scalable, that fits your existing infrastructure, seamlessly integrating with key environments such as VMware or cloud environments such as Amazon Web Services.

Changes in system components can occur for many reasons, many of which are not due to an attack against your system. That said, monitoring systems such as PoS devices for changes is becoming more and more critical to your security controls. It can not only provide an early indication of a problem, it is actually required by various compliance standards such as the PCI DSS.

Trend Micro™ Deep Security offers File Integrity Monitoring capabilities to monitor critical OS and application files such as directories, registry keys, and values to detect and report malicious and unexpected changes in real time. These include changes to PoS systems.

Deep Security can restrict communication in and out of your environment through a firewall policy that can be tailored for specific server requirements and protect against both inbound and outbound communication. Its firewall capabilities offer logging and alerting to make it easier to troubleshoot and manage.

With your business demanding constantly evolving application use, it is often difficult to keep up with patching systems against known vulnerabilities. This is where Deep Security Intrusion Prevention capabilities that protect against potential exploits on vulnerabilities are important to have on the list. An important capability of our intrusion prevention is the ability to automatically update security policies to ensure the right protection is applied, even before you have had a chance to patch.

Finally, Deep Security Anti-Malware that includes Web reputation detection will not only protect against malware but also detects and protects against known malicious URLs.

When those applications are available through the Web and provide customers, partners, or global employees the ability to share information, detection of potential threats or occasional penetration testing is not enough, especially as the number of apps increases. We offer Deep Security for Web Apps, a comprehensive, integrated software-as-a-service (SaaS) offering that continuously detects vulnerabilities, delivers actionable security insight, and protects applications with Secure Sockets Layer (SSL) certificates to encrypt transactions and communications, as well as Intrusion Prevention and Web Application Firewall (WAF) rules.

Custom Defense Security Solutions for the Retail and Hospitality Industries

In any attack, besides identifying components using endpoint or server security solutions, a network approach is also favored. Trend Micro Custom Defense solutions can support a retail organization in a number of ways.

- **Additional malware and possibly RATs downloaded to a server to facilitate lateral movement:** Trend Micro™ Deep Discovery can detect the download of malware and RATs without antivirus signatures.
- **Lateral movement and establishment of control points:** Deep Discovery can detect certain lateral movements and the spread of malware.
- **C&C communications:** Deep Discovery can detect C&C communication, both inbound and outbound.
- **PoS infection (malware are pushed to the PoS systems via network shares):** Deep Discovery can detect both external and internal C&C communication.
- **PoS systems download card data to the internal data storage server:** Deep Discovery can detect the internal data movement.
- **Data exfiltration to external server via FTP:** Deep Discovery can detect bulk data exfiltration.

What to Check in Third-Party Vendor Agreements

In several cases, businesses may opt to outsource their payment processing function. This presents an additional layer that can be found vulnerable to exposure. Therefore, organizations must make sure that vendors are contractually bound to comply with their security-related requirements.

The agreement must cover how customer data is captured, stored, processed, and transmitted, including baseline compliance requirements such as to the PCI DSS. For instance, the contract must require encryption in all stages of transmitting data. It may also set forth requiring background checks on employees with access to customer information databases.

The agreement must also clearly outline who to contact for service and support escalation when anomalies and security incidents arise. Anticipating various security breach scenarios is key to coming up with third-party outsourcing agreements that indicate responsibilities, accountabilities, liability limitations, or grounds for declaring a breach of contract.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900