Point of Sale Systems and Security: Executive Summary

A SANS Whitepaper

Written by Wes Whitteker

October 2014

Sponsored by
Bit9 + Carbon Black

©2014 SANS™ Institute
With the Target breach as the most notable example, the last year has seen scores of point of sale (POS) systems compromised by bad actors. In many cases, these environments were PCI-DSS compliant at the time of compromise. Following recent events, it is clear that executives seeking to protect their organizations and POS systems from compromise need to look beyond PCI-DSS and adopt a proactive “offense must inform defense” approach to POS security.

It is widely recognized that “2014 will be the year of the retailer.” Motivated by profit, payment card thieves are increasingly turning to compromised POS devices as a primary source for unencrypted card data that can easily be sold to “dump shops” on the black market. Recent reports put the estimated profit from POS-related cybercrime in Russia at more than $2.5 billion.

“POS attacks have a good potential to get worse. There is a vast number of vulnerable devices, random infections, targeted attacks, and a reluctance of operators to provide the necessary level of protection. The result is big leaks.” —Ilya Sachkov, CEO Group-IB

As countless retail organizations have fallen victim to POS-driven information security breaches targeting consumer payment card data, pressure on retail executives to take further action to protect POS devices has risen dramatically.

**PCI Compliance Is Not Enough**

Although, the Target breach is the most notable breach, several other well-known organizations have fallen victim to advanced POS attacks. The victims include names such as Home Depot; Neiman Marcus; Michaels Stores; Sally Beauty Holdings, Inc.; Supervalu; Albertson’s and many more. Looking deeper into this list of victims, it’s important to recognize that many of these organizations were considered PCI-DSS compliant at the time of compromise and had invested heavily in systems to meet these compliance standards.

---

3 “Russian Hackers Made $2.5B Over The Last 12 Months,” [www.darkreading.com/russian-hackers-made-$25b-over-the-last-12-months-/d/d-id/1316631](http://www.darkreading.com/russian-hackers-made-$25b-over-the-last-12-months-/d/d-id/1316631)
4 “Russian Hackers Made $2.5B Over The Last 12 Months,” [www.darkreading.com/russian-hackers-made-$25b-over-the-last-12-months-/d/d-id/1316631](http://www.darkreading.com/russian-hackers-made-$25b-over-the-last-12-months-/d/d-id/1316631)
As noted in a report about big data breaches in 2014, including Home Depot and Target, “PCI is meant to protect card issuers and make sure that consumers feel safe enough to keep using credit and debit cards, therefore ensuring card issuers make a profit.”\(^8\) That does not mean that data is absolutely safe.

While PCI-DSS provides a framework for improved payment processing, it is clear that it has been insufficient to ensure the security of modern retail POS systems. To truly improve the security posture of POS devices, organizations must take a more dynamic approach to secure POS environments moving forward—one that uses an “offense must inform defense” methodology.\(^9\)

**Why Payment Cards/POS Are Easy Targets**

To understand why POS-driven breaches continue to occur, it is important to understand key payment card characteristics and payment card system deployment models that make this information and these devices easy and attractive targets.

First, let us look at the modern payment card. The magnetic stripe of the payment card holds the vast majority of the critical payment data and is broken up into three areas, referred to as *tracks* (see Figure 1).

---

\(^8\) “PCI Compliance Under Scrutiny Following Big Data Breaches,”

\(^9\) “The United States Cyber Challenge,”
www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20%28updated%205-8-09%29.pdf
Tracks 1 and 2, which are stored in an unencrypted format, are the focus for payment card usage. It is this unencrypted track data that thieves are most often attempting to steal when compromising POS devices because it contains the information necessary to create counterfeit cards or make fraudulent online purchases.

Second, let us examine the modern POS system architectures most commonly deployed. Most retailers today rely on one of five POS deployment architectures to process in-store transactions and not all are created equal: Store Electronic Payment System (EPS) Deployment Model, the POS EPS Deployment Model, the Hybrid/POS Store Deployment Model, the Gas Station Payment System, and Mobile Payments [near-field communication (NFC) and non-NFC]. The key point to understand with the various deployment models is that the payment data is more vulnerable in certain architectures because it touches more systems while in an unencrypted format.10

With the preceding information in mind (unencrypted data, data exposure during system processing, etc.), it is no surprise that payment card information is an easy target. When processed in memory, payment data is nearly impossible to defend if a POS system is compromised. As such, memory scraping has become a popular choice among bad actors. Scraper malware is very opportunistic, and it can be easily modified to target specific patterns of data (track data) in any operating system, enabling it to bypass traditional endpoint defenses, such as antivirus software.

---

Overview of Today’s POS Attack

The basic POS breach phases include infiltration, propagation, exfiltration and aggregation. The *infiltration phase* is where the attacker gains access to the target environment. After accessing the target environment, the *propagation phase* takes place, where the bad actor spreads malware to the target systems (POS systems), which is often done via resources in the target environment (for example, domain controllers, remote administration tools, etc.). Once propagated, the malware injects itself into memory, where it collects the desired information (track data) and then *exfiltrates* the data to another system (aggregation) in the target environment. From the aggregation point, the data is uploaded to a system outside the target environment, thus reducing the chances of detection, as shown in Figure 2.

![Figure 2. Cybercriminals' Access Through POS Systems](image)

It’s important to note that POS malware continues to evolve as evasion techniques improve. These constant improvements make detection by traditional antivirus detection very difficult, and in some cases not possible.¹¹,¹²,¹³

---


Organizations worried about the security of their POS devices and looking to move beyond compliance-based security frameworks, such as PCI-DSS, should start by closely examining the Council on Cyber Security's 20 Critical Security Controls (CSCs).\(^{14}\) Developed in partnership with the NSA, international agencies and private industry, the controls use an “offense informs defense” approach to generate a prioritized list of actions designed to have the greatest impact on improving an organization’s risk posture against real-world threats.

For organizations with limited resources, or those looking to rapidly reduce the attack surface of POS devices, the following five “Quick Win” CSCs should be prioritized to most effectively address the need for greater breach protection:

1. Application whitelisting (CSC 2)
2. Use of standard, secure system configurations (CSC 3)
3. Patch application software within 48 hours (CSC 4)
4. Patch system software within 48 hours (CSC 4)
5. Reduced number of users with administrative privileges (CSC 3 and CSC 12)

Focused first on prioritizing security functions that are effective against the latest advanced targeted threats, such as the RAM-scraping malware currently targeting retail systems, these controls place a strong emphasis on security controls where products, processes, architectures and services are in use that have demonstrated real-world effectiveness. The controls have proven effectiveness, are easy to understand and provide a solid starting point for any organization looking to adopt an “offense must inform defense” approach. However, the controls should be considered only as a first step for any organization seeking to develop a robust POS security program.

\(^{14}\) Critical Security Controls for Effective Cyber Defense, [www.sans.org/critical-security-controls/control/19](http://www.sans.org/critical-security-controls/control/19)
Conclusion

The PCI Security Standards Council has made great progress in improving the security posture of retailers and payment card processors, but the standards have been unable to keep pace with the latest threat landscape. As such, until PCI-DSS can keep pace with the actual threat landscape, payment card data exposures will continue to take place. Thus, those organizations that consider PCI-DSS information security standards sufficient will remain at high risk for a payment data breach. The crux of the issue is that organizations need to broaden their security policies and procedures beyond an annual PCI-DSS compliance stamp and adopt proactive “offense must inform defense” approaches to payment card security.

Review the complete Point of Sale Systems and Security whitepaper this Executive Summary introduces at www.sans.org/reading-room/whitepapers/bestprac/point-sale-pos-systems-security-35357.
About the Author

Wes Whitteker is a SANS Technology Institute graduate student.

Sponsor

SANS would like to thank this paper’s sponsor:

Bit9+ CARBON BLACK
ARM YOUR ENDPOINTS.
<table>
<thead>
<tr>
<th>SANS Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit &amp; Training 2020</td>
<td>Munich, DE</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Budapest June 2020</td>
<td>Budapest, HU</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NV</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich June 2020</td>
<td>Zurich, CH</td>
<td>Jun 15, 2020 - Jun 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>Online GB</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>