Points of Sale Poorly Secured, Facing Sophisticated Attacks

By Brian Donohue

Published: 2014-05-12 · Archived: 2026-04-05 18:06:45 UTC

As the sophistication and deployment of PoS malware increases, organizations struggle to defend against even simple attacks.

The point-of-sale (PoS) systems on which financial transactions are conducted at nearly every physical retail location in the U.S. and and beyond are fast becoming a favorite target for sophisticated criminal organizations as well as standalone attackers.

The emergence of this trend is unsurprising given that a compromised PoS terminal could potentially yield all pertinent payment information about any credit or debit card processed in a transaction on that machine – including track one and two payment data as well as card numbers, expiration dates, security codes, and the names of the people they belong to. The problem is exacerbated – according to a PoS malware analysis published by Arbor Networks – in two ways: the maintainers of PoS systems are doing a poor job of protecting such systems against older and well-known attacks as criminals continue to create more sophisticated tools.

PoS attack campaigns, the researchers claim, have evolved from opportunistic attacks relying on simple card data theft to memory scraping PoS botnets with centralized command and control (C&C) infrastructures. The most sophisticated attacks are highly targeted, deploying hard-to-detect, customized malware, and reportedly requiring substantial lateral movement within a compromised network.

“Organizations of all sizes are encouraged to seriously consider a significant security review of any PoS deployment infrastructure to detect existing compromises as well as to strengthen defenses against an adversary that continues to proliferate and expand attack capabilities,” wrote Curt Wilson, a senior research analyst at Arbor Networks.

Another significant problem, according to the report, is that once an organization’s PoS systems are compromised, the attacker tends to maintain a presence on those networks for a long time, even within organizations with mature security postures.

“The longevity and extent of attack campaigns is a serious concern. In organizations with security teams and well managed network infrastructure, point of sale compromises have proliferated for months prior to detection. If attackers are able to launch long-running campaigns in such enterprise retail environments, one can conclude that many other organizations with less mature network and infrastructure management are also at serious risk.”

Targeted breach timelines

Company	Compromise time	Days Compromised	Number of stores
Schnucks	December 1, 2012 – March 29, 2013	119	79
Target	November 27, 2013 – December 15, 2013	19	N/A
Nieman Marcus	July 16, 2013 – October 30, 2013	107	77
Aaron Brothers	June 26, 2013 – February 27, 2014	147	54

Point of Sale Breaches

The full scope of the problem is perhaps best illustrated by Verizon's renowned Data Breach Investigation Report, which examined 198 distinct PoS intrusions in 2014 alone, the report claims.

Generally speaking, Arbor Networks has observed a substantial increase in the level of interest in PoS-related threats, both in closed and public forums. Interestingly, all of their observations regarding this increased interest came before the Target breach became public knowledge.

Specifically, in its report, Arbor Networks examines the Alina, BlackPos, Chewbacca, vSkimmer, JackPos, and PoSCardStealer malware, as well as a new PoS Attackers Toolkit. You can find the MD5 hashes associated with the command and control domains and files within each of these samples in the Arbor Networks report [pdf].

The Alina malware was developed in March 2012, with the most recent development taking place in February . Alina's command and control domains suggest that it may be a precursor to JackPoS.

BlackPoS is likely the most talked-about piece of PoS malware this year due to its affiliation with the much discussed target breach. Older versions, observed with compilation dates as far back as 2010 were simply console based, which required the attackers to maintain backdoor access to the target in order to retrieve the stolen card data. Newer versions use HTTP and FTP to exfiltrate data. The evolution of BlackPoS seems to mirror the more broad evolution of PoS threats.

The researchers point out that during the Target breach, the PoS malware was observed exfiltrating data to other internal systems before moving that data off the network to external systems. The researchers believe this staging occurred because the PoS systems could not exfiltrate directly to the Internet.

Chewbacca is another oft-discussed PoS malware toolkit – likely due to its use of the Tor network for its C&C infrastructure. vSkimmer too has been the focus of significant past research after its code likely leaked on underground forums in 2013. Arbor Networks doesn't spend a ton of time analyzing vSkimmer other than pointing out that it has the capability to perform memory scraping with exfiltration to a Command & Control point or to a USB drive and that it is easy to detect.

Arbor Networks expresses more interest in JackPoS, which they believe was developed from at least October 2013 with the most recent development on March 5, 2014. They have observed at least 33 distinct samples.

Separate research suggests that a threat actor operating under the handle Rome0 – known to be implicated with the Dexter and Project Hook PoS malware and a laundry list of other underground activity– is also associated with this malware.

Upon infection, JackPoS attempts to spread itself other systems via Windows networking. According to the research, it displays a text reading, “Hacking of the network started” and then looks for the presence of a domain controller.

“This is of course foolish design for any type of malware since no sane user would press any key in response to such a blatant “Hacking” message,” the Arbor researchers reason. “Because of this, it is possible that this was test code, proof of concept, written for a limited deployment such as an environment where the attacker has physical access, or was some type of demonstration code that leaked into the wild.”

The research also looks at a PoS attackers toolkit that first emerged in March 2014. This toolkit, the researchers claim, provides strong evidence that no zero-days are required to compromise PoS terminals. Different versions of the kit rely simply on brute-force password attacks. Arbor notes that despite this being an old technique, there have been at least ten variations of this attack kit submitted to VirusTotal in the last 10 months.

On a more sophisticated level, the toolkit also makes use of a modified version of a legitimate auditing tool called Card Recon, which is designed to find credit card data across a wide variety of systems.

“Card Recon looks to be a useful tool when wielded by an auditor or security staff, but is clearly dangerous in the wrong hands,” the researchers wrote. “The presence of an audit tool like Card Recon where it is not expected is a clear sign of trouble, as it shows that attackers are after card data anywhere that it can be found.”
