Arbor White Paper

# More Than One Way to Scrape a PoS

ARBOR NETWORKS

## About Arbor Networks

Arbor Networks, the cyber security division of NETSCOUT, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business. To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

# Looking Beyond the Headlines

Retail organizations have always been tempting targets to cyber criminals looking for payment card and personally identifiable information. And judging by recent media coverage, retail organizations certainly suffered their share of damaging breaches last year.

"The year 2013 may be tagged as the "year of the retailer breach," but a more comprehensive assessment of the InfoSec risk environment shows it was a year of transition from geopolitical attacks to large-scale attacks on payment card systems."[1]

These attacks included the largest credit card theft to date from a US retailer, and indications are PoS (Point-of-Sale) breaches are on the rise in 2014.

But the real story is the evolving scope and sophistication of these threats, encompassing older "tried and true" methods like RAM scraping, as well as more advanced attack malware penetrating corporate infrastructure. These more mature and sophisticated threats require a new approach to retail security.

Protection today requires a complete picture of the network—not just PoS systems—including all available contextual data, your unique network configuration and behavior as well as external threat intelligence, that allow you to more rapidly identify, fully scope and effectively mitigate the attacks that matter.

## Evolving Retail Threats

Attacks targeting the information on or captured by PoS systems can be characterized roughly into three categories.

- The older, traditional opportunistic attacks on vulnerable PoS machines, usually found by trolling, installing malware on those machines, then setting up a backdoor to access the results;
- Threat actors compromising PoS systems, setting up malware that communicates with a remote C&C server (basically turning them into PoS botnets at that point);
- The advanced, targeted attack focused on a specific organization; they penetrate that organization directly or through a partner (e.g., supply chain) then perform lateral movement on the networks to access payment card data—whether on the PoS system itself, or in any clear-text form in memory, on disk or in transit over the network.

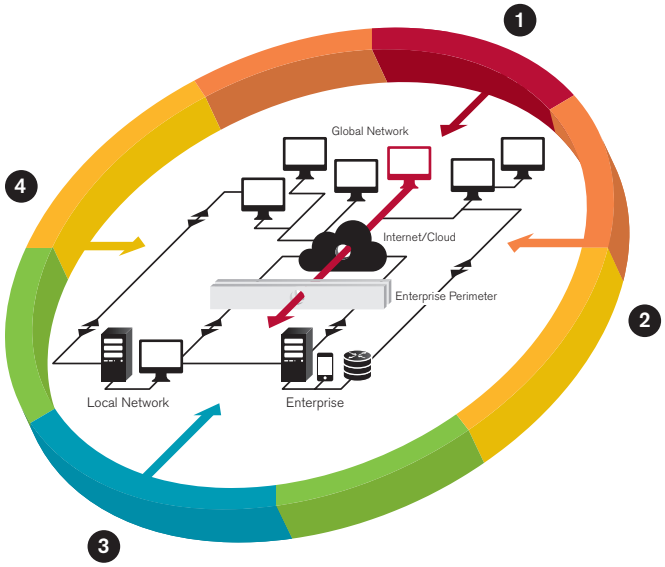


***Figure 1*** *The Target Attack: Operation Kaptoxa*

### The Target Attack: Operation Kaptoxa

1. Online malware kit customized for Target.
2. Enters via vulnerable web server. Malware infiltrates PoS servers and sets up internal server to collect data.
3. After 6 days, exfiltrated data from Target server sent to external FTP server on hijacked site.
4. Use VPS in Russia to download data for 2 weeks.

**Advanced Threats**

- Attacks planned for a specific organization.
- Multi-stage and traverse in and out of network bypassing existing controls.
- Hard to detect from regular patterns.

[1] 2014 Data Breach Investigations Report, Verizon, page 3.


***Figure 2*** *Global Dexter and Project Hook compromises*

All these threats continue to evolve and become more sophisticated. Even the opportunistic attacks have been augmented to support lateral network penetration. A good example is the Nemanja botnet, estimated to have infected 1,478 hosts in nearly 40 countries. Nemanja has penetrated PoS networks through a remote-access portal, infiltrated the network system via drive-by-downloads or other ways of breaching the organization's network perimeter. Older malware families such as Dexter and Project Hook continue to developed and used as components of more advanced, infrastructure attacks. For example, a newer variant of Dexter, Dexter Revelation, has been observed employing FTP to exfiltrate data.

The more advanced attacks seek a centralized network functionality through which to install malware on multiple PoS machines, or compromise the payment card data directly on the corporate network itself, either during transmission or in memory. This means that protecting individual PoS machines is table stakes for retailers. Bottom line is retail organizations, similarly to large segments of the financial industry, have increasing requirements (and incentives) to protect their corporate networks.

What is needed is a more proactive approach; any enterprise today overly reliant on purely preventive security mechanisms is increasingly at risk. In order to make rapid, confident decisions about real threats and how to respond you need fast, comprehensive visibility into your network traffic, the context surrounding your network behavior, and detailed external threat intelligence.

### Project Hook Indicators of Compromise IOCs

| | |
|---|---|
| **Date Observed** | • October 13, 2013<br>• November 5, 2013 |
| **MD5** | • 759154d20849a25315c4970fe37eac59<br>• 16b596de4c0e4d2acdfdd6632c80c070<br>• e3dd1dc82ddcfaf410372ae7e6b2f658 |
| **Domains/IPs Contacted** | • romeo0. biz 94.242.199.145<br>• romeo0. biz 193.106.172.131 (October 1, 2013, VirusTotal) |
| **Network Indicators** | • GET/hint/chck.php HTTP/1.1<br>• Host: rome0[.]<br>• Accept: text/html, */*<br>• Accept-Encoding: identity<br>• User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1)<br>• hxxp://rome0.biz/hint/cx.php |
| **Defense and Detection** | • PCI-DSS compliance—"minimum" (Payment card industry data security standard)<br>• Network protections<br>• Host protections<br>• Log analysis and review<br>• Auditing for security vulnerabilities<br>• Monitoring/alerting/blocking network traffic |

## Discover Attacks that Matter and Reduce Response Time

Unfortunately, the track record for retail organizations detecting PoS intrusions is not encouraging. In many cases PoS compromise is discovered by an outside party—law enforcement, payment system vendors or banking institutions investigating fraud.

Identifying the attacks that matter requires easy visibility into your network's unique behavior coupled with a context, a broader view that includes external threat intelligence. Not all Indicators of Compromise (IoC) mean you have been breached or are at risk for information loss; there is a lot of "noise" in alerts. The "contextualizing" of network traffic allows you to more easily spot PoS malware characteristics such as lateral propagation, illegitimate outbound communications, and of course data exfiltration.

**ASERT™ alerted on the Dexter and Project Hook threats in December 2013, prior to the holiday season and just before the Target breach was discovered. For more on their research findings, the "Happy Holidays: Point of Sale Malware Campaigns Targeting Credit and Debit Cards" blog post delves into this ongoing PoS malware campaign.**

Decreasing incident response times and increasing the economic application of your business resources requires prioritizing and documenting these IoC. Misguided incident response can do more harm than good by distracting from real threats, wasting precious time and resources, or by removing valuable clues to uncover the full extent of PoS intrusion and corporate compromise. While evidence suggests that current IR teams are prepared to handle certain incidents—like loss of a company PC or mobile device—responding to advanced attacks remains a challenge. Many incident response teams have cited a lack of understanding for advanced threats that is challenging their ability to respond effectively.

**The level of preparedness is being held back by a lack of understanding about threats…. Having a formal plan or team in place has a significant effect on the feeling of preparedness among executives. Even so, only 17% of business leaders feel fully prepared for an incident.**

*Source: Cyber Incident Response, Are Business Leaders Ready?, Economist Intelligence Unit, 2014, page 4.*

## Multiply your Muscle by Bringing Context to Chaos

Providing real context to your unique network behavior requires the ability to capture and view traffic data for the extended periods of time it may take to "connect the dots": where and when malware was dropped, where it moved and what it touched within the system. This capability to 'rewind' traffic data, combined with the experiential knowledge of your team and external threat intelligence, offers the best opportunity to discover, prioritize and rapidly mitigate advanced PoS intrusions in their entirety.

Arbor Networks® NSI and SA allows your team to uncover real threats, detail the attack timeline, and prioritize for rapid, effective response. NSI acts as the central nervous system for enterprise security deployments. Sitting inside the network, a dashboard presents an enterprise-wide view of all network activities. NSI monitors network traffic patterns and alerts security teams to IoC or an actual breach in progress. NSI enables organizations to prioritize attack alerts by analyzing communications with critical assets against key attack characteristics.

SA allows you to investigate suspicious IoC by rewinding network data to completely uncover attack timelines. Taken together, they allow you to fully trace intrusions, prioritize and dramatically shorten your time to effective mitigation.

### ASERT

ASERT is a world class team of security researchers dedicated to discovering and analyzing emerging Internet threats. Threat indicators are released via ASERT Threat Intelligence Bulletins, and provided directly to SA customers via the ATLAS® Intelligence Feed.

**A recent Dexter PoS Threat Intelligence Bulletin included:**

- Further insight into Dexter Revelation including a script to decode dump files.
- Additional actor insight.
- Potentially vulnerable Point of Sale solutions.
- Numerous file and network indicators.
- An analysis of possible attack vectors.
- An updated infection map.

**The full bulletin is available here.**

NSI with the advanced threat detection capabilities provided by the AIF helps organizations identify risk activity. There are several policies in AIF that identify indicators of PoS attack activity. The policies combined with the reporting functions within the product give Security Operations Center (SOC) analysts a detailed play by play of how and when the affected systems were communicating with the attacker. This detail enables the SOC team to confidently escalate an activity to the security team or IR team for further investigation.

When an incident has been identified, SA provides critical network context spanning days, weeks, even months. Leveraging awareness from internal and external alerts—and your experiential knowledge of your network's unique characteristics and behavior, you can intelligently filter on key identifiers over spans of time: finger or port listings, logins, FTPs, shell code installed, IP addresses accessed, etc. This intelligence encompasses more than malware signatures; it includes your unique network topology, methods of attack, geo-location of components and other indicators.

SA is unprecedented in its capacity to rapidly mine and work visually with terabytes of packet capture data. You can "zoom" from years to seconds of network activity in the same screen with a click of a mouse. It does not require complex configuration nor integration with other security tools. It captures all the network packets via TAP or SPAN: no log collectors, no parsers—and no gaps.

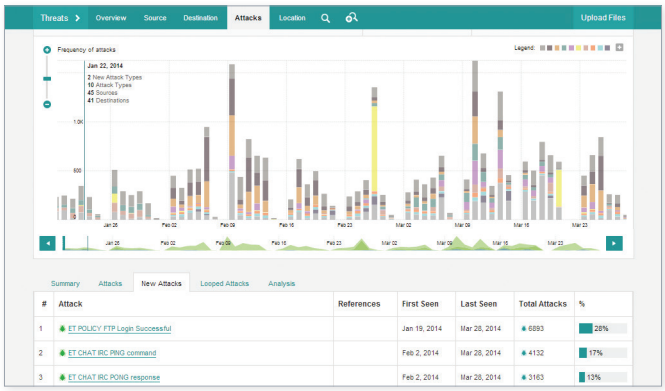


***Figure 3*** *Hunt through terabytes of data to find attacks in your network.*

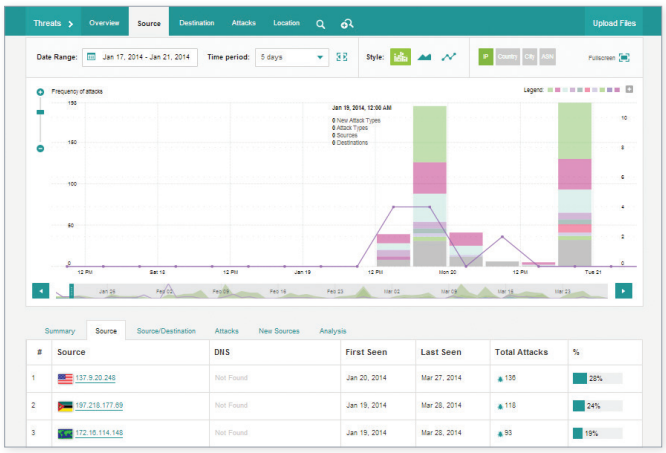


***Figure 4*** *Mine through data to investigate the sources generating attacks against your network.*

This real-time visual analysis multiplies your teams' muscle; it helps you better identify, prioritize and rapidly mitigate PoS intrusions. SA allows you to quickly document an attack's network-wide activity to see what the attackers were/are doing inside your network: lateral movement, external communications, instructions received, malware downloaded, how it spread and of course exfiltration of data.

Documenting the exact details of an intrusion are important for management, operations, budgets, etc. Now you can literally show management what is happening—and what steps should be taken. It can help you fortify threat mitigation defenses against further, potentially related attacks, and improve your incident response capabilities and processes over time.

## Changed Landscape Requires New Strategy

Retail organizations are facing increasing cyber-attack, new breeds of PoS intrusion malware and more sophisticated penetration strategies. The industry has acknowledged this new threat landscape by forming the Retail Cyber Intelligence Sharing Center (R-CISC). Retailers can learn from recent breaches and advance their protection strategies to meet the new threats that will continue to evolve.

NSI and SA help you tame the chaos of enterprise network alerts. By applying a rich threat intelligence context to visible network traffic, your team can discover and focus on the attacks that matter. Your team can trace and document complete PoS intrusion timelines, and respond more effectively, respond more rapidly to verifiable threats.

**Corporate Headquarters**
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

**North America Sales**
Toll Free USA +1 855 773 9200

**Europe**
T +44 207 127 8147

**Asia Pacific**
T +65 68096226

**www.arbornetworks.com**

ARBOR® NETWORKS

©2015 Arbor Networks, Inc. All rights reserved. Arbor Networks, the Arbor Networks logo, ArbOS and ATLAS are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.

WP/MORETHANONE/EN/1015-LETTER