SOLUTION BRIEF

Tripwire Solutions for Retail Security

Providing security throughout the cyber threat lifecycle

According to Verizon 2015 Data Breach Investigation Report:

- 70% of breaches are successful within minutes
- POS intrusions are the top security incidents with confirmed data breaches
- POS attack methods are becoming more varied and adaptable
- 91% of breaches targeting retailers take weeks to months to discover
- 78% of breaches targeting retailers take days to weeks to remediate

A retailer's reputation can make or break its success, and the quickest way to damage a good reputation is to compromise customer trust. Every time you as a retailer ask a customer for their personal data and credit card, the customer puts their trust on the line. Most customers assume that retailers have adequate security measures and technology in place to keep that data safe and private.

Unfortunately, retailers represent a prime target for cyber attackers who use sophisticated methods to infiltrate and steal a wide range of data—especially customer's personal and financial data. Today, retailers need to put better security controls in place, focusing on two key things; more proactive protection against cyber attacks so that they are not an easy target, and accurate detective controls to alert on an attack in real time—before critical data is stolen.

Today, cyber attackers have become more sophisticated than ever, using an approach referred to as the "cyber kill chain," an intelligence-driven defense process defined by Lockheed Martin's Computer Incident Response Team.

The cyber kill chain includes these phases of attacker activity:

- Reconnaissance—The attacker seeks information on the target, particularly its vulnerabilities.
- Weaponization & Delivery—The attacker develops an attack payload customized to exploit a target's vulnerabilities and then delivers it to the host machine.
- Exploitation—The attack payload compromises the host machine, allowing the attacker to establish control within the network.

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

- Command & Control—The attacker attempts to maintain their presence and control within the network to continue the exploitation.
- Malicious Action—The attacker uses the compromised host system to execute the objective, which is often to steal data or disrupt business.

From a retailer's perspective, protecting against attacks utilizing the cyber kill chain framework can be simplified into three phases:

- BEFORE—Reconnaissance and Weaponization
- DURING—Delivery, Exploitation, Command & Control
- AFTER—Malicious Action

Threats are becoming distinct to particular industries—for example, in the retail sphere there were several new families of RAM scrapers aimed at point-of-sale (POS) systems discovered in 2014. Security cannot be one size fits all.

There is no silver bullet when it comes to cyber threat protection; the best defense is a multi-layered solution approach that uses the right security solutions at each phase of the attack.

Tripwire solutions offer industry-leading detection and protection against security incidents at each phase of the cyber kill chain. Most importantly, they address a gap in the "during," or exploitation, phase, which allows retailers to detect a potential breach early in the attack cycle, before damage has occurred. Tripwire is committed to the retail industry and delivers specific policies for POS threats. Tripwire also provides industry-leading and cost-effective solutions for PCI compliance, helping retailers more easily address what is now considered a basic cost of doing business in the digital age. All this lets retail organizations focus on running their business, and not on preparing for audits or the negative impact and attention of a security breach.

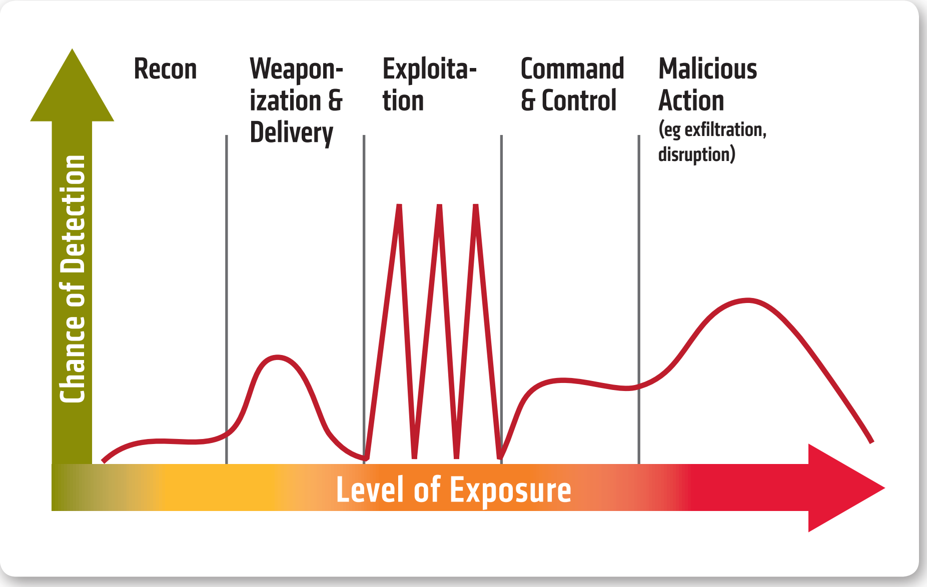

Fig. 1 The best chance to detect an attack before real damage occurs is in the "During" phase of the cyber kill chain because attackers leave digital fingerprints each time they make changes to host systems.

Traditional Security Approaches Are Not Effective

Cybercrime attacks and security breaches are top of mind amongst retailers, and there has been much discussion of the cyber kill chain. This heightened awareness has brought a new realization: traditional security, which is reliant on network- and signature-based solutions like malware protection, anti-virus and intrusion protection systems (IPS), is not enough. These solutions are key components, but leave security gaps that must be addressed on the endpoints and mission-critical servers. Retailers that incorporate endpoint security on servers and point of sale (POS) systems are better able to detect attacks earlier in the cyber kill chain, before significant damage occurs.

The Verizon Data Breach Investigation Report (DBIR) notes that 91% of intrusions involving POS systems take weeks to months to detect. This is particularly troubling from a retailer's standpoint, given that 99% of the time third parties—not the company that was breached—detect these intrusions. Clearly a new approach to threat detection and prevention is needed to enable retailers to protect their reputation and their customers' data.

How to Defend in Each Phase of the Cyber Kill Chain

Fortunately, by understanding each phase of the cyber kill chain, it is possible to identify methods and solutions that reduce the likelihood of a successful attack and its consequences.

Phase 1: Prevent – Before the Breach

In military parlance, this is the reconnaissance phase. Cyber attackers canvas and begin gathering information about system vulnerabilities, such as default or weak system passwords, out-of-date patches, incorrectly assigned ports, weak user access controls or any vulnerability that lets them gain access to a system.

Detecting the presence of a cyber-attacker in this phase is difficult because attackers leave little evidence or digital footprints of their activity, and have become skilled in camouflaging themselves as legitimate traffic and hence can go undetected by network intrusion prevention, firewall and anti-malware security products. A retailer's best defense is to make their systems unattractive targets for attackers by deploying critical preventive security controls and security configuration management. In addition, deploying enterprise-class vulnerability management and continuous monitoring will help identify security vulnerabilities in critical systems before a breach occurs. These controls can prevent breaches by securely configuring systems, and by ensuring the latest security patches have been installed. Most criminals will target an easy victim over a more challenging one; preventive controls make an organization a far less attractive target.

Phase 2: Detect – During the Breach

At this point, preventive security controls and measures have failed and the system has been breached. The attacker has infiltrated the network and is launching an attack payload designed to exploit a system vulnerability. This payload will allow the attacker to steal, or exfiltrate, sensitive customer financial and personal data. In some cases the attacker's objective may be to disrupt the retailer's business operations.

While this paints a bleak picture, this critical phase actually provides retailers an opportunity to detect a breach because in order to steal data or disrupt business operations, cyber attackers nearly always make changes to servers or other endpoint systems in the network. These system changes are the digital fingerprints of an attacker, and can, with the right security controls, be detected and help mitigate the risks before significant damage occurs.

Network intrusion prevention and detection systems can detect malicious network activity as it attempts to access the network, but, as stated earlier, attackers have become very good at making their activities look like legitimate network traffic. Malware detection solutions are best at detecting malicious traffic and payloads (which is good), but this means that the attacker has already accomplished some form of malicious activity and now the objective must turn to minimizing the loss.

Tripwire POS Threat Protection

Tripwire POS Threat Protection help retailers harden systems and detect the most commonly launched attacks on servers.

Tripwire POS Threat Protection:

- Delivers out-of-the-box breach detection rules that immediately detect changes to the most common server attack vectors—for example, local firewall configurations, scheduled and startup tasks, system services and drivers and local user accounts. Because these items should rarely change, it is important to be immediately alerted when they do.
- Detects and alerts for specific POS malware behavior like RAM scraping software, network sniffing from POS device to server, or POS application to payment application.
- Baselines your payment application configuration so if payment traffic changes to a bogus server you will be alerted.
- Monitors for encryption to be enabled, and alerts if not.

By adding security solutions that can detect host system changes in real time and determine if their legitimacy, retailers have a far more powerful defense. Ideally, multiple layers of security are used (e.g. strong network-based security and log intelligence solutions) to try and detect attackers as they enter and exit the network, and strong security controls on endpoints (especially mission-critical systems that store customer data and information) to detect suspicious activity that could be early indicators of a breach. This approach enables retailers the best opportunity to detect intrusions and minimize damage.

Phase 3: Respond – After the Breach

If not detected early on, a breach can continue for a long time. As the Verizon DBIR noted, many attacks go on for months or even years before detection. Malware protection solutions, which inspect emails and files to detect an illegal payload leaving the system, often fail to catch records being stolen. At some point, though, the attacker determines that they have stolen sufficient data or caused enough disruption, and do not want to risk getting caught.

Unfortunately, retailers that detect a breach at this point must now perform damage control with customers whose trust has been violated. They must also perform forensics (or root cause analysis) to identify what went wrong. That's when you need security solutions that maintain system activity logs and provide log intelligence and analytics.

How Tripwire Helps Reduce The Threat Gap

Tripwire offers industry-leading security and compliance solutions that fill important gaps in most retailers' security strategies, provide a set of critical components to a layered security approach and offer the best defense against cyber attacks.

Preventing a Breach in the First Place

Security control number 3 in the CSC (previously SANS) "Top 20" Critical Security Controls recommends hardening systems against attacks using security configuration management. Tripwire® Enterprise lets retailers initially deploy systems or assess and harden systems already in production with security configurations, making those systems less attractive targets for cyber criminals. For example, Tripwire Enterprise can detect a "bad" or unauthorized configuration change to POS systems in real time, and, based on predefined rules, either issue an alert or auto-remediate back to the desired "good" configuration state.

In addition, Tripwire IP360™ is a best-in-class enterprise vulnerability management solution that helps prevent attacks with device and software discovery, vulnerability identification and up-to-date coverage for the latest operating systems, applications and vulnerabilities. It even provides visibility into web application vulnerabilities.

Detecting Attacks as They Occur

Tripwire Enterprise, with its deep endpoint monitoring capability, can detect the presence of an attacker through real-time detection of the changes they make to host system configurations (including POS systems) in an attempt to exploit them. By combining Tripwire Enterprise's detected changes with security events identified in Tripwire Log Center®, retailers can even more definitively determine which changes and events correlate to indicate a true attack or breach in progress. Tripwire solutions detect attacks as they are being enacted, many times before a significant damage occurs.

Tripwire POS Threat Protection makes detecting potential breaches even easier by providing out-of-the-box breach detection rules to detect changes to the most common attack vectors. These rules and policies combine key configuration hardening standards with a collection of Tripwire-developed breach detection rules in a single, easy-to-install package. With Tripwire POS Threat Protection, retailers can take advantage of Tripwire's security research and expertise of attacks and malware to immediately protect their servers and other endpoints against the most common—yet disruptive—attacks.

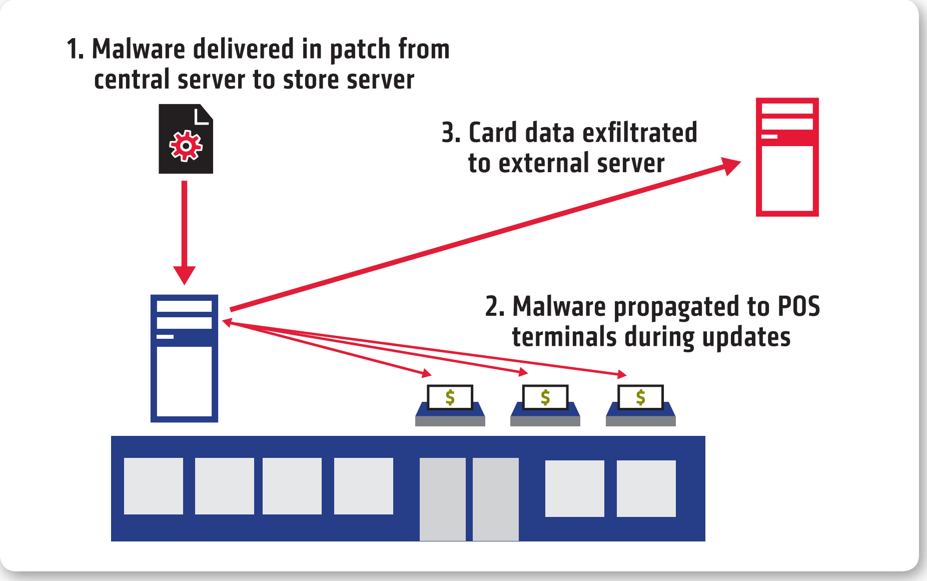
1. Malware delivered in patch from central server to store server
3. Card data exfiltrated to external server
2. Malware propagated to POS terminals during updates
$
$
$

Fig. 2 One of many possible methods to steal cardholder data from a retail environment.

Minimizing the Damage When an Attack Succeeds

Despite best efforts, attacks sometimes succeed. At this point, retailers need to minimize the damage to not only their systems, but customer trust. The best way to do this is to identify the root cause of the attack and harden it against future attacks. Tripwire Log Center provides the ideal solution for this, enabling real-time correlation and automation, security analytics and reporting and integration with existing SIEMs and security tools. Retailers can easily discover and find threat events while they are happening and analyze past events that led up to a breach to determine root cause

tripwire®

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook