THE TOP 5 Retail Point-of-Sale Cyberthreats

by Glen Jones, Visa Threat Intelligence

VISA

VISA THREAT INTELLIGENCE

THREATQUOTIENT™

THE TOP 5
Retail Point-of-Sale Cyberthreats

When the retail industry is hit with a cyberattack, it tends to be a high-profile event. Retail stores are household names and every individual, as a consumer, has the potential to be affected. Retailers are investing heavily in cybersecurity to protect payment card data and other personally identifiable information (PII). However, some of the most effective measures retailers can take to keep their brands out of the headlines are grounded in the adage: those who do not learn from history are doomed to repeat it. This is because cyber criminals reuse tactics, techniques and procedures (TTPs). In so doing, they leave a recognizable trail of breadcrumbs or indicators that provide insights into threats.

As the top five retail payment threats will show, security teams can use these indicators to their advantage. By understanding some of the most prominent breach trends and types of threats they face, retailers and other merchants can learn from history to mitigate risk sooner and even proactively prevent breaches.

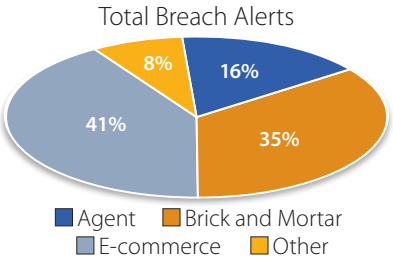
Global Breach Trends

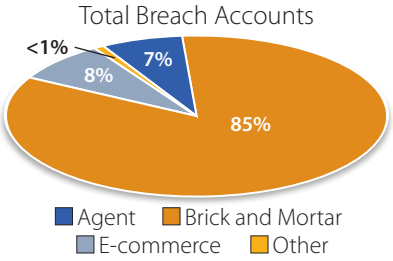
On an ongoing basis, Visa tracks global breach trends affecting retailers and other merchants. In 2017, research confirmed that the U.S. and Europe were the top two regions for payment data breaches. As Figure 1 shows, while more breaches occur at e-commerce merchants (41%), most of the leaked data (85%) comes from the largest (Level 1) brick and mortar entities. This points to two underlying trends. First, a rise in "card not present" attacks involving ecommerce merchants. And, second, although we are seeing fewer attacks against Level 1 merchants as they strengthen their defenses with Europay, Mastercard and Visa (EMV) chip technology and other secure payment technologies and techniques, like tokenization and application whitelisting at the Point of Sale, when attacks *do* happen they result in higher-impact breaches. Also, of note in 2017 is a substantial increase in breached "Agents" (banks, payment processors). But this doesn't mean merchants are out of the woods. This simply points to a shift in TTPs to be discussed later.

Looking at global breach trends by merchant type (Figure 2), restaurants, retailers, business-to-business (B2B) and lodging (hotels/hospitality) are the leading market segments in 2017. While breaches involving restaurants continued a downward trend, retail breaches continue to rise – with more than twice the number of companies affected since 2015. Another significant increase in B2B breaches over previous years is also indicative of a shift in TTPs targeting e-commerce merchants to be discussed.

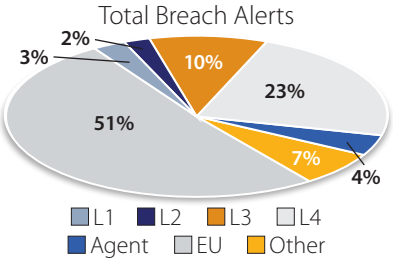
FIGURE 1. Global Threats by Channel and Entity Type

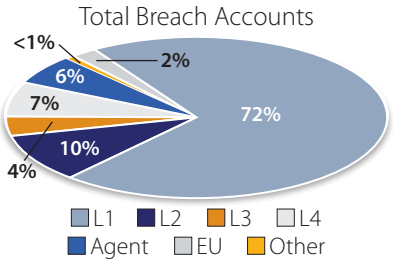
BY CHANNEL





BY ENTITY TYPE





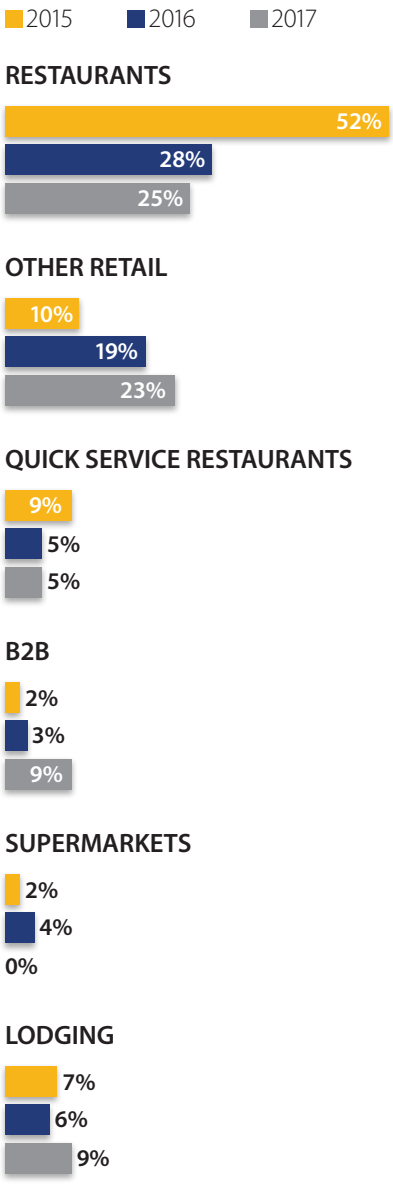
A Shift in Security Approach

Traditionally, the first sign of a cyberattack in the retail industry is fraud; a charge occurs that the cardholder did not authorize. Those affected would take steps to analyze and triangulate fraudulent charges in the hopes of identifying where the breach occurred. Once the source of the breach was identified, cleanup could begin. The problem with this approach to breach detection is that fraudulent payment card activity would often be delayed for several months (or longer) after the initial breach, a direct result of criminals deliberately withholding stolen data before selling it on underground markets. This approach served the industry well for some time but has become less reliable and effective on its own as the volume, velocity and complexity of attacks increases.

Today, leaders in the retail industry are taking a more proactive approach to cybersecurity to better protect their organizations. Threat actors reuse the same tactics – specific malware, targeted vulnerabilities and preferred infrastructure – to execute attacks across a wide range of merchants. So, security analysts are focusing on characteristics of previous attacks against the sector to determine what can be used as threat intelligence to detect attacks and mitigate risk sooner. And they are learning from the experience of others, as these indicators are shared across the industry to proactively strengthen defenses.

Analysis of the most common retail payment threats in 2017 shows the specific malware, targeted vulnerabilities and infrastructure that threat actors reuse. This information is extremely valuable as participants in the retail industry strive to protect payment card data and other PII.

FIGURE 2.
Global Breach Trends by Merchant Type



THE TOP 5
Retail Payment Threats

Visa continually monitors and analyzes threats across the retail and other industries to help merchants better understand how best to protect sensitive payment data from thieves who are constantly trying to get their hands on it. Looking back at what the payments industry faced in 2017 gives strong indications of what threats can be expected now and in the future. The following five retail payment cyberthreats were identified as the most common ones affecting retailers and can be expected to continue through 2018 and beyond.

5.

Cross-site "Land and Expand"

In this example, attackers set up a hierarchy of breached merchants for the purposes of furthering their attacks and masquerading their malicious activity to appear to be coming from legitimate websites and businesses. They then conduct reconnaissance and launch attacks on targeted merchants using another, legitimate merchant's infrastructure for command and control (C2) communication and data exfiltration. This makes it incredibly difficult to recognize malicious activity and suspicious network traffic within a Point-of-Sale (POS) environment. IP address and C2 servers appear to be legitimate at first glance, requiring heavy scrutiny to distinguish good from bad.

4.

BackOff/POSeidon

The typical targets for this attack group's attack campaign are small merchants with LogMeIn (LMI) connected to their POS vendor or integrator partners. Vendors use LogMeIn to gain remote access and genuinely maintain the environment for the merchant. In this scenario, the bad actor engages in widespread spear-phishing or a brute force compromise of remote access service credentials used by the victim's POS vendor or integrator. BackOff/POSeidon prefers LogMeIn, but will take advantage of any remote access service in use by the POS vendor. Once they obtain the POS vendor's credentials, they often have unrestricted access to the POS infrastructure for the merchants. They can install malicious bots, establish C2 communication over HTTP POST requests to relay information (BotIDs, Victim user name/host name, Windows version, malware version) and encrypt and exfiltrate payment card data. The group has been active since 2014 and continues to seek new victims and steal payment data.

3.

RawPOS

Hospitality and gaming companies are the typical targets for this threat. The threat actor compromises VPN credentials with single-factor authentication. They may also take advantage of Internet-exposed VPN password reset functionality, going through the password recovery step to establish their own VPN credentials. They compromise the Local Admin using Windows Credential Editor and then target the Active Directory Controller. They move laterally via Remote Desktop Protocol (RDP) and PsExec. The group is also known to hide their tracks using log clearing and remove malware using Sdelete so it cannot be discovered and analyzed. Because PsExec and Sdelete are legitimate tools, identifying this activity as suspicious is difficult. These bad actors have been known to lie dormant for months before launching a second breach, so thorough remediation the first time is essential.

2.

PUNCHTRACK

This threat primarily targets retail and hospitality companies. Using highly targeted phishing mails that are nearly imperceptible to discern from legitimate emails, they engage in rapid, wide-scale attacks targeting multiple merchants at the same time via a shotgun approach. They use the PUNCHBUGGY downloader to transmit malicious code through HTTPS and take advantage of zero-day or unknown flaws for credential takeover and privilege escalation. Once they reach their targeted systems they deploy custom-written, POS RAM-scraping malware to collect payment card data encoded on the magnetic stripe.

1.

Vulnerable E-commerce Payment Applications

Any type of merchant with an e-commerce website is a potential target for this top retail payment threat. Vulnerable e-commerce payment applications are the primary method threat actors use to steal payment card data throughout the payment ecosystem. They use bots to scan for Magento vulnerabilities (for example admin pages that are unprotected or unsecured file upload capabilities) and will also use the cross-site request forgery (CSRF) vulnerability which can result in a compromise of the payment application or the underlying web server itself. From there, they typically modify the checkout code and after successfully installing a malicious webshell, they introduce some malicious modifications that automatically capture and write card data to files on the web servers. The data is subsequently retrieved by the attacker. A "signature" image is often used in these attacks and IOCs are associated with this image.

While "card not present" data has a lower value on dark market websites than full magnetic stripe card data, between the combination of a wide number of targets and the efficiencies gained by using bots, bad actors will continue to use this method as they can reap an equal return over time. For the foreseeable future vulnerable payment applications will likely continue to be the number one target of payment data theft.

With an understanding of these top threats, retailers and other merchants can begin to look for indicators within their environments that can tip them off to an attack in progress or a vulnerability that makes them an attractive target. Appendix A provides an example of the Visa Threat Intelligence IOCs related to these threats, including network and host-based indicators, the threat actors represented and the attack phase associated with each.

Threat Preparation and Countermeasures

All retailers are subject to the Payment Card Industry Data Security Standard (PCI DSS) requirements. Implementing these controls across the environment prevent many attacks and go a long way to mitigating risk to card data. But leading retailers also engage in other activities to strengthen their defenses, including:

- **Operationalizing threat intelligence.** Subscribing to threat data feeds isn't enough. Organizations need a way to aggregate and de-duplicate all external and internal threat data, filter out the noise, assess and prioritize threat intelligence and use that threat intelligence to act – detecting and responding to threats faster. The faster a team can streamline their ability to import, enrich, deploy and make use of that information, the more pressure defenders are applying to the adversary which leads to offensive mistakes and oversights. Operationalizing threat intelligence also allows teams to learn from industry peers and their own past experiences to discover adversarial TTPs and proactively reassess and strengthen defenses to mitigate future attacks.
- **Application whitelisting** on POS systems. Knowing which applications POS systems are interacting with and limiting the list as much as possible.
- **Network egress monitoring** in cardholder data environments, including POS networks. Although this takes some effort, there are a number of tools available to help and incorporating threat intelligence into this process increases the ability to recognize suspicious activity and breach activity.
- **Secure payment technology** including EMV, tokenization and encryption. While not applicable to every merchant, the extra layer of point-to-point encryption has proven to protect payment card data despite an attack.

Conclusion

There is no end in sight to the relentless cyberattacks on the retail industry. However, there are ways to avoid the nightmare that all too often comes with a payment card breach. The retailers and merchants who are the most successful at managing threats and protecting their brands respond quickly to suspicious events. They have programs in place that include technology, people and processes to strengthen controls and effectively manage threats so that when an attack *does* happen they have the right threat intelligence to take the right actions fast to limit the impact.

ABOUT THE AUTHOR

Glen Jones is involved in initiatives centered on cyber threats to the Visa payment system, including fraud and risk product development, payment system cyber intelligence and emerging threat information sharing. In addition to overseeing the Visa Threat Intelligence product, he frequently advises financial institutions and merchants on cyber threats and payment card data protection. He has over 20 years' experience in corporate information security, cybercrime investigations, digital forensics, incident response and ethical hacking.

VISA

ABOUT VISA

Visa Inc. (NYSE: V) is a global payments technology company that connects consumers, businesses, financial institutions and governments in more than 200 countries and territories to fast, secure and reliable electronic payments. We operate one of the world's most advanced processing networks — VisaNet — that is capable of handling more than 65,000 transaction messages a second, with fraud protection for consumers and assured payment for merchants. Visa is not a bank and does not issue cards, extend credit or set rates and fees for consumers. Visa's innovations, however, enable its financial institution customers to offer consumers more choices: pay now with debit, ahead of time with prepaid or later with credit products. For more information, visit www.visathreatintelligence.com.

THREATQUOTIENT™

ABOUT THREATQUOTIENT

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system. For additional information, please visit threatq.com.

APPENDIX A
Top 5 Threats: Indicators of Compromise

Visa Threat Intelligence IOCs

Indicator	Description	Attack Phase	Attribution	Victim Types
Wendortales.ru	Backoff/POSeidon malware C2 domain	Command and Control	Backoff/ PoSeidon	Retail
82009e1c6df655d8b85dd0af503876c1	Remote access Trojan (RAT). Registry Settings: Software\Microsoft\ Windows\ CurrentVersion\Run	Command and Control	Backoff/ POSeidon	Retail
87c6fff744e2f7b7d332cff4a09a0b68	This file is RAM Scraping malware, which was saved to the desktop for user Microssupport.	Action on Objective	PwnPOS/ Backoff/ POSeidon	Other Retail
9ab1603f1b29724f391637cc7d82fe2d	RawPOS backdoor, used to communicate over port 3389. Part of RawPOS malware toolkit. Acts as tunneler and port forwarder for RawPOS to maintain control over compromised systems.	Command and Control	FIN5/RawPOS	Retail, Hospitality
62.210.112.158	IP addresses used by the attackers.	Command and Control	FIN5/RawPOS	Hospitality
52bdcf59b99101b611e9293fc6b675dc	BATCH script to uninstall and delete RawPOS malware trio from a target system(s)	Action on Objective	FIN5/RawPOS	Hospitality
931EEB5D9CEC9537EC232B24D3A89945	psv.exe is executed expecting 3 parameters: process to monitor for card data, time to scan for card data and process to inject.	Action on Objective	PowerSniff, PunchTrack POS malware family	Retail
magescripts.info	Exfiltration domain	Exfiltration	Linked with Magento attack campaign	Retail
fee3c3d1ee144cb1bc1fc0df62027d32	This remote file contained the exfiltration code.	Exfiltration	Linked with Magento attack campaign	Retail
f9785ab638185d86a663941b60fab62c	Payment card stealing Javascript code	Exploitation	Linked with Magento attack campaign	Retail