How Can a Breach Help Protect Your Company?

Visa Threat Intelligence
September 2016

In this age of ever-evolving technology, the threat of cyber attacks is an ongoing reality. No company is exempt from the threat, and in fact, many experts believe it's a matter of when, not if, a company will become the victim of a compromise. The repercussions of cyber attacks can be detrimental, and they extend far beyond financial ramifications.

For most organizations, undertaking a risk assessment to identify the biggest threats to the business and diverting resources to offset the risk is imperative. If your organization accepts electronic payments, imagining the consequences of a successful cyber attack is one of the most important parts of your protection strategy.

One of the first steps in assessing cyber risk is to ask:

1. Would a cyber attack against your organization cause you or your company great harm?
2. Are you prepared?
3. How can a successful payment system breach at another company help protect your company?

Most people will agree that the answer to the first question is yes. The answer to the second is likely, "I hope so." The third question can be confusing, and to answer it properly, you'll need to understand more about your market, the customers you serve, and the business outcomes your stakeholders are expecting. Security technologies have long played a critical role in defending against malicious behaviors, but even when fully implemented and integrated, these technologies may not have kept pace with the ever-evolving attack surface and threat landscape.

In the payment industry, attack surfaces are expanding in ways never before possible. Mobile apps, e-commerce, and supply-chain partnerships all introduce new vectors for exploitation. Plastic is no longer the only payment method, and even with the introduction of EMV, cybercrime is finding its way into corporate networks as criminals continue to seek bigger payouts.

So how can a breach help protect your company?

Imagine your company is your home, and houses on either side of you have been burglarized. Government agencies and law enforcement have performed their investigations and documented the manner in which the burglars targeted, planned and executed their invasion, and how they were able to steal personally identifiable information such as health records and bank account information, even though everything was safely locked away in a tamper-proof safe.

Now imagine there is a Neighborhood Watch that can securely share the results of the investigation with you and other concerned homeowners. You and your neighbors now have advanced insight and detailed, specific knowledge about how the burglars were successful, and exactly what to do to protect your home, your family, and your personal information from this type of intrusion. It's unfortunate your neighbors didn't have this level of advanced insight and actionable awareness before they were targeted.

The concept of the Neighborhood Watch that shares information to protect others is the premise behind **Visa Threat Intelligence, *powered* by FireEye®**. Visa has long been a leader in cyber intelligence for payment systems, providing a variety of protections to reduce fraud on every swipe, dip or tap of your payment card. Now, to address the changing payment threat landscape, Visa Threat Intelligence addresses the concerns of InfoSec and Security Operations, helping enterprises prevent fraud by preventing and detecting breaches long before fraud can occur.

What is Visa Threat Intelligence?

Visa Threat Intelligence (VTI) is a partnership between Visa and FireEye, two of the most trusted names in payment and cyber security. The two firms have teamed up to create a powerful tool to combat breaches. It leverages FireEye's expansive knowledge of the threat landscape with Visa's unmatched knowledge of the threats affecting the payment ecosystem to help prioritize and prepare for threats.

By working together, we are providing intelligence that enables:

- faster detection of and response times for payment threats
- up-to-date threat awareness for security teams, which reduces the likelihood of a breach
- less time spent chasing false positives and more time on actual threats

Visa and FireEye have combined forces to give subscribers access to a library of known payment system breach activities, arming companies with the who, what, where, why, and how behind payment-related cybercrime.

The intelligence included in VTI is curated from a variety of sources, including Visa's threat analysts, who use Visa's global network to identify the latest fraud and attacks targeting their end users, FireEye's 11 million sensors around the world detecting the latest attacks, and incident-response engagements on some of the largest breaches in the world.

Visa's Unique Visibility

Visa has broad visibility into how payment system breaches occur. Its role in protecting the payment ecosystem encompasses analysis of attacker tactics, root causes, indicators of compromise, and new and emerging threats to payment data across the entire spectrum of merchants. Visa is right there with the victims of cybercrime, from small brick-and-mortar restaurants to large retailers and e-commerce giants, showing them what to look for, where to look and how best to defend against aggressive cybercriminals who are determined to find ways to bypass traditional security measures.

Over the years, the threat landscape has changed dramatically from hackers targeting stored payment data in smash-and-grab-style attacks to the highly orchestrated network intrusions of today involving encryption, advanced data hiding and custom-written malware. One thing remains consistent through the years: there will always be threats to payment data as long as there is payment data worth stealing.

There has also been a transition in how stolen data is monetized by elaborate cybercriminal organizations that are relentless in their efforts to avoid being discovered. Within the past year, the mean time a breach goes unnoticed has decreased but is still measured in months, not weeks or days. Many of the merchant attacks Visa analyzes involve elements of stealth, obfuscation and anti-forensics. Hackers are deliberately covering their tracks throughout their attacks to throw incident responders off the trail.

They've also gotten smarter about fraud detection and what happens if they dump millions of stolen payment cards onto the black market at once, so they're holding on to data for longer periods of time before selling in order to limit their risk of exposure. This means it's no longer effective to rely on fraud alone as an early warning that your enterprise has been breached. There may not be any fraud at all to alert you to a data compromise.

Every time a merchant is breached, Visa learns a little more about what the bad guys are up to. Did they target a company IT admin in a spear-phishing campaign or hack into a business partner with access to the payment network? Did they use a RAM scraper to capture payment data? Did they use a tool from a known malware family or one custom-written for that compromise? What other tools and techniques did they use? Exactly how did the hackers bypass security controls at the merchant? How did they exfiltrate the card data from the merchant's systems? Visa is in a unique position to understand how breaches happen, what signs to look for and how to prepare for and protect against them.

Payment Ecosystem Indicators of Compromise (IOCs)

Few things are more valuable to a merchant information security team than the detailed knowledge of how an attack against their point-of-sale network would appear. Monitoring systems for signs of attack, however, is only as effective as the signs being watched. The most effective ones are vetted, verified and updated as soon as the threats change. Knowing where the attackers will likely come from, which tools they'll use to compromise the network and how to spot signs of payment data exfiltration are all invaluable pieces of information in preventing a breach. Visa Threat Intelligence members have this information and can use it to target their defenses to threats actually observed in their line of business, avoiding the false positives that often occur with unverified threat intelligence.

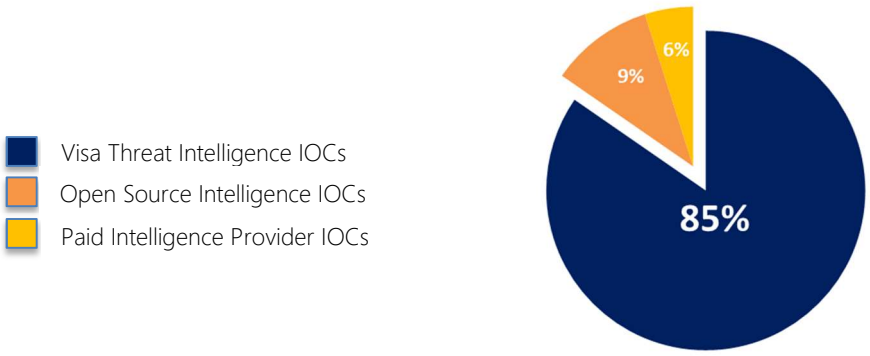
IOCs are a critical element in preparing for the inevitable attack while also assessing whether you've already experienced a breach. Visa's goal is to keep its customers more secure by detecting breaches earlier (or preventing breaches altogether), minimizing fraud and reducing the cost associated with remediation and clean-up. Because of our unique role in the payment ecosystem, Visa sees signs of nefarious activity months ahead of the reported fraud. As a Visa Threat Intelligence member, your organization can take a more proactive approach to anticipating threats and protect itself by using Visa's insight and actionable IOCs to understand what a successful breach looks like and how to spot one in your environment.

Visa Threat Intelligence IOCs are obtained from confirmed breaches across the payment ecosystem. When investigators begin their work examining a digital crime scene to learn how payment data was accessed, forensic artifacts are uncovered. No hacker can remove all evidence of their attack; they all leave traces. Those traces—the source of the attack, malware and other tools used, remote systems where payment card data was leaked—all play a powerful role in breach prevention if used correctly. They take the form of IP addresses, domain names, cryptographic file hashes, and URLs identified during the investigation. These IOCs represent the best way to detect an ongoing or future attack. Truly adaptive security needs to be intelligent, flexible and based upon relevant intelligence. When a retailer is victimized by the latest sophisticated attack campaign, there's no more relevant intelligence than the forensic details of the attack.

Differentiated Intelligence

Plenty of security solutions are designed to recognize and stop attacks. Add to that the wide array of commercial threat intelligence offerings, which all promise to detect and/or prevent breaches. There's a strong temptation to deploy one or many of these solutions and believe your problems to be solved. However, Visa's ongoing investigations have revealed that merchants relying on one silver bullet security control or questionable threat intelligence are not immune to breaches. Only after they're victimized do many of them engage in a critical examination of their intelligence and then learn that it failed them and gave them a false sense of security. Visa Threat Intelligence was developed out of the need to provide focus on what is relevant for payment security and to avoid meaningless noise and intelligence overload.

85% of forensic indicators are *exclusive* to Visa Threat Intelligence*



*Source: Visa. Based on a sample of Visa Threat Intelligence Indicators compared against four commercial threat intelligence sources/vendors (2016).

While many other intelligence providers focus on putting out volumes of generic data, Visa recognizes generic indicators and unverified threat intelligence have little effectiveness in actually protecting payments. Visa's intelligence is targeted, focused on specific threats to the payment ecosystem, and highly actionable to shorten the time and effort required to put it to work protecting your organization. Visa Threat Intelligence IOCs are a critical layer in existing security defenses due to Visa's unique position in understanding threats and their impact on the payment ecosystem. In fact, 85% of the IOCs in Visa Threat Intelligence are unique and not found in other open or paid threat intelligence sources. Combined with FireEye's unmatched insight into threat actors, their tactics and techniques, VTI is an invaluable tool in an age of unrelenting cyber attacks.

For More Information

If you have questions, please reach out to us:

Email visathreatintelligence@visa.com

Website Visathreatintelligence.com