How Can a Breach Help Protect Your Company?

VISA THREAT INTELLIGENCE

THE INITIAL STEPS IN ASSESSING CYBER-RISK ARE TO ASK:

1. Would a cyber-attack against your organization harm your reputation?

2. Are you prepared?

3. Would knowledge of a successful breach at another company help you detect and prevent the next attack on your company?

In this age of ever-evolving technology, cyber-attacks are a constant threat. No company is exempt, and 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. If your organization accepts or processes electronic payments, understanding the consequences of a cyber-attack is vital to your protection strategy.

In the payment industry, attack surfaces are expanding in ways never before possible. Mobile apps, e-commerce, and supply-chain partnerships have introduced 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 your neighbor was recently burglarized. Law enforcement and government agencies have performed their investigations and documented the manner in which the burglars were able to steal health records and bank account information, despite everything being locked away in a tamper-proof safe.

Now imagine a Neighborhood Watch that can securely share the results of the investigation with you and other concerned homeowners. You now have advanced insight and detailed 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.

The concept of the Neighborhood Watch is the premise behind Visa Threat Intelligence. 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 evolving payment threat landscape, Visa Threat Intelligence is addressing the concerns of Cyber Security Operations, helping enterprises prevent fraud by detecting and preventing a breach before fraud can occur.

What is Visa Threat Intelligence?

Visa Threat Intelligence (VTI) is a powerful tool to combat payment-related breaches. It uses Visa's extensive knowledge of the threats affecting the payment ecosystem to help prioritize and prepare for threats.

VTI provides actionable, differentiated indicators of compromise with contextual information, sourced from investigations of breaches targeting payment data. This essential intelligence enables:

- Faster detection of and response times for payment related cyber threats
- Less time spent chasing false positives and more time on actual threats

VTI also offers subscribers access to a library of known payment system breach data, arming companies with Tools, Tactics, and Procedures (TTPs) behind payment-related cybercrime.

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 cyber-crime – 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.

There will always be threats to payment data as long as there is payment data worth stealing. Over the years, Visa has seen the threat landscape change 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.

> “
> **Many of the merchant attacks Visa analyzes involve elements of stealth, obfuscation and anti-forensics.**

There has also been a transition in how stolen data is monetized by elaborate cyber-criminal organizations that are relentless in their efforts to avoid being discovered. Many of the merchant attacks Visa analyzes involve elements of stealth, obfuscation and anti-forensics, and the mean time a breach goes unnoticed is still measured in months, not weeks or days. Hackers are deliberately covering their tracks throughout their attacks to throw incident responders off the trail. Criminals have gotten smarter about fraud detection. Rather than dumping millions of stolen payment cards onto the black market at once, 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's global payment network and oversight allow us to capture and curate this intelligence, and to use it to undertand how breaches happen, what signs to look for, and how to prepare for and protect against them.

Payment Ecosystem Indicators of Compromise

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 clients have access to 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.

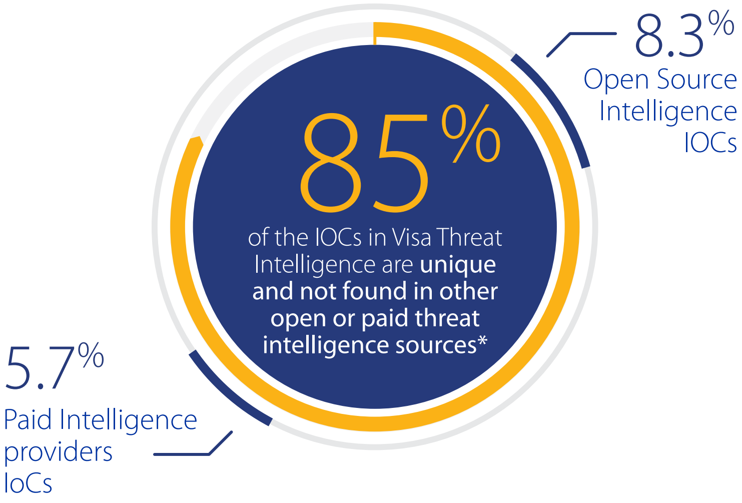
IoCs are a critical element in preparing for the inevitable attack, as well as assessing whether you've already experienced a breach. Visa's goal is to keep its customers more secure by detecting breaches earlier (or preventing breaches altogether), minimizing fraud, and reducing the cost associated with remediation and clean-up. Because of our prominent 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 examine 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

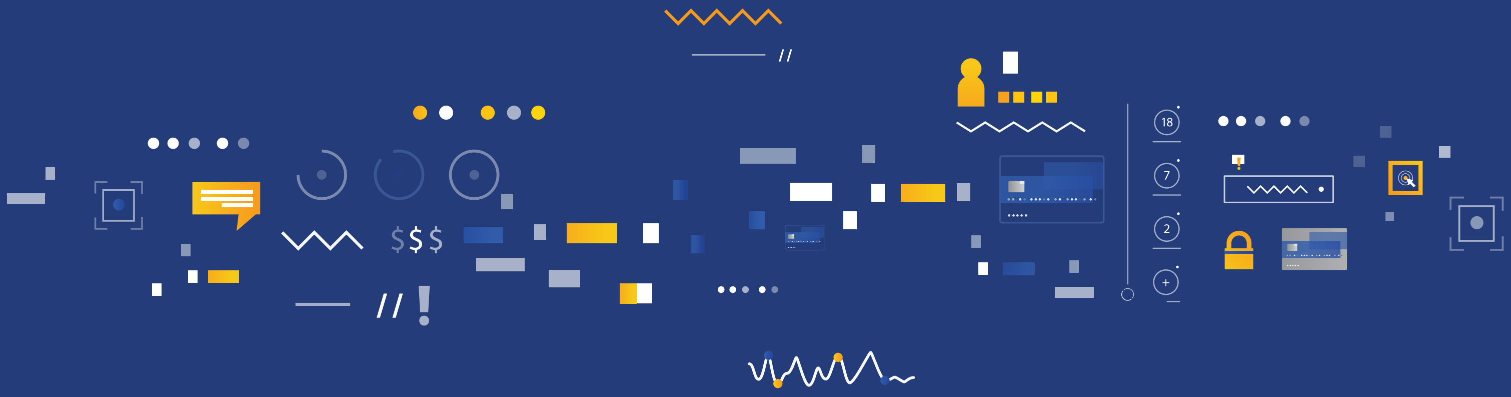
Plenty of security solutions are designed to recognize and stop attacks. Add to that the wide array of commercial threat intelligence offerings, which all promise to detect and/or prevent breaches. There's a strong temptation to deploy one or many of these solutions and believe your problems to be solved. However, Visa's ongoing investigations have revealed that merchants relying on one "silver bullet" security control or undifferentiated 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.

Forensic indicators



85% of the IOCs in Visa Threat Intelligence are **unique and not found in other open or paid threat intelligence sources***

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



For More Information

To learn more about how effective cyber threat intelligence can reduce your risk of fraud, or to view sample Visa Threat Intelligence IoCs, visit us online:

Email: visathreatintelligence@visa.com
Website: Visathreatintelligence.com

VISA