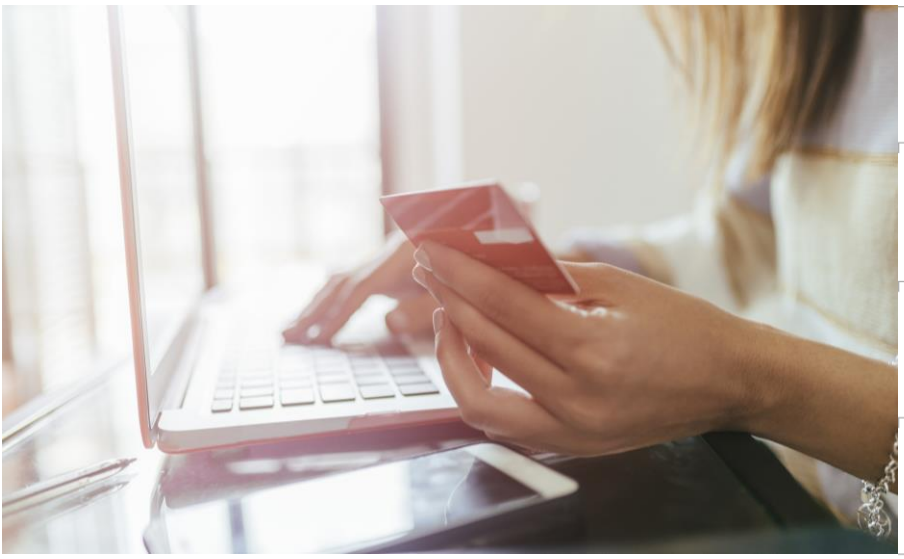
Detecting compromised eCommerce merchants and disrupting fraud

Case Study – Restaurant & Online Ordering Service Provider



- Proactive fraud detection; no waiting for fraud reports
- Utilizes patent-pending technology and investigation techniques
- Disrupts eCommerce compromises early
- Merchants that accept Visa automatically opted-in for free

Visa's eCommerce Threat Disruption (eTD) was able to quickly identify a widespread online service provider compromise and, in the process, potentially **save as much as $141 million.**

About eTD

Visa's eCommerce Threat Disruption uses patent-pending technology and investigation techniques to proactively identify compromises in the eCommerce environment. By analyzing merchant websites for malicious payment-data-skimming malware, Visa is able to identify a potential compromise and provide guidance on how to remove the malware, thereby limiting the amount of time a merchant is compromised and the window of exposure where payment data is at risk.

Case Study Background

Visa's Payment Fraud Disruption team received a tip from an issuer identifying a potential compromise of one local restaurant's online ordering system. Using Visa's eTD detection capability, Visa found payment-data-skimming malware hidden in a legitimate file hosted by the restaurant's online ordering service provider—not on the restaurant's own website. The Payment Fraud Disruption team promptly began searching for other merchants using the same ordering service provider, and found that the infected file was shared across many of the service's 1,500+ customers.

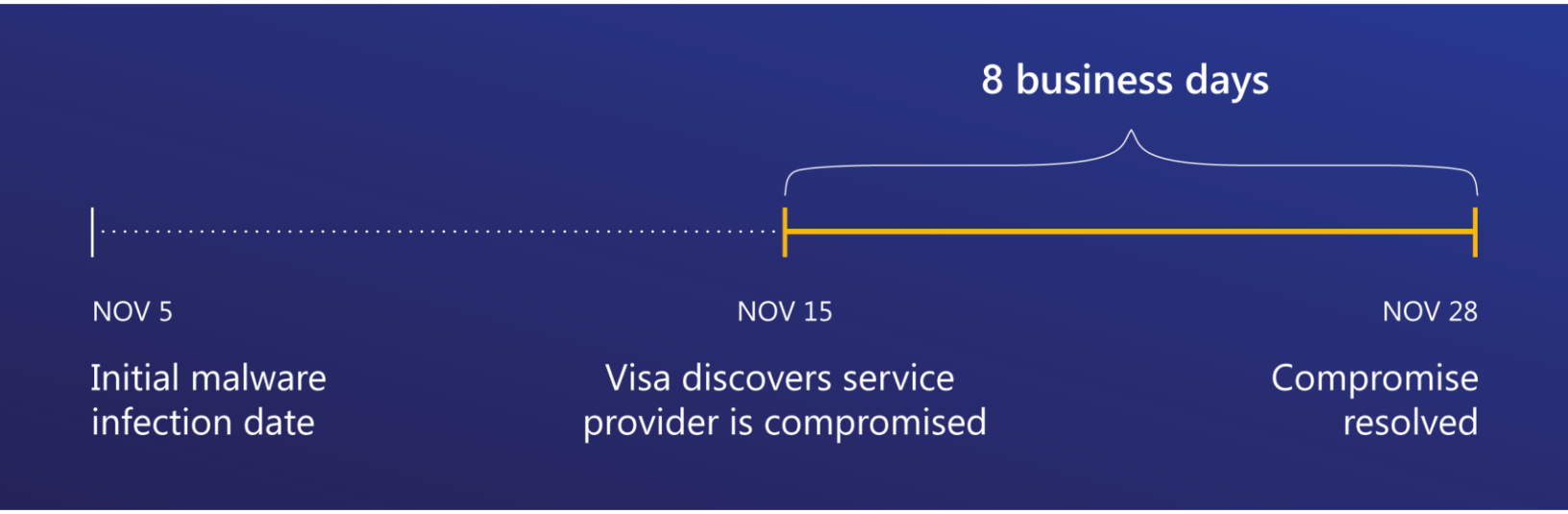
Results

Visa's eTD capability was pivotal in tracking down the source of the compromise. Because of this capability, Visa was able to identify the broader nature of the threat beyond the fraud tied back to a single merchant. Before this advance, only a single individual restaurant would have been investigated and remediated, and the malware infection on the service provider's system (and subsequent fraud) would have continued until enough evidence could be gathered to identify the actual source of compromise.

One-third of the service provider's 1,500+ customers were found to also be compromised by the malware-infected file, and Visa effectively prevented the remaining two-thirds serviced by this provider from being compromised as well.

Additionally, unlike a normal compromise investigation, Visa was able to enhance its reporting with direct evidence of malware, including the exact file and location that was infected. Because of Visa's highly actionable intelligence, the service provider was able to quickly identify the malware, clean the infection, and lock down the system to prevent reinfection. The compromise was fully remediated in just 8 business days—the time that it typically takes to hire a PCI Forensics Investigation (PFI) company.

eTD discovered the source of the compromise only 10 days after the initial malware infection and the total window of exposure was limited to just 23 days. Because of Visa's eTD capability and the quick response of Visa's Payment Fraud Disruption team, Visa potentially saved the infected merchants as much as $141 million.



Contact paymentintelligence@visa.com to learn more about eTD.

