Payment Systems Intelligence – Security Bulletin JANUARY 2018

PROTECT AGAINST ECOMMERCE MALWARE

Distribution: Visa Issuers, Acquirers, Processors, and Merchants

Summary

eCommerce malware infections are a continued contributor to global fraud in the Card-Not-Present space.

To help merchants combat fraud resulting from these global and persistent attacks, Visa is providing guidance and best practices for merchants to help secure their online stores.

Defining eCommerce Malware

eCommerce malware is generally malicious code that targets the eCommerce website itself. It does not intend to infect users who visit an eCommerce website.

The malware is best likened to an online payment data skimmer—similar to physical skimming, card data and personal information are stolen to be used illegally or sold. It can be an appealing and lucrative endeavor for criminals. Compared to physical skimming, online skimming affords criminals a degree of physical separation from a compromise and can be more difficult to identify due to the lack of any physical presence. In general, these malware infections are unsophisticated, hidden in plain sight, and persistent. Because of these factors, merchants need to be especially vigilant to eCommerce malware attacks.

How eCommerce Malware Works

Skimming malware can be hosted two ways: remotely and locally.

- Locally-hosted malware means that the malware has been placed into a merchant's website code directly
- Remotely-hosted malware lives in a separate malicious domain and is loaded by the merchant's website

In both of these cases, the attacker must gain access to the eCommerce site's server to place their skimming code.

Criminals gain access to an eCommerce site using a variety of methods, most commonly by using stolen or guessed administrator credentials for the website. Other methods include exploiting out-of-date software that contains unpatched vulnerabilities, software that does not provide adequate security, or insecure web server settings.

Regardless of how the attackers compromise the eCommerce environment, the next step remains the same: they place their skimming code to begin stealing cardholder data during customer checkout. Under control of an attacker, a (JavaScript) wiretap is installed that funnels live payment data to the criminal's collection server, or command and control domain. This funneling of data operates transparently and undetected for both the customer and the merchant.

Recommendations for Preventing Compromises

Knowledge and vigilance can help ensure that breaches to merchant eCommerce sites do not occur.
To reduce risk further, merchants should:

- Regularly scan and test eCommerce sites for vulnerabilities or malware. Hire a trusted professional or service provider with a reputation of security to secure the eCommerce environment. Ask questions and require a report of what was done—trust, but verify the steps taken by the company you hire
- Consider using a fully-hosted checkout solution where customers enter their payment details on another webpage hosted by that checkout solution, separate from the merchant's site. This is the most secure way to protect the merchant and their customers from eCommerce skimming malware. Hosted checkout forms embedded inline on the merchant's checkout page, such as Visa Checkout, are another secure option
- Use a Payment Card Industry Data Security Standard validated third-party service provider to store, process or transmit cardholder data. Criminals commonly target merchant websites that process payment data. When merchants use a validated and secure service provider, risk exposure for CNP fraud and compromise decreases. A list of validated, registered service providers is available on the Global Registry of Service Providers.
- Comply consistently with industry security standards such as the Payment Card Industry Data Security Standard (PCI DSS)
- Set up a Web Application Firewall to block suspicious and malicious requests from reaching the website—there are options that are free, simple to use, and practical for small merchants
- Limit access to the administrative portal and accounts to those who need them
- Require strong administrative passwords (use a password manager for best results) and enable two-factor authentication
- Regularly ensure shopping cart, other services, and all software are upgraded or patched to the latest versions to keep attackers out
- Monitor for suspicious activity—regularly check logs and receive alerts if changes to the site are made
- Ensure staff are trained in security best practices and follow the designated procedures

If a merchant suspects a compromise, they should contact their acquiring bank immediately for guidance on next steps and to ensure compliance with all Visa investigation and compliance guidelines.

Additional Resources

Visa eCommerce Malware Webinar - usa.visa.com/dam/VCOM/global/support-legal/documents/emerging-threat-card-not-present-breaches-webinar.pdf

Visa Merchant Library - usa.visa.com/support/merchant/library.html

PCI Best Practices for Securing e-Commerce, January 2017 - www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

PCI How-to Guide for Incident Management - www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

PCI Data Security Standard - www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

For more information, please contact, paymentintelligence@visa.com.