Visa Security Alert

AUGUST 2019

eCommerce JavaScript Skimming Campaign Targeting Service Providers

Distribution: Public

Summary

Since April 2019, there have been reports of JavaScript skimming attacks against eCommerce service providers. In this activity, the attackers inject malicious JavaScript code into the websites of merchants and service providers to harvest payment information, such as billing address, account number, expiration date, and CVV2 from the checkout forms on eCommerce pages. These skimming campaigns, especially against service providers, are ubiquitous and pose a larger threat than initially believed.

Criminals are increasingly targeting service providers that supply solutions such as analytics code, advertising integrations, mobile application video advertisements, general IT-based services, etc. to various eCommerce merchants, as a means to compromise the merchant website. In April 2019, at least eight web-based service providers were targeted with JavaScript skimming attacks. The attackers compromised the content delivery network (CDN) implementation for these service providers and modified JavaScript files hosted on the CDN. The malicious code within these modified files was then integrated into the eCommerce environments of merchants using the service provider's solutions. This enabled the attackers to harvest payment details from any eCommerce website that utilized the code of the compromised provider on their checkout pages, effectively compromising numerous eCommerce merchants with one successful code inject. Visa Payment Fraud Disruption (PFD) also found the **same malware and the same infrastructure** for data exfiltration used across all eight cases.

In July 2019, researchers reported that these service provider attacks were much more significant than initially believed and affected over 17,000 domains that integrated code from the service providers targeted in April. The attacks were reportedly successful due to an automated process whereby the attackers scanned for misconfigured write permissions in a widely-used CDN.

Service Providers Targeted under Multiple CDNs

Visa's eCommerce Threat Disruption (eTD) program conducted independent analysis on these service provider attacks and found that **the targeted service providers hosted code on at least two different CDNs**. The attacks occurred via two methods depending on the CDN that was utilized by the service provider. In the first method, which targeted service providers hosting legitimate code on one specific CDN, the attackers exploited misconfigurations in the service provider's implementation of the CDN, which enabled the attackers to write malicious code into the hosted service provider files. In the second method, which targeted service providers hosting on another CDN, the attackers likely compromised credentials for the service provider's CDN implementation and subsequently injected malicious code into the hosted files. There was no evident

misconfiguration in the CDN implementation targeted in the second method. The same malicious payload, *Inter*, was used in both methods.

PFD assesses that cybercriminals are actively seeking to target service providers hosting code on CDNs that is integrated into eCommerce environments for the purpose of compromising payment account information, regardless of the specific CDN that is being leveraged by the service provider. The recent attacks highlight the necessity for service providers to properly configure CDN solutions and adequately secure access to and implementation of their services. In addition to this, it is also crucial that eCommerce merchants utilizing third-party service providers closely vet these providers and ensure familiarity with the code being integrated into their environment.

'Inter' Malware

PFD attributed the JavaScript skimming attacks targeting the eight service providers that utilized at least two CDNs in April 2019 to the customizable *Inter* digital skimming kit. It should be noted that *Inter* is widely available on the underground and that the use of the malware in the recent service provider attacks does not necessarily indicate that the malware creators perpetrated the attacks. The *Inter* skimmer observed in the attacks targets all form fields, such as input, select, and text area on an eCommerce website and stores the harvested data by creating a data dictionary of the information included in the website forms. The code then checks potential payment account numbers within these forms against the Luhn algorithm and configured regular expressions. If the data passes this check, an "IsValid" flag is included to indicate valid payment account data is present. No data is exfiltrated unless the "IsValid" flag is set to 'true'.

In the service provider attacks observed in April 2019, PFD found that the data exfiltrates as a base64 encoded JavaScript Object Notation (JSON) object, is sent as an image GET request, and exfiltrates to a configurable filename, '/img'. *Inter* logs a hash of each dataset sent to the exfiltration server in memory to avoid sending duplicate data in a single session. *Inter* also uses the ubiquitous JavaScript Obfuscator tool to avoid detection and make analysis more difficult.

Researchers attributed the following Command and Control servers (C2s) to the *Inter* skimming kit:

C2s	Tracker-visitors[.]com Jquery-web[.]com Jquery-stats[.]com jsreload[.]pw routingzen[.]com
Notes	Inter Skimming Kit

While PFD did not directly observe the above *Inter* C2s in the activity targeting the service providers, the following C2s were identified in the service provider attacks attributed to *Inter*:

C2s	font-assets[.]com/img cdn-c[.]com/img ww1-filecloud[.]com/img
Notes	Inter Skimming Kit (Service Providers)

Mitigation

eTD continues to monitor, investigate and analyze the numerous and varied threats to eCommerce and is well positioned to identify, mitigate, and prevent infections resulting from eCommerce malware such as *Inter*. Visa recommends the following best practices to reduce the risk of exposure:

- **Institute recurring checks in eCommerce environments** for communications with the C2s provided in this report.
- **Ensure familiarity and vigilance with code integrated into eCommerce environments** via service providers.
- **Closely vet utilized Content Delivery Networks (CDN),** and ensure CDN implementations are secure.
- **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.
- **Regularly ensure shopping cart, other services, and all software are upgraded or patched** to the latest versions to keep attackers out. 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.
- **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.
- **Implement Best Practices for Securing eCommerce** as outlined by the **PCI Security Standards Council.**
- **Refer to Visa's What to do if Compromised (WTDIC) document,** published August 2016.

Contact Information

For more information, please contact paymentintelligence@visa.com