APRIL 2021

THREAT ACTORS INCREASINGLY USE WEB SHELLS IN ESKIMMING CAMPAIGNS

1. Summary

The ongoing COVID-19 pandemic has had a profound impact on the payments ecosystem threat landscape throughout 2020 and into 2021. While restrictions on in-person commerce were implemented globally, consumers increasingly utilized eCommerce channels. As a result, eSkimming, or digital skimming, is among the top threats to the payments ecosystem. eSkimming attacks involve the injection of malicious code into a merchant's eCommerce environment to harvest payment account numbers that are entered into the checkout pages of the targeted merchants.

Throughout 2020, Visa Payment Fraud Disruption (PFD) identified a trend whereby many eSkimming attacks used web shells to establish a command and control (C2) during the attacks. Web shells are tools used by threat actors to establish and maintain access to compromised servers, deploy additional malicious files/payloads, facilitate lateral movement within a victims network, and remotely execute commands. Actors employ numerous methods to deploy web shells, but often use application plugins and PHP code.

PFD confirmed at least 45 eSkimming attacks in 2020 using web shells, and security researchers similarly noted increasing web shell use across the wider information security threat landscape. Given this trend, PFD is providing an overview on recent findings from investigations, suggested mitigations, and further information regarding exploited vulnerabilities in these attacks. Visa recommends that acquirers and ecommerce merchants, as well as onboarding and security partners, use this information to form a plan to identify and mitigate the common vulnerabilities exploited by attackers to gain access and deploy eSkimmers to obtain the payment data from targeted merchants. Identifying tactics, such as the use of web shells, also assists in identifying compromises when eSkimmers are not detected on the merchant website.

2. Web Shells in eCommerce Attacks

The majority of the investigated attacks utilized web shells to establish persistent backdoor access to the victim's network and create a C2 infrastructure to facilitate the transfer of data and communications between attacker-controlled assets and the victim's environment. The actors used various tactics to gain initial access to the victim's network, the most common of which are:

a) Vulnerabilities in unsecured administrative infrastructure

In one incident, the merchant's administrative database credentials were stored in clear text and hardcoded into database-related PHP files. This provided the actors with relatively easy access to the credentials necessary to deploy the web shells and gain root access to the database and web servers.

In another incident, the merchant utilized a jump box to deploy code changes to the eCommerce environment. The administrative credentials for this jump box were compromised through unidentified means and subsequently used to deploy malicious code. Moreover, targeted merchants often employed weak, easy to guess passwords for administration panels, which were easily cracked by the threat actors and used to gain access to the network.

b) eCommerce-related application/website plugins

Another common tactic used by threat actors is the use of plugins that integrate with the eCommerce environment. For example, in one incident, actors modified the code of a legitimate file related to a plugin for the content management system that was used to build the merchant's website. The modifications injected malicious code into this plugin that provided the actors with administrative privileges to the eCommerce environment. In another incident, actors exploited a vulnerability in a plugin that was integrated into the merchant's website via a third-party service provider. PFD previously reported on the use of merchant service providers to facilitate eSkimming attacks.

c) Outdated/unpatched eCommerce platforms

In many cases, the merchants were running outdated or unpatched eCommerce platforms. PFD recently warned of the dangers of using outdated, end-of-life or unpatched technologies within an eCommerce environment, especially as Magento Version 1 reached its end-of-life in the summer of 2020. Merchants that continued to run this platform were targeted with eSkimming attacks that exploited unpatched vulnerabilities stemming from the end-of-life.

3. Identifying Web Shells and Mitigating the Threat

While the above tactics, techniques and procedures are not an exhaustive list of the various methods and exploits that attackers used in these web shell attacks, they are some of the leading methodologies identified. The use of web shells to facilitate eSkimming attacks will likely persist, especially as the restrictions around in-person, brick-and-mortar commerce remain in place as the pandemic continues. As such, **Visa recommends that acquirers and merchants:**

- **Ensure familiarity and vigilance with code integrated** into eCommerce environments via service providers by reviewing and validating the code and updates, and closely vet utilized Content Delivery Networks (CDN) and other third-party resources.
- **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 portals** and accounts to those who need them.
- **Ensure administrative panels and other privileged accesses are properly secured** and not publicly accessible.
- **Require strong administrative passwords** (use a password manager for best results) and enable two-factor authentication.

- **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 thorough report. Trust, but verify the steps taken by the company you hire.
- **Log eCommerce environment network activity** and regularly review for unusual, suspicious activity.
- **Implement network segmentation** to prevent threat actor movement and ensure the cardholder data environment (CDE) is sufficiently protected.
- **Log network and web server activity,** and regularly review and audit these logs for unusual and suspicious activity.
- **Use a secure and PCI compliant hosting provider.**
- **Ensure familiarity with third-party integrations and services** utilized in an eCommerce environment, and a comprehensive understanding of direct internet exposure.
- **Refer to the Best Practices** as stated in Visa's 'Website Security for Ecommerce Merchants' document, September 2020.
- **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 October 2019.

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

For Visa Europe region requirements and questions please contact **datacompromise@visa.com**