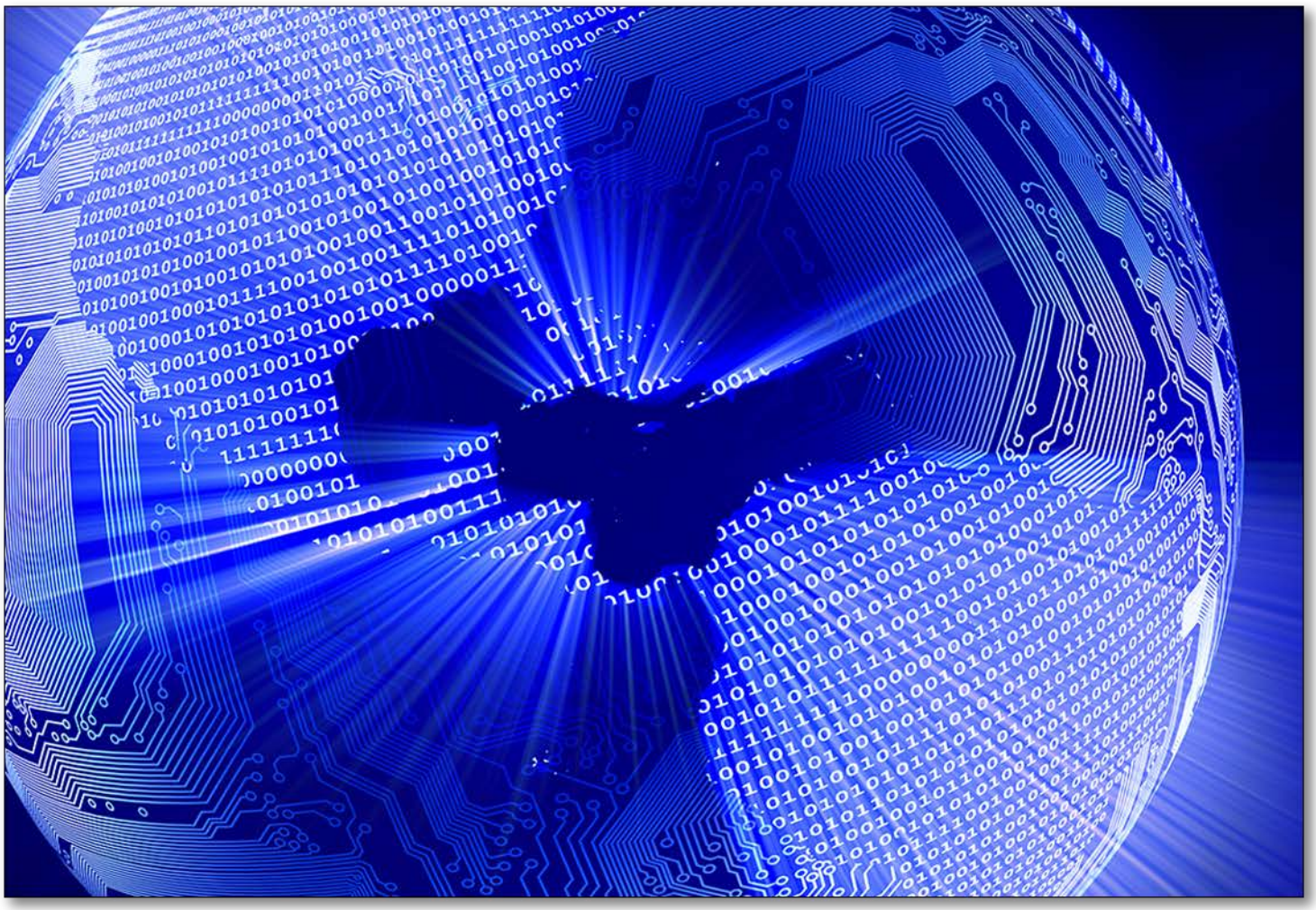
Mastercard Fusion Center

Security Bulletin

SUBJECT:	**E-Commerce Sites Targeted by MageCart Digital Skimming**
REPORT ID:	MFSIB-15-101818
ISSUED:	November 15, 2018



For Additional Information Please Contact:

Fusion.Center@Mastercard.com

Bottom Line

As highlighted in recent publicized events and a recent Mastercard case attribution, the Magecart attack technique has impacted multiple third-party suppliers as well as several high-profile e-commerce sites including a major international airline and a popular tech-focused retailer. For those unaware, "Magecart" is an umbrella term used to describe malicious attack groups who insert digital skimmers into the checkout page of e-commerce merchants to extract cardholder data and PII (Personally Identifiable Information). The respective groups are using various injection points on Magento e-commerce platforms.

Threat Overview

- Initial Magecart attacks dating back to 2015 were focused on small e-commerce merchants that primarily used the Magento e-commerce platform but has since expanded to third-party service providers (using platform extensions and plugins, chatbots/AI, marketing analytics) and larger merchants.
- Recent attacks have involved newly developed and varied methods to inject the digital skimmers into the checkout process, which fraudulently captures consumer PII and credit card data.
- Threat groups continue to identify targets susceptible to initial compromise, usually through a brute-force method of the administrative console on the CMS (Content Management System). Susceptibility is not limited to only these methods and can be highly targeted towards large merchants and/or third-party service providers through hub-and-spoke configurations.
- According to the research firm FireEye, several ongoing campaigns have been identified and the number of impacted companies is likely to grow due to increased reporting, increased cybercriminal interest in compromising e-commerce websites and the increased amount of vulnerable e-commerce sites.
- E-commerce sites who fail to maintain PCI DSS compliance in regards to timely patching, tracking additions/deletions/modifications to code tied to payment processing, appropriate logging and alerts and use of secure authentication protocols for local and remote access are at risk of attack.
- Magecart attack statistics for the last six months:
    - Over 7,000 Magento e-commerce sites infected (reported by Bleeping Computer)
    - Several hundred Feedify javascripts infected (reported by ZDNet)

Assessment

Magecart and other digital-skimming campaigns highlight the growing threat to the e-commerce industry. Digital-skimming operations have proven to be highly successful and have recently received significant media attention that may entice additional threat actors to conduct similar campaigns. They also provide an attractive alternative to POS malware operations, which have become more difficult with the implementation of EMV chip technology. Consequently, Mastercard anticipates cybercriminal operations targeting e-commerce sites and platforms will continue to grow for the foreseeable future.

Recommendations

To prevent a Magecart attack, merchants and third-party entities should follow the requirements put forward by PCI DSS or start using enhanced, validated payment technologies which are PCI approved and use validated cryptographic payment protections. Patching systems and maintaining appropriate logging, file integrity monitoring, multiple factor authentication and threat scanning are essential first steps to guarding against Magecart attacks. Enhanced payment technologies do not guarantee the elimination of an attack, but minimize the risk and/or impact to payment card data.

To identify whether a merchant or third-party entity using Magento has the latest patching there are external scans that can be performed for quick validations. Note: these scans are not always accurate due to different configuration put in place by merchants and/or their third-party entity. Once the scans are run and vulnerabilities are identified, then the merchant or their third-party entity should apply the prescribed patch or fix to mitigate the threat posed by the vulnerability in a timely fashion.

1. Magento's Security Scan Tool: https://magento.com/security/best-practices/detect-malware-new-discovery-rules
2. Hypernode: https://support.hypernode.com/knowledgebase/recover-a-hacked-magento-shop/

If other e-commerce platforms are used, similar patch notification should be available for merchants and their third-party entities to apply patches within an appropriate time frame.

If an entity believes they have been impacted leading to an account data compromise event where cardholder data is potentially impacted, the following actions should be taken:

1. Report the event to the acquirer of record. The acquirer should then report the potential account data compromise event through the "Manage My Fraud and Risk" tool located within Mastercard Connect. By following this notification, Mastercard can partner with the acquirer to help validate if an event has occurred.
2. Notify the proper authorities for assistance.*
3. Preserve evidence for further investigation.
    a. Do not reboot/power down system without taking a forensic image that can maintain chain of custody.
    b. Do not modify data/systems believed to be impacted by a potential account data compromise event without having a forensic image taken.
4. Validate logging and monitoring are functioning to PCI DSS requirements.
    a. 90 days onsite, 1 year offsite logs
    b. Ability to rebuild all actions taken
5. Validate that payment process code at checkout is being monitored for any changes through the File Integrity Monitoring configuration.
6. Restrict access to the administrative panel login page to a white listed IP address(es) via configuration rules for the respective platform.

7. Ensure authentication is utilizing appropriate MFA (multiple factor authentication) for appropriate systems.
    a. Where MFA is not in place, evaluate whether the passwords need to be changed for elevated privilege accounts.
    b. Change user, administrative and/service passwords to restrict continued access through an organizational account.

References

- Bleeping Computer
- ZDNet
- GWillem's Lab
- Magento
- Hypernode/Mage Report
- *U.S. Authority Contact List (available to provide assistance):
    a. Federal Bureau of Investigation:
        i. CYWATCH@fbi.gov
    b. United States Secret Service:
        i. GIOC@usss.dhs.gov