NOVEMBER 2016

blackfoot

BLACKFOOT NEWSFLASH

The Magecart exploit injects keyloggers into Direct Post and i-Frame e-commerce payment pages to harvest payment card details

During October 2016, security researchers reported on a criminal campaign where a large number of e-commerce sites had been compromised, and customers' payment card details stolen. Over recent years, merchants have moved away from in-house payment pages to i-Frames or Direct Post, in order to reduce risk and reduce the cost of achieving PCI compliance. But it is these solutions which Magecart attacks.

Attackers have targeted sites based on several popular e-commerce platforms including Magento, Powerfront and OpenCart, and several payment processing services including Braintree and VeriSign. Magecart infection has been found on more than 100 e-commerce sites, including the website of publishers Faber & Faber.

Unlike other e-commerce breaches seen in the past, a successful Magecart attack involves only a small change to the site code. This change points to JavaScript hosted on a separate site controlled by the criminals. When a customer visits the payment page, the criminal's JavaScript is loaded along with the merchant's payment page, and a keylogger or form scraper silently harvests the customer's payment card details. The attack does not rely on criminals breaching the site and remaining undetected for a long time while they discover then exfiltrate data, it can happen very quickly. The malicious JavaScript does not reside on, nor is it run from the merchant's e-commerce site.

Magecart infection to date has succeeded through exploiting vulnerabilities in the e-commerce platforms, or by obtaining site administrator credentials.

What is the threat?

Because Magecart silently harvests payment card details, a compromised e-commerce site could go undetected for weeks or months, allowing the criminals to gather a large number of payment card details until they are ready to cash out.

The criminals have taken steps to avoid detection and raising suspicions. The JavaScript may not execute on every checkout, which prevents customers and staff noticing anomalous behaviour. Additionally, criminals may detect client sessions running from within the merchant's IP address ranges, or from an IP address belonging to known payment industry or information security organisation, in which case the JavaScript may not execute to avoid detection.

What is the potential impact?

The impact of a Magecart or similar breach would be significant to merchants. There would be costs in terms of forensics, remediation, breach fines and reduced revenue resulting from loss of reputation.

Note that whilst the Magecart campaign is focused on stealing payment card data, any web form data would be vulnerable to the same attack. This creates a potential risk to personal data and sensitive personal data.

How to tell if you are affected or vulnerable

There is no simple check to detect a Magecart infection or susceptibility.

Blackfoot has been warning clients for some months about the risk represented by third party tags on e-commerce sites, especially on payment pages. And whilst Magecart infections to date have not arisen through this route, a similar attack might easily occur in future through a compromised third party.

Detection relies on identifying the malicious JavaScript either on the e-commerce site or as the page is delivered to the client's browser.

The following steps are recommended (this is a summary list; a fuller list is available):

- Implement a robust SSDLC methodology, including a rigorous deployment authorisation process.
- Minimise JavaScript/styles from third parties, and where possible place risk assessed versions on your hosting servers.
- Eliminate tags on payment pages.
- Keep e-commerce platform patched and updated.
- Protect administrator access with multi-factor authentication.
- Set permissions on application artefacts to read-only after deployment.
- Raise alerts if out-of-process permission changes are made.
- Perform regular infrastructure pen tests against the hosting environment.
- Perform regular web application pen tests.
- Use File Integrity Monitoring (FIM) to detect changes on the web server.
- Conduct mystery shopping from random locations outside of the company network.
- Consider reverse proxy to test outbound traffic.
- Train support staff to understand that reports of anomalous website behaviour might indicate a breach.
- Conduct social media monitoring to look for reports of anomalous behaviour and fraud.

Blackfoot statement of opinion

The discovery of emerging exploits is often welcome news to would-be attackers who, armed with technically competent resources, are often quick to develop ever more effective and simple-to-use attack tools.

As news spreads, tools evolve and the required attacker skill level reduces. Therefore this exploit will undoubtedly become increasingly common. To this end, it is recommended that clients move quickly to identify whether they are vulnerable and reduce or eliminate the likelihood of risk.

Next steps

Contact your Blackfoot account manager to discuss early detection and assessment services, call 0845 805 2409 or email info@blackfootuk.com

Further reading

https://www.riskiq.com/blog/labs/magecart-keylogger-injection/
http://labs.sucuri.net/?note=2016-06-30

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >

This material is for information purposes only and does not take into consideration the particular circumstances or objectives of your business. Whilst every reasonable effort has been made to ensure the accuracy of the information in this document, Blackfoot UK Limited shall not be held liable for any errors or omissions.