Magento Sites Targeted with Sneaky Credit Card Skimmer via Swap Files

Jul 23, 2024 Newsroom

Threat actors have been observed using swap files in compromised websites to conceal a persistent credit card skimmer and harvest payment information.

The sneaky technique, observed by Sucuri on a Magento e-commerce site's checkout page, allowed the malware to survive multiple cleanup attempts, the company said.

The skimmer is designed to capture all the data into the credit card form on the website and exfiltrate the details to an attacker-controlled domain named "amazon-analytic[.]com," which was registered in February 2024.

"Note the use of the brand name; this tactic of leveraging popular products and services in domain names is often used by bad actors in an attempt to evade detection," security researcher Matt Morrow said.

This is just one of many defense evasion methods employed by the threat actor, which also includes the use of swap files ("bootstrap.php-swapme") to load the malicious code while keeping the original file ("bootstrap.php") intact and free of malware.

"When files are edited directly via SSH the server will create a temporary 'swap' version in case the editor crashes, which prevents the entire contents from being lost," Morrow explained.

"It became evident that the attackers were leveraging a swap file to keep the malware present on the server and evade normal methods of detection."

Although it's currently not clear how the initial access was obtained in this case, it's suspected to have involved the use of SSH or some other terminal session.

The disclosure arrives as compromised administrator user accounts on WordPress sites are being used to install a malicious plugin that masquerades as the legitimate Wordfence plugin, but comes with capabilities to create rogue admin users and disable Wordfence while giving a false impression that everything is working as expected.

"In order for the malicious plugin to have been placed on the website in the first place, the website would have already had to have been compromised — but this malware could definitely serve as a reinfection vector," security researcher Ben Martin said.

"The malicious code only works on pages of WordPress admin interface whose URL contains the word 'Wordfence' in them (Wordfence plugin configuration pages)."

Site owners are advised to restrict the use of common protocols like FTP, sFTP, and SSH to trusted IP addresses, as well as ensure that the content management systems and plugins are up-to-date.

Users are also recommended to enable two-factor authentication (2FA), use a firewall to block bots, and enforce additional wp-config.php security implementations such as DISALLOW_FILE_EDIT and DISALLOW_FILE_MODS.

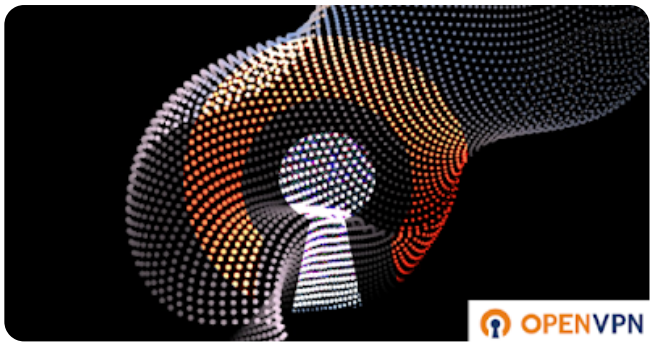
Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

CYBERSECURITY WEBINARS

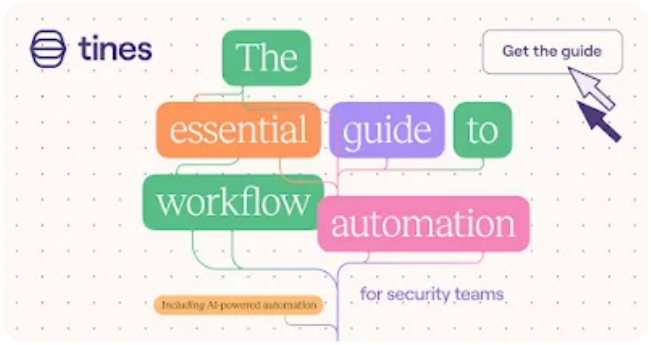
— Breaking News

— Cybersecurity Resources

25 Key Tips to Ensure DORA Compliance



SMBs are left out of the network security conversation, but not by threat actors.



Essential Guide to Workflow Automation for Security Teams

Want To Excel as a Cybersecurity Professional?

— Expert Insights

Leveraging AI as a Tool in Threat Management

7 Resources to Inform Your Next Hunt for Malicious Infrastructure

Exploitability is the Missing Puzzle Piece of SCA (Software Composition Analysis)

9 Customer Service Chatbots Ranked For Risk Exposure

Get Latest News in Your Inbox

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders – all for free.

Your e-mail address

Connect with us!

Company

About THN
Advertise with us
Contact

Pages

Webinars
Deals Store
Privacy Policy

Contact Us