Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

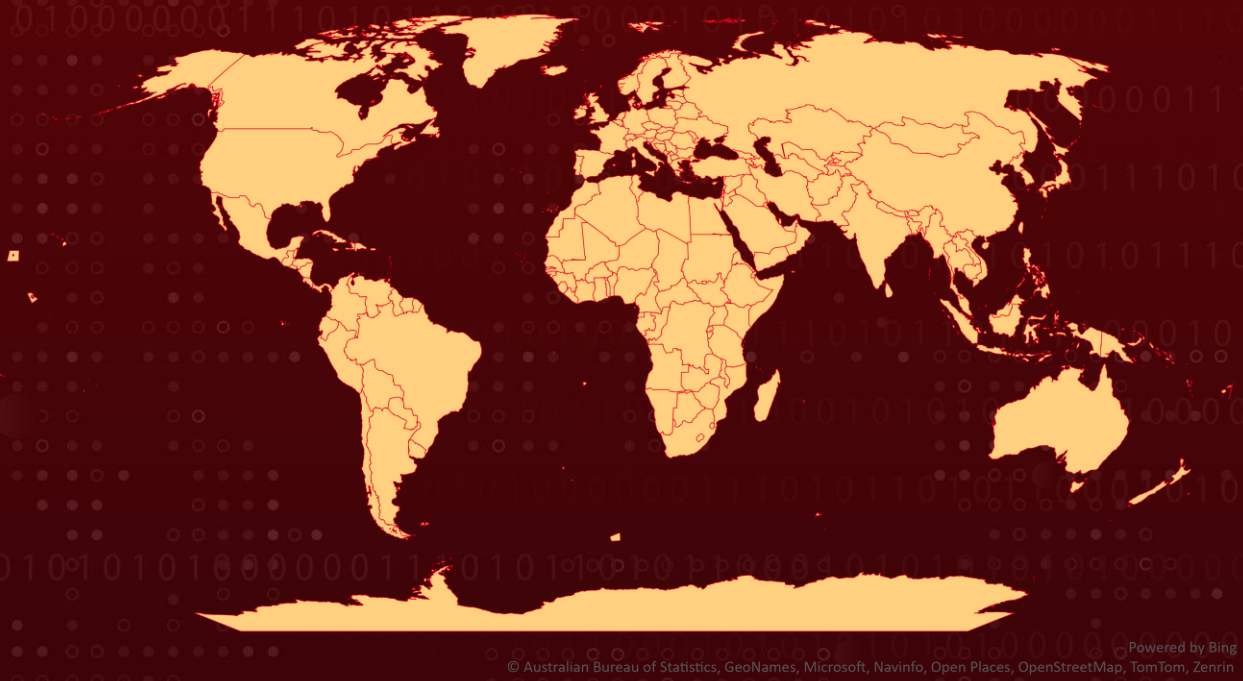
Balada Injector: A Large-Scale Malware Campaign Targeting WordPress

Date of Publication	Admiralty Code	TA Number
October 12, 2023	A1	TA2023412

Summary

Attack Began: September 2023
Attack Region: Worldwide
Malware: Balada Injector
Attack: In September 2023, over 17,000 WordPress websites fell victim to a malware called Balada Injector. The substantial surge in attacks is linked to the exploitation of a recently disclosed security vulnerability found in the tagDiv Composer plugin (CVE-2023-3169). This specific vulnerability allows unauthenticated users to execute stored cross-site scripting (XSS) attacks on vulnerable websites.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-3169	tagDiv Unauthenticated Stored XSS Vulnerability	WordPress sites	✗	✗	✓

Attack Details

#1 The notorious Balada Injector campaign has been attributed to the compromise of more than 17,000 WordPress websites. Balada Injector, which was originally discovered in 2022 but is believed to have been operational since 2017, is a threat that exploits vulnerabilities found in premium WordPress themes and plugins, ultimately enabling the injection of malicious backdoors into compromised websites.

#2 The recent surge in attacks is linked to the exploitation of the CVE-2023-3169 cross-site scripting (XSS) vulnerability in the tagDiv Composer plugin. This plugin is associated with the Newspaper and Newsmag WordPress themes, both of which are premium offerings, and it is used on an estimated 155,000 websites, significantly increasing the potential targets for these attacks.

#3 Balada Injector is known for exploiting Wordpress vulnerabilities, infecting multiple pages, stealing admin credentials, and establishing backdoors to maintain persistent access. This malware redirects users to fake tech support sites, lottery scams, and push notification frauds. Attacks follow a cyclical pattern, occurring every few weeks.

#4 In the recent string of security breaches, this campaign capitalized on the CVE-2023-3169 vulnerability and have introduced new techniques to compromise WordPress websites. One method involves randomized code injections, where code is injected to download and execute a second-stage malware from a remote server. This malware is utilized to install the wp-zexit plugin on the compromised sites.

#5 Additionally, Balada Injector malware employs String.fromCharCode obfuscation in the injected scripts. These scripts are responsible for transmitting visitor's cookies to a URL controlled by the attackers. Balada Injector poses a continuous threat to WordPress sites by exploiting new vulnerabilities, highlighting attackers' evolving tactics and sophisticated methods to compromise websites.

Recommendations

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the XSS vulnerability, providing an additional layer of protection.

Apply Patches and Updates: Immediately apply the latest security patches for tagDiv Composer plugin for CVE-2023-3169.

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Monitor Integrity of deployed Files: Utilize continuous File Integrity Monitoring checks to vigilantly scan deployed webpage source code, promptly alerting administrators to any unauthorized modifications and enabling rapid response to potential security threats. Additionally, employ a website scanner to identify and remove any embedded malicious scripts.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0003** Persistence	**TA0002** Execution
TA0004 Privilege Escalation	**TA0011** Command and Control	**T1136** Create Account	**T1203** Exploitation for Client Execution
T1587 Develop Capabilities	**T1587.001** Malware	**T1566** Phishing	**T1608** Stage Capabilities
T1608.001 Upload Malware	**T1190** Exploit Public-Facing Application	**T1189** Drive-by Compromise	**T1001** Data Obfuscation
T1505 Server Software Component	**T1505.003** Web Shell		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	decentralappps[.]com, statisticscripts[.]com, dataofpages[.]com, listwithstats[.]com, promsmotion[.]com, stablelightway[.]com, specialtaskevents[.]com, getmygateway[.]com, stratosbody[.]com, specialnewspaper[.]com
IPv4	2.59.222[.]113, 2.59.222[.]119, 2.59.222[.]121, 2.59.222[.]122, 2.59.222[.]158, 185.39.206[.]158, 185.39.206[.]159, 185.39.206[.]160, 185.39.206[.]161, 80.66.79[.]252, 80.66.79[.]253, 88.151.192[.]253, 88.151.192[.]254, 89.23.103[.]32, 89.23.103[.]246
SHA1	C1620c4a48a3dcb1d27e587f456b371fc43bcb3d, 9e6178d90f58e9459377a17a7ec2f5bedecd7515, 6bcbd2a5dbfc9a5763c47b7eb327e7df35b401d1, C0053393f9dbe6113bef85dd88b02fa101df030c, C9f7cbc5e634370c396b88c74f426e7a82e23455, 2e995ec1ecfd9b747174e9a19f43d3307c345382, 4ecd9ce89864da0bb758b8a9564976bbe6235aa0, 297e08c30bb487b2820c891e4c9628a04a4fafdc, 3efbd95631e49828a43e8dc5b0035003c96c29b0, 16c737e9d223b9349538e5366963744b3c811a25, F7ae703e2413600ecf2d0c3c20023a45958ab20b, 3284c52eeb26abe796070645a1dabb4009fa61f7, 616b98f0c7d28140c841ffb0acef4d0e7fd63abf, 1e950dfa3f6e44a066b4228658e1de1152ba738e, 215a4470063080696630fb6015378938e8c16a15, 39dea5cb680488e2942641d85c53a80d3b6e03b7, 077d581dbe356bd1ccb94d1833fa368e3f61b5ed, Dfb751fa4c393e0748fe29450b0c9953d6c2e005, C4fcfe1599b2e145d7a4249bd9360968d0706ee2, 565a1e98ef9ac549a8594b2e3777d378ef66251c,

TYPE	VALUE
SHA1	Df4b067cbe01b1ff02aa9ccd5ae37b04830f3cd7, 155171bfca23d3c25fe8b1ac211141c0d1216d62, E11628ab66e4616d22eb150d121ccf9710069474, D5f59dba969401c546ffc9b293223b9c6ce229df, C017a4b93e702120ec64befacfa085bd2d0f3a93, F402fb0b305ea3b65cbd6d6eeeb0084a434ce258, 57a23460fb58c2198ec4acc6a6de79284650aa2d, D3c262d5a12e91921d5a09b746d51fc53e7fbc9f, 076b8e6ef4f800aa458b627dc3caae63718ef6fb, 4a54b885617dc613d28f071af58196f5197f0b5b, 8bd3f72333f50962efaa01d927c6cbc3517d986e, Eeb05978ede31b163912300ee05d45be9f2a0ccd, Bc85aa5917c050311e8889dad3de9a77abdacf13, 22a0c4debdb1f9f99d00b0f818da88f7429798a3, B581d939def9328b0d985b2b1df38cd25fc475d9, 6cedba22594c52d5dd9c5b66ffa175c26ff06025, 09a0d142eb51d2a59ebb88627b3579cfb2083f7b, C19bd1a1b2b18b48273cda326154a369fd07b96d, 344ec12182ab2bf79a10dec7f7c27b3b0e0b2fa0, A3f6f731a0ca6455e4817aa7c68d47a0464691eb, E5bb95687d464ada71c9f06497140a57a8c03ec2, 3e1204224b1492b06107a61ab7f11ad8b50ef456, Fdeeb68a92a7805ecb7bb7f728d9f28f322a536f, Acd4339fa505d9ff76d85633fcae4265ebebd135, 215a4470063080696630fb6015378938e8c16a15, 6d61e0c0343c5de5881cbf7a149106947090e101

Patch Link

https://wpscan.com/vulnerability/e6d8216d-ace4-48ba-afca-74da0dc5abb5/

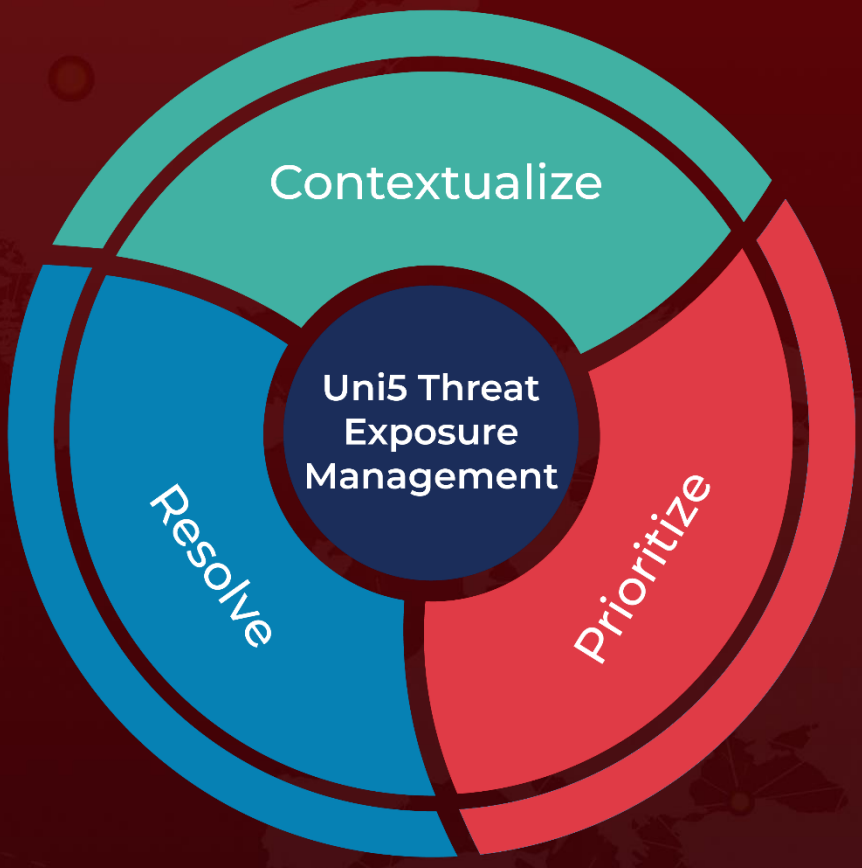
References

https://blog.sucuri.net/2023/10/balada-injector-targets-unpatched-tagdiv-plugin-newspaper-theme-wordpress-admins.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 12, 2023 . 7:00 AM

More at www.hivepro.com