Golang Bot Starts Targeting WordPress Websites

labs.bitdefender.com/2021/03/golang-bot-starts-targeting-wordpress-websites/

Miscellaneous
3 min read

Bitdefender researchers have identified a new version of an already-known vulnerability scanner that looks for a specific flaw in the “Ultimate GDPR & CCPA Compliance Toolkit” plugin for WordPress.

Zero-day vulnerabilities get all the attention, but n-day vulnerabilities cause most security issues. These flaws are already known, and many already have patches. The problem is that people and companies don’t patch their systems or software, giving attackers a way in.

Bitdefender security researchers found a new version of an already-known vulnerability scanner. The bot, written in Golang, targets the “Ultimate GDPR & CCPA Compliance Toolkit” plugin for WordPress. This particular plugin has a critical vulnerability that lets attackers redirect traffic to a malicious website.

Why WordPress plugins?

WordPress, the largest platform of its kind, uses countless plugins. Its modularity allowed it to grow, but it's also a reason threat actors target it often. Vulnerable and unpatched plugins pose a serious security problem, creating a gold mine for criminals.

The "Ultimate GDPR & CCPA Compliance Toolkit" lets websites adhere to the strict rules of The General Data Protection Regulation in Europe. Failure to comply with this regulation exposes website owners to huge fines. If they want European visitors, they need something in place to deal with the data collected from them.

When researchers found the vulnerability in the "Ultimate GDPR & CCPA Compliance Toolkit," the plugin had around 6,000 sales. Anyone using version 2.4 or lower was exposed to this vulnerability. The developer team fixed the issue on January 28, 2021, bringing us full circle to the n-day vulnerabilities. Simply put, if the websites using this plugin haven't upgraded, they are prone to attacks.

How does it work?

The bot retrieves the front page of the web service and looks for certain strings. These correspond to attacker-controlled domains; their presence indicates that the target has already been compromised. Otherwise, subsequent checks show whether the target uses the vulnerable WordPress plugin, in which case the exploit is launched.

The following excerpt from the main.make_ct_ultimate_gdpr function shows the validation performed prior to launching the exploit:

Attacker-controlled domains:

- travelfornamewalking[.]ga
- lovegreenpencils[.]ga
- linetoadsactive[.]ga
- lowerthenskyactive[.]ga
- transandfiestas[.]ga
- strongcapitalads[.]ga
- talkingaboutfirms[.]ga
- daryinformtrand[.]com
- dontkinhooot[.]tw
- declarebusinessgroup[.]ga

As described in the advisory, the vulnerability lets the attacker overwrite the settings file. The JSON file containing the new settings is not bundled in the malware, being retrieved from the filesystem ("cc4.json").

In previous campaigns by this threat actor, the chain through which a WordPress instance is compromised was leading visitors to malicious pages:

Typical exploit flow in previous campaigns
• the bot queries the C2 for a target domain
• the bot scans the target for vulnerabilities and sends reports to the C2
• in some cases, the bot launches the exploit, compromising the target by injecting data
• visitors of the target site execute the attacker-supplied script and are redirected to a malicious website

For example, the actor injects an external script into the index page (sample: d492dd3608741c9128eb5a8dfc1ae688b63bfe8daf9ecaa3ca784aa654a92ef8):

The chain of redirects that leads the visitor from the initial injected script to the malicious website can be easily followed:

This time, the vulnerability enables the attacker to reach the same goal without extra steps.

Based on previous campaigns from the same threat actor, we can assert that its likely goal remains the same, to infect websites and redirect visitors to malicious pages.

Fortunately, a few indicators of compromise can help us identify it more easily.

IOCs

Hashes:

b8aa5b2d7a9febcbca31a6efd3327319c2efe4857e082e65f1333caf65b4f3be (scanner bot)
4277afc7be775bdad3b7c1be0e793401f79136c120cb667c00b55bec2d23a07e (scanner bot)
15117f2d1783063f26c58d1c0ea755d952facbf12e7fd8efc077a0a2780e5906 (archive)
d492dd3608741c9128eb5a8dfc1ae688b63bfe8daf9ecaa3ca784aa654a92ef8 (script)

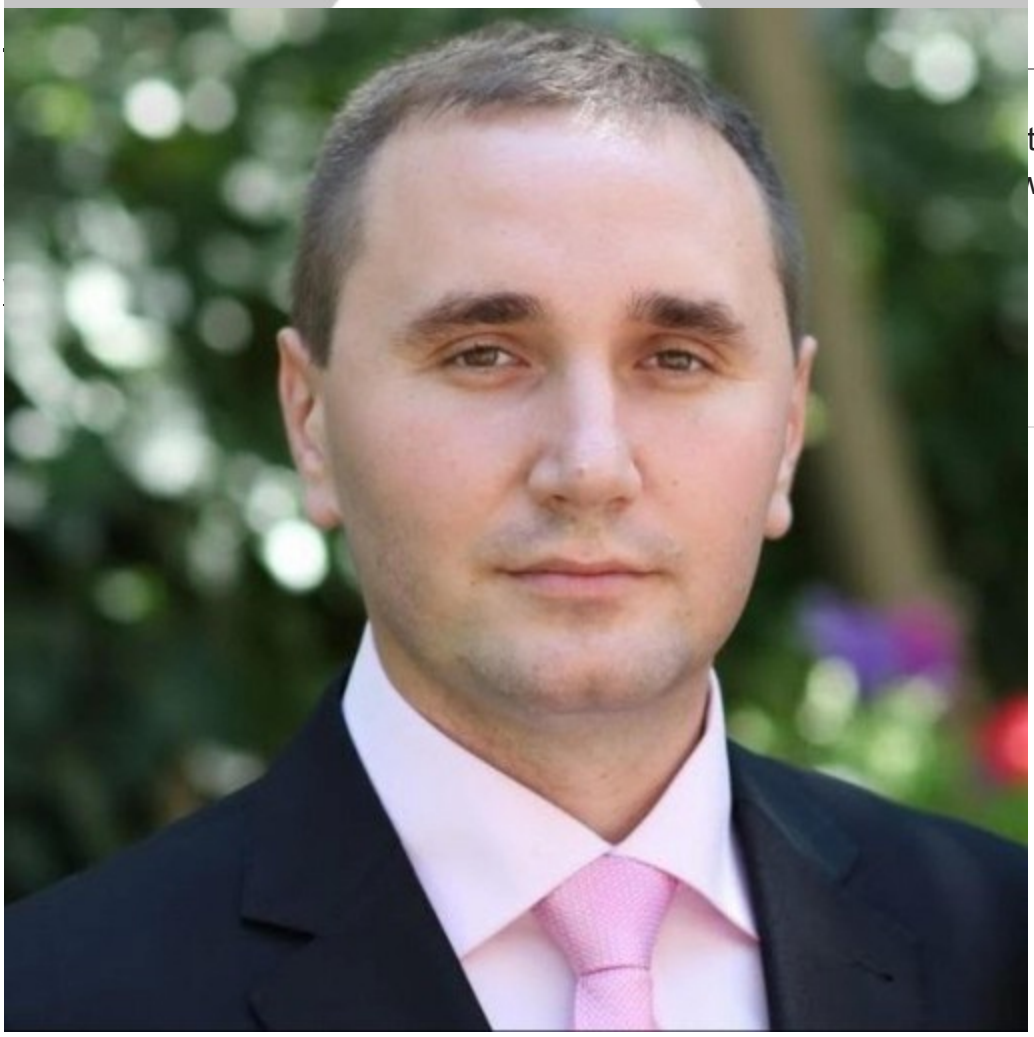
Network indicators:

- lovegreenpencils[.[ga
- travelfornamewalking[.]ga
- linetoadsactive[.]ga
- lowerthenskyactive[.]ga
- transandfiestas[.]ga
- strongcapitalads[.]ga
- talkingaboutfirms[.]ga
- daryinformtrand[.]com
- dontkinhooot[.]tw
- declarebusinessgroup[.]ga
- 195.2.71.173:4112

TAGS

miscellaneous

AUTHOR



two decades,
ween.