Dec 05 2023

NETMANAGEIT

Intelligence Report

PSA: Fake CVE-2023-45124 Phishing Scam Tricks Users Into Installing Backdoor Plugin

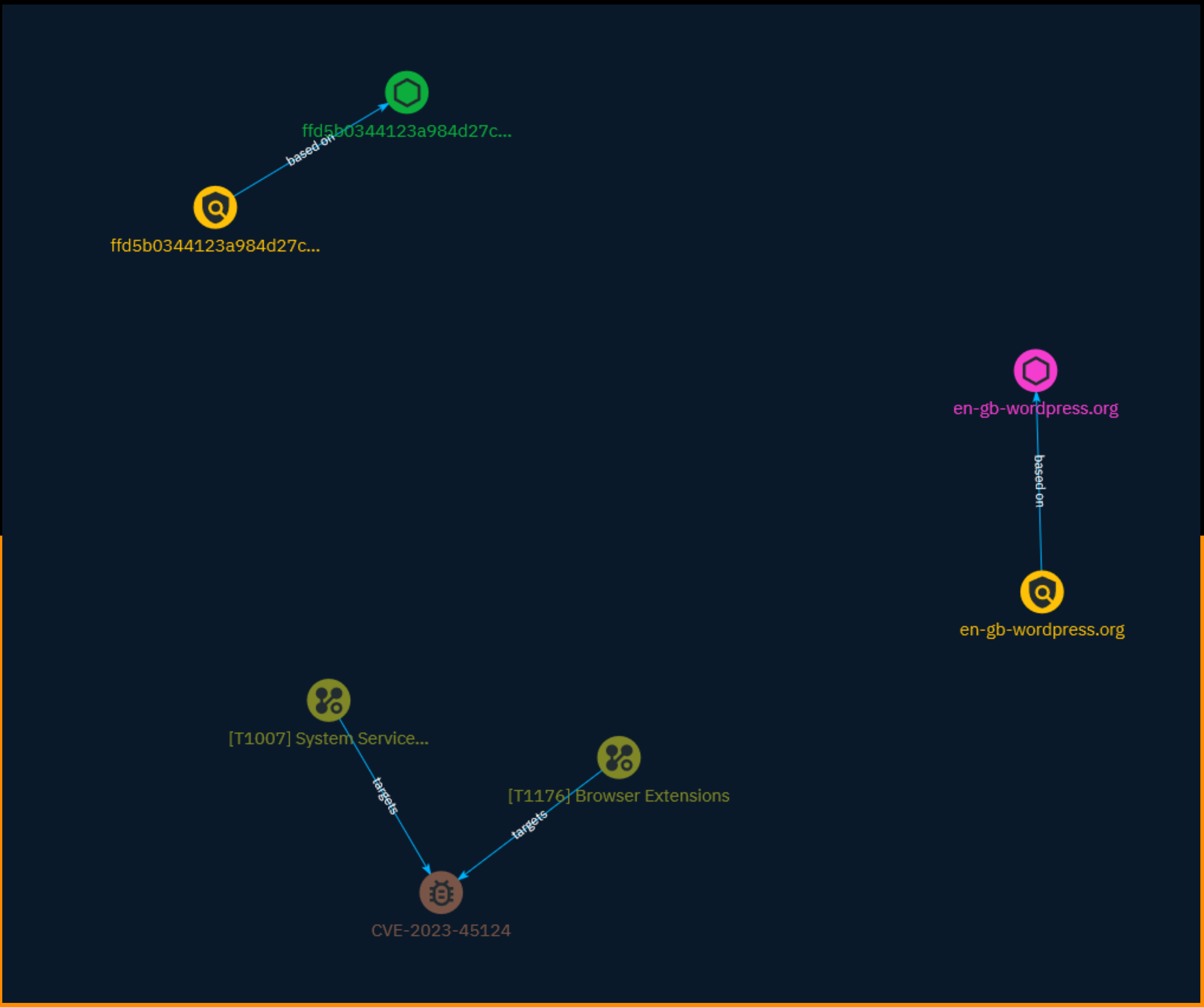

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Wordfence has issued a PSA warning about a phishing campaign targeting users of WordPress, which includes a malicious backdoor that allows attackers to gain full control of the WordPress site and access to a hidden administrator user.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

System Service Discovery

ID

T1007

Description

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Indicator

Name

en-gb-wordpress.org

Pattern Type

stix

Pattern

[domain-name:value = 'en-gb-wordpress.org']

Name

ffd5b0344123a984d27c4aa624215fa6452c3849522803b2bc3a6ee0bcb23809

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ffd5b0344123a984d27c4aa624215fa6452c3849522803b2bc3a6ee0bcb23809']

Vulnerability

Name
CVE-2023-45124

Domain-Name

Value
en-gb-wordpress.org

StixFile

Value
ffd5b0344123a984d27c4aa624215fa6452c3849522803b2bc3a6ee0bcb23809

External References

- https://otx.alienvault.com/pulse/656f2ee901a8cdd523b08cb8
- https://www.wordfence.com/blog/2023/12/psa-fake-cve-2023-45124-phishing-scam-tricks-users-into-installing-backdoor-plugin/