

PurpleFox Using WPAD to Target Indonesian Users

By Trend Micro (words)

Published: 2021-07-01 · Archived: 2026-04-06 00:57:12 UTC

In September 2020, we published a blog describing how the [PurpleFox Exploit Kit used Cloudflare services](#) to maintain an infrastructure resilient to blocking and detection attempts. Since then, PurpleFox has been maintaining this strategy while at same time improving its attack chain by incorporating the latest [public vulnerabilities](#) into its arsenal.

Recently, we found that PurpleFox added a very old tactic to increase its delivering performance. This time PurpleFox EK is [making use of WPAD domains](#) to infect users. While a WPAD abuse attack is a technique that has been around for approximately 14 years, it still works. [Initiatives to prevent this attack](#) help, but they are not sufficient.

Our systems started detecting victims accessing the “wpad.id” domain, which makes use of the Indonesian top level domain (*.id). We did not find any other country top level domain affected. Using this technique, a zero-click attack can be implemented, as the WPAD URL is accessed whenever the system starts, without any user input.

PurpleFox WPAD landing page

To abuse WPAD, the PurpleFox authors registered the domain “wpad.id” with Cloudflare. They then load the URL for WPAD services, which is located at `http://wpad[.]id/wpad[.]dat`. At the time of analysis, this would return a standalone JavaScript version of the [CVE-2019-1367](#) with custom shellcode to follow the attack chain setup for the WPAD attack. Figure 1 shows the WPAD resolution and malicious sample delivery.

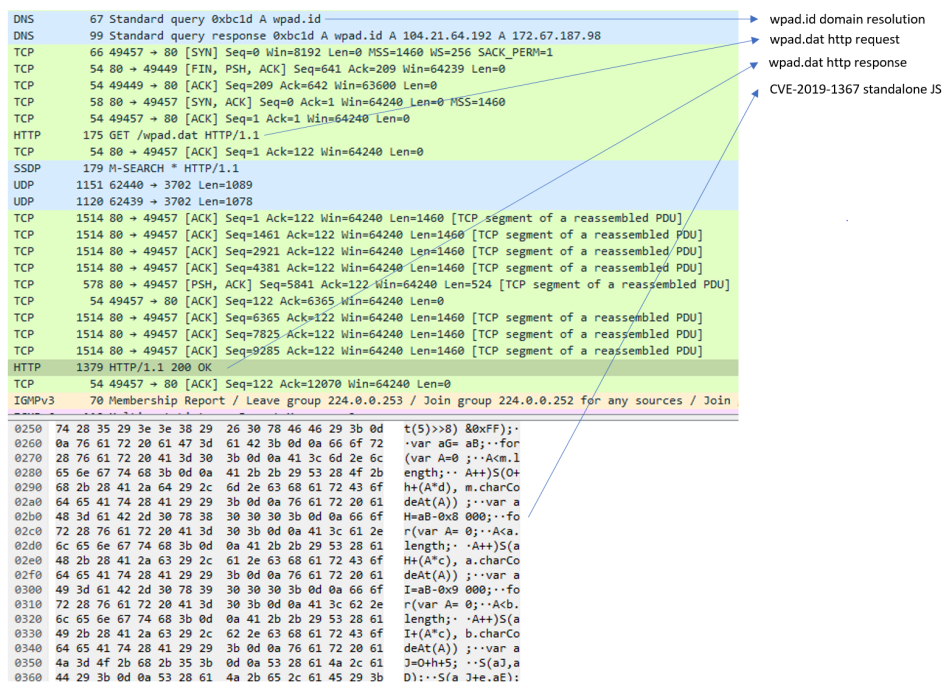


Figure 1. CVE-2019-1367 exploit delivery using WPAD

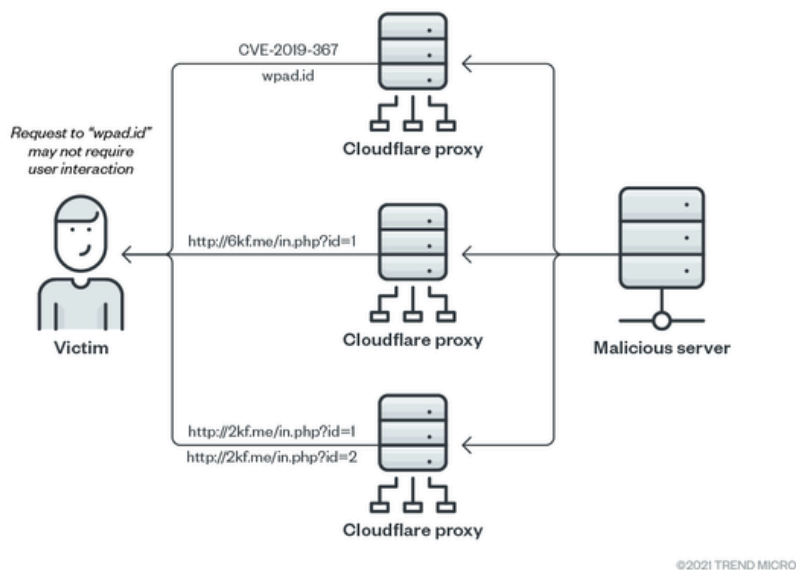


Figure 4. The attack chain

Analysis of the full chain revealed that the following CVEs were being exploited: [CVE-2020-1054](#), [CVE-2018-8120](#), as well as an [exploit for MS15-051](#). The binary exploiting the MS15-051 leak the symbols path `C:\Users\K8team\Desktop\ms15-051\ms15-051\ms15-051\Win32\ms15-05`, suggesting that PurpleFox is reusing tools from [K8team](#), which is responsible for maintaining public repositories of CVE exploits POCs and hack tools.

Defending against PurpleFox

The PurpleFox Exploit Kit continues to be very active and appear to be looking for new infection tactics. Our feedback shows that this specific attempt is not only affecting Indonesian victims, as users in other countries who are using the Indonesian TLD are being affected as well. At same time, PurpleFox is trying to reach servers where the user interaction is minimal but are potentially affected by the WPAD technique, such as unattended machines.

Continuous vigilance against threat groups is an important aspect of keeping up with — if not staying one step ahead of — threats. To protect systems from this type of threat, users can use multilayered security solutions like [Trend Micro Protection Suites](#) that help detect and block attacks. [Trend Micro Vision One™](#) also provides visibility, correlated detection, and behavior monitoring across multiple layers, such as emails, endpoints, servers, and cloud workloads. This ensures that no significant incidents go unnoticed and allows faster response to threats before they can do any real damage to the system.

Indicators of Compromise

Files

SHA256	Filename	Trend Micro Detection N
1aa1df57f786224f4997f1d6284a123176291f3f3d43bc4b942ae423c58cc356	winupdate64.log	Trojan.Win64.FUPORPL
3039208b2a34bb2e71bc6a77ae3be2fa588abd359fdb0068253739f3839f3425	2020-09-09_16-25-29_764_raw.githuback.store_P1-1-2_PurpleFox.exe.bak	Trojan.Win32.CVE2018
36725374d7ec66c9876eb1d5edc2a5889643e01dbd0ac7a6705babb3c3ea6a9	M0011.cab	Trojan.Win32.FUPORPL
61113a0acd6469ce0d860db55c2afa3cdcbac2f5411fe8259cca43c10c042239	1505132.jpg	TROJ_CVE20151701.B
905cc7b3027cad361ae7a29969dfd7e63f8f1189d7e0abdf5b2efe0f1ec13e5c	pe_1	Trojan.Win32.CVE2019C
db7c4a360b460a13148d6e5fff530afaa0fa161959166cdab342d0aa9760ba68	sysupdate.log	Backdoor.Win32.FUPOR

f09c502f4b5862641b3c3eff19ae96d949fab465b3fddd1888fe945817c9e2fd	N/A	Trojan.Win32.FUPORPL
--	-----	----------------------

URLs

- [http://2kf\[.\]me/in\[.\]php](http://2kf[.]me/in[.]php)
- [http://6kf\[.\]me/in\[.\]php](http://6kf[.]me/in[.]php)
- [http://9kf\[.\]me/in\[.\]php](http://9kf[.]me/in[.]php)

Tags

Source: https://www.trendmicro.com/en_us/research/21/g/purplefox-using-wpad-to-targent-indonesian-users.html