THREAT ADVISORY

Prophet Spider exploits Log4j and Citrix vulnerabilities to deploy webshells

TA2022055

Threat Level RED

Published Date – March 10, 2022

Prophet Spider is a well-known Initial Access Broker (IAB) group. Prophet Spider's tradecraft continues to grow while exploiting known web-server vulnerabilities such as Citrix and Log4j.

A remote code execution (RCE) vulnerability(CVE-2021-22941) affecting Citrix ShareFile Storage Zones Controller, was used by Prophet Spider to attack a Microsoft Internet Information Services (IIS) web server. The attacker took advantage of the flaw to launch a WebShell that allowed the download of further tools.

Prophet Spider also exploits known Log4j vulnerabilities in VMware Horizon (CVE-2021-44228, CVE-2021-45046, CVE-2021-44832). Prophet Spider most typically used encoded PowerShell instructions to download a second-stage payload to the targeted PCs after exploiting the vulnerabilities. The specifics of that payload are determined by the attacker's motivations and aims, such as crypto mining, ransomware, and extortion.

The MITRE TTPs commonly used by **Prophet Spider** are:
TA0001: Initial Access
T1190: Exploit Public Facing Application
TA0002: Execution
T1059.001: Command and Scripting Interpreter: PowerShell
TA0003: Persistence
T1505.003: Server Software Component: Web Shell
TA0011: Command and Control
T1071: Application Layer Protocol
T1105: Ingress Tool Transfer

Actor Details

Name	Target Locations	Target sectors
PROPHET SPIDER	India, UK, USA	Healthcare, Energy, Manufacturing, Financial Services, Retail, Technology, Media, Telecommunications

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-22941	Citrix ShareFile storage zones controller before 5.11.20	cpe:2.3:a:citrix:sharefile_storagezones_controller:*:*:*:*:*:*:*:*	Citrix ShareFile storage zones controller security bypass	CWE-284, CWE-269
CVE-2021-44228	Apache log4j versions 2.0 to 2.14.1	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j remote code execution	CWE-20 CWE-400 CWE-502
CVE-2021-45046	Apache log4j versions 2.0 to 2.15.0 excluding version 2.12.2	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j denial of service	CWE-502
CVE-2021-44832	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4)	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j remote code execution	CWE-20 CWE-74

Indicators of Compromise (IoCs)

Type	Value
IPV4	45.61.136[.]39 107.181.187[.]184 188.119.149[.]160 138.68.246[.]18 140.246.171[.]141 150.158.189[.]96 159.65.48[.]154 167.71.13[.]196 170.210.45[.]163 175.6.210[.]66 185.220.100[.]240 185.220.100[.]241 185.220.100[.]244 185.220.100[.]251 185.220.100[.]252 185.220.101[.]152 185.220.101[.]158 185.220.101[.]171 185.220.101[.]184 185.220.101[.]188 185.220.101[.]190 185.220.101[.]36 185.220.101[.]53 185.220.102[.]248 185.56.80[.]65 192.160.102[.]170 194.48.199[.]78 198.98.56[.]151 216.144.180[.]171 23.129.64[.]218 23.236.146[.]162 45.146.165[.]168 45.154.255[.]147 45.61.146[.]242 5.157.38[.]50 51.222.121[.]180 62.102.148[.]68 79.172.212[.]132
URL	hxxps[:]//raw.githubusercontent[.]com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1 hxxp://149.28.200[.]140:443/wget.bin hxxp://lurchmath[.]org/wordpress-temp/wp-content/plugins/xmrig.zip hxxp://72.46.52[.]135/mad_micky.bat hxxp://api.rogerscorp[.]org:80 hxxp://80.71.158[.]96/xms.ps1 hxxp://149.28.200[.]140:443/winntaa.exe hxxp://185.112.83[.]116:8080/drv hxxp://137.184.17[.]252:443/dd.ps1 hxxp://101.79.1[.]118/2.ps1 hxxp://72.46.52[.]135/kill.bat

Type	Value
File Path	c:\windows\system32\config\systemprofile\mimu\nssm.exe c:\windows\system32\config\systemprofile\mimu2\nssm.exe C:\Windows\system32\config\systemprofile\mimu\xmrig.exe c:\windows\temp\winntaa.exe C:\Windows\temp\wget.bin C:\Windows\system32\config\systemprofile\AppData\Roaming\network02.exe C:\Windows\TEMP\network02.exe
Domain	b.oracleservice[.]top api.rogerscorp[.]org
IPV4/Port	80.71.158[.]96:80 72.46.52[.]135:80 51.79.175[.]139:8080 198.23.214[.]117:8080 185.112.83[.]116:8080 167.114.114[.]169:8080 149.28.200[.]140:443
File Name	kill.bat xms.ps1 mad_micky.bat xmrig.zip wget.bin dd.ps1 2.ps1 absg-worker.js

Patch Link

https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.15.0/
https://logging.apache.org/log4j/2.x/manual/migration.html
https://github.com/apache/logging-log4j2/pull/607/files
https://www.citrix.com/downloads/sharefile/product-software/sharefile-storagezones-controller-511.html

References

https://blogs.blackberry.com/en/2022/01/log4u-shell4me
https://www.crowdstrike.com/blog/prophet-spider-exploits-citrix-sharefile/