ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices

Cisco Talos ⋮⋮ 4/24/2024

By Cisco Talos

Wednesday, April 24, 2024 11:54
Threat Advisory Threats APT

**Updated 2024-04-25 16:57 GMT with minor wording corrections regarding the targeting of other vendors.*

ArcaneDoor is a campaign that is the latest example of state-sponsored actors targeting perimeter network devices from multiple vendors. Coveted by these actors, perimeter network devices are the perfect intrusion point for espionage-focused campaigns. As a critical path for data into and out of the network, these devices need to be routinely and promptly patched; using up-to-date hardware and software versions and configurations; and be closely monitored from a security perspective. Gaining a foothold on these devices allows an actor to directly pivot into an organization, reroute or modify traffic and monitor network communications. In the past two years, we have seen a dramatic and sustained increase in the targeting of these devices in areas such as telecommunications providers and energy sector organizations — critical infrastructure entities that are likely strategic targets of interest for many foreign governments.

Cisco's position as a leading global network infrastructure vendor gives Talos' Intelligence and Interdiction team immense visibility into the general state of network hygiene. This also gives us uniquely positioned investigative capability into attacks of this nature. Early in 2024, a vigilant customer reached out to both Cisco's Product Security Incident Response Team (PSIRT) and Cisco Talos to discuss security concerns with their Cisco Adaptive Security Appliances (ASA). PSIRT and Talos came together to launch an investigation to assist the customer. During that investigation, which eventually included several external intelligence partners and spanned several months, we identified a previously unknown actor now tracked as UAT4356 by Talos and STORM-1849 by the Microsoft Threat Intelligence Center. This actor utilized bespoke tooling that demonstrated a clear focus on espionage and an in-depth knowledge of the devices that they targeted, hallmarks of a sophisticated state-sponsored actor.

UAT4356 deployed two backdoors as components of this campaign, "Line Runner" and "Line Dancer," which were used collectively to conduct malicious actions on-target, which included configuration modification, reconnaissance, network traffic capture/exfiltration and potentially lateral movement.

Critical Fixes Available

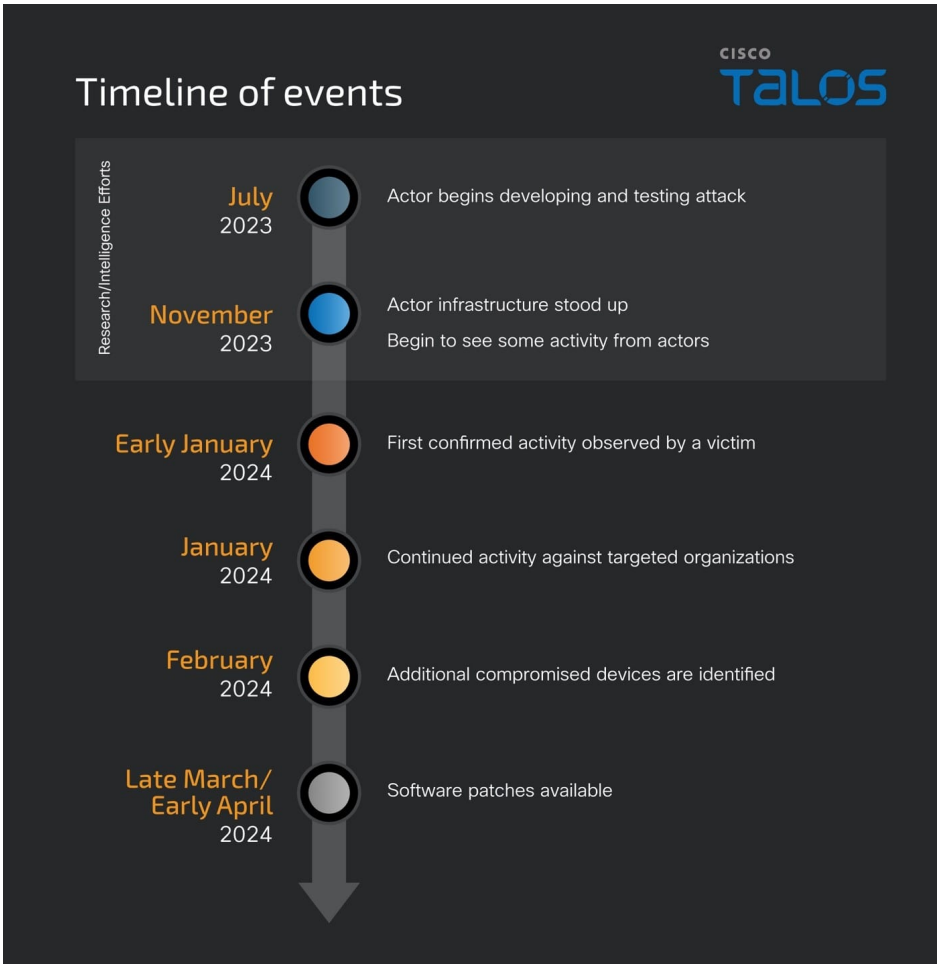
Working with victims and intelligence partners, Cisco uncovered a sophisticated attack chain that was used to implant custom malware and execute commands across a small set of customers. While we have been unable to identify the initial attack vector, we have identified two vulnerabilities (CVE-2024-20353 and CVE-2024-20359), which we detail below. Customers are strongly advised to follow the guidance published in the security advisories discussed below.

Further, network telemetry and information from intelligence partners indicate the actor is interested in — and potentially attacking — Microsoft Exchange servers and network devices from other vendors. Regardless of your network equipment provider, now is the time to ensure that the devices are properly patched, logging to a central,

secure location, and are configured to have strong, multi-factor authentication (MFA). Additional recommendations specific to Cisco are available here.

Timeline

Cisco was initially alerted to suspicious activity on an ASA device in early 2024. The investigation that followed identified additional victims, all of which involved government networks globally. During the investigation, we identified actor-controlled infrastructure dating back to early November 2023, with most activity taking place between December 2023 and early January 2024. Further, we have identified evidence that suggests this capability was being tested and developed as early as July 2023.



Cisco has identified two vulnerabilities that were abused in this campaign (CVE-2024-20353 and CVE-2024-20359). Patches for these vulnerabilities are detailed in the Cisco Security Advisories released today.

Initial Access

We have not determined the initial access vector used in this campaign. We have not identified evidence of pre-authentication exploitation to date. Our investigation is ongoing, and we will provide updates, if necessary, in the security advisories or on this blog.

Line Dancer: In-Memory Implant Technical Details

The malware implant has a couple of key components. The first is a memory-only implant, called “Line Dancer.” This implant is a memory-resident shellcode interpreter that enables adversaries to upload and execute arbitrary shellcode payloads.

On a compromised ASA, the attackers submit shellcode via the host-scan-reply field, which is then parsed by the Line Dancer implant. Note that the use of this field does not indicate the exploitation of CVE-2018-0101 which was NOT used as a component of this campaign. The host-scan-reply field, typically used in later parts of the SSL VPN session establishment process, is processed by ASA devices configured for SSL VPN, IPsec IKEv2 VPN with “client-services" or HTTPS management access. The actor overrides the pointer to the default host-scan-reply code to instead point to the Line Dancer shellcode interpreter. This allows the actor to use POST requests to interact with the device without having to authenticate and interact directly through any traditional management interfaces.

Line Dancer is used to execute commands on the compromised device. During our investigation, Talos was able to observe the threat actors using the Line Dancer malware implant to:

- Disable syslog.
- Run and exfiltrate the command show configuration.
- Create and exfiltrate packet captures.
- Execute CLI commands present in shellcode; this includes configuration mode commands and the ability to save them to memory (write mem).
- Hook the crash dump process, which forces the device to skip the crash dump generation and jump directly to a device reboot. This is designed to evade forensic analysis, as the crash dump would contain evidence of compromise and provide additional forensic details to investigators.
- Hook the AAA (Authentication, Authorization and Accounting) function to allow for a magic number authentication capability. When the attacker attempts to connect to the device using this magic number, they are able to establish a remote access VPN tunnel bypassing the configured AAA mechanisms. As an alternate form of access, a P12 blob is generated along with an associated certificate and exfiltrated to the actor along with a certificate-based tunnel configuration.

Host-Scan-Reply hook overview

In the Line Dancer implant's process memory, we found a function (detailed below) that checks if a 32-byte token matches a pattern. If so, it base64-decodes the payload, copies it into the attacker's writable and executable memory region, and then calls the newly decoded function. Either way, it ends by calling `processHostScanReply()`.

The function `processHostScanReply()` is normally accessed through a function pointer in the `elementArray` table, associated with the string `host-scan-reply`. In the captured memory, the entry that should point to `processHostScanReply()` now instead points to the attacker's function that decodes and runs its payload. Since this change is in the data section of memory, it doesn't show up in hashes/dumps of text.

The attacker function that decodes and runs its payload has the following decompilation:

```
{
long payload;
int iVar2;
uint len;
void *decoded_payload;
if (ip_pak != 0) {
payload = ip_pak + 0x20; iVar2 =
memcmp(s_[redacted]_55824e200200,ip_pak,0x2
0); if (iVar2 == 0) {
len = __wrap_strlen(payload); decoded_payload = malloc(len);
if (decoded_payload != (void *)0x0) {
base64_decode(payload,decoded_payload);
memcpy(CUS_shellcode_payload,decoded_payload,(ulong)len);
free(decoded_payload);
CUS_shellcode_payload();
} }
} processHostScanReply(param_1); return;
}
```

Line Runner: Persistence Mechanism

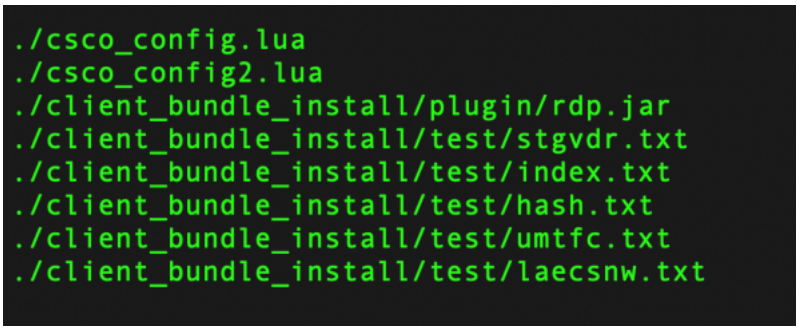
The threat actor maintains persistence utilizing a second, but persistent, backdoor called "Line Runner" on the compromised ASA device using functionality related to a legacy capability that allowed for the pre-loading of VPN clients and plugins on the device. At boot, the ASA is designed to look for the presence of a file on disk0: matching the Lua regular expression:

```
^client_bundle[%w_-]*%.zip$
```

If the file exists, it will unzip it and execute the script csco_config.lua. Once processed, the ZIP file is deleted. This is assigned CVE-2024-20359 and more details are available in this Cisco Security Advisory.

In at least one case, there is another vulnerability, CVE-2024-20353, that was abused by the actor to facilitate this process. The attackers were able to leverage this vulnerability to cause the target ASA device to reboot, triggering the unzipping and installing the second component of the threat actor's malware implant, Line Runner.

The threat actor's ZIP file has the following files:



The scripts in the zip file allow the threat actor to maintain a persistent HTTP-based Lua backdoor to the ASA, which survives across reboots and upgrades. Line Runner was observed being used by UAT4356 to retrieve information that was staged through the use of Line Dancer.

csco_config.lua

The csco_config.lua file is run at boot and makes the following modifications to the system:

• Create `disk0:/csco_config/97/webcontent/` if it doesn't already exist
• Create `disk0:/csco_config/97/webcontent/1515480F4B538B669648B17C02337098` from hash.txt
• Append index.txt to `disk0:/csco_config/97/webcontent/index_bp.ini` and put the result in `disk0:/csco_config/97/webcontent/index.ini`
• Move the original `client_bundle.zip` file to `/run/lock/subsys/krbkdc6`
• Prepend `umtfc.txt` to `/etc/init.d/umountfs`
• Copy `stgvdr.txt` to `/asa/scripts/lina_cs`
• Backup `/asa/scripts/lina_exe_cs.sh` to `/asa/scripts/lina_exe_cs_bp.sh`
• Replace `/asa/scripts/lina_exe_cs.sh` with `laecsnw.txt`
• Copy `csco_config2.lua` over `csco_config.lua`
• Disable the `importPlugin` function for the next call only

csco_config2.lua

The csco_config2.lua file cleans up the modifications made by csco_config.lua (above) and removes itself.

hash.txt

Used as content for `disk0:/csco_config/97/webcontent/1515480F4B538B669648B17C02337098`.

Intercepts HTTP requests to the ASA. The threat actor's code looks for an HTTP request with a set of 32-character parameters that are victim-dependent. If they match, then the payload contained within one of these parameters is written to a Lua script and executed. This is the backdoor's command and control mechanism.

index.txt

Adds webContent information so hash.txt is processed.

laecsnw.txt

Temporarily replaces `/asa/scripts/lina_exe_cs.sh`.

Executes `/asa/scripts/lina_cs` as a background process (see below). Removes itself. Then restore the backup `/asa/scripts/lina_exe_cs_bp.sh`.

stgvdr.txt

Runs as `/asa/scripts/lina_cs`.

After sleeping for 30 seconds, sets expected owner and times on `/etc/init.d/umountfs`. Removes the hash API endpoint, the index.ini, and either restores the backup index.ini or removes the webcontent directory entirely. Finally, removes itself.

umtfc.txt

Prepended to /etc/init.d/unmountfs.

The unmountfs script is called at shutdown to unmount the filesystems. The threat actor's modifications perform the following functionality:

• If `disk0:/csco_config/97/webcontent/1515480F4B538B669648B17C02337098` exists, it removes it and `index.ini`.
• Copy `/run/lock/subsys/krbkdc6 to disk0:client_bundle_install.zip`

This sets up the zipfile to be executed at the next boot, maintaining persistence.

Forensic Recovery and Identification of Line Runner

To identify the presence of Line Runner on an ASA, the following methods can be used. Note also that the device should be upgraded to a fixed version as identified in the first method.

Method 1:

After updating the device to a software release that contains the fix for CVE-2024-20359, a review of the contents of disk0: should be conducted. If a new file (e.g., “client_bundle_install.zip” or any other unusual .zip file) appears on `disk0:` following the update, this suggests that Line Runner was present on the device in question. Note that because the updated software is not vulnerable to CVE-2024-20359, Line Runner will no longer be active on the device.

Method 2:

To detect (and remove) Line Runner, the following series of commands will create an innocuous file with a .zip extension. Note that it will not create a valid zip file, but the file will still be read by the ASA at reboot. Upon execution of the following commands, if a new .zip file appears on disk0: following the reload, this suggests that Line Runner was present on the device in question. Deletion of the “client_bundle_install.zip” file will remove Line Runner. Note that the malicious ZIP containing the Line Runner functionality could have other names that fit the naming pattern outlined previously.

If you discover a newly created .zip file, copy that file off the device using the **copy** command and contact psirt@cisco.com referencing CVE-2024-20359. Include the outputs of the **dir disk0:** and **show version** commands from the device and the **.zip** file extracted from the device.

```
asa> enable
asa# show version | redirect disk0:/client_bundle.zip
asa# show disk0:
# ... Verify `client_bundle.zip` is present
asa# reload
# ... Device reboots
asa> enable
asa# show disk0:
# ... If the device had the persistence mechanism in place
# ... a new file `client_bundle_install.zip` will be present on disk0:
# ... Suggest retrieving and then deleting `client_bundle_install.zip`
# ... from disk0:
```

Anti-Forensics/Anti-Analysis Capabilities

UAT4356 took clear and deliberate steps to attempt to prevent forensic capture of malicious artifacts. This tradecraft suggests a thorough understanding of the ASA itself and of the forensic actions commonly performed by Cisco for network device integrity validation. Additional steps were taken on a case-by-case basis to hide actions being taken on the device. These steps included hooking the AAA (Authentication, Authorization and Accounting) function of the device to allow the actor to bypass normal AAA operations. We also identified some instances where UAT4356 disabled logging to perform operations on or from the ASA and not have those operations or actions logged.

Line Dancer appears to have been intentionally placed into a difficult-to-reach region of memory. In addition, it hooks into functions such as the core dump function, which is commonly used to collect information for debugging and forensic purposes, which were made in memory such that this function simply jumped to a reboot. This means that on reboot, Line Dancer itself would no longer be present and none of the collections present in the core dump function would have been executed, all resulting in a complete loss of debug information and memory-based forensic artifacts.

Attribution

As a part of our ongoing investigation, we have also conducted analysis on possible attribution of this activity. Our attribution assessment is based on the victimology, the significant level of tradecraft employed in terms of capability development and anti-forensic measures, and the identification and subsequent chaining together of 0-day vulnerabilities. For these reasons, we assess with high confidence that these actions were performed by a state-sponsored actor.

Recommendations

There are some known indicators of compromise that customers can look for if they suspect they may have been targeted in this campaign. First, organizations should look for any flows to/from ASA devices to any of the IP addresses present in the IOC list provided at the bottom of this blog. This is one indication that further investigation is necessary.

Additionally, organizations can issue the command `show memory region | include lina` to identify another indicator of compromise. If the output indicates more than one executable memory region (memory regions having `r-xp` permissions, see output examples), especially if one of these memory sections is exactly 0x1000 bytes, then this is a sign of potential tampering.

```
# show memory region | include lina

Address                   Perm Offset   Dev   Inode                     Pathname
561d9d853000-561d9fee9000 r-xp 00000000 00:02 5955                      /asa/bin/lina
561d9fee9000-561d9feea000 r-xp 02696000 00:02 5955                      /asa/bin/lina
561d9feea000-561da2452000 r-xp 02697000 00:02 5955                      /asa/bin/lina
561da2651000-561da3949000 rw-p 04bfe000 00:02 5955                      /asa/bin/lina


# show memory region | include lina

Address                   Perm Offset   Dev   Inode                     Pathname
561d9feea000-561da2452000 r-xp 02697000 00:02 5955                      /asa/bin/lina
561da2651000-561da3949000 rw-p 04bfe000 00:02 5955                      /asa/bin/lina
```

Output of the 'show memory region' command for a compromised device (top) vs. a clean device (bottom).

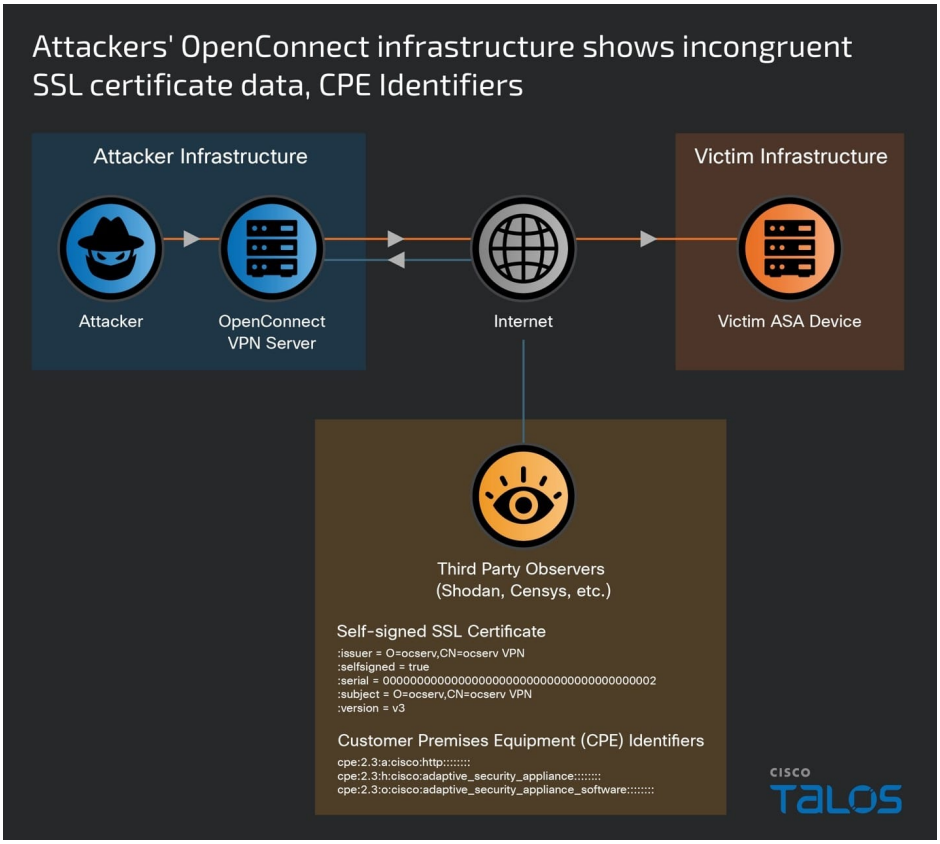
Note that the earlier provided steps to identify the presence of Line Runner can still be followed even in the absence of more than one executable memory region as we have seen cases where Line Runner was present without Line Dancer being present. We still recommend following the steps to upgrade to a patched version even if customers believe that their device has not been compromised.

Next, follow the steps detailed in the Cisco ASA Forensic Investigation Procedures for First Responders. **When following these procedures first responders should NOT attempt to collect a core dump (Step 5) or reboot the device if they believe that the device has been compromised, based on the lina memory region output.** The previous steps up to and including a collection of the memory text section should be followed. In addition, we have released some Snort signatures to detect the activity on the wire including access attempts. Signatures 63139, 62949, and 45575 have been released to detect the implants or associated behaviors. Please note that the device must be set up to decrypt TLS for these signatures to be effective.

- CVE-2024-20353 (ASA DOS/Reboot) - 3:63139
- 'Line Runner' – Persistence Mechanism Interaction – 3:62949
- 'Line Dancer' – In-Memory Only Shellcode Interpreter Interaction – 3:45575
- Note that this signature was originally built to detect an unrelated CVE but it also detects Line Dancer interaction

If your organization does find connections to the provided actor IPs and the crash dump functionality has been altered, please open a case with Cisco TAC.

UAT4356 Infrastructure



Key components of the actor-controlled infrastructure used for this operation had an interesting overlap of SSL certificates which match the below pattern while also appearing as an ASA, during the same period, to external scanning engines such as Shodan and Censys as reported by the CPE data on the same port as the noted SSL certificate. The SSL certificate information suggests that the infrastructure is making use of an OpenConnect VPN Server (https://ocserv.openconnect-vpn.net) through which the actor appeared to be conducting actions on target.

Certificate Pattern:
:issuer = O=ocserv,CN=ocserv VPN
:selfsigned = true
:serial = 00000000000000000000000000000000000000000000000000000002
:subject = O=ocserv,CN=ocserv VPN
:version = v3

CPE identifiers:
cpe:2.3:a:cisco:http:*:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:*:*
cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*

MITRE TTPs

This threat demonstrates several techniques of the MITRE ATT&CK framework, most notably:

- Line Runner persistence mechanism (T1037),
- The reboot action via CVE-2024-20353 (T1653),
- Base64 obfuscation (T1140),
- Hooking of the processHostScanReply() function (T0874),
- Disabling syslog and tampering with AAA (T1562-001),
- Injection of code into AAA and Crash Dump processes (T1055)
- Execution of CLI commands (T1059),
- Bypassing of the AAA mechanism (T1556),
- Removal of files after execution (T1070-004),
- HTTP interception for C2 communications (T1557),
- HTTP C2 (T1071-001),
- HTTP C2 one-way backdoor (T1102-003),
- Data exfiltration over C2 (T1041),
- Network sniffing (T1040)

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
N/A	N/A	N/A	✓
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
N/A	N/A	✓	N/A

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Umbrella, Cisco's secure internet gateway (SIG) blocks devices from connecting to malicious IPs. Sign up for a free trial of Umbrella here.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. Snort SIDs for this threat are 45575, 62949 and 63139.

Indicators of Compromise (IOCs)

There are several known indicators of compromise that defenders can look for when assessing whether their ASA device has been compromised as a result of this attack, as outlined earlier in this post. For example, if any gaps in logging or any recent unexpected reboots are observed, this should be treated as suspicious activity that warrants further investigation. Also, below is a list of IP addresses we identified as having been used by UAT4356. Please note that some of these IPs are part of publicly known anonymization infrastructure and not directly controlled by the attackers themselves. If your organization does find connections to the provided actor IPs and the crash dump functionality has been altered, please open a case with Cisco TAC.

Likely Actor-Controlled Infrastructure:

192.36.57[.]181
185.167.60[.]85
185.227.111[.]17
176.31.18[.]153
172.105.90[.]154
185.244.210[.]120
45.86.163[.]224
172.105.94[.]93
213.156.138[.]77
89.44.198[.]189
45.77.52[.]253
103.114.200[.]230
212.193.2[.]48
51.15.145[.]37
89.44.198[.]196
131.196.252[.]148
213.156.138[.]78
121.227.168[.]69
213.156.138[.]68
194.4.49[.]6
185.244.210[.]65
216.238.75[.]155

Multi-Tenant Infrastructure:

5.183.95[.]95
45.63.119[.]131
45.76.118[.]87
45.77.54[.]14
45.86.163[.]244
45.128.134[.]189
89.44.198[.]16
96.44.159[.]46
103.20.222[.]218
103.27.132[.]69
103.51.140[.]101
103.119.3[.]230
103.125.218[.]198

104.156.232[.]22
107.148.19[.]88
107.172.16[.]208
107.173.140[.]111
121.37.174[.]139
139.162.135[.]12
149.28.166[.]244
152.70.83[.]47
154.22.235[.]13
154.22.235[.]17
154.39.142[.]47
172.233.245[.]241
185.123.101[.]250
192.210.137[.]35
194.32.78[.]183
205.234.232[.]196
207.148.74[.]250
216.155.157[.]136
216.238.66[.]251
216.238.71[.]49
216.238.72[.]201
216.238.74[.]95
216.238.81[.]149
216.238.85[.]220
216.238.86[.]24

Acknowledgments

Cisco would like to thank the following organizations for supporting this investigation:

- Australian Signals Directorate’s Australian Cyber Security Centre
- Black Lotus Labs at Lumen Technologies
- Canadian Centre for Cyber Security, a part of the Communications Security Establishment
- Microsoft Threat Intelligence Center
- The UK's National Cyber Security Centre (NCSC)
- U.S. Cybersecurity & Infrastructure Security Agency (CISA)