UAT-7290 targets high value telecommunications infrastructure in South Asia

By Asheer Malhotra

Published: 2026-01-08 · Archived: 2026-04-05 15:27:27 UTC

Thursday, January 8, 2026 06:00

- Cisco Talos is disclosing a sophisticated threat actor we track as UAT-7290, who has been active since at least 2022.
- UAT-7290 is tasked with gaining initial access as well as conducting espionage focused intrusions against critical infrastructure entities in South Asia.
- UAT-7290's arsenal includes a malware family consisting of implants we call RushDrop, DriveSwitch, and SilentRaid.
- Our findings indicate that UAT-7290 conducts extensive technical reconnaissance of target organizations before carrying out intrusions.

Talos assesses with high confidence that UAT-7290 is a sophisticated threat actor falling under the China-nexus of Advanced Persistent Threat actors (APTs). UAT-7290 primarily targets telecommunications providers in South Asia. However, in recent months we have also seen UAT-7290 expand their targeting into Southeastern Europe.

In addition to conducting espionage focused attacks where UAT-7290 burrows deep inside a victim enterprise’s network infrastructure, their tactics, techniques and procedures (TTPs) and tooling suggests that this actor also establishes Operational Relay Box (ORBs) nodes. The ORB infrastructure may then be used by other China-nexus actors in their malicious operations, signifying UAT-7290's dual role as an espionage motivated threat actor as well as an initial access group.

Active since at least 2022, UAT-7290 has an expansive arsenal of tooling, including open-source malware, custom developed malware, and payloads for 1-day vulnerabilities in popular edge networking products. UAT-7290 primarily leverages a Linux based malware suite but may also utilize Windows based bespoke implants such as RedLeaves or Shadowpad commonly linked to China-nexus threat actors.

Our findings suggest that the threat actor conducts extensive reconnaissance of target organizations before carrying out intrusions. UAT-7290 leverages one-day exploits and target-specific SSH brute force to compromise public facing edge devices to gain initial access and escalate privileges on compromised systems. The actor appears to rely on publicly available proof-of-concept exploit code as opposed to developing their own.

UAT-7290 shares overlapping TTPs with known China-nexus adversaries, including the exploitation of high-profile vulnerabilities in networking devices, use of open-source web shells for persistence, leveraging UDP listeners, and using compromised infrastructure to facilitate operations.

Specifically, we have observed technical indicators that overlap with RedLeaves, a malware family attributed to APT10 (a.k.a. MenuPass, POTASSIUM and Purple Typhoon), as well as infrastructure associated with ShadowPad, a malware family used by a variety of China-nexus adversaries.

Additionally, UAT-7290 shares a significant amount of overlap in victimology, infrastructure, and tooling with a group publicly reported by Recorded Future as Red Foxtrot. In a 2021 report, Recorded Future linked Red Foxtrot to Chinese People's Liberation Army (PLA) Unit 69010.

UAT-7290's malware arsenal for edge devices

Talos currently tracks the Linux-based malware families associated with UAT-7290 in this intrusion as:

- RushDrop – The dropper that kickstarts the infection chain. RushDrop is also known as ChronosRAT.
- DriveSwitch – A peripheral malware used to execute the main implant on the infected system.
- SilentRaid – The main implant in the intrusion meant to establish persistent access to compromised endpoints. It communicates with its command-and-control server (C2) and carries out tasks defined in the malware. SilentRaid is also known as MystRodX.

Another malware implanted on compromised devices by UAT-7290 is Bulbature. Bulbature, first disclosed by Sekoia in late 2024, is an implant that is used to convert compromised devices into ORBs.

RushDrop and DriveSwitch

RushDrop is a malware dropper that consists of three binaries encoded and embedded within it. RushDrop first makes rudimentary checks to ensure it is running on a legitimate system instead of a sandbox.

```
if ( (unsigned __int8)vm_checks() )
{
  remove_file_or_folder(*(char **)self_name);
  return 0;
}
```

Figure 1. RushDrop deleting itself if VM checks fail.

Then it either checks for the existence of, or creates a folder called ".pkgdb" in the current working directory of the dropper. RushDrop then decodes and drops three binaries to the ".pkgdb" folder:

- "daytime" - A malware family that simply executes a file called "chargen" from the current working directory. This executor is being tracked as DriveSwitch.
- "chargen" - The central implant of the infection chain, tracked as SilentRaid. SilentRaid communicates with its C2 server, usually in the form of a domain and can carry out action as instructed by the C2.
- "busybox" - Busybox is a legitimate Linux utility that can be used to execute arbitrary commands on the system.

```
    if ( find_or_mkdir_pkgdb() < 0 || write_files_to_pkgdb() < 0 )
    {
LABEL_10:
      delete_file_or_folder(*(char **)self_name);
      return 0;
    }
    else
    {
      sleep(100);
      delete_file_or_folder(*(char **)self_name);
      cleanup_dlog_clog_files();
      p_execve_daytime();
      return 0;
    }
```

Figure 2. RushDrop setting up files on disk.

DriveSwitch simply executes the SilentRaid malware on the system.

```
mov     dword ptr [esp+8], 0 ; char
mov     dword ptr [esp+4], offset a_chargen ; <path_to_chargen>
mov     [esp], ebx      ; file
call    p_sys_execve
```

Figure 3. DriveSwitch executing SilentRaid.

SilentRaid: The multifunctional malware

SilentRaid is a malware written in C++ and consists of multiple functionalities, written in the form of “plugins” embedded in the malware. On execution, it does certain rudimentary anti-VM and analysis checks to ensure it isn’t running in a sandbox. Then the malware simply initializes its “plugins” and contacts the C2 server for instructions to carry out malicious tasks on the infected endpoint. The plugins are built in functionalities, but modular enough to enable the threat actor to stitch together a combination of them during compilation.

Plugin: my_socks_mgr

This plugin handles communication to C2 server. It obtains the C2 IP by resolving a domain using “8[.]8[.]8[.]8” and passes commands received from the C2 to the appropriate plugin.

Plugin:my_rsh

This plugin opens a remote shell by executing “sh” either via either “busybox” or “/bin/sh”. This remote shell is then used to run arbitrary commands on the infected system.

```
mov     byte ptr [edi+edx], 2Fh ; '/'
mov     [esp+210Ch+readfds], offset a_busybox_0
mov     [esp+210Ch+file], eax
call    sub_80ABE3D
mov     [esp+210Ch+readfds], 0
mov     [esp+210Ch+file], edi
call    sys_access
test    eax, eax
jnz     short loc_8055CE6
mov     eax, [esp+210Ch+var_20F4]
mov     [esp+210Ch+except_fds], 0
mov     [esp+210Ch+writefds], offset a_sh_0 ; char
mov     [esp+210Ch+readfds], offset a_busybox_0 ;
mov     [esp+210Ch+file], eax ; file
call    p_sys_execve
jmp     loc_8055C1C
-------------------------------------------------

                        ; CODE XREF: open_sh_termi
mov     [esp+210Ch+writefds], 0 ; char
mov     [esp+210Ch+readfds], offset a_sh ; int
mov     [esp+210Ch+file], offset a_bin_sh ; file
call    p_sys_execve
```

Plugin:port_fwd_mgr

This plugin sets up port forwarding between ports specified — a local port and a port on a remote server. It can also set up port forwarding across multiple ports.

Plugin:my_file_mgr

This is the file manager of the backdoor. It allows the SilentRaid to:

- Read contents of “/etc/passwd”
- Execute a specified file on the system
- Archive directories specified by the C2 using “tar -cvf” - executed via busybox
- Check if a file is accessible
- Remove a file or directory using the “rm” command - via busybox
- Read/write a specified file

SilentRaid can also parse thru x509 certificates and collect attribute information such as:

- id-at-dnQualifier | Distinguished Name qualifier
- id-at-pseudonym | Pseudonym

- id-domainComponent | Domain component
- id-at-uniqueIdentifier | Unique Identifier

Bulbature

The Bulbature malware discovered consisted of the same string encoding scheme as the other UAT-7290's malware illustrated earlier. Usually UPX compressed, Bulbature can bind to and listen to either a random port of its choosing or one specified via command line via the "-d <port_number>" switch.

Bulbature obtains the local network interface's name by executing the command:

```
cat /proc/net/route | awk '{print $1,$2}' | awk '/00000000/ {print $1}'
```

It also obtains basic system information and the current user using the command:

```
echo $(whoami) $(uname -nrm)
```

The malware typically records its C2 address in a config file in the /tmp directory. The file will have the same name as the malware binary with the ".cfg" extension appended to it. The C2 address may be an encoded string.

Bulbature can obtain additional or new C2 addresses from the current C2 and can switch over communications with them instead. The malware can open up a reverse shell with its C2 to execute arbitrary commands on the infected system.

A recent variant of Bulbature contained an embedded self-signed certificate that it used for communicating with the C2. This certificate matches the one from the sample disclosed by Sekoia as well:

```
509 Certificate:
Version: 3
Serial Number: 81bab2934ee32534
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
    Algorithm Parameters:
    05 00
Issuer:
    O=Internet Widgits Pty Ltd
    S=Some-State
    C=AU
  Name Hash(sha1): d398f76c7ba0bbf79b1cac0620cdf4b42e505195
  Name Hash(md5): 4a963519b4950845a8d76668d4d7dd29

NotBefore: 8/8/2019 3:33 AM
NotAfter: 12/24/2046 3:33 AM

Subject:
```

```
    O=Internet Widgits Pty Ltd
    S=Some-State
    C=AU
  Name Hash(sha1): d398f76c7ba0bbf79b1cac0620cdf4b42e505195
  Name Hash(md5): 4a963519b4950845a8d76668d4d7dd29

Cert Hash(sha256): 918fb8af4998393f5195bafaead7c9ba28d8f9fb0853d5c2d75f10e35be8015a
```

Censys data shows that this certificate, with the exact Serial number, is present on at least 141 hosts, all either located in China or Hong Kong. On Virus Total, many of the IPs identified hosting this certificate are associated with other malware typically associated with China-nexus of threat actors such as SuperShell, GobRAT, Cobalt Strike, etc.

Coverage

The following ClamAV signatures detect and block this threat:

- Unix.Dropper.Agent
- Unix.Malware.Agent
- Unix.Packed.Agent

The following Snort Rule (SIDs) detects and blocks this threat: 65124

IOCs

723c1e59accbb781856a8407f1e64f36038e324d3f0bdb606d35c359ade08200

59568d0e2da98bad46f0e3165bcf8adadbf724d617ccebcfdaeafbb097b81596

961ac6942c41c959be471bd7eea6e708f3222a8a607b51d59063d5c58c54a38d

---