UAT-7290 Exploits Public-Facing Edge Devices to Target Telecommunications in South Asia

Original report published on: Jan 8, 2026[Error! Reference source not found.]

Executive Summary

Cisco Talos has identified a threat actor, **UAT-7290**, active since at least 2022 and primarily targeting telecommunications providers in South Asia, with recent expansion into Europe. The group conducts espionage-focused intrusions into critical infrastructure while simultaneously building Operational Relay Box (ORB) networks[2] that other threat actors use to conduct their own operations. Talos assesses with high confidence that UAT-7290 is a state-sponsored threat actor based on strong technical and behavioural links.

Background

The group shares significant overlap in victimology, tooling and infrastructure with Red Foxtrot, a threat cluster previously reported by Recorded Future. Additional technical indicators align with APT10 (also known as MenuPass, POTASSIUM, and Purple Typhoon), an espionage actor with a known history of targeting telecommunications and managed service providers globally.

Beyond espionage, UAT-7290 establishes ORB infrastructure on compromised devices. The ORB infrastructure serves as an anonymised relay nodes for command-and-control (C2) communications and has been observed being reused by other threat actors in separate operations.

Initial access is obtained through two primary methods. First, the exploitation of one-day vulnerabilities and second, target-specific SSH brute-force attacks.

UAT-7290 operates a Linux-based malware suite specifically engineered for edge network devices. The malware chain is modular and designed with sandbox-evasion and anti-analysis capabilities built in.

RushDrop (also known as ChronosRAT)

RushDrop is the initial-stage dropper that kickstarts the infection chain. Key behaviours include:

- Performs anti-VM and sandbox-evasion checks on execution. If the checks fail, it deletes itself from disk to prevent analysis.
- Creates a hidden directory named ".pkgdb" in the working directory and decodes three embedded binaries into it: "daytime" (DriveSwitch), "chargen" (SilentRaid), and "busybox" (a legitimate Linux utility weaponised for arbitrary command execution).
- Deletes itself after deployment to reduce forensic artefacts.

DriveSwitch

DriveSwitch is a peripheral component whose sole function is to execute the SilentRaid implant ("chargen") on the infected system.

SilentRaid (also known as MystRodX)

Written in C++, it is built around a modular plugin architecture that enables the threat actor to compose a tailored capability set at compile time. Key capabilities include:

- Anti-VM and anti-analysis checks on startup.

- Plugin: my_socks_mgr — Manages C2 communications. Resolves the C2 IP address using an octet-formatted domain pattern ("8[.]8[.]8[.]8" style) and routes operator commands to the appropriate plugin.
- Plugin: my_rsh — Opens a remote shell by executing "sh" via either busybox or "/bin/sh", enabling arbitrary remote command execution on the compromised system.
- Additional capability plugins for file operations, port forwarding, and network monitoring may be deployed based on operational requirements.
- C2 address is stored in an encoded configuration file in the /tmp directory, with the same filename as the malware binary and a ".cfg" extension appended.

Bulbature

Bulbature is an additional implant deployed on compromised devices for the specific purpose of converting them into Operational Relay Boxes (ORBs). Key characteristics:

- Records its C2 address in a config file in /tmp directory.
- Can obtain new or additional C2 addresses from the current C2 server and dynamically switch communications.
- Opens a reverse shell with C2 to execute arbitrary commands.
- A recent variant embeds a self-signed certificate for encrypted C2 communications.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the UAT-7290-related activities identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Search for hidden directories in edge devices named “.pkgdb” that contain ELF binaries named “daytime”, “chargen”, and/or busybox co-located within the same directory. Flag any instance where these three filenames coexist in a non-standard path such as /tmp/, /var/tmp/, or a web-accessible directory, regardless of file permissions.
- Hunt for the command string *cat /proc/net/route | awk '{print $1,$2}' | awk '/00000000/ {print $1}'* in process execution logs on edge devices via auditd or equivalent. Review any instance where this awk chain is spawned by an unexpected parent process
- Log and alert on any unexpected UDP listener processes on edge devices.
- Review SSH authentication logs on all externally exposed edge devices for (1) evidence of brute-force attempts leading to successful login, (2) reconciliation of successful privileged account logins against authorised access requests
- Restrict SSH, telnet access to edge devices or use source IP allowlisting.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise [Error! Reference source not found.]

SHA256 Hash
723c1e59accbb781856a8407f1e64f36038e324d3f0bdb606d35c359ade08200
59568d0e2da98bad46f0e3165bcf8adadbf724d617ccebcfdaeafbb097b81596
961ac6942c41c959be471bd7eea6e708f3222a8a607b51d59063d5c58c54a38d

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Privilege Escalation	T1078.003	Valid Accounts: Local Accounts
Credential Access	T1552.001	Unsecured Credentials: Credentials In Files
Discovery	T1083	File and Directory Discovery
Command and Control	T1071.001	Application Layer Protocol: Web Protocols

References

1. UAT-7290 targets high value telecommunications infrastructure in South Asia
2. An operational relay box (ORB) network is a traffic relay system, generally composed of a mix of compromised devices and leased servers – used to obfuscate the origin and destination of malicious traffic. While similar to botnets, ORBs are used by state-nexus targeted intrusion actors and display unique characteristics.