ADVISORY FOR ICM SECTOR

ApolloNode RAT observed in Telecom environments

Original report published on: March 02, 2026

Executive Summary

In early 2026, CrowdStrike observed ApolloNode, a low-prevalence remote access tool (RAT) deployed in various South Asian telecommunications providers. Since June 2025, ApolloNode has been detected in Linux-based systems within telecom environments: providing remote shell access, file system manipulation and network traffic relay capabilities. These capabilities allow a Threat Actor (TA) to maintain access to isolated systems and enable lateral movement across compromised networks. The deployment of ApolloNode is assessed as consistent with a long-term intrusion capability focused on maintaining persistent access within targeted environments.

Background

Between January and February 2026, ApolloNode variants were observed on Linux servers within South Asian telecom providers. To establish persistence, the malware adds an entry containing the command nohup /usr/bin/vnxf & to the host's /etc/rc.local file, while in other instances, ApolloNode is launched via /usr/sbin/ssl_update or located in the same directory. The malware leverages Secure WebSockets (SWS) for command-and-control (C2) communications and was observed to use Cloudflare CDN infrastructure to evade detection.

CrowdStrike attributed this activity to HORDE PANDA with low confidence, based on observed overlaps in malware code, techniques and victimology. This TA has historically targeted telecommunications organisations in South Asia and demonstrated a consistent interest in maintaining covert access to strategic telecommunications networks. The observed activity is consistent with espionage-oriented intelligence collection objectives, with no indication of disruptive or destructive intent.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the ApolloNode RAT activity 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.
- Enforce strict network segmentation and restrict unnecessary outbound connectivity to reduce the risk of command-and-control relay and proxy-based communication.
- Enforce least privileged access and monitor usage of privileged or service accounts, validate that activity is legitimate and remove accounts that are no longer required.
- Improve detection of persistence mechanisms such as modifications to system startup files (e.g., /etc/rc.local), cron jobs, and system-level service abuse on Linux hosts.
- Strengthen monitoring of lateral movement involving Linux-to-Windows interactions, including unexpected RDP sessions initiated from internal Linux systems.
- Extend XDR, improve network visibility via regular scans of new systems and deploy EDR, where possible

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

SHA256 Hash	Description
024384f03caf5d92ce8d08951868517c608bd7fd6e17866f046bf836e3683814	ApolloNode version
f9e54b1c33fea58e6cbdd61503f3f6d979d7d0b262dfcc4387e45e9180e2ea0e	ApolloNode version
1096e35b5757e4014d578bbbdea096b53c465aee2c16bafaf590c6f83c500b9c	Unidentified backdoor

Domain	Description
logs[.]opinioncraftnow[.]com	ApolloNode C2
ssl[.]wiseopx[.]com	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Resource Development	T1583.001	Acquire Infrastructure: Domains
	T1583.006	Acquire Infrastructure: Web Services
	T1587.001	Develop Capabilities: Malware
	T1585	Establish Accounts
Persistence	T1037.004	Boot or Logon Initialization Scripts: RC Scripts
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
Command and Control	T1090.004	Proxy: Domain Fronting