Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

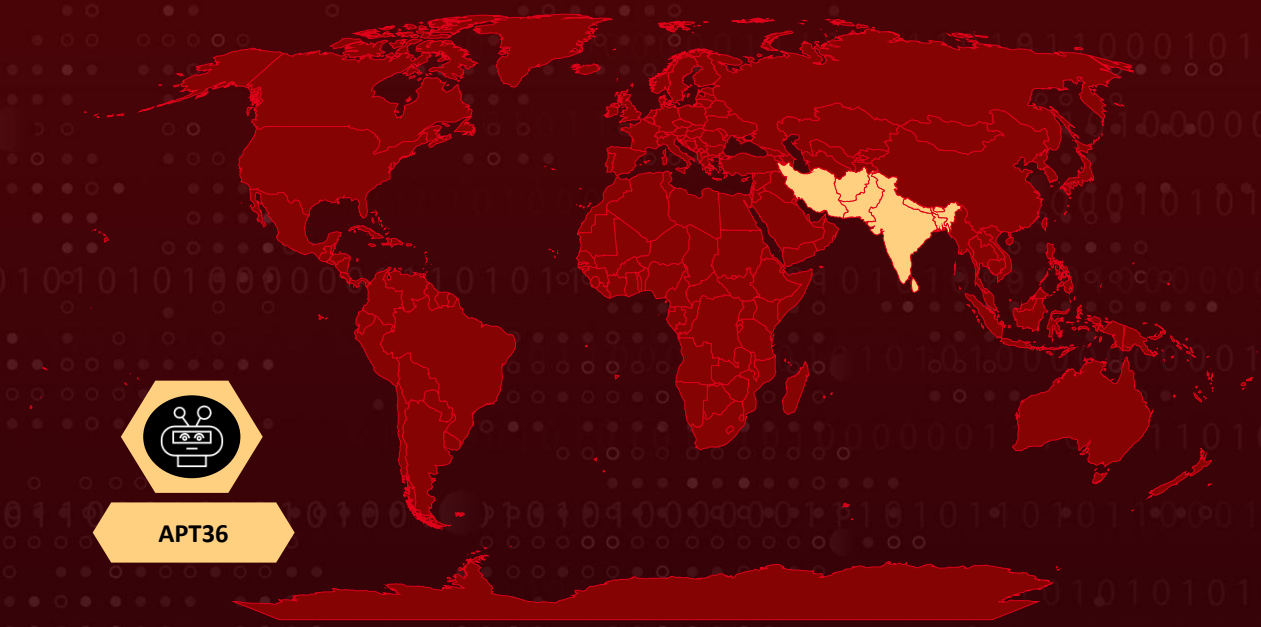
PATCHCORD Cluster Targets South Asian Infrastructure

Date of Publication	Admiralty Code	TA Number
August 14, 2026	A2	TA2026234

Summary

First Seen: 2025
Targeted Regions: Afghanistan, India, South Asia
Targeted Platforms: Windows (primary); Linux via internet-facing OpenSSH; network devices and iOS/mobile targets indicated
Targeted Industries: Telecommunications, Government, Defense, Energy, Critical Infrastructure
Threat Actor: APT36 (alias Transparent Tribe, ProjectM, TEMP.Lapis, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco)
Malware: PATCHCORD, SHEETCORD, HACKERAI C2 Agent
Attack: An espionage operation is delivering three custom backdoors via sector-specific lures, including a fake Afghan Telecom VPN, transport-management installers, and a spoofed Indian National Informatics Centre portal. PATCHCORD, a C/C++ implant, hijacks browser shortcuts for persistence, fingerprints the host, and beacons to a hardcoded server for tasking such as in-memory shellcode execution and remote command execution. Two related implants extend the toolkit: SHEETCORD abuses the Google Sheets API for command-and-control, and HACKERAI C2 Agent abuses GitHub Gists. A staging server also held exploit tooling for CVE-2024-6387 (regreSSHion), suggesting the operator pursues network-level access to internet-facing telecom and government infrastructure before deploying endpoint implants.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-6387	regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)	OpenSSH server	✗	✗	✓

Attack Details

#1

An ongoing espionage campaign is targeting Afghan telecom providers and South Asian critical infrastructure organizations with three previously undocumented backdoors, each delivered through lures tailored to the victim's sector. Afghan telecom targets receive fake VPN installers and a bogus telecom management tool impersonating Afghan Telecom, packaged inside ZIP archives carrying an Inno Setup installer crafted to look genuine, down to the publisher's name and a link to the real Afghan Telecom portal. Indian government targets are lured by a spoofed National Informatics Centre site that serves a fake employee-benefits update. In parallel, a staging server holds exploit tooling for CVE-2024-6387, the OpenSSH flaw known as regreSSHion, alongside brute-forcing utilities. That vulnerability is a signal-handler race condition in OpenSSH's server (sshd), a regression of an older 2006 bug, which can let an unauthenticated remote attacker who fails to complete login within the grace period execute code on the host; it carries a high-severity CVSS 8.1 rating. Its presence points to a second route in: breaking into internet-facing telecom and government systems to gain a network-level foothold before any endpoint implant is dropped.

#2

Once the installer runs, it launches PATCHCORD, which hides its console window and establishes persistence by hijacking browser shortcuts, backing up each original and rewriting it so the implant runs first and then silently launches the real browser. It also writes its path to a registry Run key to survive reboots, fingerprints the host, registers with its server, and polls for commands. Tasking lets the operator adjust the check-in interval, list processes, run shell commands, and decode and run shellcode entirely in memory so nothing touches disk. The Go-based SHEETCORD extends the same shortcut hijacking to six browsers, runs commands through PowerShell, and adds a startup-folder script, while the AI-assisted HACKERAI C2 Agent reuses the same fingerprinting and persistence with its own channel.

#3

To widen access, the operator favors credential theft over noisy exploitation. The staging server held an open-source browser credential-harvesting tool tied to this actor's past operations, alongside brute-forcing artifacts, indicating it collects stored logins and hammers exposed services for valid credentials. The regreSSHion tooling signals intent to compromise network-facing infrastructure directly, opening movement into telecom and government environments beyond the initial endpoint. PATCHCORD also checks for elevated privileges before altering shortcuts, showing awareness of its privilege context.

#4

For getting data out, each implant uses a different channel to blend into normal traffic. PATCHCORD encodes command output with a custom scheme and posts it to its own server over HTTP on a non-standard port. SHEETCORD reads and writes per-victim tabs in a Google spreadsheet, turning a legitimate cloud service into a two-way control and exfiltration path, while HACKERAI C2 Agent uses GitHub Gists with dedicated upload and download routines. Router and session backups and an apparent iOS call-history database recovered from the staging server suggest the operator has also pulled data from network devices and mobile targets, not just Windows machines. Taken together, the focus on Afghan and Indian telecom, government, and defense entities, the SHEETCREEP-style Google Sheets C2, and toolkit overlaps such as GateSentinel and HackBrowserData point to APT36, also known as Transparent Tribe, a Pakistan-aligned espionage group assessed with moderate confidence to be behind the campaign.

Recommendations

Patch OpenSSH Against regreSSHion: Update all internet-facing OpenSSH servers to version 9.8/9.8p1 or later to close CVE-2024-6387, and restart the sshd service after upgrading so the fix takes effect. Prioritize telecom and government-facing hosts that are directly exposed to the internet.

Block Known C2 Infrastructure: Block the command-and-control IP 46[.]30[.]188[.]13 and every listed impersonation domain at the firewall, proxy, and DNS resolver. Raise alerts on outbound TCP/8080 connections to unfamiliar external hosts, which matches this actor's C2 pattern.

Hunt for Browser Shortcut Hijacking: Inspect browser .lnk shortcuts for targets that point to a non-browser executable while passing the real browser path as an argument, and search for shortcut copies ending in .backup, both of which are direct signs of PATCHCORD or SHEETCORD persistence.

Monitor Suspicious Run Keys and Startup Entries: Alert on registry Run values named BeaconBrowserHijack and SystemHelper under HKCU, and on the presence of SystemHelper.vbs in the user Startup folder, as these are the actor's persistence footholds.

Restrict Abuse of Legitimate Cloud Services: Monitor endpoints for programmatic traffic to the Google Sheets API and GitHub Gists that does not match normal user behavior, since these services double as C2 and exfiltration channels for SHEETCORD and HACKERAI C2 Agent.

Rotate Potentially Exposed Credentials: Reset credentials on any host where browser credential harvesting or brute-forcing may have occurred, and enforce multi-factor authentication on remote-access and administrative services.

Enforce Network Segmentation: Separate internet-facing telecom and government infrastructure from internal endpoints and management networks to limit how far an attacker can move after exploiting an exposed service.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1583: Acquire Infrastructure	T1583.006: Web Services
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
	T1190: Exploit Public-Facing Application	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell
		T1059.005: Visual Basic
	T1620: Reflective Code Loading	

Tactic	Technique	Sub-technique
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
Defense Evasion	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1622: Debugger Evasion	
	T1140: Deobfuscate/Decode Information	
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
Credential Access	T1555: Credentials from Password Stores	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1571: Non-Standard Port	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	cf7184c0dfe882dc6e3016f16e4ede32b75d7648f83d6f4f87eb6a703be7b8d6, 1774e15e8eb96eb89bc03cb4768fc0620e10c09c5f795297f36dcc2aa5d9dd94, ea0934472121848b80455581d289ce4480b1e5cc05678c1b90ecfc465b5ec350, 5e17360d32e9b272bb7e1b97c8e4dca34622ec9ce08fd240fe2758cc3f67dc4a, 378484112b4e837d3850b5b0802fc509202c232bb124d6944a59fe66525ba668, b56fab5a6834c51d85787e7c1177720dfba5a5823763f3fcf432196cd2a1bdf3, 2323b55ea743c813e48689318e8ed54ae838cf9e8a2adbfc2488ea8a36dd0126, 2eddfebb3f7419af27493a6a3bb601372cf6c494da8df62640cce7f830b4a73b, d46ee94d6a27ff9f02cff6fb57780acac2833ce48c95e63042a6274e24a040bb, 50fc220347f9e281037e831c3755dc70a8ba7f663025aea35b301226918b016b, 0f4073d3c866bc3daf55b25f71250b96ec120db94a4f9cc8fe85b7c9f9d346b3, 959bbb09cd86ce3930406bf1cf32776ca477dfefe3fd63e90bf0017fccd90587, 74d347785dc47f8cda3876826cdd3fb3935ac55dc8e9e0c0f96d5ef4e00089a2
Domains	appstoore[.]solutions, www[.]appstoore[.]solutions, afghantelecom[.]site, afghanistanupdates[.]site, www[.]afghanistanupdates[.]site, caprispine[.]health, www[.]caprispine[.]health, servicesindia[.]services, www[.]servicesindia[.]services, zala-aer[.]info, www[.]zala-aer[.]info, nicservice[.]org, www[.]nicservice[.]org, nic-support[.]site, appstoore[.]duckdns[.]org, defence[.]cdga[.]site

TYPE	VALUE
IPv4	46[.]30[.]188[.]13
IPv4:Port	46[.]30[.]188[.]13[:]8080
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\BeaconBrowserHijack, HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SystemHelper
File Path	%APPDATA%\Microsoft\Windows\Star, Menu\Programs\Startup\SystemHelper.vbs

Patch Links

https://www.openssh.com/txt/release-9.8

https://www.openssh.org/releasenotes.html

References

https://www.acronis.com/en/tru/posts/patchcord-new-malware-cluster-targets-afghan-telecom-and-south-asian-critical-infrastructure/

https://www.hivepro.com/threat-advisory/regresshion-exploiting-signal-handler-race-condition-in-openssh

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 14, 2026 • 09:30 AM

More at www.hivepro.com