IMPORTANT CYBERSECURITY NEWS: OVER 70 ORGANIZATIONS ACROSS MULTIPLE SECTORS TARGETED BY CHINA-LINKED CYBER ESPIONAGE GROUP

Vairav Cyber Security News Report

Date: June 10, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Between July 2024 and March 2025, over 70 organizations across multiple industries—including cybersecurity, government, finance, manufacturing, telecommunications, and media were targeted in a China-linked cyber espionage campaign. The campaign involved reconnaissance and intrusion activities, most notably impacting SentinelOne's IT infrastructure. Security researchers attribute the operation to a cluster known as PurpleHaze, linked to APT groups like **APT15 and UNC5174**. This campaign is significant due to its wide reach, multiple industry targeting, and use of sophisticated backdoors, signaling a serious threat to global cybersecurity resilience

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The threat comprised reconnaissance and intrusions into diverse organizations. Attackers leveraged advanced tools like ShadowPad with ScatterBrain obfuscation, GoReShell reverse shells, and custom commands from The Hacker's Choice group—technique sets associated with Chinese-linked clusters PurpleHaze, APT15, and UNC5174.

Identification: SentinelOne detected the first reconnaissance activity in April/October 2024 targeting its internet-connectable servers. The full scope of the intrusions—spanning 70+ organizations—was revealed in a report published on June 9, 2025, by SentinelOne researchers Aleksandar Milenkoski and Tom Hegel.

Threat Actor: The campaign is attributed to China-nexus threat actors, specifically the **PurpleHaze** cluster, with observed overlap to **APT15 and UNC5174** (also known as Uteus), suggesting possible access brokering and shared infrastructure from China.

Affected Entities/Industries: Over 70 organizations including sectors such as:

- Cybersecurity
- Government bodies in South Asia
- European media companies

- Organizations involved in Manufacturing, Finance, Telecommunications, and logistics/IT services

Potential Impact:

- Espionage through data compromise
- Exposure of sensitive governmental or proprietary commercial information
- Reputational harm
- Groundwork for future disruptive operations

Exploitation Methods:

- ShadowPad deployment via vulnerability exploits (initial access is suspected via CVE-2024-8963 and CVE-2024-8190).
- GoReShell (SSH-based reverse shell) inserted into logistics and media orgs.
- Use of The Hacker's Choice toolset for lateral movement and privilege escalation.
- Heavy use of custom backdoors and C2 infrastructure operating from China.

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 103.248.61[.]36
- 107.173.111[.]26
- 128.199.124[.]136
- 142.93.212[.]42
- 142.93.214[.]219
- 143.244.137[.]54
- 45.13.199[.]209
- 65.38.120[.]110

Suspicious Domains

- cloud.trendav[.]co
- downloads.trendav[.]vip

- dscriy.chtq[.]net
- epp.navy[.]ddns[.]info
- mail.ccna[.]organiccrap[.]com
- mail.secmailbox[.]us
- network.oossafe[.]com
- news.imaginerjp[.]com
- notes.oossafe[.]com
- secmailbox[.]us
- sentinelxdr[.]us
- tatacom.duckdns[.]org
- trendav[.]vip
- updata.dsqurey[.]com

Malware Hashes (SHA1)

- 106248206f1c995a76058999ccd6a6d0f420461e
- 411180c89953ab5e0c59bd4b835eef740b550823
- 4896cfff334f846079174d3ea2d541eec72690a0
- 5ee4be6f82a16ebb1cf8f35481c88c2559e5e41a
- 7dabf87617d646a9ec3e135b5f0e5edae50cd3b9
- a31642046471ec138bb66271e365a01569ff8d7f
- a88f34c0b3a6df683bb89058f8e7a7d534698069
- aa6a9c25aff0e773d4189480171afcf7d0f69ad9
- c43b0006b3f7cd88d31aded8579830168a44ba79
- cb2d18fb91f0cd88e82cb36b614cfedf3e4ae49b
- cbe82e23f8920512b1cf56f3b5b0bca61ec137b9
- ebe6068e2161fe359a63007f9febea00399d7ef3
- f52e18b7c8417c7573125c0047adb32d8d813529

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Conduct threat hunting for ShadowPad and GoReShell artifacts.
- Scan influenced servers for indicators related to PurpleHaze, including ORB communication.
- Audit exposure of internet-facing infrastructure to unpatched vulnerabilities (particularly CVE-2024-8963 & 8190).

Security Best Practices

- Apply timely patching to public-facing systems.
- Restrict and monitor SSH access meticulously.
- Implement network segmentation and zero-trust policies.
- Employ EDR solutions capable of detecting obscure backdoors and abnormal PowerShell/Go binary execution.

For Advanced Security Teams

- Collaborate with external threat intel providers to obtain IOCs and TTP profiles for PurpleHaze, UNC5174, and APT15.
- Conduct comprehensive incident response drills for espionage-style intrusions.
- Look into C2 connectivity via ORB infrastructure in outbound traffic analytics.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/06/over-70-organizations-across-multiple.html
- https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com