Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

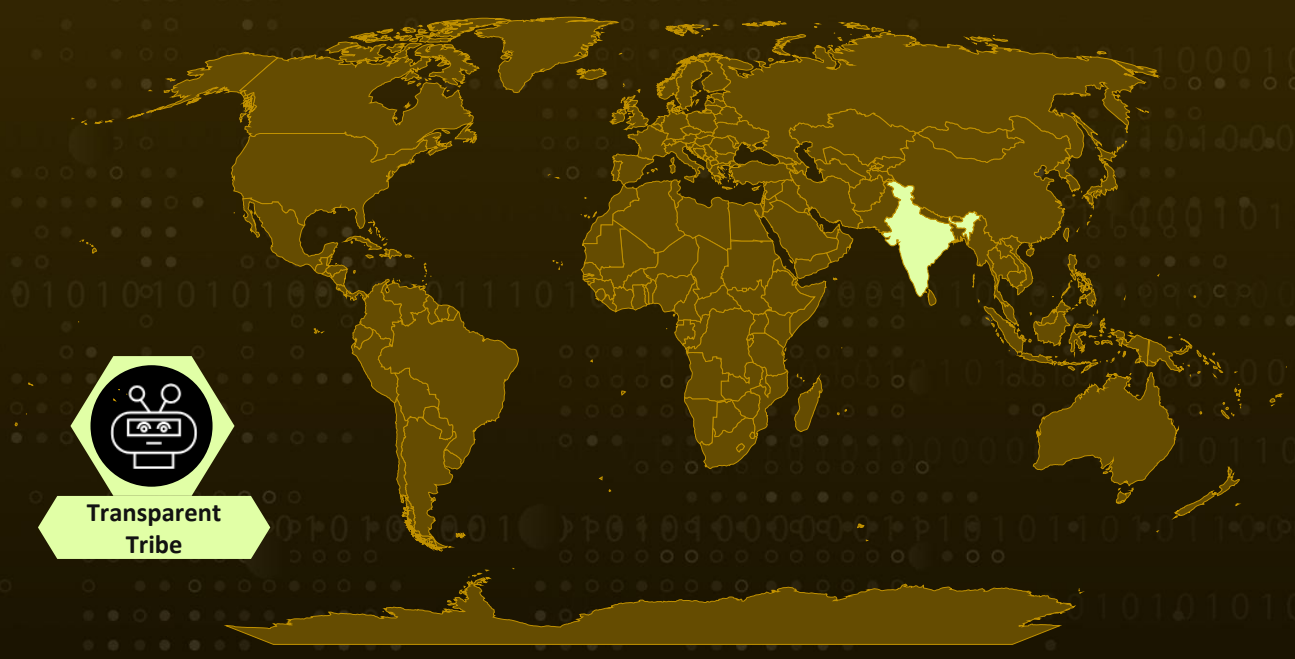
Transparent Tribe Targets India's Startup Ecosystem with Crimson RAT

Date of Publication	Admiralty Code	TA Number
February 06, 2026	A1	TA2026039

Summary

First Seen: February 2026
Targeted Region: India
Targeted Platforms: Windows
Targeted Industries: Startups, Technology, Government, Defense, Military, Education
Threat Actor: Transparent Tribe (also known as APT36, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, G0134))
Malware: Crimson RAT, GymRAT
Attack: Transparent Tribe (aka APT36) has expanded its cyber-espionage operations to target India's startup ecosystem, particularly cybersecurity and intelligence-adjacent organizations. The campaign uses tailored social engineering and malicious ISO files to bypass Windows security controls and deploy Crimson RAT. The activity is linked to previous Transparent Tribe operations and remains focused on strategic intelligence collection rather than financial gain.

Attack Regions



Attack Details

#1 Transparent Tribe (also tracked as APT36), a Pakistan-aligned threat group, has expanded its long-standing cyber-espionage operations by targeting India's rapidly growing startup ecosystem. This marks a notable shift from its traditional focus on government, military, and defense-related entities. The group has begun focusing on startups and professionals operating in cybersecurity, technology, and intelligence-adjacent domains, likely viewing them as indirect gateways to sensitive information, government collaborations, or strategic insights.

#2 The attack campaign relies heavily on tailored social engineering, using lures themed around startup culture, professional opportunities, or industry-specific documentation. Victims are typically delivered malicious container files, such as ISO images, which help bypass certain built-in Windows security mechanisms while appearing legitimate. Once opened, these files deploy malicious shortcut (LNK) launchers or staged executables that initiate the infection chain with minimal user interaction. Batch scripts observed in the campaign leverage PowerShell to remove Mark-of-the-Web protections, effectively suppressing SmartScreen warnings and other security prompts.

#3 At the core of the campaign is the deployment of Crimson RAT, a remote access trojan consistently associated with Transparent Tribe. The malware employs several anti-analysis techniques, including artificial on-disk file inflation to approximately 34MB through embedded junk data, despite the functional malicious payload being only 80–150KB in size. This approach helps evade file-size-based scanning and automated analysis environments. Crimson RAT also uses a custom TCP-based command-and-control protocol rather than standard HTTP/HTTPS, complicating network-level detection. Once active, the implant enables system reconnaissance, file exfiltration, remote command execution, and long-term persistence.

#4 Infrastructure reuse, malware code similarities, and consistent victimology allow this activity to be attributed to Transparent Tribe with high confidence. The command-and-control infrastructure overlaps with previous Transparent Tribe campaigns, including operations that deployed the GymRAT implant against Indian government-sector targets. While the lure themes and victim profile have evolved, the underlying motivation remains intelligence collection rather than financially motivated cybercrime. This campaign underscores how nation-state actors increasingly view startups as high-value intelligence targets, particularly when they operate at the intersection of innovation, security research, and government collaboration.

Recommendations

- **Block ISO File Attachments at Email Gateway:** Configure email security gateways to quarantine or block ISO, IMG, and other container-based file attachments, which are a primary delivery mechanism used by Transparent Tribe in this campaign.
- **Enforce Mark-of-the-Web Protections:** Ensure SmartScreen and MotW enforcement policies are active across endpoints, and monitor for PowerShell commands that attempt to strip Zone.Identifier alternate data streams from downloaded files.
- **Block Known C2 Infrastructure:** Add the identified C2 indicators to network-level blocklists across firewalls, proxies, and DNS filtering solutions to prevent communication with threat actor infrastructure.
- **Deploy Detection Rules for LNK-Based Execution Chains:** Create endpoint detection rules targeting execution patterns where LNK files invoke cmd.exe or %COMSPEC% to launch batch scripts, particularly with the /MIN flag to minimize the window, as this is a consistent TTP of this campaign.
- **Monitor for Anomalous TCP-Based C2 Traffic:** Since Crimson RAT uses a custom TCP protocol rather than HTTP/HTTPS for C2 communications, deploy network detection rules to identify non-standard TCP connections from endpoints to external IP addresses on uncommon ports.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell

Tactic	Technique	Sub-technique
Defense Evasion	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.002: Software Packing
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Persistence	T1547: Boot or Logon Autostart Execution	
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1016: System Network Configuration Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
Collection	T1113: Screen Capture	
	T1125: Video Capture	
	T1123: Audio Capture	
Command and Control	T1095: Non-Application Layer Protocol	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4570e3543a1877f38b21d2ad7825b43cc81bfb75ebfd5c693cf737461abef0e6, 94719581be164d57ce482f3759dbc40d772a6b469687b88036e3075cca784ea5, 1092761df305e910f806834fb774dfb09dc64a4d399d578a0d1bf1dd5daf0f98, 3fb89bc2d94530a1a3f9b237ece4993863f563a2d28b071b1e7d0ff9e61c5c1f
MD5	5c4488b4eda72d245dac5382f3587f09, 4976ef0054b0283c0d013be2f442e17b, 5b4a48815446cd40d8e141cbf8582296, 22218f19425b78dfd6a4f42e43f5486f, 47a55959c1eee2ea3a8885f8e08eb3ab
IPv4	93[.]127[.]133[.]9
Domains	Sharmaxme11[.]org, Certstorein[.]shop

References

https://www.acronis.com/en/tru/posts/new-year-new-sector-transparent-tribe-targets-indias-startup-ecosystem/

https://hivepro.com/threat-advisory/silent-clicks-lasting-access-apt36s-fileless-espionage-playbook/

Recent Breaches

https://sis.voldebug.in/

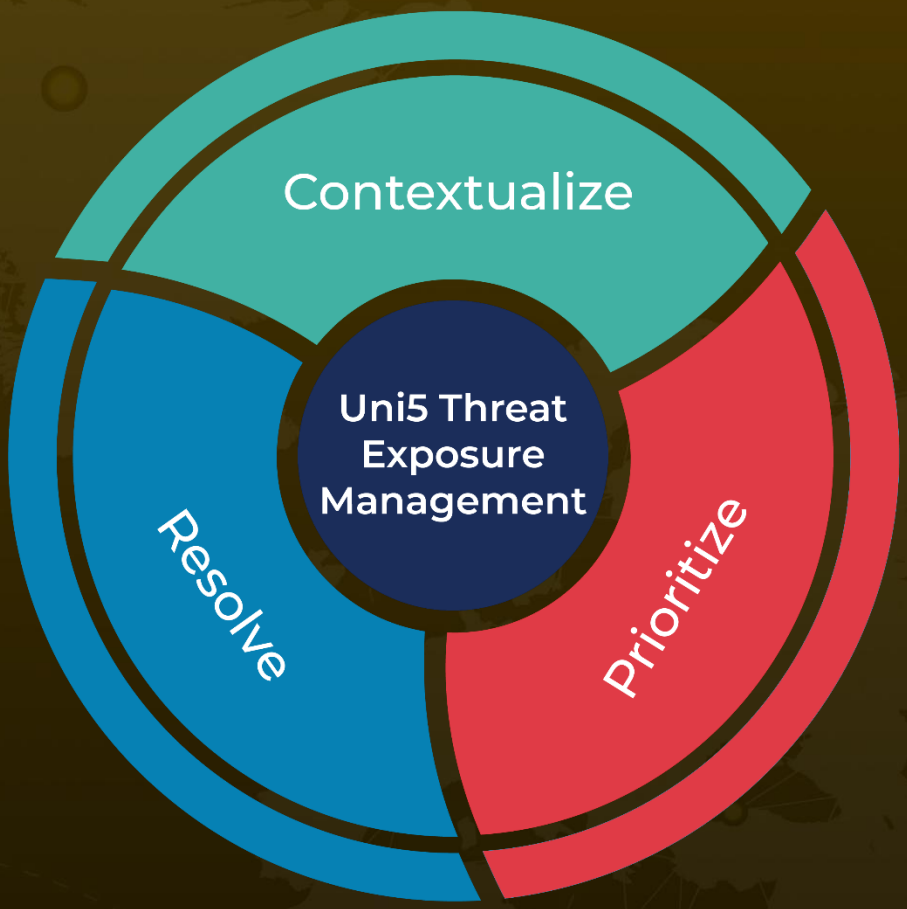
References

https://www.acronis.com/en/tru/posts/new-year-new-sector-transparent-tribe-targets-indias-startup-ecosystem/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 06, 2026 • 02:40 PM

More at www.hivepro.com