Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Transparent Tribe's DeskRAT Campaign Targets Indian Military Systems

Date of Publication

October 28, 2025

Admiralty Code

A1

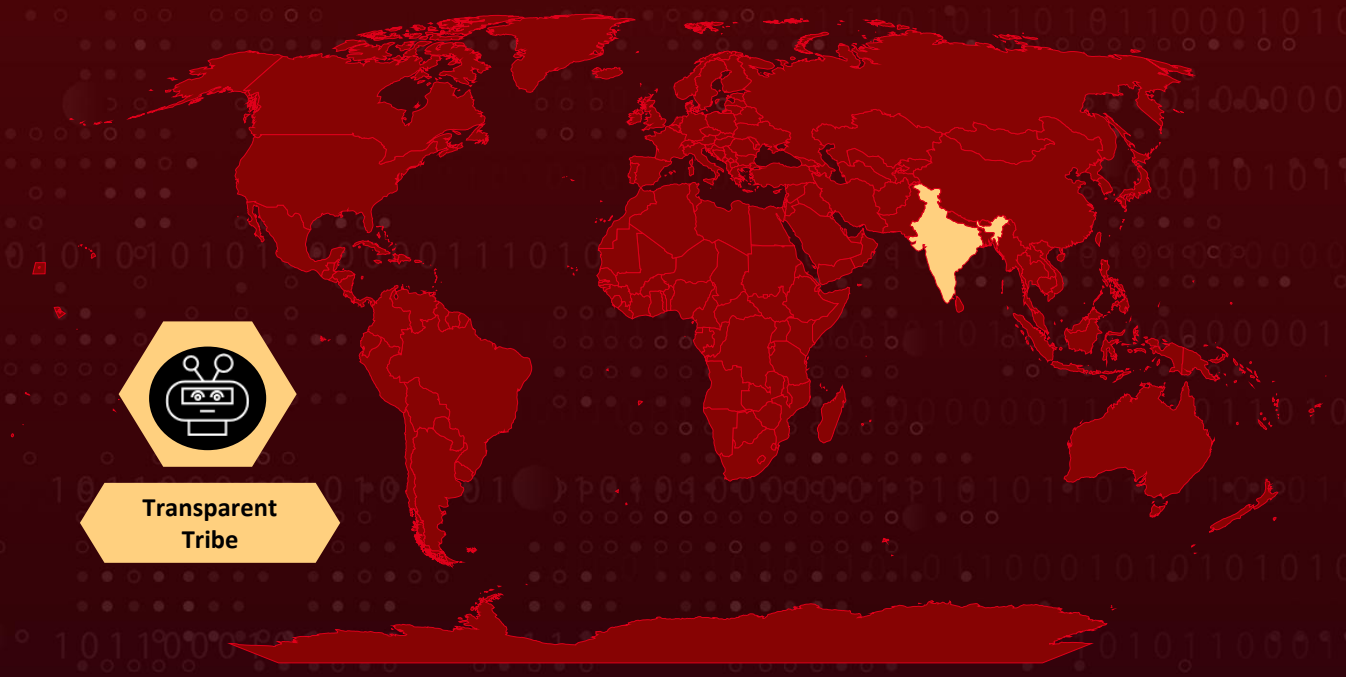
TA Number

TA2025327

Summary

First Seen: June 7, 2025
Targeted Country: India
Targeted Platform: Linux (Specifically BOSS distributions)
Malware: DeskRAT
Targeted Industries: Military, Defense, and Government Organizations
Threat Actor: Transparent Tribe (aka Mythic Leopard, APT36, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, C-Major)
Attack: Transparent Tribe (APT36), a Pakistan-linked group, recently targeted Indian military and government BOSS Linux systems via spear-phishing attacks delivering DeskRAT, a Golang-based RAT that achieves stealthy access, file exfiltration, and long-term persistence by chaining dropper scripts, decoy PDFs, and multiple Linux-specific startup methods; the campaign demonstrates strategic, persistent espionage intent using evolving social engineering lures and advanced cross-platform tooling.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

Transparent Tribe (APT36), a Pakistani-nexus espionage group, continues its targeted campaign against Indian military and government organizations as of October 2025. The group's latest activity involves a focused campaign deploying DeskRAT, a custom Golang-based Remote Access Trojan (RAT) specifically built to compromise Linux systems, notably those running the BOSS distribution favored by Indian governmental bodies. The attack exploits spear-phishing, with emails crafting lures around real-world defense incidents and civil unrest to appear credible and timely.

#2

Recent campaign updates reveal that Transparent Tribe has transitioned away from using legitimate cloud hosting for payloads, now relying on dedicated staging domains (such as modgovindia[.]space) to serve ZIP archives. These archives contain a malicious .desktop dropper file and a decoy PDF. Once executed, the dropper uses Bash one-liners and built-in utilities to fetch, decode, and launch DeskRAT, using evasion tactics to bypass cybersecurity controls in BOSS Linux. Notably, the infection process attempts to distract targets by opening a real-looking government document in Firefox, masking the malware deployment.

#3

DeskRAT establishes a WebSocket-based C2 channel, communicating with multiple hidden servers. Its initial beacon contains fake metadata and bogus Office/Chrome info to evade initial triage and fingerprinting. The RAT enables remote operators to browse directories, exfiltrate sensitive files under 100MB, and deploy additional payloads on compromised systems. DeskRAT supports four Linux-centric persistence mechanisms: systemd units, cron jobs, autostart desktop files, and bash startup scripts embedded in .bashrc. This resilience signals the group's intent for prolonged espionage access.

#4

The malware codebase shows evidence of LLM-assisted development, with numerous "dummy" or placeholder functions, complicating reverse engineering efforts. DeskRAT's design also leverages real-time geopolitical lures, such as directives linked to outbreaks of unrest in Ladakh and protest events in New Delhi, and targets military personnel with documents demanding fast operational responses. This reflects APT36's strategic focus on intelligence collection in defense sectors. The timing and targeting indicate a long-term espionage strategy supporting Pakistani national interests in the region.

Recommendations

Harden Linux System Defenses: Ensure all critical military and government BOSS Linux systems are fully updated and configured with a minimal attack surface. Remove unnecessary utilities (such as xxd if not required) and restrict execution permissions in user and temporary directories. This limits the ability of dropper scripts or malware binaries to run undetected.

Monitor and Block Spear-Phishing Vectors: Deploy advanced email filtering, attachment sandboxing, and URL reputation analysis to block phishing attempts that use themed lures or weaponized ZIP archives. Train personnel to identify suspicious communications, especially document-themed emails referencing defense activities or regional unrest.

Detect Suspicious .desktop and Startup Artifacts: Continuously hunt for unauthorized .desktop files, new executables in /tmp, modified .bashrc entries, and abnormal systemd or cron jobs. Use file integrity monitoring and EDR tools to detect DeskRAT's persistence mechanisms early and trigger automated alerts for remediation.

Inspect WebSocket Traffic and C2 Indicators: Monitor outbound network traffic for unexpected ws:// connections to unknown domains, particularly on port 8080. Review handshake logs and block any communication with known Transparent Tribe infrastructure. Maintain updated threat intelligence feeds to promptly identify new C2 or staging domains.

Strengthen Email and User Security Controls: As the infection begins with spear-phishing, tighten email gateway rules to block ZIP archives containing .desktop files or suspicious scripts. Implement robust attachment scanning and sandboxing, and conduct targeted awareness training for personnel handling defense-related communication. Reinforcing user vigilance is crucial to stopping the initial compromise vector.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0009 Collection
TA0011 Command and Control	T1566.001 Spearphishing Attachment	T1566 Phishing	T1204 User Execution
T1059.004 Unix Shell	T1059 Command and Scripting Interpreter	T1140 Deobfuscate/Decode Files or Information	T1204.002 Malicious File
T1543.003 Windows Service	T1547 Boot or Logon Autostart Execution	T1027 Obfuscated Files or Information	T1041 Exfiltration Over C2 Channel
T1082 System Information Discovery	T1005 Data from Local System	T1564.001 Hidden Files and Directories	T1564 Hide Artifacts

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	43715401531e0060827d3dcfd406add434829192051fe76d5ffdbb22602cc136, 567dfbe825e155691329d74d015db339e1e6db73b704b3246b3f015ffd9f0b33
MD5	4c56fedd177108a8849cec423f020625, 3563518ef8389c7c7ac2a80984a2c4cd
Domain	modgovindia[.]com
URLs	hxxps[://]modgovindia[.]com/download[.]php?file=Gimpfile[.]txt, hxxps[://]modgovindia[.]com/CDS_Directive_Armed_Forces[.]pdf

TYPE	VALUE
File name	MoM_regarding_Defence_Sectors_by_Secy_Defence_25_Sep_2025.zip, MoM_regarding_Defence_Sectors_by_Secy_Defence_25 Sep_2025.desktop,
IPv4	147[.]93[.]155[.]118
File path	/tmp/MoM_regarding_Defence_Sectors_by_Secy_Defence_25-Sep_2025-<timestamp>, $HOME/.config/autostart/system-backup.desktop, $HOME/.config/system-backup/startup.sh, $HOME/.config/system-backup/client.log

References

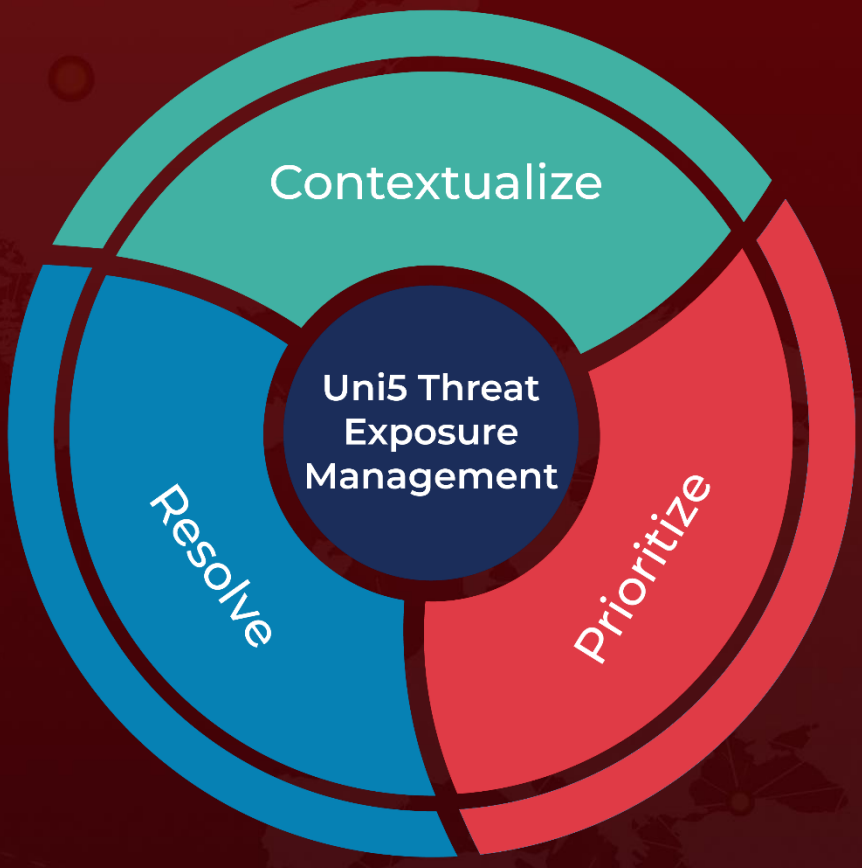
https://blog.sekoia.io/transparenttribe-targets-indian-military-organisations-with-deskrat/

https://hivepro.com/threat-advisory/apt36s-covert-linux-attack-on-indias-defense-sector/

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

October 28, 2025 . 7:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com