Transparent Tribe, APT 36 - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Transparent Tribe, APT 36

Names	Transparent Tribe *(Proofpoint)* APT 36 *(Mandiant)* ProjectM *(Palo Alto)* Mythic Leopard *(CrowdStrike)* TEMP.Lapis *(FireEye)* Copper Fieldstone *(SecureWorks)* Earth Karkaddan *(Trend Micro)* STEPPY-KAVACH *(Securonix)* Green Havildar *(PWC)* APT-C-56 *(Qihoo 360)* Storm-0156 *(Microsoft)* Opaque Draco *(Palo Alto)* G0134 *(MITRE)*
Country	Pakistan
Motivation	Information theft and espionage
First seen	2013
Description	(Proofpoint) Proofpoint researchers recently uncovered evidence of an advanced persistent threat (APT) agai Indian diplomatic and military resources. Our investigation began with malicious emails sent to Indian emba in Saudi Arabia and Kazakstan but turned up connections to watering hole sites focused on Indian military personnel and designed to drop a remote access Trojan (RAT) with a variety of data exfiltration functions. O analysis shows that many of the campaigns and attacks appear related by common IOCs, vectors, payloads, a language, but the exact nature and attribution associated with this APT remain under investigation. At this time, the background and analysis in this paper provide useful forensics and detail our current thinkin the malware that we have dubbed “MSIL/Crimson”. Transparent Tribe may be related to Gorgon Group and SideCopy. Their malicious infrastructure was infiltrated by Turla, Waterbug, Venomous Bear in 2022. Transparant Tribe has been observed to use the Andromeda botnet (operated by Andromeda Spider).
Observed	Sectors: Defense, Education, Embassies, Government. Countries: Afghanistan, Australia, Austria, Azerbaijan, Belgium, Botswana, Bulgaria, Canada, China, Czech Germany, India, Iran, Japan, Kazakhstan, Kenya, Malaysia, Mongolia, Nepal, Netherlands, Oman, Pakistan, Romania, Saudi Arabia, Spain, Sweden, Thailand, Turkey, UAE, UK, USA.

Tools used	Amphibeon, Android RAT, beendoor, Bezigate, Bozok, BreachRAT, CapraRAT, Crimson RAT, DarkComet, ElizaRAT, Limepad, Luminosity RAT, Mobzsar, MumbaiDown, njRAT, ObliqueRAT, Peppy RAT, QuasarR/ SilentCMD, Stealth Mango, UPDATESEE, USBWorm, Waizsar RAT.	
Operations performed	2012	Operation “Transparent Tribe” On February 11, 2016, we discovered two attacks minutes apart directed towards officials at I embassies in both Saudi Arabia and Kazakhstan. Both e-mails (Fig. 1, 2) were sent from the s originating IP address (5.189.145[.]248) belonging to Contabo GmbH, a hosting provider that seems to be currently favored by these threat actors. The e-mails also likely utilized Rackspac MailGun service and both of them were carrying the same exact attachment. <https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf>
	Mar 2016	Indian TV station CNN-IBN has discovered that Pakistani officials were collecting data about Indian troop movements using an Android app called SmeshApp. <https://news.softpedia.com/news/smeshapp-removed-from-play-store-because-pakistan-used to-spy-on-indian-army-501936.shtml>
	Mar 2016	Operation “C-Major” Trend Micro is reporting on a third campaign, which they’ve named Operation C-Major. According to the security firm, this campaign targeted Indian military officials via spear-phish emails, distributing spyware to its victims via an Adobe Reader vulnerability. <https://news.softpedia.com/news/another-case-of-a-pakistani-apt-spying-on-indian-military-personnel-502093.shtml> <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-c-major-actors-also-us android-blackberry-mobile-spyware-targets/>
	Feb 2017	This blog post describes another attack campaign where attackers impersonated identity of Inc think tank IDSA (Institute for Defence Studies and Analyses) and sent out spear-phishing ema target officials of the Central Bureau of Investigation (CBI) and possibly the officials of India Army. <https://cysinfo.com/cyber-attack-targeting-cbi-and-possibly-indian-army-officials/>
	Jun 2019	Over the past year, we have seen this group undergo an evolution, stepping up its activities, starting massive infection campaigns, developing new tools and strengthening their focus on Afghanistan. <https://securelist.com/transparent-tribe-part-1/98127/> <https://securelist.com/transparent-tribe-part-2/98233/>
	Jan 2020	Investigating APT36 or Earth Karkaddan’s Attack Chain and Malware Arsenal <https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-a chain-and-malware.html>
	Jan 2020	Transparent tribe is back with a new campaign after several years of (apparently) inactivity. W can confirm that this campaign is completely new, relying on the registration record of the C2 dates back to 29 January 2020. <https://blog.yoroi.company/research/transparent-tribe-four-years-later/>
	Early 2020	TransparentTribe started using a new module named USBWorm at the beginning of 2020, as v as improving its custom .NET tool named CrimsonRAT. <https://securelist.com/apt-trends-report-q1-2020/96826/>

	Mar 2020	APT36 spreads fake coronavirus health advisory <https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/>
	Apr 2020	Operation “Honey Trap” APT36 Targets Defense Organizations in India <https://www.seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/>
	Feb 2021	ObliqueRAT returns with new campaign using hijacked websites <https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html>
	Jun 2021	Transparent Tribe campaign uses new bespoke malware to target Indian government officials <https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html>
	Dec 2021	Transparent Tribe begins targeting education sector in latest campaign <https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html>
	2022	APT-36 Uses New TTPs and New Tools to Target Indian Governmental Organizations <https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations>
	Jul 2022	Love scam or espionage? Transparent Tribe lures Indian and Pakistani officials <https://www.welivesecurity.com/2023/03/07/love-scam-espionage-transparent-tribe-lures-inc pakistani-officials/>
	Jul 2022	Pakistan-Aligned Threat Actor Expands Interest in Indian Education Sector <https://www.sentinelone.com/labs/transparent-tribe-apt36-pakistan-aligned-threat-actor-expa interest-in-indian-education-sector/>
	Nov 2022	New STEPPY#KAVACH Attack Campaign Likely Targeting Indian Government: Technical Insights and Detection Using Securonix <https://www.securonix.com/blog/new-steppykavach-attack-campaign/>
	Apr 2023	Cyber Espionage in India: Decoding APT-36's New Linux Malware Campaign <https://www.uptycs.com/blog/cyber_espionage_in_india_decoding_apt_36_new_linux_malv
	Apr 2023	CapraTube | Transparent Tribe’s CapraRAT Mimics YouTube to Hijack Android Phones <https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/>
	Sep 2023	The Evolution of Transparent Tribe’s New Malware <https://blog.checkpoint.com/research/the-evolution-of-transparent-tribes-new-malware/>
	Late 2023	Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cı Platform Programming Languages <https://blogs.blackberry.com/en/2024/05/transparent-tribe-targets-indian-government-defens and-aerospace-sectors>
	Jun 2024	CapraTube Remix | Transparent Tribe’s Android Spyware Targeting Gamers, Weapons Enthus <https://www.sentinelone.com/labs/capratube-remix-transparent-tribes-android-spyware-targe gamers-weapons-enthusiasts/>
	Mar 2025	APT36-Style ClickFix Attack Spoofs Indian Ministry to Target Windows & Linux <https://hunt.io/blog/apt36-clickfix-campaign-indian-ministry-of-defence>

Information	<https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html> <https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/> <https://cyberstanc.com/blog/a-look-into-apt36-transparent-tribe/> <https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html> <https://blog.talosintelligence.com/2022/02/whats-with-shared-vba-code.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0134/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
