Donot Team - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:13:44 UTC

APT group: Donot Team

Names	Donot Team *(ASERT)* APT-C-35 *(Qihoo 360)* SectorE02 *(ThreatRecon)* Mint Tempest *(Microsoft)* Origami Elephant *(Kaspersky)*
Country	India
Motivation	Information theft and espionage
First seen	2016
Description	(ASERT) In late January 2018, ASERT discovered a new modular malware framework we call “yty”. The framework shares a striking resemblance to the EHDevel framework. We believe with medium confidence that a team we call internally as “Donot Team” is responsible for the new malware and will resume targeting of South Asia. In a likely effort to disguise the malware and its operations, the authors coded several references into the malware for football—it is unclear whether they mean American football or soccer. The theme may allow the network traffic to fly under the radar. The actors use false personas to register their domains instead of opting for privacy protection services. Depending on the registrar service chosen, this could be seen as another cost control measure. The actors often used typo-squatting to slightly alter a legitimate domain name. In contrast, the registration information used accurate spelling, possibly indicating the domain naming was intentional, typos included. Each unique registrant usually registered only a few domains, but mistakenly reused phone numbers or the registration data portrayed a similar pattern across domains.
Observed	Sectors: Embassies, Defense, Government. Countries: Argentina, Bangladesh, India, Nepal, Pakistan, Philippines, Sri Lanka, Thailand, Togo, UAE, UK.
Tools used	BackConfig, EHDevel, yty.

Operations performed	Mar 2019	From March to July this year, the ThreatRecon team noticed a spear phishing campaign by the SectorE02 group going on against the Government of Pakistan and organizations there related to defense and intelligence. <https://threatrecon.nshc.net/2019/08/02/sectore02-updates-yty-framework-in-new-targeted-campaign-against-pakistan-government/>
	Apr 2019	StealJob: New Android Malware Recently, we have observed a large-scale upgrade of its malicious Android APK framework to make it more stable and practical. Since the new APK framework is quite different from the one used in the past, we named it as StealJob since “job” is frequently used in the code. <https://ti.360.net/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group-en/>
	Dec 2019	Togo: Prominent activist targeted with Indian-made spyware linked to notorious hacker group <https://www.amnesty.org/en/latest/news/2021/10/togo-activist-targeted-with-spyware-by-notorious-hacker-group/>
	May 2020	An Indicator From Twitter Brings The Donot Android Espionage Group Back Into Focus <https://www.riskiq.com/blog/external-threat-management/donot-mobile-malware-espionage/>
	2020	ESET researchers take a deep look into recent attacks carried out by Donot Team throughout 2020 and 2021, targeting government and military entities in several South Asian countries <https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/>
	Aug 2022	APT-C-35 Gets a New Upgrade <https://blog.morphisec.com/apt-c-35-new-windows-framework-revealed>
	Jun 2023	DoNot APT Elevates its Tactics by Deploying Malicious Android Apps on Google Play Store <https://www.cyfirma.com/outofband/donot-apt-elevates-its-tactics-by-deploying-malicious-android-apps-on-google-play-store/>
	Oct 2024	Android Malware in DONOT APT Operations <https://www.cyfirma.com/research/android-malware-in-donot-apt-operations/>

Information	<https://ti.360.net/blog/articles/donot-group-is-targeting-pakistani-businessman-working-in-china-en/> <https://www.netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia> <http://blog.ptsecurity.com/2019/11/studying-donot-team.html> <https://www.trellix.com/blogs/research/from-click-to-compromise-unveiling-the-sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
