Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:03:35 UTC

APT group: RedAlpha

Names	RedAlpha *(Recorded Future)* DeepCliff *(?)* Red Dev 3 *(PWC)*
Country	China
Sponsor	State-sponsored, possibly PLA and/or Nanjing Qinglan Information Technology Co. Ltd
Motivation	Information theft and espionage
First seen	2015
Description	The original research from Citizen Lab did not give this group a name. (Recorded Future) Recorded Future's Insikt Group has identified two new cyberespionage campaigns targeting the Tibetan community over the past two years. The campaigns, which we are collectively naming RedAlpha, combine light reconnaissance, selective targeting, and diverse malicious tooling. We discovered this activity as the result of pivoting off of a new malware sample observed targeting the Tibetan community based in India. Insikt Group's analysis of infrastructure overlap among the new campaigns reveals wider targeting of the Chinese "Five Poisons," in addition to South and Southeast Asian governments. Based on the campaign's targeting of "Five Poisons"-related organizations, overlapping infrastructure, and links to malware used by other Chinese APTs uncovered during our research, we assess with medium confidence that the RedAlpha campaigns were conducted by a Chinese APT. Infrastructure overlaps have been found with APT 17, Deputy Dog, Elderwood, Sneaky Panda, Icefog, Dagger Panda and NetTraveler, APT 21, Hammer Panda.
Observed	Sectors: Government and the Tibetan and Uyghur communities and Falun Gong supporters. Countries: Hong Kong, India, Myanmar, Pakistan, Sri Lanka, Thailand and South and Southeast Asia.

Tools used	FormerFirstRAT, Gh0st RAT, NetHelp Infostealer, njRAT, RedAlpha and a vulnerability in MS Office.	
Operations performed	2017	RedAlpha: New Campaigns Discovered Targeting the Tibetan Community <https://www.recordedfuture.com/redalpha-cyber-campaigns/> <https://go.recordedfuture.com/hubfs/reports/cta-2018-0626.pdf>
	2021	RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations <https://go.recordedfuture.com/hubfs/reports/ta-2022-0816.pdf>
Information	<https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/>	

Last change to this card: 10 March 2024

Download this actor card in PDF or JSON format
