Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:38:37 UTC

APT group: RedEcho

Names	RedEcho *(Recorded Future)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2020
Description	(Recorded Future) Since early 2020, Recorded Future's Insikt Group observed a large increase in suspected targeted intrusion activity against Indian organizations from Chinese state-sponsored groups. From mid-2020 onwards, Recorded Future's midpoint collection revealed a steep rise in the use of infrastructure tracked as AXIOMATICASYMPTOTE, which encompasses ShadowPad command and control (C2) servers, to target a large swathe of India's power sector. 10 distinct Indian power sector organizations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for operation of the power grid through balancing electricity supply and demand, have been identified as targets in a concerted campaign against India's critical infrastructure. Other targets identified included 2 Indian seaports. Using a combination of proactive adversary infrastructure detections, domain analysis, and Recorded Future Network Traffic Analysis, we have determined that a subset of these AXIOMATICASYMPTOTE servers share some common infrastructure tactics, techniques, and procedures (TTPs) with several previously reported Chinese state-sponsored groups, including APT 41 and Tonto Team, HartBeat, Karma Panda. Despite some overlaps with previous groups, Insikt Group does not currently believe there is enough evidence to firmly attribute the activity in this particular campaign to an existing public group and therefore continue to track it as a closely related but distinct activity group, RedEcho. Also see TAG-38.
Observed	Sectors: Energy, Maritime and Shipbuilding. Countries: India.

Tools used	ShadowPad Winnti.
Information	<https://go.recordedfuture.com/redecho-insikt-group-report> <https://therecord.media/redecho-group-parks-domains-after-public-exposure/>

Last change to this card: 08 April 2022

Download this actor card in PDF or JSON format
