38 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:00:30 UTC

APT group: TAG-38

Names	TAG-38 *(Recorded Future)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2021
Description	(Recorded Future) In recent months, we observed likely network intrusions targeting at least 7 Indian State Load Despatch Centres (SLDCs) responsible for carrying out real-time operations for grid control and electricity dispatch within these respective states. Notably, this targeting has been geographically concentrated, with the identified SLDCs located in North India, in proximity to the disputed India-China border in Ladakh. One of these SLDCs was also targeted in previous RedEcho activity. This latest set of intrusions, however, is composed of an almost entirely different set of victim organizations. In addition to the targeting of power grid assets, we also identified the compromise of a national emergency response system and the Indian subsidiary of a multinational logistics company by the same threat activity group. To achieve this, the group likely compromised and co-opted internet-facing DVR/IP camera devices for command and control (C2) of Shadowpad malware infections, as well as use of the open source tool FastReverseProxy (FRP). Despite a partial troop disengagement between India and China from February 2021, the prolonged targeting of Indian critical infrastructure continues to raise concerns over pre-positioning activity being conducted by Chinese adversaries. While this latest activity displays targeting and capability consistencies with previously identified RedEcho activity, there are also some notable distinctions. At this time, we have not identified technical evidence allowing us to attribute it to RedEcho, and we are currently clustering this latest activity under the temporary group name Threat Activity Group 38 (TAG-38).
Observed	Sectors: Energy. Countries: India.
Tools used	FRP, ShadowPad Winnti.

Information	<https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/> <https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf>

Last change to this card: 08 April 2022

Download this actor card in PDF or JSON format
