# China accused of cyberattacks on Indian power grid

By Laura Dobberstein

Published: 2022-04-08 · Archived: 2026-04-05 17:11:40 UTC

China has been accused of conducting a long-term cyber attack on India's power grid, and has been implicated in cyber attacks against targets in Ukraine.

Cybersecurity firm Insikt Group found network intrusions at seven Indian State Load Dispatch Centers (SLDCs) that conduct real-time operations for grid control and electricity dispatch, according to a report released Wednesday. All seven SLDCs were located near the disputed India-China border in Ladakh.

Although one of the SLDCs had been previously targeted – in a 2020 incident that Insikt Group named RedEcho and credited to Beijing – the newly identified intrusions target an almost entirely different set of victims.

Insikt stated that in addition to attacking grid assets, the operation impacted a national emergency response team and the Indian subsidiary of a logistics company.

The operation used a trojan called ShadowPad, thought to have links to contractors serving China's Ministry of State Security (MSS).

The attackers, sometimes identified a Threat Activity Group 38 (TAG-38), are believed to have infiltrated the system via third-party devices like IP cameras that may have been left vulnerable when their default credentials were kept in place.

"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)," opined Insikt Group in its report.


- Russia (still) trying to weaponize Facebook for spying, Ukraine-war disinfo
- How do China's cyber-spies snoop on governments, NGOs? Probably like this
- US State Department opens cybersecurity policy bureau
- China, India face tech brain drain through US universities


The cybersecurity group said that because the targeting was prolonged, it was most likely a mission to gather information about critical infrastructure, rather than seeking immediate-term benefit. Such information could later be used to gain access across a system to take (presumably disruptive) action.

Beijing, predictably, denied involvement. Foreign spokesperson Zhao Lijian asserted that China firmly opposed all forms of cyber attacks, in accordance with the law. He added that one should be "all the more prudent when associating cyber attacks with the government of a certain country."

The past few weeks have also brought a string of reported attacks emanating from China against targets in Ukraine.

SentinelLabs concluded in late March that malware sent throughout the country disguised as a call to send in video documentation of Russian aggression was associated with the suspected Chinese threat actor known as Scarab.

"The malicious activity represents one of the first public examples of a Chinese threat actor targeting Ukraine since the invasion began," said SentinelOne's Tom Hegel.

American enterprise security company Proofpoint also identified ongoing threat activity from China last month. Researchers said TA416 is targeting European diplomatic entities, including an individual involved in refugee and migrant services.

Proofpoint said the activity showed "an interest in refugee policies and logistics across the APT actor landscape which coincides with increased tensions and now armed conflict between Russia and Ukraine."

But according to the anonymous collective Intrusion Truth – a group that analyses China-linked cyber attacks – state-sponsored threat actor FunnyDream had also targeted the Kremlin, Russian private bank Alfabank, and the Federal Guard Service of the Russian Federation.

"Wonder what that says about China's trust in Russia?" mused Intrusion Truth. ®

---