RedEcho group parks domains after public exposure

therecord.media/redecho-group-parks-domains-after-public-exposure/

March 29, 2021

A Chinese hacking group linked to a campaign that targeted India's power grid and critical infrastructure entities has taken down its attack infrastructure after having its operations exposed at the end of February 2021.

Known as **RedEcho**, the group is one of many Chinese government-sponsored cyber-espionage entities active today.

The earliest signs of RedEcho attacks date back to early 2020, but operations gained a significant momentum after a May 2020 border dispute between Indian and Chinese troops that devolved into violence and heightened political tensions between the two neighboring countries.

Subsequent RedEcho attacks shifted to target India's power sector primarily, and the group is believed to have breached at least a dozen of Indian power sector organizations, including four of India's five Regional Load Despatch Centres (RLDCs) and two State Load Despatch Centres (SLDCs), where it deployed backdoor malware such as PlugX and ShadowPad, allowing the group easy access at any further date.

These attacks came to light in February 2021, when Recorded Future's Insikt Group published a report detailing RedEcho's Indian operations after analysts managed to find unique characteristics in the communications between the malware and its backend infrastructure, allowing them to track attacks by using a combination of proactive infrastructure detections, domain, and network traffic analysis.

Last activity spotted on March 11, 2021

But less than two weeks after Recorded Future published its findings, the Insikt Group told *The Record* that RedEcho has now taken down part of its domain infrastructure.

More specifically, RedEcho has now parked web domains it previously used to control ShadowPad malware inside the hacked Indian power grid, and which Recorded Future ousted in its report.

“The most recently identified victim communications with RedEcho infrastructure was from an Indian IP address on March 11, 2021 to the RedEcho IP 210.92.18[.]132,” the Insikt Group said.

But this was to be expected. Advanced persistent threat (APT) groups like RedEcho often react to public disclosure by moving infrastructure to new servers.

“This is likely due to a combination of defensive measures taken by targeted organizations to block published network indicators and the aforementioned steps taken by the group to move away from publicized infrastructure,” Insikt Group analyst said.

Furthermore, cyber-espionage operations are most efficient when undetected. Once operations get exposed, security firms will often work in the shadows to notify victims and intelligence services in the targeted countries, and even poison the attacker’s collected data.

Tags

- APT
- China
- domain
- India
- Insikt Group
- nation-state
- parked domain
- Recorded Future
- RedEcho

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.