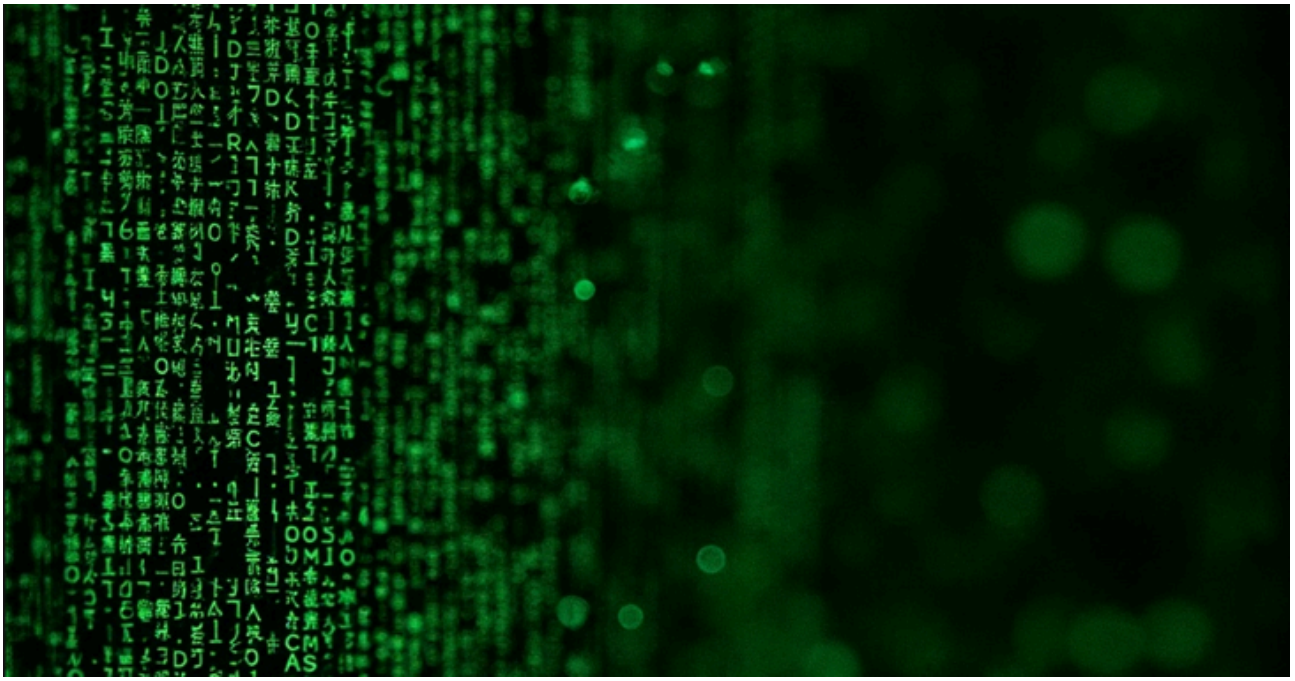
Chinese Hackers Infiltrate U.S. Internet Providers in Cyber Espionage Campaign

By The Hacker News

Published: 2024-09-26 · Archived: 2026-04-05 21:10:20 UTC



Nation-state threat actors backed by Beijing broke into a "handful" of U.S. internet service providers (ISPs) as part of a cyber espionage campaign orchestrated to glean sensitive information, The Wall Street Journal reported Wednesday.

The activity has been attributed to a threat actor that Microsoft tracks as Salt Typhoon, which is also known as FamousSparrow and GhostEmperor.

"Investigators are exploring whether the intruders gained access to Cisco Systems routers, core network components that route much of the traffic on the internet," the publication was quoted as saying, citing people familiar with the matter.

The end goal of the attacks is to gain a persistent foothold within target networks, allowing the threat actors to harvest sensitive data or launch a damaging cyber attack.

GhostEmperor first came to light in October 2021, when Russian cybersecurity company Kasperksy detailed a long-standing evasive operation targeting Southeast Asian targets in order to deploy a rootkit named Demodex.

Targets of the campaign included high-profile entities in Malaysia, Thailand, Vietnam, and Indonesia, in addition to outliers located in Egypt, Ethiopia, and Afghanistan.

As recently as July 2024, Sygnia revealed that an unnamed client was compromised by the threat actor in 2023 to infiltrate one of its business partner's networks.

"During the investigation, several servers, workstations, and users were found to be compromised by a threat actor who deployed various tools to communicate with a set of [command-and-control] servers," the company said. "One of these tools was identified as a variant of Demodex."

The development comes days after the U.S. government said it disrupted a 260,000-device botnet dubbed Raptor Train controlled by a different Beijing-linked hacking crew called Flax Typhoon.

It also represents the latest in a string of Chinese state-sponsored efforts to target telecom, ISPs, and other critical infrastructure sectors.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2024/09/chinese-hackers-infiltrate-us-internet.html