Chinese Hackers RedNovember Target Global Governments Using Pantegana and Cobalt Strike

By The Hacker News

Published: 2025-09-24 · Archived: 2026-04-05 18:13:12 UTC

A suspected cyber espionage activity cluster that was previously found targeting global government and private sector organizations spanning Africa, Asia, North America, South America, and Oceania has been assessed to be a Chinese state-sponsored threat actor.

Recorded Future, which was tracking the activity under the moniker TAG-100, has now graduated it to a hacking group dubbed **RedNovember**. It's also tracked by Microsoft as Storm-2077.

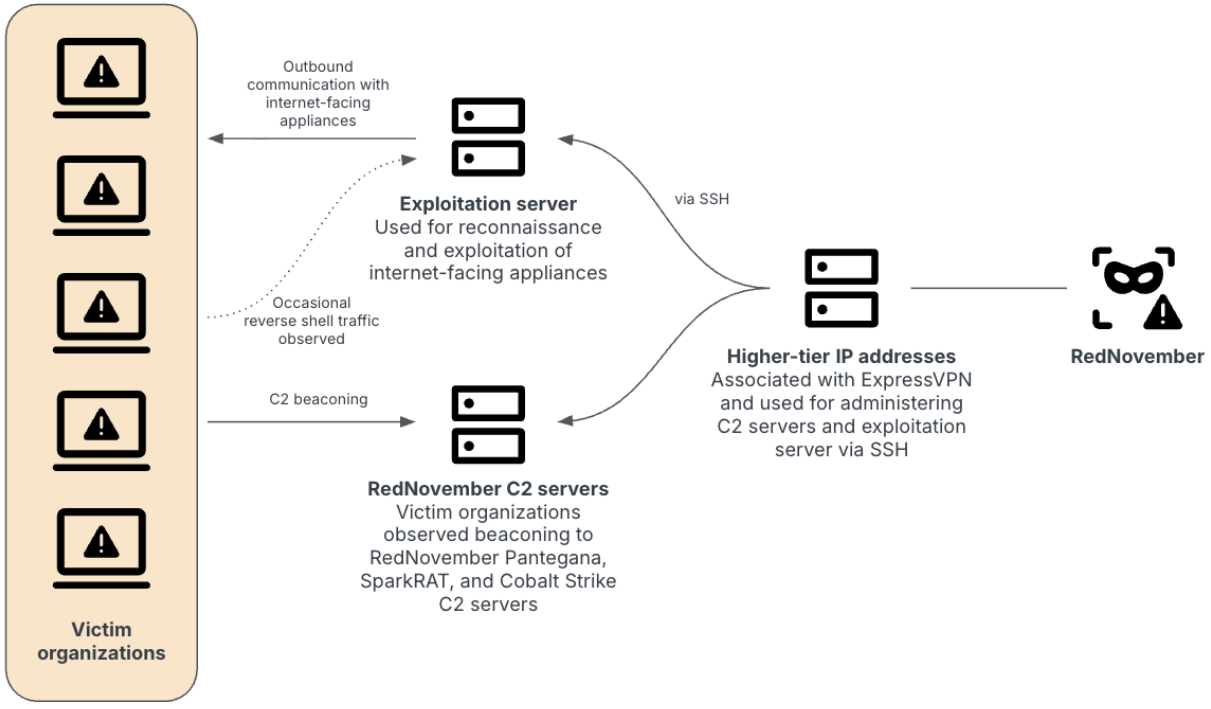
"Between June 2024 and July 2025, RedNovember (which overlaps with Storm-2077) targeted perimeter appliances of high-profile organizations globally and used the Go-based backdoor Pantegana and Cobalt Strike as part of its intrusions," the Mastercard-owned company said in a report shared with The Hacker News.

"The group has expanded its targeting remit across government and private sector organizations, including defense and aerospace organizations, space organizations, and law firms."

Some of the likely new victims of the threat actor include a ministry of foreign affairs in central Asia, a state security organization in Africa, a European government directorate, and a Southeast Asian government. The group is also believed to have breached two at least two United States (U.S.) defense contractors, a European engine manufacturer, and a trade-focused intergovernmental cooperation body in Southeast Asia.

RedNovember was first documented by Recorded Future over a year ago, detailing its use of the Pantegana post-exploitation framework and Spark RAT following the weaponization of known security flaws in several internet-facing perimeter appliances from Check Point (CVE-2024-24919), Cisco, Citrix, F5, Fortinet, Ivanti, Palo Alto Networks (CVE-2024-3400), and SonicWall for initial access.

The focus on targeting security solutions such as VPNs, firewalls, load balancers, virtualization infrastructure, and email servers mirrors a trend that has been increasingly adopted by other Chinese state-sponsored hacking groups to break into networks of interest and maintain persistence for extended periods of time.



A noteworthy aspect of the threat actor's tradecraft is the use of Pantegana and Spark RAT, both of which are open-source tools. The adoption is likely an attempt to repurpose existing programs to their advantage and confuse attribution efforts, a hallmark of espionage actors.

The attacks also involve the use of a variant of the publicly available Go-based loader LESLIELOADER to launch Spark RAT or Cobalt Strike Beacons on compromised devices.

RedNovember is said to make use of VPN services like ExpressVPN and Warp VPN to administer and connect to two sets of servers that are used for exploitation of internet-facing devices and communicate with Pantegana, Spark RAT, and Cobalt Strike, another legitimate program that has been widely abused by bad actors.

Between June 2024 and May 2025, much of the hacking group's targeting efforts have been focused on Panama, the U.S., Taiwan, and South Korea. As recently as April 2025, it has been found to target Ivanti Connect Secure appliances associated with a newspaper and an engineering and military contractor, both based in the U.S.

Recorded Future said it also identified the adversary likely targeting the Microsoft Outlook Web Access (OWA) portals belonging to a South American country before that country's state visit to China.

"RedNovember has historically targeted a diverse range of countries and sectors, suggesting broad and changing intelligence requirements," the company noted. "RedNovember's activity to date has primarily focused on several key geographies, including the U.S., Southeast Asia, the Pacific region, and South America."

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

Source: https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html