ANSSI Exposes "Houken": China-Linked APT Exploiting Ivanti CSA Zero-Days & Deploying Linux Rootkits

By ddos

Published: 2025-07-07 · Archived: 2026-04-05 13:48:29 UTC

The French cybersecurity agency has announced a large-scale cyberattack targeting key sectors of the nation. Government institutions, telecommunications firms, media organizations, the financial sector, and transport entities were all placed in the crosshairs. The malicious campaign has been attributed to a Chinese hacking group that exploited previously unknown vulnerabilities in Ivanti's Cloud Services Appliance (CSA).

Hacking & Cracking

The discovered attacks date back to September 2024. Responsibility has been assigned to a group known as Houken, whose activities, according to experts, overlap with those of the cybercriminal cluster UNC5174—also referred to as Uteus or Uetus—which has previously been tracked by Google's Mandiant team.

France's National Agency for the Security of Information Systems (ANSSI) reported that the attackers employed not only zero-day vulnerabilities and a sophisticated rootkit but also an extensive array of open-source tools, predominantly developed by Chinese-speaking programmers. Houken's infrastructure includes the use of commercial VPNs and dedicated servers, allowing it to effectively obfuscate the origins of its attacks.

According to French analysts, Houken has been actively utilized by so-called initial access brokers since 2023. These intermediaries breach systems and subsequently sell access to other cybercriminals, who then carry out further exploitation of the compromised networks. This modular approach suggests the involvement of multiple threat groups, each responsible for a different phase of the operation—from vulnerability discovery to monetization.

HarfangLab notes that typically, one group identifies a vulnerability, another exploits it at scale to infiltrate networks, and the resulting access is sold to interested third parties—often those with ties to state entities.

Experts believe that the primary objective of UNC5174 and Houken is to infiltrate strategically valuable targets and sell access to government-aligned buyers seeking intelligence. However, these actors are not confined to cyber espionage. In at least one instance, the gained access was used to install cryptocurrency miners, indicating financial motivations as well.

UNC5174 has previously been linked to attacks on SAP NetWeaver systems, deploying malware such as GOREVERSE, a variant of GoReShell. The group has also been associated with exploitation of vulnerabilities in products from Palo Alto Networks, ConnectWise ScreenConnect, and F5 BIG-IP, through which they distributed malware known as SNOWLIGHT—used to install a Go-based tunneling tool called GOHEAVY.

SentinelOne has reported that the same group breached a major European media company in September 2024. In the recent attacks on French organizations, the perpetrators exploited three vulnerabilities in Ivanti CSA—CVE-2024-8963, CVE-2024-9380, and CVE-2024-8190. These zero-day flaws allowed the attackers to stealthily infiltrate systems, obtain credentials, and establish persistent access within targeted infrastructures.

Hacking & Cracking

To maintain their foothold, the attackers employed three methods: installing PHP web shells directly, modifying existing PHP scripts to embed stealthy web shell functions, and deploying a rootkit injected at the kernel level.

Well-known public web shells such as Behinder and neo-reGeorg were actively used. Once persistence was achieved, lateral movement across networks was executed using GOREVERSE, alongside the suo5 HTTP proxy tunnel and a Linux kernel module dubbed “sysinitd.ko,” previously observed by Fortinet researchers.

According to ANSSI, the sysinitd.ko module and its associated user-space executable “sysinitd” were deployed via a script named install.sh. This toolkit enabled attackers to intercept all inbound TCP traffic and execute commands with root privileges.

Beyond technical sophistication, experts noted a distinct operational trait: the attackers operated from the UTC+8 time zone, aligning with Chinese standard time. Moreover, the perpetrators attempted to patch exploited vulnerabilities post-compromise to prevent rival hacking groups from gaining access.

ANSSI concludes that the scale of these attacks indicates a broad array of targets—including government and academic institutions in Southeast Asia, NGOs in China, Hong Kong, and Macau, as well as governmental, defense, educational, media, and telecom entities in Western nations.

The striking similarity in tactics between Houken and UNC5174 suggests that both may be fronts for a single criminal entity, operating as a private syndicate that trades in system access and confidential data while simultaneously conducting its own lucrative operations.

Post navigation
