Rapport menaces et incidents - CERT-FR

Archived: 2026-04-05 17:22:40 UTC

Une gestion de version détaillée se trouve à la fin de ce document.

In September 2024, ANSSI observed an attack campaign seeking initial access to French entities' networks through the exploitation of several zero-day vulnerabilities on Ivanti Cloud Service Appliance (CSA) devices. French organizations from governmental, telecommunications, media, finance, and transport sectors were impacted. ANSSI's investigations led to the conclusion that a unique intrusion set was leveraged to conduct this attack campaign. The Agency named this intrusion set « Houken ». Moderately sophisticated, Houken can be characterized by an ambivalent use of resources. While its operators use zero-day vulnerabilities and a sophisticated rootkit, they also leverage a wide number of open-source tools mostly crafted by Chinese-speaking developers. Houken's attack infrastructure is made up of diverse elements - including commercial VPNs and dedicated servers.

ANSSI suspects that the Houken intrusion set is operated by the same threat actor as the intrusion set previously described by MANDIANT as UNC5174. Since 2023, Houken is likely used by an access broker to gain a foothold on targeted systems, which could eventually be sold to entities interested in carrying out deeper post-exploitation activities. Though already documented for its opportunistic exploitation of vulnerabilities on edge devices, the use of zero-days by a threat actor linked to UNC5174 is new to ANSSI's knowledge. The operators behind the UNC5174 and Houken intrusion sets are likely primarily looking for valuable initial accesses to sell to a state-linked actor seeking insightful intelligence. However, ANSSI also observed one case of data exfiltration as well as an interest in the deployment of cryptominers, indicating straight-forward profit-driven objectives.

Download the report

Gestion détaillée du document

le 01 juillet 2025
Version initiale

le 04 juillet 2025
Version 1.1