IMPORTANT CYBERSECURITY NEWS: CHINA-LINKED ATTACKERS EXPLOIT CHECK POINT FLAW TO DEPLOY SHADOWPAD AND RANSOMWARE

Vairav Cyber Security News Report

Date: 2025-02-21

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident has emerged involving the exploitation of a vulnerability in Check Point network gateway security products (CVE-2024-24919) by Chinese-linked attackers. This breach has led to the deployment of sophisticated malware, including ShadowPad and PlugX, and in some instances, the NailaoLocker ransomware. The primary targets have been European organizations, notably within the healthcare sector. This incident underscores the critical importance of promptly addressing security vulnerabilities to prevent unauthorized access and potential operational disruptions.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Attackers exploited a recently patched security flaw in Check Point products (CVE-2024-24919) to gain unauthorized access to systems. Utilizing DLL search-order hijacking, they deployed malware which are commonly associated with Chinese espionage activities.

Identification: The attacks were observed at least between June and October 2024. Orange Cyberdefense CERT identified the malicious activities, noting the exploitation of the CVE-2024-24919 vulnerability and the subsequent deployment of malware.

Threat Actor: The activity has been attributed with medium confidence to Chinese-aligned threat actors, based on the malware used and the techniques employed.

Affected Entities/Industries: European organizations, particularly those in the healthcare sector, have been primarily targeted in this campaign.

Potential Impact: The exploitation of this vulnerability poses several risks, including unauthorized access to sensitive data, potential data exfiltration, operational disruptions due to ransomware encryption, and significant financial losses associated with ransom payments and remediation efforts.

Exploitation Methods: The attackers employed DLL search-order hijacking to deploy malware. They gained initial access by exploiting the CVE-2024-24919 vulnerability, retrieved user credentials, connected to VPNs using legitimate accounts, and conducted lateral movements within networks to escalate privileges.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Apply the latest security patches to Check Point products to address CVE-2024-24919.
- Conduct a thorough network audit to identify and remediate unauthorized access points.
- Isolate affected systems to prevent further lateral movement by attackers.

Security Best Practices

- Regularly update all software and hardware with the latest security patches.
- Implement multi-factor authentication (MFA) to enhance access security.
- Educate employees about phishing attacks and safe email practices.
- Maintain regular data backups and ensure they are stored securely offline.

For Advanced Security Teams

- Deploy advanced threat detection tools to monitor for signs of DLL side-loading and other malicious activities.
- Analyze network traffic for anomalies indicative of data exfiltration attempts.
- Develop and test incident response plans tailored to ransomware and malware attacks.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/02/chinese-linked-attackers-exploit-check.html
- https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com