Dutch intelligence warns that China-linked APT Salt Typhoon targeted loca

Data: 2025-08-29 07:43:43

Autor: Inteligência Against Invaders

Dutch intelligence warn that China-linked APT Salt Typhoon targeted local critical infrastructure

Dutch intelligence reports Chinese cyber spies (Salt Typhoon, RedMike) targeted the Netherlands, hitting critical infrastructure.

The Dutch intelligence and security services MIVD and AIVD say Chinese cyber spies linked to Salt Typhoon (RedMike) targeted the Netherlands in a campaign hitting global critical infrastructure.

In late 2024, a large-scale Chinese cyberespionage campaign targeting global telecoms was exposed and attributed by the US to state-backed group Salt Typhoon.

In December 2024, President Biden's deputy national security adviser Anne Neuberger said that China-linked APT groupSalt Typhoonbreached telecommunications companies in dozens of countries.

The Wall Street Journalreportedthat the senior White House official revealed that at least eight U.S. telecommunications firms were compromised in the attack.

The Salt Typhoon hacking campaign, active for 1–2 years, has targeted telecommunications providers in several dozen countries, according to a U.S. official.

Dutch intelligence agencies MIVD and AIVD confirmed parts of the US findings with their own sources, endorsing warnings from the NSA, CISA, and FBI. European agencies including Germany's BND, Finland's SUPO, the UK's NCSC, and Italy's AISE also backed the alerts, highlighting the campaign's global scope and strategic risk.

According to Dutch intelligence agencies, the China-linked APT group targeted the Netherlands, focusing not on major telecoms but on smaller internet service and hosting providers.

"An investigation by the MIVD and AIVD (General Intelligence and Security Service) has revealed that the Chinese hacking organization had access to routers belonging to the Dutch targets." reads the advisory *published by the Ministry of Defence. "As far as we know, the hackers did not penetrate any further into their internal networks. Where possible, the MIVD, AIVD, and the NCSC (National Cyber ??SecurityCentre) have previously shared threat intelligence with targets and other relevant audiences."*

Dutch authorities warn that advanced cyber operations require constant monitoring to reduce, but not eliminate, risks, challenging national cyber resilience.

Recently, Dutch intelligence co-issued an advisory blaming three Chinese tech firms for intrusions linked to Salt Typhoon, and other campaigns affecting multiple countries.

This week, Dutch intelligence agencies, the U.S. National Security Agency (NSA), the UK's National Cyber Security Centre (NCSC), and allies warned that Chinese APT actors, linked toSalt Typhoon, are targeting global telecom, government, transport, lodging, and military sectors.

*"The National Security Agency (NSA) and other U.S. and foreign organizations are releasing a*joint Cybersecurity Advisory*to expose advanced persistent threat (APT) actors sponsored by the Chinese government targeting telecommunications, government, transportation, lodging, and military infrastructure networks globally and outline appropriate mitigation guidance." reads the***report***published by NSA. "The malicious activity outlined in the advisory partially overlaps with cybersecurity industry reporting on Chinese state-sponsored threat actors referred to by names such as Salt Typhoon."*

A joint Cybersecurity Advisory (CSA) ("Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System,") published by the intelligence and cybersecurity agencies has linked these malicious activities to multiple China-based entities, including Sichuan Juxinhe Network Technology Co. Ltd., Beijing Huanyu Tianqiong Information Technology Co., Ltd., and Sichuan Zhixin Ruijie Network Technology Co., Ltd.. These Chinese tech firms provide cyber products and services to China's Ministry of State Security and People's Liberation Army.

The "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," provides details on tactics, techniques, and procedures (TTPs) associated with these nation-state actors.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,Chinese cyberspies)