Singapore Takes Unprecedented Military Action Against Chinese State-Sponsored Hackers

opforjournal.com/p/singapore-takes-unprecedented-military

Share this post

OPFOR Journal

Singapore Takes Unprecedented Military Action Against Chinese State-Sponsored Hackers

Singapore's critical infrastructure is currently under attack by UNC3886, a sophisticated cyber espionage group affiliated with the Chinese state. This situation report discusses the unusually forceful response that the Singaporean government has launched, the broader strategic context, and what it says about the growing threat of Chinese cyber attacks for the US and its Indo-Pacific allies and partners.

OVERVIEW:

The exact nature of the ongoing cyber attack in Singapore has not been disclosed, other than that the hackers targeted the country's critical infrastructure. The country's response over the last week indicates that the attack is unusually severe.

On July 18, Singapore's Coordinating Minister for National Security K. Shanmugam announced that the government was responding to an attack by an advanced persistent threat actor (APT) on its critical infrastructure. Shanmugam then took the unusual step of attributing the attacks to a group known as UNC3886. The naming of UNC3886 was a significant public declaration because the group is widely believed to be affiliated with the Chinese state. Previously, Singapore avoided directly linking cyberattacks to Chinese-affiliated groups, including when Singtel, its top telecom company, was targeted in 2024.

While Singapore did not explicitly state China's involvement, the Chinese government nevertheless vehemently denied all responsibility for the attack. Statements by the Chinese Embassy to Singapore called attempts by the media to link UNC3886 to China were smears against a country who itself "is a major victim of cyber attacks."


中华人民共和国驻新加坡共和国大使馆

EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE REPUBLIC OF SINGAPORE

Home | Embassy Information | Consular & Visa Services | Economic & Trade Information | Educational Exchanges | Cultural Exchanges | Science & Technological Exchanges | Contact Us

Home > Embassy News

Embassy Spokesperson's Response to Some Singaporean Media Outlets' Attempt to Link China to Cyberattacks in their Reporting

2025-07-19 16:30

The Chinese Embassy in Singapore has noticed that when reporting the story of attacks on Singapore by the cyberattack group UNC3886 on July 19, Singaporean media outlets such as The Straits Times, Lianhe Zaobao and Channel News Asia cited so-called information from a certain country's cybersecurity company and claimed that this group is linked to China. The Chinese government expresses its strong dissatisfaction with this and opposes any groundless smears and accusations against China. In fact, China is a major victim of cyberattacks. The Embassy would like to reiterate that China is firmly against and cracks down all forms of cyberattacks in accordance with law. China does not encourage, support or condone hacking activities. Keeping the cyberspace safe is a global challenge and China stands ready to work with Singapore and the rest of the world to jointly protect cybersecurity.

Denial of responsibility by the Chinese Embassy in Singapore. Source: Embassy of the People's Republic Of China in the Republic of Singapore

A day later, Singapore's Minister of Defence Chan Chun Sing announced that the country's response to the attacks had escalated to include the Singapore Armed Forces (SAF) and Ministry of Defence (MINDEF) as part of a "whole of government" effort to uproot the attackers from the country's networks.

BIGGER PICTURE:

Singapore's Cyber Security Act classifies the following 11 sectors of its economy as critical infrastructure: "Energy, Water, Banking & Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Government, Infocomm, Media, and Security & Emergency Services."

This is not the first time one of the 11 sectors of Singapore's critical infrastructure has come under attack. A particularly bad attack in 2018 targeted Singapore's largest healthcare provider SingHealth, stealing the medical records from 1.5 million Singaporeans, including those of the Prime Minister Lee Hsien Loong and other members of Parliament.

The response to this attack has been unusually forceful compared with previous incidents, such as SingHealth which had been criticized as slow and disorganized. This suggests either a new approach by the government or an unusually significant threat. Recent patterns of attacks by Chinese-state affiliated groups raise questions as to whether the Singapore Armed Force and Ministry of Defence were called in to support a whole of government response, or whether the country's Security and Emergency Services infrastructure was itself a target of the attack.

UNC3886 Operations in Context

A July 2023 report by Google's Mandiant cybersecurity firm identified UNC3886 as a top Chinese cyber espionage group. The group has targeted top firms in the defense, technology and telecommunications industries in the US and across Asia using complex and stealthy attacks to conduct long-term surveillance.

Mandiant researchers allege that UNC3886 has demonstrated an ability to penetrate tightly secured networks, entering through network edge devices such as routers, using multiple Zero-Day exploits.1 Once inside, UNC3886 goes to great lengths to retain a long-term

presence in its victim's systems, using custom malware to circumvent security controls and modify system logs.

UNC3886 is one of many Chinese cyber espionage groups, which Mandiant alleges have become significantly more sophisticated over the last decade due to a restructuring of China's national security apparatus which more deeply integrates cyber capabilities:

> "We suggest that the military and intelligence restructure, evidence of shared development and logistics infrastructure, and legal and institutional structures directing vulnerability research through government authorities point to long term investments in equipping Chinese cyber operators with more sophisticated tactics, tools, and exploits to achieve higher success rates in gaining and maintaining access to high value networks."

Escalating Threat of Chinese Cyberattacks to US and Indo-Pacific Allies

---

The effects of this restructuring are clearly visible in the number of recorded attacks by Chinese state-affiliated groups. Cybersecurity firm CrowdStrike has reported that attacks by Chinese affiliated cyber espionage groups increased over 150% year-on-year in 2024. Many of the most high profile targets of Chinese state cyber attacks have been the US as well as its allies in the Indo-Pacific.

Other Notable Chinese State-affiliated Groups and Cyber Campaigns

Salt Typhoon

Salt Typhoon (aka UNC2286) conducted one of the largest cyber espionage operations in history. In October 2024, it was publicly reported that the group hacked into at least nine US telecom corporations including Verizon, AT&T, T-Mobile, Spectrum, Lumen, and Viastat. Salt Typhoon attempted to collect massive amounts of user data from the company networks, including from both the Trump and Harris Presidential Campaigns.

The group used access to these corporations as a springboard for hacks into wider government systems. The hackers were able to access wire taps and other electronic intercepts used by law enforcement and the intelligence community. A June 2025 memo issued by the Department of Homeland Security confirmed the group was able to gain access to networks used by at least one state's Army National Guard. More recent reporting by Bloomberg on July 22, suggested the group breached the servers of Department of Energy's National Nuclear Security Agency.

Flax Typhoon

Since 2021, the Integrity Technology Group, Incorporated (aka Flax Typhoon), a Beijing-based cybersecurity firm has targeted critical infrastructure across the US, Europe, and Asia. While several US firms have been targeted by Flax Typhoon, most of the group's operations

have focused on Taiwanese organizations, including electronics manufacturers, universities and government institutions.

The group's global operations, consisting of over 200,000 bot nets, were disrupted by an FBI operation in the summer of 2024.

Linen Typhoon, Violet Typhoon, Storm-2603

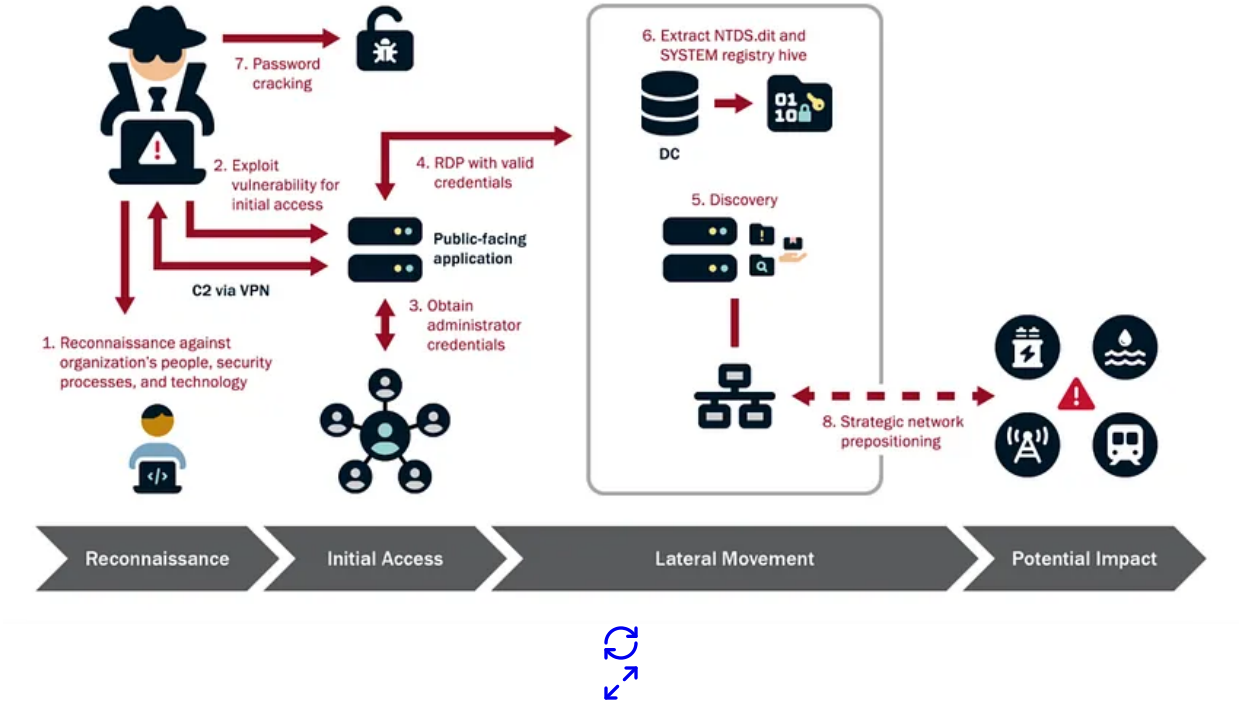
On July 22, as Singapore battled to remove UNC3886 from its digital infrastructure, Microsoft's Security Response Center announced that it had concluded that two Chinese hacker groups, Linen Typhoon and Violet Typhoon, were responsible for massive infiltration of its SharePoint systems in a series of months-long attacks. Linen Typhoon is a known cyber theft group which steals intellectual property from government, defense and human rights organizations in opportunistic attacks. Violet Typhoon is a cyber espionage group that, according to Microsoft, embeds itself in systems to conduct long-term surveillance of political and social elites across the US, Europe, and East Asia.

Another Chinese cyber crime group, Storm-2603, is believed to have also attempted to exploit the vulnerabilities created by the Typhoon groups.

Volt Typhoon (aka UNC3236)

Volt Typhoon is a Chinese cyber warfare group which infiltrates critical infrastructure systems to create a long-term presence that may be used to compromise operational technology (OT). A February 2024 advisory by the US Cybersecurity and Infrastructure Agency (CISA) described the group's activities:

> "The U.S. authoring agencies have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions."



Characteristics of Volt Typhoon attacks outlined by the US Cyber and Infrastructure Security Agency (CISA). Indicative of broader strategy by the Chinese government to access critical infrastructure. Source: CISA advisory "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" February 2024.

In addition to targeting US critical infrastructure, the group also targeted Singtel Singapore's largest telecom operator, and parent company to Australia's second largest telecom provider.

IMPLICATIONS:

While the information about the current attack is limited, several factors can be inferred about why Chinese groups targeted Singapore and why Singapore may have responded in the way it did.

China is Linking Cyber Attacks to Support for Taiwan

The Wall Street Journal reported on April 10, 2025, that Chinese officials allegedly told US counterparts in December that China's years-long cyber attacks on American critical infrastructure were conducted in response to US support for Taiwan.

Singapore has long tried to conduct a diplomatic balancing act over the Taiwan issue. The country maintains a "One China Policy" but has robust trade and military relations with Taiwan. Singapore has conducted joint military training with Taiwan since 1975 under "Project Starlight." The countries signed a new Agreement on Defense Exchanges and

Security Cooperation in 2019, which has been the focus of Beijing's ire. Singapore is also a key partner supporting US naval operations in the Indo-Pacific aimed at deterring a Chinese invasion.

Chinese attacks may be designed to develop leverage that deters Singapore from taking a more active role in US strategy.

Threat Posed by Chinese Cyber Groups Worsening

Singapore's robust response, which both calls out China and incorporates the military into its cyber operations, is likely Singapore's own attempt to deter worsening attacks in the future. Singapore's Coordinating Minister for National Security K. Shanmugam says that the number of advanced persistent threat attacks on the country has quadrupled between 2021 and 2024. As discussed above, attacks by Chinese cyber groups are not only increasing in frequency but also escalating in severity, evolving from traditional theft and surveillance operations to targeting critical infrastructure.

It is not certain, but plausible that the involvement of Singapore's military may not have been a strategic escalation but rather a protective measure, designed to prevent the kind of cascading breach that allowed Chinese Salt Typhoon hackers to use compromised telecom companies' networks to access systems used by US Army National Guard and National Nuclear Security Administration. It is also plausible that the attack was severe and complex enough to require the support of Singapore's military to respond effectively.

Thanks for reading! If you enjoyed this article, please like and share it so others can stay informed on critical developments involving China, Russia, Iran and North Korea

Share

1
"Zero-days" are vulnerabilities unknown to security teams giving developers "0" days to fix them. Zero-day threats tend to be especially dangerous as they can be difficult to detect until an attacker is wreaking havoc within a system.

❤
6

Share this post

OPFOR Journal

Singapore Takes Unprecedented Military Action Against Chinese State-Sponsored Hackers

3

Share

Discussion about this post

No posts