Chinese group accused of hacking Singtel in telecom attacks

Published: 2024-11-05 · Archived: 2026-04-05 13:20:34 UTC

SINGAPORE – Singtel, Singapore's largest mobile carrier, was breached by Chinese state-sponsored hackers this summer as part of a broader campaign against telecommunications companies and other critical infrastructure operators around the world, according to two people familiar with the matter.

The previously undisclosed breach was discovered in June, and investigators believe it was pulled off by a hacking group known as Volt Typhoon, according to the two people, who asked not to be identified to discuss a confidential investigation.

Officials in the United States, Australia, Canada, Britain and New Zealand – the "Five Eyes" intelligence-sharing alliance – warned earlier in 2024 that Volt Typhoon was embedding itself inside compromised IT networks to give China the ability to conduct disruptive cyber attacks in the event of a military conflict with the West.

The breach of Singtel, a carrier with operations throughout South-east Asia and Australia, was seen as a test run by China for further hacks against US telecommunications companies, and information from the attack has provided clues about the expanding scope of suspected Chinese attacks against critical infrastructure abroad, including in the US, the people said.

In a joint statement on Nov 5, the Cyber Security Agency of Singapore (CSA) and Infocomm Media Development Authority (IMDA) said they understood from Singtel that no service was affected, and no data loss was reported from the incident.

They added that in this case, early detection and mitigation measures were in place.

"Based on current investigations, the threat has been dealt with and the overall telecommunications infrastructure remains secure and unaffected. CSA and IMDA will continue to work with organisations, especially key service providers including Singtel to strengthen the security and resilience of our digital infrastructure," they said.

Singtel on Nov 5 said "there was a malware detected in June which was subsequently dealt with and reported to relevant authorities", but added that the telco cannot confirm or ascertain if that was the exact same event reported by Bloomberg.

"We do not comment on speculation. Singtel conducts regular malware sweeps as part of its cyber posture," it noted.

Spokesperson Liu Pengyu for the Chinese Embassy in Washington said he was not aware of the specifics as relayed by Bloomberg, but that in general, China firmly opposes and combats cyber attacks and cyber theft.

The US is currently battling its own suspected Chinese attacks of political campaigns and telecommunications companies. Officials have described the telecom breaches as one of the most damaging campaigns on record by suspected Chinese hackers and one that they are still seeking to fully understand and contain.

In the US telecommunications attacks, which investigators have attributed to another Chinese group called Salt Typhoon, AT&T Inc and Verizon Communications Inc were among those breached, and the hackers potentially accessed systems the federal government uses for court-authorised network wiretapping requests, the Wall Street Journal reported in early October.

US intelligence officials think the Chinese hacking group that Microsoft Corp dubbed Salt Typhoon may have been inside US telecommunications companies for months and found a route into an access point for legally authorised wiretapping, according to a person familiar with their views.

AT&T declined to comment. Verizon did not respond to a request for comment.

Through those intrusions, the hackers are believed to have targeted the phones of former president and Republican presidential candidate Donald Trump, his running mate J.D. Vance and Trump family members, as well as members of Vice-President Kamala Harris' campaign staff and others, The New York Times has reported.

In the case of the alleged Singtel breach, one of the people familiar with that incident said the attack relied on a tool known as a web shell.

In August, researchers at Lumen Technologies Inc said in a blog post they assessed with "moderate confidence" that Volt Typhoon had used such a web shell.

A sample of the malware was first uploaded to VirusTotal, a popular site for security experts to research malicious code, on June 7 by an unidentified entity in Singapore, according to Lumen researchers.

The web shell allowed hackers to intercept and gather credentials to gain access to a customer's network disguised as a bona fide user, they said. The hackers then breached four US firms, including internet service providers, and another in India, according to Lumen researchers.

General Timothy Haugh, director of the National Security Agency (NSA), said in early October that the investigations into the latest telecommunications breaches were at an early stage.

Later in October, the FBI and the Cybersecurity and Infrastructure Security Agency (Cisa) said they had identified specific malicious activity by actors affiliated with the Chinese government and immediately notified affected companies and "rendered technical assistance".

A spokesperson for the National Security Council last week referred to the "ongoing investigation and mitigation efforts", but directed further questions to the FBI and Cisa.

Singtel uncovered the breach of its network after detecting suspicious data traffic in a core back-end router and finding what it believed was sophisticated, and possibly state-sponsored, malware on it, according to the other person familiar with the investigation.

The malware was in "listening" mode and didn't appear to have been activated for espionage or any other purpose, the person said, adding that it reinforced a suspicion that the attack was either a test run of a new hacking capability or that its purpose was to create a strategic access point for future attacks.

There is evidence that Salt Typhoon reached the US at least as early as spring 2024, and possibly long before, and investigators tracking the group think it has infiltrated other telecommunications companies throughout Asia, including in Indonesia, Nepal, the Philippines, Thailand and Vietnam, according to two people familiar with those efforts.

The NSA has warned since 2022 that telecommunications infrastructure was vulnerable to Chinese hacking. Volt Typhoon has been active since at least mid-2020, having attacked sensitive networks in Guam and elsewhere in the US with a goal of burrowing into critical infrastructure and staying undetected for as long as possible.

The hacks by both Chinese Typhoon groups have alarmed Western officials and raised concerns about the number and severity of back doors – a way to get around security tools and gain high-level access to a computer system – that China has placed inside critical IT systems. Those entry points could be used to conduct espionage or prepare the battlespace for use in a potential military conflict with the West.

Chinese hackers have long been accused of conducting espionage attacks against the US – including, most notably, the theft of security clearance applications for tens of millions of US government workers held by the Office of Personnel Management.

But officials say the latest hacks go a step further and in some cases suggest China may be amassing capabilities to disrupt or degrade critical services in the US and abroad.

Retired general Paul Nakasone, who led the NSA for nearly six years until February, told reporters in October that the latest telecommunications hacks by Salt Typhoon were distinguished by their scale, and that the two Chinese groups represent a tremendous challenge for the government. “I am not pleased in terms of where we’re at with either of the Typhoons,” he said. BLOOMBERG

Source: https://www.straitstimes.com/business/chinese-group-accused-of-hacking-singtel-in-telecom-attacks