Volt Typhoon false narrative a collusion among US politicians, intelligence community and companies to cheat funding, defame China: report

By Yuan Hong Published: Apr 15, 2024 09:01 AM Updated: Apr 15, 2024 10:30 PM

Cartoon: GT

Labelling Volt Typhoon, a hacker group, as a China-sponsored actor, has been found to be an underhanded campaign by US politicians, intelligence community and companies, which intended to "kill two birds with one stone" - hyping the "China threat theory" and cheating funding from the US Congress and taxpayers, according to a latest report from China's National Computer Virus Emergency Response Center obtained by the Global Times.

On May 24, 2023, the cybersecurity authorities from The Five Eyes countries - the US, UK, Australia, Canada and New Zealand, issued a joint cybersecurity advisory, claiming that they had discovered cluster of activity of interest associated with a "China state-sponsored cyber actor," known as Volt Typhoon, and these activities "affected networks across US critical infrastructure sectors."

The advisory cited a report, which was released by Microsoft on the same day as its main reference with the name Volt Typhoon also cited in the Microsoft report. In the report, Microsoft claimed that the Volt

Typhoon is a state-sponsored actor based in China that typically focuses on espionage and information gathering.

Later, major Western news outlets such as Reuters, Wall Street Journal and New York Times widely reported about the advisory and the Microsoft report. In a report on May 24, The New York Times wrote that US intelligence agencies identified cyberattacks against telecom operator in Guam and other US territory, and connected it with the advisory.

Using this as an excuse, the US has taken a series of actions targeting so-called "cyberattack" from China. For example, In February, 2024, the White House issued an executive order that is designed to improve maritime port security by creating new requirements for stronger cyber defenses in the sector while expanding the authorities of the US Coast Guard to respond to cybersecurity incidents. And US media noted that such an action followed the warning about the "China-linked hacking group Volt Typhoon."

In response, China's National Computer Virus Emergency Response Center, National Engineering Laboratory for Computer Virus Prevention Technology and 360 Digital Security Group conducted a joint investigation and further analysis found that Volt Typhoon has more correlation with ransomware group or other cybercriminals.

Multiple cybersecurity authorities in the US have been pushing "China-sponsored" Volt Typhoon false narrative just for seeking more budgets from the US Congress. Meanwhile, Microsoft and other US cybersecurity companies also want more big contracts from US cybersecurity authorities, according to a report about the investigation.

A related investigation began since May 2023 when the US started to "disclosed" information about Volt Typhoon, an expert familiar with the investigation told the Global Times.

Although the advisory of the Five Eyes and the report of Microsoft described the tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs) of Volt Typhoon, they labeled it a "China State-Sponsored Cyber Actor" without offering any attribution details.

The investigation group made statistics of the sample information given by Microsoft report and the advisory released by the Five Eyes and obtained 29 samples after removing duplicates. They then used VirusTotal - a multi-engine virus scanner platform of Google to search the samples one by one and only found 13 samples.

Each of the 13 samples is associated with multiple IP addresses and each IP address links to multiple samples.

Experts analyzed five IP addresses and discovered that they are related to other cyberattack events and there are multiple IP addresses associated with the same cyberattack event or cybersecurity risk. The five IP addresses also related to one cyberattack event, which ThreatMon - a US cybersecurity vendor mentioned on April 11, 2023 in a report titled "The Rise of Dark Power: A Close Look at the Group and their Ransomware."

According to ThreatMon, Dark Power was first observed to have started its attacks in January 2023, which means the group was active before 2023. And at least 10 institutions worldwide were attacked and blackmailed by Dark Power in March 2023 alone, and "there was no country and sectoral connection." The victims were from Algeria, Egypt, the Czech Republic, Turkey, Israel, Peru, France and the US.

Experts from the investigation group also searched the malware samples and IP address in the report published by Lumen Technologies but could not find any link to the IoCs of the Microsoft's technical analysis report and the cybersecurity advisory of the Five Eyes alliance.

Lumen Technologies also released an analysis report linking the KV-botnet - a small office and home office (SOHO) router botnet that forms a covert data transfer network for advanced threat actors, to Volt Typhoon, on December 13, 2023.

Following further analysis, it was found that the actor of Volt Typhoon is related to the cybercriminal group named Dark Power, but Microsoft and the Five Eyes were very hasty to label it as "China-sponsored actor," according to the report.

Volt Typhoon hacker group is a ransomware cybercriminal organization without state or regional support background, Chinese Foreign Ministry spokesperson Lin Jian said at a regular press conference on Monday commenting on the investigation report, saying that various signs indicate that US intelligence community and cybersecurity companies are colluding to fabricate so-called evidence and spread false information that the Chinese government supports cyberattacks against the US, in order to seek congressional budget appropriations and government contracts.

The spokesperson stated that it is known to all that the US is the biggest source of cyberattacks and the biggest threat to cybersecurity. For some time, some people in the US have been using "cyberattacks tracing" as a tool to suppress China, politicizing cybersecurity issues, and seriously infringing on China's legitimate rights and interests. China urges the US to immediately cease cyberattacks against China and stop slandering and smearing China, Lin noted.

For the money

Why is the US which boasts most powerful internet technology, so eager to pin the blame of Volt Typhoon on China? The report on the investigation offered some clues.

The report revealed that the two US companies that mentioned Volt Typhoon are partners of the US government. Just two months before Microsoft released its report, it received the first list of task orders worth approximately $3.8 million for the $9 billion Joint Warfighting Cloud (JWCC) project from the US Department of Defense on March 24, 2023.

And one month before Lumen Technologies released an analysis report linking the KV-Botnet to the Volt Typhoon, Lumen Technologies had just won a five-year contract order worth $110 million from the US Defense Information Systems Agency (DISA) on November 7, 2023, according to the report.

Moreover, under the Budget and Accounting Act issued by 1921, the US president must submit a budget report, including the federal government's budget request for the next fiscal year, to the Congress on first Monday in February. Coincidently, a hearing held by the House Select Committee on cyberattack of China to the American Homeland and National Security was held on January 31, 2024.

During the hearing, officials from US cyber agencies claimed that Volt Typhoon posed a threat to the US national security and asked the Congress to increase more funds in the field of cybersecurity.

Eventually, in the 2025 fiscal year budget request announced by the Biden administration on March 11, the federal government's cybersecurity budget in the civil administrative departments and agencies reached a record $13 billion, according to public information.

Among listed items, the budget for the Cybersecurity and Infrastructure Security Agency, reached $3 billion, an increase of $103 million from the previous year. The budgets of the US Department of Justice and the Federal Bureau of Investigation increased by $25 million specifically for the "cyber and counterintelligence investigative capabilities."

The 2024 US Presidential election is approaching. Neither the Republican nor Democratic parties want to lose votes on the issue of China during the campaign, and by openly denouncing China, members of Congress can also attract public attention and gain influence, analysts said.

Some US departments and companies are seeking to make a fortune from the related false narrative of Volt Typhoon while attempting to defame China, sow discords between China and other countries to contain China's development, said the report.

The US government and politicians always keep "small yard and high fence" policies, and even politicizing cyberattacks origin-tracing, manipulating Microsoft and other companies to launch a smearing campaign against China to line their own pockets, according to the report.

These Volt Typhoon narratives are not beneficial to the normal order of the international public cyberspace but only undermine China-US relations, and finally eat their own bitter fruit, according to the report.

https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf