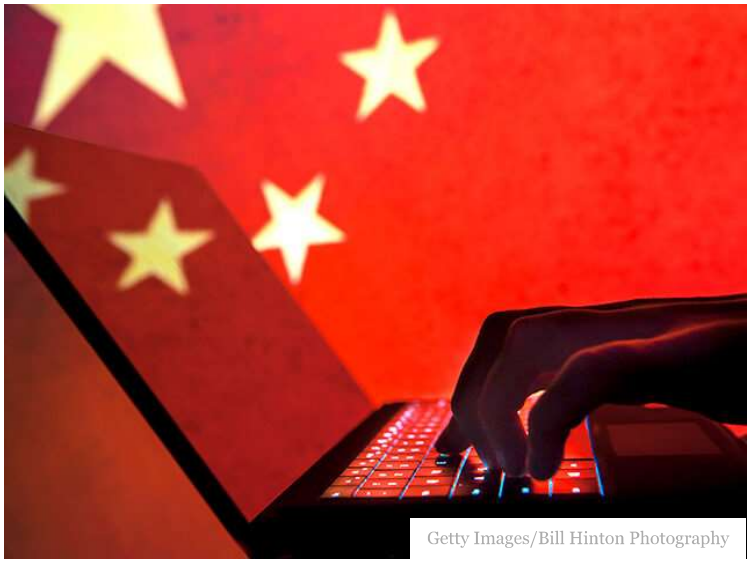
BREITBART

FBI FINDS CHINESE STATE HACKER MALWARE ON HUNDREDS OF U.S. INFRASTRUCTURE-RELATED ROUTERS



Getty Images/Bill Hinton Photography

by JOHN HAYWARD | 1 Feb 2024

The Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) on Wednesday announced they were able to disrupt a massive Chinese cyber-espionage campaign called Volt Typhoon that penetrated critical American infrastructure systems.

Volt Typhoon was detected and made public by Microsoft's cybersecurity team in May 2023. Microsoft described the perpetrators as state-sponsored hackers from China who were developing "capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises."

Microsoft's conclusions were backed by the intelligence agencies of the "Five Eyes" alliance: the U.S., UK, Canada, Australia, and New Zealand. China denied the allegations and accused the Five Eyes nations of pushing "disinformation."

Volt Typhoon's activities were originally thought to be centered on Guam, with the goal of disrupting American network communications across the Pacific in the event of a conflict with China, such as China might cause by invading Taiwan. Further investigation showed the scope of the operation was much greater, with targets including West Coast ports, oil pipelines, and the power grid of Texas.

The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) said in December that China was clearly "pre-positioning" cyber warfare assets to "disrupt or destro that critical infrastructure in the event of a conflict, to either prevent the United States from being able to project power into Asia or to caus societal chaos inside the United States."

Volt Typhoon was cited by cybersecurity experts as one of the biggest, most dangerous examples of "living off the land," a technique in which hackers infiltrate a system without causing any damage or revealing their presence, using tools that mimic normal network activity. As DH put it, the Chinese operation was all about scouting ahead and preparing for destructive attacks that could be triggered if the U.S. and China came into conflict.

DOJ said on Wednesday that the U.S. and its allies have stepped up their efforts against threats like Volt Typhoon, and that particular threat has been "disrupted" by purging its malicious software from hundreds of routers. U.S. officials remained certain that Chinese state-sponsored hackers were responsible for the intrusions.

Sean Newell, deputy chief of the Justice Department's National Security Division, explained that Volt Typhoon's hackers created a "botnet" hidden inside network routers that concealed their other hacking activities. The compromised routers, which were mostly older Cisco and Netgear models nearing the end of their operational lifespans, allowed the hackers to work in secret, without security programs detecting their unusual network traffic.

CISA Director Jen Easterly warned that China's hackers have grown very adept at lurking undetected inside computer systems.

"They've elevated their ability to act like a system administrator so you really can't tell that's a Chinese actor," Easterly said.

Security Week reported some concerns in the cybersecurity community that Volt Typhoon might not be completely "disrupted," because it was able to penetrate "thousands of organizations," but the FBI's court orders covered only hundreds of infected routers.

The FBI essentially managed to find a way to order the malware in the infected routers to delete itself, without damaging the routers or the systems that relied upon them. The owners of those routers do not appear to have been warned in advance, but the FBI said it is attempting to notify all of them now and provide some security advice.

Some hardware experts said the routers may not be completely purged of Volt Typhoon's influence, so it would be safest to replace them all, as quickly as possible.

FBI Director Christopher Wray told the House Select Committee on the Chinese Communist Party that the nearly-obsolete routers were "easy targets" for the hackers, whose activities targeted water, power, oil, and transportation systems.

Wray said the FBI also believes China will try to interfere in the 2024 elections, as it did in Taiwan's recent presidential race. He pointed to the tremendous amount of information Chinese applications like TikTok collect about their users as potential espionage weapons since the Chinese military apparatus is legally guaranteed at-will access to all data compiled by Chinese corporations.

"Today, and literally every day, they're actively attacking our economic security, engaging in wholesale theft of our innovation, and our personal and corporate data," said Wray.

CISA issued a bulletin to router manufacturers this week that explained how Volt Typhoon was able to hijack their hardware. CISA and the FBI asked manufacturers to eliminate the vulnerabilities that were exploited by the Chinese hacking group and "build security into the design, development, and maintenance" of their products. Among the suggestions included in the bulletin was programming routers to download software updates automatically, and making it harder to disable network security remotely.