# What is Volt Typhoon? Cybersecurity expert explains the Chinese hackers targeting US critical infrastructure

April 1 2024, by Richard Forno

Credit: Karolina Grabowska from Pexels

Volt Typhoon is a Chinese state-sponsored hacker group. The United States government and its primary global intelligence partners, known as the Five Eyes, issued a warning on March 19, 2024, about the group's activity targeting critical infrastructure.

The warning echoes analyses by the cybersecurity community about Chinese state-sponsored hacking in recent years. As with many cyberattacks and attackers, Volt Typhoon has many aliases and also is known as Vanguard Panda, Bronze Silhouette, Dev-0391, UNC3236, Voltzite and Insidious Taurus. Following these latest warnings, China again denied that it engages in offensive cyberespionage.

Volt Typhoon has compromised thousands of devices around the world since it was publicly identified by security analysts at Microsoft in May 2023. However, some analysts in both the government and cybersecurity community believe the group has been targeting infrastructure since mid-2021, and possibly much longer.

Volt Typhoon uses malicious software that penetrates internet-connected systems by exploiting vulnerabilities such as weak administrator passwords, factory default logins and devices that haven't been updated regularly. The hackers have targeted communications, energy, transportation, water and wastewater systems in the U.S. and its territories, such as Guam.

In many ways, Volt Typhoon functions similarly to traditional botnet operators that have plagued the internet for decades. It takes control of vulnerable internet devices such as routers and security cameras to hide and establish a beachhead in advance of using that system to launch future attacks.

Operating this way makes it difficult for cybersecurity defenders to accurately identify the source of an attack. Worse, defenders could accidentally retaliate against a third party who is unaware that they are caught up in Volt Typhoon's botnet.

## Why Volt Typhoon matters

Disrupting critical infrastructure has the potential to cause economic harm around the world. Volt Typhoon's operation also poses a threat to the U.S. military by potentially disrupting power and water to military facilities and critical supply chains.

Microsoft's 2023 report noted that Volt Typhoon could "disrupt critical communications infrastructure between the United States and Asia region during future crises." The March 2024 report, published in the U.S. by the Cybersecurity and Infrastructure Security Agency, likewise warned that the botnet could lead to "disruption or destruction of critical services in the event of increased geopolitical tensions and/or military conflict with the United States and its allies."

Volt Typhoon's existence and the escalating tensions between China and the U.S., particularly over Taiwan, underscore the latest connection between global events and cybersecurity.

## Defending against Volt Typhoon

The FBI reported on Jan. 31, 2024, that it had disrupted Volt Typhoon's operations by removing the group's malware from hundreds of small office/home office routers. However, the U.S. is still determining the extent of the group's infiltration of America's critical infrastructure.

On March 25, 2024, the U.S. and U.K. announced that they had imposed

sanctions on Chinese hackers involved in compromising their infrastructures. And other countries, including New Zealand, have revealed cyberattacks traced back to China in recent years.

All organizations, especially infrastructure providers, must practice time-tested safe computing centered on preparation, detection and response. They must ensure that their information systems and smart devices are properly configured and patched, and that they can log activity. And they should identify and replace any devices at the edges of their networks, such as routers and firewalls, that no longer are supported by their vendor.

Organizations can also implement strong user-authentication measures such as multifactor authentication to make it more difficult for attackers like Volt Typhoon to compromise systems and devices. More broadly, the comprehensive NIST Cybersecurity Framework can help these organizations develop stronger cybersecurity postures to defend against Volt Typhoon and other attackers.

Individuals, too, can take steps to protect themselves and their employers by ensuring their devices are properly updated, enabling multifactor authentication, never reusing passwords, and otherwise remaining vigilant to suspicious activity on their accounts, devices and networks.

For cybersecurity practitioners and society generally, attacks like Volt Typhoon can represent an enormous geopolitical cybersecurity threat. They are a reminder for everyone to monitor what's going on in the world and consider how current events can affect the confidentiality, integrity and availability of all things digital.

This article is republished from The Conversation under a Creative

Commons license. Read the original article.

Provided by The Conversation

Citation: What is Volt Typhoon? Cybersecurity expert explains the Chinese hackers targeting US critical infrastructure (2024, April 1) retrieved 2 May 2024 from https://techxplore.com/news/2024-04-volt-typhoon-cybersecurity-expert-chinese.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.