Volt Typhoon's future war

By Barracuda Networks

Published: 2024-03-14 · Archived: 2026-04-05 21:02:47 UTC

There are many dangerous threat actors out there, but Volt Typhoon could be the most dangerous to our physical safety and well-being. We already know that cyberattacks have an impact beyond the digital realm. Colonial Pipeline and JBS Foods suffered ransomware attacks that disrupted critical supply chains in the United States. Threat actors have already interfered with the U.S. economy and critical infrastructure. Most of this cybercrime is motivated by financial gain. Lockbit and ALPHV both claimed to be apolitical and only interested in money.

Other threat actors engage in cyber espionage and cyber warfare. Traditional cyber espionage refers to attacks that give the threat actors a competitive edge over another company or government entity. One example of cyber espionage is the string of attacks on universities that conduct research and development activities for military applications. Espionage usually involves the work of Advanced Persistent Threats (APTs) that stay in the system and gather information or perform destructive activities for as long as possible. In contrast, cyber warfare is likely to be a fast attack intended to disrupt activities and create chaos for strategic purposes. The 2017 Russian attack on Ukrainian targets (WannaCry, NotPetya) was an act of cyber warfare.

We're all familiar with cyberattacks, cyber espionage, and cyber warfare. So, what's the big deal about Volt Typhoon?

What is Volt Typhoon?

Volt Typhoon is also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus. This group is an APT actor sponsored by the People's Republic of China (PRC). Volt Typhoon has been conducting traditional cyber espionage activities against U.S. targets since mid-2021, though. U.S. officials have since discovered that Volt Typhoon has been "maintaining access and footholds within some victim IT environments for at least five years." These victim organizations operate primarily in communications, energy, transportation, and water/wastewater sectors in the United States. Targeting critical sectors is nothing new, but Volt Typhoon's targets hint at a different type of attack. From Reuters:

"We are extraordinarily concerned about malicious cyber activity from the PRC state-sponsored actor that industry calls Volt Typhoon," a senior CISA official, Eric Goldstein, referring to the People's Republic of China, told Reuters ahead of the statement's release. "Most of the victims we have identified have no legitimate espionage value."

This brings us to the Cybersecurity Advisory published in February, alerting U.S. entities and the public about something called 'pre-positioning.'

Traditional cyber espionage vs. pre-positioning.

Pre-positioning attacks are attempts to infiltrate critical systems for potential future sabotage. This differs from traditional cyber espionage motivated by immediate data theft or intelligence gathering. When Volt Typhoon compromises a system, a human threat actor begins hands-on-keyboard activity and uses living-off-the-land techniques to move laterally through the network, avoid detection, and establish a long-term hidden and dormant threat. The group rarely uses malware in its attacks. The hands-on activity and the absence of malware show a high level of engagement and sophistication by Volt Typhoon.

Pre-positioning represents a strategic shift by a PRC threat actor to prepare for future tensions or military conflicts. Although U.S. officials now have evidence of long-term pre-positioning activity, this Center for Strategic and International Studies (CSIS) research on Chinese espionage does not mention pre-positioning in any attack. The CSIS research studied attacks on U.S. entities during the years 2000–2023. This is a partial demographic breakdown of that data:

- 49% of incident directly involved Chinese military or government employees.
- 46% of incidents involved cyber espionage, usually by State-affiliated actors.

- 29% of incidents sought to acquire military technology.
- 54% of incidents sought to acquire commercial technologies.
- 17% of incidents sought to acquire information on U.S. civilian agencies or politicians.

This research only analyzed attacks that were known to the public. Unreported attacks and classified information are excluded.

The ability of state-sponsored actors to embed themselves within essential systems poses a direct physical threat to the people of the United States and other targeted countries. A disruption in the critical systems in the U.S. could force a federal response that consumes a significant portion of U.S. resources. This could then reduce U.S. capability to assist foreign allies. In June 2022, the PRC denied any involvement in cyber espionage:

A spokesman for the Chinese embassy in Washington, Liu Pengyu, rejected the allegations from the western leaders, saying in an emailed statement to the Associated Press that China "firmly opposes and combats all forms of cyber-attacks" and calling the accusations groundless.

"We will never encourage, support or condone cyber-attacks," the statement said.

The U.S. isn't the only target of Volt Typhoon and other PRC threat actors. Volt Typhoon has attacked critical infrastructure and economic sectors in Australia, Canada, and the United Kingdom. It has also conducted extensive reconnaissance attacks on electric transmission and distribution organizations in African nations. The intent of these attacks in Africa is unknown, though experts speculate the threat actors were looking for geographic information systems (GIS) data, which would help Volt Typhoon infiltrate clusters of Industrial Control Systems (ICS) and other Internet of Things (IoT) devices. There may also be a connection to China's Digital Silk Road Initiative, which aims to offer infrastructure assistance and other aid to recipient nations. The People's Republic of China has strategic interests around the world.

China routinely denies any involvement in state-sponsored hacking, and has promised the U.S. that it would not interfere with 2024 elections. Despite these denials, law enforcement agencies around the world have compiled decades of evidence of PRC-sponsored cyber espionage. Federal Bureau of Investigation (FBI) Director Christopher Wray believes "China's cyber operatives outnumber all FBI agents by at least 50 to 1."

KV Botnet

Volt Typhoon uses the KV Botnet, a covert network, to conceal malicious traffic by blending it with regular internet traffic. The botnet uses routers and VPN devices that are 'end of life' and no longer receive security updates from the manufacturer. The U.S. Department of Justice (DoJ) recently announced a successful disruption of the botnet, though Volt Typhoon is attempting a rebuild.

Volt Typhoon moves its traffic through two separate KV Botnet clusters known as KV and JDY. This table outlines the purposes of these clusters and the key differences between them.:

Aspect	KV Cluster	JDY Cluster

Primary Purpose	Proxying manual operations against high-profile targets	Scanning and reconnaissance activities
Complexity of Work	Sophisticated, targeted efforts	Less sophisticated, automated tasks
Type of Infected Devices	Small office/home office routers and certain IP cameras	Cisco RV320 and RV325 routers
Use of Infected Nodes	Effective use for manual covert operations	Effective for automated scanning and reconnaissance
Risk Management	Lower risk of detection for manual operations. Higher-risk JDY activities do not endanger KV cluster activities.	Higher risk of detection due to automated widespread activities

The technical breakdown of the KV Botnet is here.

Conclusion

Volt Typhoon is a sophisticated, state-sponsored threat actor that will find its way into any opening of any system. They have the skills and resources to attack any weakness they find. A good defense against them is to make sure they do not find any weaknesses. U.S. Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly recently stated that the U.S. has made it easy for PRC threat actors to attack. “The truth is that, in many cases, the PRC is taking advantage of known product defects.” The KV Botnet is the perfect example of how threat actors take advantage of neglected security risks.

Protecting your systems from sophisticated threat actors like Volt Typhoon requires a multi-layered approach to cybersecurity that defends the entire system, including remote workers and edge devices:

1. Strong Access Controls and Authentication Measures – Enforce policies that require multi-factor authentication (MFA) and good password hygiene. Use the principle of least privilege to ensure that users have only the access rights they need to perform their work.

2. Regular Software and System Updates – Regularly update all software, operating systems, and firmware using automated patch management tools when possible. Conduct regular scans to identify any vulnerabilities in the environment.

3. Advanced Security Measures – Deploy cybersecurity solutions that protect your email, network, applications, and data. Barracuda Email Protection and Barracuda SecureEdge defend your systems, backup your Microsoft 365 data, and provide security awareness training to help employees spot phishing attacks and other scams.

Continuous monitoring, regular updates to your security protocols, and staying informed about the latest threats are crucial to maintaining robust security.

Barracuda Cybersecurity Platform

Only Barracuda provides multi-faceted protection that covers all the major threat vectors, protects your data, and automates incident response. Over 200,000 customers worldwide count on Barracuda to protect their email, networks, applications, and data.
