Volt Typhoon - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:30:37 UTC

APT group: Volt Typhoon

Names	Volt Typhoon *(Microsoft)* Vanguard Panda *(CrowdStrike)* Bronze Silhouette *(SecureWorks)* Redfly *(Symantec)* Insidious Taurus *(Palo Alto)* VOLTZITE *(Dragos)* Dev-0391 *(Microsoft)* Storm-0391 *(Microsoft)* UNC3236 *(Mandiant)* UAT-5918 *(Talos)* UAT-7237 *(Talos)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2020
Description	(Microsoft) Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises. Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States. In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible. Microsoft is choosing to highlight this Volt Typhoon activity at this time because of our significant concern around the potential for further impact to our customers. Although our visibility into

	these threats has given us the ability to deploy detections to our customers, the lack of visibility into other parts of the actor's activity compelled us to drive broader community awareness and further investigations and protections across the security ecosystem.	
Observed	Sectors: Construction, Education, Energy, Government, Industrial, IT, Maritime and Shipbuilding, Manufacturing, Telecommunications, Transportation, Utilities. Countries: Australia, Canada, India, Singapore, Taiwan, UK, USA.	
Tools used	FRP, Impacket, Living off the Land.	
Operations performed	Jun 2021	Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations <https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations>
	Feb 2022	Routers Roasting on an Open Firewall: the KV-botnet Investigation <https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/>
	2023	Hunting Active Threats in Littleton's Grid with the Dragos Platform and OT Watch <https://www.dragos.com/wp-content/uploads/2025/03/Dragos_Littleton_Electric_Water_CaseStudy.pdf>
	2023	UAT-5918 targets critical infrastructure entities in Taiwan <https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/>
	Feb 2023	Redfly: Espionage Actors Continue to Target Critical Infrastructure <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks>
	Jun 2023	Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign <https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign>
	Jun 2023	Business as Usual: Falcon Complete MDR Thwarts Novel VANGUARD PANDA (Volt Typhoon) Tradecraft <https://www.crowdstrike.com/blog/falcon-complete-thwarts-vanguard-panda-tradecraft/>
	Jul 2023	China's Volt Typhoon APT Burrows Deeper Into US Critical Infrastructure <https://www.darkreading.com/vulnerabilities-threats/china-s-volt-typhoon-apt-burrows-us-critical-infrastructure>

	Dec 2023	Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days <https://resources.securityscorecard.com/research/volt-typhoon>
	Dec 2023	KV-Botnet: Don’t call it a Comeback <https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/>
	Jun 2024	Taking the Crossroads: The Versa Director Zero-Day Exploitation <https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/>
	Jun 2024	Chinese group accused of hacking Singtel in telecom attacks <https://www.straitstimes.com/business/chinese-group-accused-of-hacking-singtel-in-telecom-attacks>
	Aug 2025	UAT-7237 targets Taiwanese web hosting infrastructure <https://blog.talosintelligence.com/uat-7237-targets-web-hosting-infra/>
Counter operations	Dec 2023	U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>
Information	<https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/> <https://www.securityweek.com/mandiant-intelligence-chief-raises-alarm-over-chinas-volt-typhoon-hackers-in-us-critical-infrastructure/> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> <https://hub.dragos.com/hubfs/116-Datasheets/Dragos_IntelBrief_VOLTZITE_FINAL.pdf> <https://blog.barracuda.com/2024/03/14/volt-typhoon-future-war> <https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c.pdf> <https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/> <https://therecord.media/china-accused-misusing-western-cybersecurity-research-volt-typhoon> <https://therecord.media/china-cyber-agency-claims-us-interference-volt-typhoon-research> <https://thehackernews.com/2024/10/china-accuses-us-of-fabricating-volt.html> <https://www.securityweek.com/china-admitted-to-us-that-it-conducted-volt-typhoon-attacks-report/> <https://therecord.media/china-typhoon-hackers-nsa-fbi-response>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
