Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:39:30 UTC

APT group: UNC5221, UTA0178

Names	UNC5221 *(Mandiant)* UTA0178 *(Volexity)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2022	
Description	(Mandiant) Note: This is a developing campaign under active analysis by Mandiant and Ivanti. We will continue to add more indicators, detections, and information to this blog post as needed. On January 10, 2024, Ivanti disclosed two vulnerabilities, CVE-2023-46805 and CVE-2024-21887, impacting Ivanti Connect Secure VPN (“CS”, formerly Pulse Secure) and Ivanti Policy Secure (“PS”) appliances. Successful exploitation could result in authentication bypass and command injection, leading to further downstream compromise of a victim network. Mandiant has identified zero-day exploitation of these vulnerabilities in the wild beginning as early as December 2023 by a suspected espionage threat actor, currently being tracked as UNC5221.	
Observed	Countries: Worlwide.	
Tools used	BRICKSTORM, GLASSTOKEN, LIGHTWIRE, PySoxy, THINSPOOL, WARPWIRE, WIREFIRE, ZIPLINE.	
Operations performed	2022	NVISO analyzes BRICKSTORM espionage backdoor <https://blog.nviso.eu/wp-content/uploads/2025/04/NVISO-BRICKSTORM-Report.pdf>
	Mar 2025	Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) <https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability>

Information	<https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day> <https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/> <https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/>

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
