[Unnamed groups: China] - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:25:59 UTC

APT group: [Unnamed groups: China]

Names	[Unnamed groups: China] *(?)*	
Country	China	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
First seen	2018	
Description	These are reported APT activities attributed to a country, but not to an individual threat group.	
Observed	Sectors: Defense, Government. Countries: Cambodia, Japan, Myanmar, Netherlands, Taiwan, USA and Worlwide.	
Tools used	COATHANGER.	
Operations performed	Jan 2018	China blamed for data theft from US Navy contractor <https://www.zdnet.com/article/china-blamed-for-data-theft-from-us-navy-contractor/>
	Jun 2019	Mitsubishi Electric discloses security breach, China is main suspect <https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/>
	Feb 2020	China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware <https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5>
	Mar 2020	Unknown China-Based APT Targeting Myanmarese Entities <https://www.anomali.com/blog/unknown-china-based-apt-targeting-myanmarese-entities#When:14:00:00Z>
	Oct 2020	China hacked Japan’s sensitive defense networks, officials say <https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/>

	2021	Minority report: Fake human rights documents and websites used in cyberattacks targeting Uyghurs, a Turkic ethnic minority in China <https://blog.checkpoint.com/security/minority-report-fake-human-rights-documents-and-websites-used-in-cyberattacks-targeting-uyghurs-a-turkic-ethnic-minority-in-china/>
	Jan 2022	News Corp discloses hack from 'persistent' nation state cyber attacks <https://www.bleepingcomputer.com/news/security/news-corp-discloses-hack-from-persistent-nation-state-cyber-attacks/>
	Oct 2022	Amnesty International Canada breached by suspected Chinese hackers <https://www.bleepingcomputer.com/news/security/amnesty-international-canada-breached-by-suspected-chinese-hackers/>
	Oct 2022	Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China <https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally>
	Oct 2022	Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475) <https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw>
	2023	Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT <https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf> <https://english.ncsc.nl/latest/news/2024/june/10/ongoing-state-sponsored-cyber-espionage-campaign-via-vulnerable-edge-devices>
	Apr 2023	China-Taiwan Tensions Spark Surge in Cyberattacks on Taiwan <https://www.trellix.com/blogs/research/china-taiwan-tensions-spark-surge-in-cyberattacks-on-taiwan/>
	Sep 2023	Chinese APT Targeting Cambodian Government <https://unit42.paloaltonetworks.com/chinese-apt-linked-to-cambodia-government-attacks/>
	Oct 2023	Likely China-based Attackers Target High-profile Organizations in Southeast Asia <https://www.security.com/threat-intelligence/china-southeast-asia-espionage>
	Feb 2024	Hackers stole 'sensitive' data from Taiwan telecom giant: ministry <https://www.france24.com/en/live-news/20240301-hackers-stole-sensitive-data-from-taiwan-telecom-giant-ministry>
Counter operations	Jul 2021	The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-

		united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/>
	May 2024	Treasury Sanctions a Cybercrime Network Associated with the 911 S5 Botnet <https://home.treasury.gov/news/press-releases/jy2375>
	May 2024	911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation <https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation>
	Dec 2024	Treasury Sanctions Cybersecurity Company Involved in Compromise of Firewall Products and Attempted Ransomware Attacks <https://home.treasury.gov/news/press-releases/jy2742>
	Mar 2025	Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks <https://home.treasury.gov/news/press-releases/sb0042>
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2021-0727.pdf> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a> <https://us-cert.cisa.gov/ncas/alerts/aa20-258a> <https://www.cisa.gov/uscert/ncas/alerts/aa22-279a> <https://go.recordedfuture.com/hubfs/reports/cta-2024-0320.pdf> <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf> <https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks> <https://www.cyber.gc.ca/en/news-events/statement-peoples-republic-china-reconnaissance-canadian-systems> <https://www.sophos.com/en-us/content/pacific-rim> <https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/> <https://news.sophos.com/en-us/2024/10/31/pacific-rim-timeline/>	

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
