Salt Typhoon, GhostEmperor - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Salt Typhoon, GhostEmperor

Names	Salt Typhoon *(Microsoft)* GhostEmperor *(Kaspersky)* UNC2286 *(Mandiant)* FamousSparrow *(ESET)* Earth Estries *(Trend Micro)* RedMike *(Recorded Future)* Operator Panda *(CrowdStrike)*
Country	China
Sponsor	State-sponsored, Ministry of State Security
Motivation	Information theft and espionage
First seen	2020
Description	(Kaspersky) GhostEmperor is a Chinese-speaking threat actor that has mostly focused on targets in Southeast Asia, including several government entities and telecom companies. The group stands out because it uses a formerly unknown Windows kernel-mode rootkit. Rootkits provide remote control access over the servers they target. Acting covertly, rootkits are notorious for hiding from investigators and security solutions. To bypass the Windows Driver Signature Enforcement mechanism, GhostEmperor uses a loading scheme involving a component of an open-source project named “Cheat Engine.” This advanced toolset is unique and Kaspersky researchers see no similarity to already known threat actors. Kaspersky experts have surmised that the toolset has been in use since at least July 2020.
Observed	Sectors: Chemical, Education, Engineering, Government, Hospitality, Technology, Telecommunications, Transportation, NGOs and law firms. Countries: Afghanistan, Argentina, Bangladesh, Brazil, Burkina Faso, Canada, Egypt, Ethiopia, France, Germany, Guatemala, India, Indonesia, Israel, Lithuania,

	Malaysia, Mexico, Netherlands, Pakistan, Philippines, Saudi Arabia, Singapore, South Africa, Swaziland, Taiwan, Thailand, UK, USA, Vietnam.	
Tools used	certutil, Cobalt Strike, Crowdoor, Cryptmerlin, Deed RAT, Demodex, FuxosDoor, GHOSTSPIDER, HemiGate, MASOL RAT, Mimikatz, nbtscan, NinjaCopy, PsExec, PsList, ProcDump, SparrowDoor, TrillClient, WinRAR, Zingdoor.	
Operations performed	2020	Earth Estries Targets Government, Tech for Cyberespionage <https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html>
	Mar 2021	FamousSparrow: A suspicious hotel guest <https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/>
	Late 2023	The Return of Ghost Emperor's Demodex <https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/>
	Mar 2024	Chinese hackers breached National Guard to steal network configurations <https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-national-guard-to-steal-network-configurations/>
	Jul 2024	Chinese Hackers Infiltrate U.S. Internet Providers in Cyber Espionage Campaign <https://thehackernews.com/2024/09/chinese-hackers-infiltrate-us-internet.html>
	Jul 2024	You will always remember this as the day you finally caught FamousSparrow <https://www.welivesecurity.com/en/eset-research/you-will-always-remember-this-as-the-day-you-finally-caught-famoussparrow/>
	Sep 2024	AT&T, Verizon reportedly hacked to target US govt wiretapping platform <https://www.bleepingcomputer.com/news/security/atandt-verizon-reportedly-hacked-to-target-us-govt-wiretapping-platform/>
	Sep 2024	T-Mobile confirms it was hacked in recent wave of telecom breaches <https://www.bleepingcomputer.com/news/security/t-mobile-confirms-it-was-hacked-in-recent-wave-of-telecom-breaches/> <https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-t-mobiles-routers-to-scope-out-network/>
	Dec 2024	White House links ninth telecom breach to Chinese hackers <https://www.bleepingcomputer.com/news/security/white-house-

		links-ninth-telecom-breach-to-chinese-hackers/>
	Dec 2024	Chinese hackers also breached Charter and Windstream networks <https://www.bleepingcomputer.com/news/security/charter-and-windstream-among-nine-us-telecoms-hacked-by-china/>
	Dec 2024	RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers <https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf>
	Feb 2025	Telecom giant Viasat breached by China's Salt Typhoon hackers <https://www.bleepingcomputer.com/news/security/telecom-giant-viasat-breached-by-chinas-salt-typhoon-hackers/>
	Feb 2025	Canada says Salt Typhoon hacked telecom firm via Cisco flaw <https://www.bleepingcomputer.com/news/security/canada-says-salt-typhoon-hacked-telecom-firm-via-cisco-flaw/>
Counter operations	Jan 2025	US sanctions Chinese firm, hacker behind telecom and Treasury hacks <https://www.bleepingcomputer.com/news/security/us-sanctions-chinese-firm-hacker-behind-telecom-and-treasury-hacks/>
Information	<https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/> <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/30094337/GhostEmperor_technical-details_PDF_eng.pdf> <https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html> <https://content.govdelivery.com/accounts/USDHSCISA/bulletins/3c1b400> <https://www.politico.com/news/2024/11/06/chinese-hackers-american-cell-phones-00187873> <https://therecord.media/us-agencies-confirm-china-telecom-hack-wiretaps> <https://www.trendmicro.com/en_us/research/24/k/earth-estries.html> <https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure> <https://therecord.media/eight-telcos-breached-salt-typhoon-nsc> <https://therecord.media/salt-typhoon-csrb-review> <https://docs.fcc.gov/public/attachments/DOC-408945A1.pdf> <https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor> <https://blog.talosintelligence.com/salt-typhoon-analysis/> <https://www.darkreading.com/cyberattacks-data-breaches/salt-typhoon-wake-up-call-critical-infrastructure> <https://www.darkreading.com/cyberattacks-data-breaches/what-should-us-do-salt-typhoon>	

	<https://www.bleepingcomputer.com/news/security/fbi-seeks-help-to-unmask-salt-typhoon-hackers-behind-telecom-breaches/> <https://spycloud.com/blog/state-secrets-for-sale-chinese-hacking/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
