Flax Typhoon - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:38:26 UTC

APT group: Flax Typhoon

Names	Flax Typhoon *(Microsoft)* Ethereal Panda *(CrowdStrike)* RedJuliett *(Recorded Future)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2021
Description	(Microsoft) Flax Typhoon has been active since mid-2021 and has targeted government agencies and education, critical manufacturing, and information technology organizations in Taiwan. Some victims have also been observed elsewhere in Southeast Asia, as well as in North America and Africa. Flax Typhoon focuses on persistence, lateral movement, and credential access. As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments. Flax Typhoon is known to use the China Chopper web shell, Metasploit, Juicy Potato privilege escalation tool, Mimikatz, and SoftEther virtual private network (VPN) client. However, Flax Typhoon primarily relies on living-off-the-land techniques and hands-on-keyboard activity. Flax Typhoon achieves initial access by exploiting known vulnerabilities in public-facing servers and deploying web shells like China Chopper. Following initial access, Flax Typhoon uses command-line tools to first establish persistent access over the remote desktop protocol, then deploy a VPN connection to actor-controlled network infrastructure, and finally collect credentials from compromised systems. Flax Typhoon further uses this VPN access to scan for vulnerabilities on targeted systems and organizations from the compromised systems.
Observed	Sectors: Education, Government, IT, Manufacturing. Countries: Djibouti, Hong Kong, Kenya, Laos, Malaysia, Philippines, Rwanda, South Korea, Taiwan, USA.

Tools used	China Chopper, BadPotato, JuicyPotato, Metasploit, Mimikatz, SoftEther VPN, Living off the Land.	
Operations performed	Mid 2023	Derailing the Raptor Train <https://blog.lumen.com/derailing-the-raptor-train/>
	Nov 2023	Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation <https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-0624.pdf>
Information	<https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/> <https://www.ic3.gov/CSA/2024/240918.pdf>	

Last change to this card: 22 February 2025

Download this actor card in PDF or JSON format
