Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:19:05 UTC

APT group: Gallium

Names	Gallium *(Microsoft)* Phantom Panda *(CrowdStrike)* Granite Typhoon *(Microsoft)* Alloy Taurus *(Palo Alto)* G0093 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2018	
Description	(Microsoft) To compromise targeted networks, GALLIUM target unpatched internet-facing services using publicly available exploits and have been known to target vulnerabilities in WildFly/JBoss. Once persistence is established in a network, GALLIUM uses common techniques and tools like Mimikatz to obtain credentials that allows for lateral movement across the target network. Within compromised networks, GALLIUM makes no attempt to obfuscate their intent and are known to use common versions of malware and publicly available toolkits with small modifications. The operators rely on low cost and easy to replace infrastructure that consists of dynamic-DNS domains and regularly reused hop points. This activity from GALLIUM has been identified predominantly through 2018 to mid-2019. GALLIUM is still active; however, activity levels have dropped when compared to what was previously observed.	
Observed	Sectors: Financial, Government, Telecommunications.	
Tools used	BlackMould, China Chopper, Cobalt Strike, Gh0stCringe RAT, HTran, LaZagne, Mimikatz, nbtscan, netcat, PingPull, Plink, Poison Ivy, PsExec, QuarkBandit, QuasarRAT, Reshell, SoftEther VPN, Sword2033, Windows Credentials Editor, WinRAR.	
Operations performed	Sep 2021	Chinese Alloy Taurus Updates PingPull Malware <https://unit42.paloaltonetworks.com/alloy-taurus/>

	Early 2022	Persistent Attempts at Cyberespionage Against Southeast Asian Government Target Have Links to Alloy Taurus <https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/>
	Jun 2022	GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool <https://unit42.paloaltonetworks.com/pingpull-gallium/>
Information	<https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0093/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
