Leviathan, APT 40, TEMP.Periscope - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:57:07 UTC

APT group: Leviathan, APT 40, TEMP.Periscope

Names	Leviathan *(CrowdStrike)* Kryptonite Panda *(CrowdStrike)* APT 40 *(Mandiant)* TEMP.Periscope *(FireEye)* TEMP.Jumper *(FireEye)* Bronze Mohawk *(SecureWorks)* Mudcarp *(iDefense)* Gadolinium *(Microsoft)* ATK 29 *(Thales)* ITG09 *(IBM)* TA423 *(Proofpoint)* Red Ladon *(PWC)* Gingham Typhoon *(Microsoft)* ISLANDDREAMS *(Google)* Jumper Taurus *(Palo Alto)* G0065 *(MITRE)*
Country	China
Sponsor	State-sponsored, Ministry of State Security, Hainan province
Motivation	Information theft and espionage
First seen	2013
Description	(FireEye) FireEye is highlighting a cyber espionage operation targeting crucial technologies and traditional intelligence targets from a China-nexus state sponsored actor we call APT40. The actor has conducted operations since at least 2013 in support of China’s naval modernization effort. The group has specifically targeted engineering, transportation, and the defense industry, especially where these sectors overlap with maritime technologies. More recently, we have also observed specific targeting of countries strategically important to the Belt and Road Initiative including Cambodia, Belgium, Germany, Hong Kong, Philippines, Malaysia,

	Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom. This China-nexus cyber espionage group was previously reported as TEMP.Periscope and TEMP.Jumper. Also see Hafnium.	
Observed	Sectors: Defense, Engineering, Government, Manufacturing, Research, Shipping and Logistics, Transportation and other Maritime-related targets across multiple verticals. Countries: Belgium, Cambodia, Germany, Hong Kong, Indonesia, Laos, Malaysia, Myanmar, New Zealand, Norway, Philippines, Saudi Arabia, Switzerland, Thailand, UK, USA, Vietnam and Asia Pacific Economic Cooperation (APEC).	
Tools used	AIRBREAK, BADFLICK, BlackCoffee, China Chopper, Cobalt Strike, DADJOKE, Dadstache, Derusbi, Gh0st RAT, GRILLMARK, HOMEFRY, LUNCHMONEY, MURKYTOP, NanHaiShu, PlugX, scanbox, SeDLL, Windows Credentials Editor, ZXShell, Living off the Land.	
Operations performed	2014	Spear-phishing maritime and defense targets Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe. <https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets>
	May 2017	Targeting UK-Based Engineering Company Using Russian APT Techniques Employees of a U.K.-based engineering company were among the targeted victims of a spear-phishing campaign in early July 2018. The campaign also targeted an email address possibly belonging to a freelance journalist based in Cambodia who covers Cambodian politics, human rights, and Chinese development. We believe both attacks used the same infrastructure as a reported campaign by Chinese threat actor TEMP.Periscope (also known as Leviathan), which targeted Cambodian entities in the run-up to their July 2018 elections. Crucially, TEMP.Periscope's interest in the U.K. engineering company they targeted dates back to attempted intrusions in May 2017. <https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/>

	2017	The current campaign is a sharp escalation of detected activity since summer 2017. Like multiple other Chinese cyber espionage actors, TEMP.Periscope has recently re-emerged and has been observed conducting operations with a revised toolkit. Known targets of this group have been involved in the maritime industry, as well as engineering-focused entities, and include research institutes, academic organizations, and private firms in the United States. <https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html>
	Jul 2018	Targeting Cambodia Ahead of July 2018 Elections FireEye has examined a range of TEMP.Periscope activity revealing extensive interest in Cambodia's politics, with active compromises of multiple Cambodian entities related to the country's electoral system. This includes compromises of Cambodian government entities charged with overseeing the elections, as well as the targeting of opposition figures. This campaign occurs in the run up to the country's July 29, 2018, general elections. <https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html>
	Jan 2020	The Malaysian Computer Emergency Response Team, a government-backed organization, said it had "observed an increase in [the] number of artifacts and victims involving a campaign against Malaysian government officials." <https://www.zdnet.com/article/malaysia-warns-of-chinese-hacking-campaign-targeting-government-projects/>
	2021	Parliamentary network breached by the PRC <https://www.beehive.govt.nz/release/parliamentary-network-breached-prc>
Counter operations	Jul 2021	Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>
Information	<https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html> <https://intrusiontruth.wordpress.com/2020/01/09/what-is-the-hainan-xiandun-technology-development-company/>	

	<https://intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu/> <https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/> <https://us-cert.cisa.gov/sites/default/files/publications/CSA_TTPs-of-Indicted-APT40-Actors-Associated-with-China-MSS-Hainan-State-Security-Department.pdf> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0065/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
