APT40

[/ˌeɪ.piːˈtiː ˈfɔːr.ti/]

APT40 is a China-aligned cyber espionage group active since the early 2010s and assessed to support PRC military and intelligence objectives. It primarily targets maritime, naval, defense, academic, and government sectors, especially in the Indo-Pacific region. The group poses a high risk due to its persistence, strong resources, and long-term access to victim networks, with recent activity observed through 2025.

IDENTITY

Attribution	: China-aligned APT widely assessed to support PRC military and intelligence priorities, often linked to naval and maritime strategic interests.
Active Since	: Early 2010s; continuously active through 2025.
Aliases	: ATK29, BRONZE MOHAWK, G0065, GADOLINIUM, Gingham Typhoon, ISLANDDREAMS, ITG09, KRYPTONITE PANDA, Leviathan, MUDCARP, Red Ladon, TA423, TEMP.Jumper, TEMP.Periscope.
Motivation	: Long-term cyber espionage focused on naval modernization, maritime logistics, defense research, and regional security planning.

TTPs

Initial Access	- Highly targeted spearphishing using maritime, defense, academic, and conference-related lures. - Impersonation of journalists, researchers, academics, and conference organizers. - Delivery of malicious attachments (documents, archives) and links to credential-harvesting portals. - Exploitation of known vulnerabilities in internet-facing services when available.
Execution	- Deployment of custom backdoors including ISLANDDREAMS and MUDCARP families. - Use of lightweight RATs for reconnaissance and command execution. - Fileless or semi-fileless execution using PowerShell and WMI.
Persistence	- Registry run keys and scheduled tasks. - Installation of malicious services masquerading as legitimate software. - Multiple redundant backdoors to maintain access if one is removed.
Command & Control (C2)	- Encrypted HTTPS-based C2 communications. - Use of hard-coded fallback domains and dynamic DNS. - Hosting of C2 on compromised servers and commercial VPS providers.
Defense Evasion	- Obfuscation of malware code and configuration data. - Extensive use of LOLBins to reduce malware footprint. - Low-and-slow operational tempo to avoid behavioral detection.
Data Exfiltration	- Exfiltration of emails, documents, engineering data, and credentials. - Compression and encryption prior to transfer. - Gradual, segmented data theft to evade monitoring and DLP controls.

TARGET PROFILE

Primary Sectors	: Naval and maritime industries, shipbuilding and repair companies, defense contractors, logistics
Secondary Sectors	: Government agencies, academic institutions, think tanks, aerospace and advanced manufacturing.
Geographic Focus	: Indo-Pacific nations, especially those involved in South China Sea disputes; additional targeting in North America and Europe.

THREAT ASSESSMENT

Risk Level	: High – disciplined, persistent, and strategically aligned with PRC maritime objectives.
Recent Activity	: Continued spearphishing campaigns and espionage operations against maritime, defense, and research targets.
Evolution	: Stable core tooling with gradual improvements in social engineering, infrastructure resilience, and OPSEC rather than radical technique shifts.

NOTABLE OPERATIONS

- **Maritime and Naval Espionage Campaigns:** Long-term intrusions into shipbuilding firms, naval suppliers, and maritime research institutions.
- **Government and Defense Targeting:** Compromise of agencies involved in maritime security and regional defense cooperation.
- **Academic Surveillance:** Persistent targeting of universities and think tanks researching naval strategy, maritime law, and Indo-Pacific security.