

BLACKTECH

[/ˈblæk tɛk/]

BlackTech (Canary Typhoon / CIRCUIT PANDA) is a China-aligned espionage group active since at least 2010, targeting government, defense, and telecommunications sectors across East Asia, Southeast Asia, and North America. The group specializes in router and edge device compromise, embedding backdoors into network firmware for long-term covert persistence.

IDENTITY

Attribution	: China-aligned APT assessed to operate on behalf of PRC state intelligence or military cyber units.
Active Since	: Early 2010s, with sustained and continuous activity through 2025.
Aliases	: CIRCUIT PANDA, Canary Typhoon, Earth Hundun, G0098, HUAPI, Manga Taurus, Palmerworm, Red Djinn, T-APT-03, Temp.Overboard.
Motivation	: Long-term cyber espionage focused on government policy, military planning, telecommunications visibility, and advanced technology acquisition.

TTPs

Initial Access	- Spearphishing with government, defense, or industry-specific lures. - Exploitation of vulnerabilities in internet-facing services, routers, VPNs, and firewalls. - Compromise of trusted third-party service providers and managed infrastructure. - Abuse of weak authentication and misconfigured remote management interfaces.
Execution	- Deployment of custom backdoors including Palmerworm and HUAPI variants. - Use of modular loaders for flexible payload delivery. - Heavy reliance on built-in system and network utilities rather than noisy malware.
Persistence	- Modification of firmware or startup scripts on network devices. - Creation of hidden or low-visibility administrative accounts. - Installation of stealth backdoors embedded within legitimate services. - Redundant access mechanisms to survive partial remediation.
Command & Control (C2)	- Encrypted communications over HTTPS or proprietary protocols. - Use of compromised routers and servers as relay and proxy nodes. - Frequent rotation of domains, IPs, and infrastructure to evade detection.
Defense Evasion	- Minimal on-disk artifacts and limited malware deployment. - Extensive use of legitimate administrative features and LOLBins. - Avoidance or suppression of logging on compromised devices. - Long dwell times with very low observable activity.
Data Exfiltration	- Collection of emails, documents, credentials, network configurations, and traffic metadata. - Compression and encryption prior to exfiltration. - Use of trusted or compromised infrastructure to mask outbound data flows.

TARGET PROFILE

Primary Sectors:	: Government ministries, defense agencies, telecommunications providers, ISPs, critical infrastructure operators.
Secondary Sectors	: Technology vendors, semiconductor and electronics manufacturers, research institutions.
Geographic Focus	: East Asia and Southeast Asia as primary regions; selective targeting in Europe and North America.

THREAT ASSESSMENT

Risk Level	: High – demonstrates advanced tradecraft, patience, and strategic alignment with PRC interests.
Most Recent Activity	: Ongoing infrastructure-centric espionage campaigns against telecoms and government networks; increased targeting of edge devices.
Evolution	: Reduced malware reuse, improved OPSEC, deeper focus on network-level access and long-term surveillance rather than rapid exploitation.

NOTABLE OPERATIONS

- **East Asian Government Espionage:** Long-term intrusions into government and defense networks to collect diplomatic and military intelligence.
- **Telecommunications Infrastructure Compromise:** Persistent access to ISP and telecom routers enabling network visibility and potential traffic manipulation.
- **Technology Sector Espionage:** Targeting of advanced electronics and semiconductor firms to acquire sensitive IP.
- **Infrastructure Reuse Campaigns:** Repurposing compromised routers and servers as C2 relays and staging points for further operations.