APT27

[/ˌeɪ piː tiː ˈtwɛnti ˈsɛvən/]

APT27 is a China-aligned cyber espionage group active since at least 2012, supporting PRC intelligence objectives. It targets governments, defense, critical infrastructure, and technology sectors worldwide, and in 2024–2025 focused on high-impact operations using improved OPSEC and DLL side-loading techniques.

IDENTITY

Attribution	: China-aligned APT assessed to operate in support of PRC military and/or state security intelligence requirements.
Active Since	: At least 2012; sustained operations observed through 2025.
Aliases	: BRONZE UNION, Budworm, Circle Typhoon, EMISSARY PANDA, Earth Smilodon, G0027, GreedyTaotie, Group 35, Iron Taurus, Iron Tiger, Linen Typhoon, Lucky Mouse, Red Phoenix, TEMP.Hippo, TG-3390, ZipToken.
Motivation	: Long-term strategic cyber espionage targeting foreign governments, defense capabilities, and economic interests.

TTPs

Initial Access	- Spearphishing emails themed around diplomatic, military, or policy matters. - Malicious attachments and links delivering backdoors or loaders. - Exploitation of known vulnerabilities in internet-facing services and web servers. - Credential harvesting via spoofed government or enterprise login portals.
Execution	- Deployment of Remote Access Trojans such as PlugX and HyperBro variants. - Custom loaders, shellcode runners, and reconnaissance modules. - Use of PowerShell and native Windows utilities for execution.
Persistence	- Registry run keys and scheduled tasks. - DLL side-loading using legitimate signed applications. - Web shells on compromised servers for long-term access. - Redundant backdoors to maintain persistence after partial remediation.
Command & Control (C2)	- Globally distributed C2 infrastructure using compromised servers. - Dynamic DNS, fast-flux domains, and frequent infrastructure rotation. - Encrypted HTTPS or custom binary protocols to blend with normal traffic.
Defense Evasion	- Payload obfuscation and encryption. - Living-off-the-land techniques to minimize dropped binaries. - Selective activation of malware modules to reduce noise.
Data Exfiltration	- Collection of documents, credentials, and internal communications. - Compression and encryption prior to exfiltration. - Low-and-slow data transfer to evade detection and DLP controls.

TARGET PROFILE

Primary Sectors	: Government ministries, military and defense contractors, aerospace firms, energy and critical infrastructure operators.
Secondary Sectors	: Telecommunications providers, technology companies, academic and policy research institutions.
Geographic Focus	: East and Southeast Asia, Europe, North America.

THREAT ASSESSMENT

Risk Level	: High – experienced, persistent actor with broad geographic reach and long dwell times.
Recent Activity	: Continued targeting of government, defense, and infrastructure sectors with refined spearphishing and malware delivery.
Evolution	: Increased focus on stealth, infrastructure hygiene, and selective high-value targets rather than widespread compromise.

NOTABLE OPERATIONS

- **Government & Defense Espionage:** Long-term intrusions into government agencies and defense-related networks to collect strategic intelligence.
- **Critical Infrastructure Reconnaissance:** Targeting of energy and telecom organizations to map network architecture and operational dependencies.
- **Think Tank & Policy Surveillance:** Compromise of organizations analyzing China-related geopolitical and economic issues.
- **Persistent Web Shell Campaigns:** Maintenance of server-side access for opportunistic intelligence gathering.