DarkHotel
(APT-C-06 / ATK52 / DUBNIUM)

[/ ˈdɑːrk həʊˈtɛl /]

DarkHotel is a high-risk, South Korea–linked espionage group active since 2007, known for targeting government officials, defense contractors, and business travelers across East Asia and beyond. Evolved from hotel Wi-Fi interception to sophisticated supply chain and cloud-based attacks, the group continues to deploy zero-day exploits and tailored malware against diplomatic and defense targets worldwide.

IDENTITY

Attribution	: South Korea–linked advanced persistent threat (APT) group specializing in cyber-espionage operations. Known for targeting high-value individuals and organizations across East Asia and globally.
Active Since	: ~2007
Aliases	: ATK52, DUBNIUM, Zigzag Hail, G0012, APT-C-06, Fallout Team, Karba, Luder, Nemim, Nemin, Tapaoux, Pioneer, Shadow Crane, SIG25, TUNGSTEN BRIDGE, T-APT-02.
Motivation	: Strategic intelligence collection targeting government, defense, and corporate entities for political, economic, and technological advantage.

TTPs

Initial Access	: Spearphishing, watering-hole attacks, and supply chain compromises. Early campaigns used malicious hotel Wi-Fi networks to deliver custom malware to business travelers.
Persistence	: Use of signed malware, DLL hijacking, and registry manipulation. Establishes persistence via scheduled tasks and browser extensions.
Command & Control (C2)	: Encrypted HTTPS and proxy C2 servers; employs domain shadowing and compromised web infrastructure for command relay.
Tools & Malware	: Inexsmar, Karba, Nemim, Tapaoux, and Pioneer backdoors. Known for zero-day exploitation in Internet Explorer, Flash, and Microsoft Office.
Techniques	: Credential theft, exfiltration of sensitive documents, lateral movement via SMB and WMI, and evasion through code obfuscation and steganography.

TARGET PROFILE

Target Sectors	: Government, Defense, Telecommunications, Hospitality, Technology, and Research.
Geographies Targeted	: East Asia (South Korea, Japan, China), United States, Europe, and the Middle East.

THREAT ASSESSMENT

Risk Level	: High (Regional to Global)
Most Recent Activity	: 2025 operations observed against diplomatic institutions and defense contractors in South Korea and Japan, leveraging updated Karba and Inexsmar variants.
Evolution	: Progressed from direct hotel network attacks to complex multi-stage intrusion chains leveraging cloud services and compromised software updates. Increasing use of modular implants and supply chain infiltration.

NOTABLE OPERATIONS

- **2021 – Website Defacement Campaigns:** Conducted ideological defacements of government and media portals in Algeria and Tunisia.
- **2014 – Hotel Wi-Fi Espionage Campaign:** Targeted executives and diplomats through infected hotel networks; delivered zero-day exploits via drive-by downloads.
- **2017 – Defense Industry Intrusions:** Conducted cyber-espionage against Japanese and South Korean defense contractors using Inexsmar and Tapaoux malware.
- **2020 – Diplomatic Data Theft:** Targeted foreign ministries and trade organizations across Asia with spearphishing campaigns distributing Karba implants.
- **2023 – Supply Chain Compromise:** Infiltrated a regional IT service provider to deliver secondary payloads to multiple defense clients. 2025 – Advanced Cloud Exploitation: Leveraged Microsoft 365 and cloud storage abuse for credential theft and long-term espionage persistence.