WIRTE

[/wɜːrt/]

WIRTE is a Hamas-linked espionage group active since 2018, conducting multi-stage spearphishing campaigns using modular implants, VBA backdoors, and cloud-based C2 against government, diplomatic, and defense targets across the Middle East and Europe.

IDENTITY

Attribution	: Gaza Cybergang-linked (Hamas-aligned) advanced persistent threat (APT) group, operating within the Palestinian cyber ecosystem. Distinct from Iranian groups like OilRig or MuddyWater, with unique tradecraft.
Active Since	: ~2018
Aliases	: Ashen Lepus (formally tracked under the Gaza Cybergang umbrella).
Motivation	: Strategic espionage supporting Palestinian political and defense interests, with a focus on regional surveillance of neighboring Middle Eastern states, shifting alliances, and diplomatic entities.

TTPs

Initial Access	: Spearphishing emails using Arabic- or English-language decoy documents themed around regional politics or defense cooperation ; malicious Office macros and embedded PowerShell commands.
Persistence	: Custom VBA-based implants, registry persistence, and scheduled task creation; sometimes leverages cloud storage tokens for remote persistence.
Command & Control (C2)	: HTTPS and cloud C2 channels using Google Drive, Dropbox, and OneDrive; employs obfuscated PowerShell scripts for communication.
Malware & Tools	: LitePower, Ferocious, SurveyScript, and VBS implant frameworks. Frequently uses remote template injection and chained loaders.
Techniques	: Credential harvesting, network reconnaissance, data compression and exfiltration through encrypted traffic, and evasion through LOLBins and script obfuscation.

TARGET PROFILE

Primary Sectors:	: Government, Diplomatic, Defense, Telecommunications, and Technology.
Geographic Focus	: Middle East (Saudi Arabia, Jordan, UAE, Lebanon), North Africa, and selected European states involved in Middle Eastern foreign policy.

THREAT ASSESSMENT

Risk Level	: High (Regional Espionage)
Most Recent Activity	:2025 operations targeting Middle Eastern ministries and regional authorities using updated LitePower and SurveyScript implants. Expanded phishing campaigns distributing Arabic-language defense policy lures.
Evolution	: Progressed from generic malware distribution to modular espionage frameworks integrating cloud C2 and PowerShell automation. Increasing operational maturity within the Gaza Cybergang cluster.

NOTABLE OPERATIONS

- **2019 – Middle East Government Intrusions:** Conducted spearphishing campaigns targeting government ministries in Jordan and Lebanon.
- **2021 – Ferocious Campaign:** Used VBA macros and PowerShell payloads to infiltrate diplomatic networks in Saudi Arabia and the UAE.
- **2023 – Cloud C2 Expansion:** Shifted to using Google Drive and OneDrive as C2 infrastructure, improving stealth and persistence.
- **2025 – Strategic Espionage Wave:** Deployed updated LitePower implants against European foreign policy research institutes and Middle Eastern telecommunications companies.