Handala

[/ˈhæn.də.lə/]

Handala is a pro-Palestinian hacktivist collective active since 2022, conducting increasingly sophisticated cyberattacks—ranging from defacements to data leaks—mainly targeting Israeli, Western, and pro-Israeli government, media, telecom, and financial sectors during regional conflicts.

IDENTITY

Attribution	: Pro-Palestinian hacktivist collective believed to operate across decentralized Arabic-speaking networks, with possible alignment to Iranian cyber influence operations.
Active Since	: -2022
Aliases	: Sometimes linked to or amplified by other pro-Palestinian entities (e.g., Anonymous Sudan, Cyber Av3ngers).
Motivation	: Ideological — to promote Palestinian causes, retaliate against perceived Israeli or Western aggression, and raise awareness through cyber disruption and information warfare.

TTPs

Initial Access	: Opportunistic exploitation of web application vulnerabilities, credential leaks, and public-facing misconfigurations.
Persistence	: Limited; typically focuses on short-term impact operations such as DDoS, defacements, or one-time data leaks.
Command & Control (C2)	: Relies on Telegram and dark web channels for coordination and publicity; distributed denial-of-service (DDoS) tools and botnets often sourced from open hacktivist ecosystems.
Malware & Tools	: DDoS kits (Low Orbit Ion Cannon variants), website defacement scripts, information-stealing utilities, and credential dumps from open breaches.
Techniques	: Web defacement, DDoS attacks, data exposure, and ransomware-style leaks for propaganda rather than profit.

TARGET PROFILE

Target Sectors	: Government, Defense, Financial Services, Media, and Telecommunications.
Geographies Targeted	: Primarily Israel and Western-aligned states (United States, UK, Germany), as well as corporations supporting Israeli operations.

THREAT ASSESSMENT

Risk Level	: Medium to High (Regional Impact, High Media Visibility)
Most Recent Activity	: 2025 campaigns timed with Middle East conflict escalations; multi-vector DDoS and defacement operations against Israeli government and energy firms.
Evolution	: Transitioned from symbolic hacktivism to targeted propaganda-driven operations using leaked or stolen data for psychological and political impact.

NOTABLE OPERATIONS

- **2023 – #OpIsrael Campaign:** Coordinated website defacements and social media account compromises of Israeli institutions.
- **2024 – Data Leak Campaign:** Released stolen credentials and documents allegedly belonging to Israeli defense contractors.
- **2025 – Infrastructure Disruption:** Claimed responsibility for DDoS attacks on Israeli telecommunications providers and partial data leaks from financial institutions.
- **2025 – Joint Ops with Anonymous Sudan:** Coordinated propaganda campaign amplifying messages across Telegram and dark web platforms during regional conflict escalation.