VOID MANTICORE

[/ vɔɪd ˈmæn.tɪ.kɔːr/]

Void Manticore is an Iran-aligned hacktivist/APT group active since 2022, conducting ideologically driven cyberattacks—including wipers and data leaks—against Israel, Albania, the U.S., and other NATO-aligned states. Targeting government and critical infrastructure sectors, the group uses social media and Telegram for propaganda, making it a high-risk threat actor.

IDENTITY

Attribution / Origin	: Iran-aligned hacktivist and APT group.
Active Since	: 2022.
Aliases	: STORM-842, Homeland Justice, Karma.
Motivation	:Politically and ideologically motivated operations promoting Iranian state interests through hacktivism, disinformation, and cyber sabotage.

TTPs

Initial Access

- Exploitation of public-facing vulnerabilities in web servers, VPN gateways, and unpatched applications.
- Use of stolen credentials and brute-force attempts to access government and infrastructure systems.
- Phishing and credential harvesting via spoofed news and NGO portals.

Execution & Persistence:

- Deployment of wiper-style malware disguised as ransomware (notably CaddyWiper and ZeroCleare-like variants).
- Use of batch scripts and PowerShell for mass file deletion and exfiltration.
- Establishment of persistence through scheduled tasks and remote access software.

Command & Control (C2)

- HTTP/S-based C2 channels routed through compromised servers.
- Use of VPN and proxy infrastructure located in Eastern Europe and the Middle East.
- Leverage of cloud hosting providers to mask infrastructure changes.

Malware & Tools

- CaddyWiper, ZeroCleare variants, Atena, and custom disk wipers.
- Open-source penetration tools (Metasploit, SharpHound) and remote administration utilities.
- Encrypted payloads disguised as ransomware notes, serving propaganda purposes instead of ransom collection.

Techniques

- Data destruction under the guise of extortion.
- Double extortion model adapted for ideological messaging rather than profit.
- Social media amplification of leaks and false-flag campaigns.

TARGET PROFILE

Target Sectors	: Government, critical infrastructure, telecommunications, finance, energy, and transportation.
Geographies Targeted	: Israel, Albania, United States, Greece, and NATO-aligned European nations.
Notable Targets	: Israeli government ministries, Albanian critical services, Western NGOs, and technology providers supporting NATO missions.

THREAT ASSESSMENT

Risk Level	: High
Most Recent Activity	: Late 2024 through 2025, focused on destructive attacks and large-scale data leaks targeting Israeli and Albanian government infrastructure.
Evolution	: Shifted from simple website defacements to destructive cyber operations coordinated with Iranian state messaging. Increasing sophistication in propaganda dissemination and integration of cyberattacks with geopolitical events.

NOTABLE OPERATIONS

- **2022 – Operation Homeland Justice:** A coordinated defacement and data leak campaign against Albanian government websites, disrupting public services and releasing stolen documents as part of a political statement.
- **2023 – Israeli Infrastructure Attacks:** Targeted water, energy, and transportation sectors in Israel using wiper malware and ransomware-themed decoys to mask sabotage.
- **2024 – Western Media & NGO Intrusions:** Breach of European and U.S.-based NGOs to leak politically sensitive data; aligned with concurrent diplomatic tensions between Iran and Western states.
- **2025 – “Karma” Campaign:** Claimed responsibility for a series of leaks targeting Israeli critical infrastructure providers, combining cyber sabotage with disinformation narratives amplified on Telegram.