Dark Storm Team — Threat Intelligence Report

Report Information

Report Title: Dark Storm Team -Threat Intelligence Report **Researcher**: Lee Green **Date**: 05-04-2025
Sources Used: Telegram, ThreatFox, Google Dorking, OSINT platforms (tgstat, telemetr), news reports, cybersecurity blogs

---

Threat Actor Overview

Group Name(s): Dark Storm Team

Description:
Pro Palestinian Hacktivist group that utilizes DDOS attacks on Nation States that are in support of Israel. The group claims responsibility for the recent Blackout in Portugal, Spain, and parts of France.

First Identified: Late 2023 following October 7th Hamas attack

Known Motivations:

- Political Hacktivism, Anti-West Sentiment, Anti-Israel Sentiment

Associated Malware/Tools:

- Botnet Utilization: Dark Storm Team is known to leverage botnets composed of compromised devices to execute DDoS attacks. These botnets often consist of infected routers and other Internet of Things (IoT) devices.
- Exploitation of Vulnerable Devices: Reports indicate that the group has previously exploited vulnerabilities in devices such as MikroTik routers, utilizing them alongside open proxies and the Tor network to amplify their attacks.

Recent Campaigns & Activities

Campaign: Portugal and Spain Blackouts / DDoS Attacks

- Date: May 2024
- Target(s): Power grid companies and telecom providers in Portugal and Spain

- Methods: DDoS attacks via botnet, Telegram propaganda, public claims of responsibility
- Notes: Dark Storm Team publicly claimed responsibility through their Telegram channel following widespread disruptions in Portugal and Spain. The attacks coincided with pro-Palestinian protests and targeted critical infrastructure, causing regional internet outages and service disruptions.

Infrastructure & Indicators of Compromise (IOCs)

Type	Value	Date Observed	Notes
IP Address	5.188.87[.]58	2024-05-21	Associated with DarkGate malware C2 server
Domain	N/A	N/A	No specific domain publicly attributed
Telegram Channel	@DarkStormTeams	2025-03-11	Main propaganda and coordination channel
Telegram Channel	@darkstormteambackup2	2025-02-14	Backup channel after main channel was banned

---

Tactics, Techniques & Procedures (TTPs)

Initial Access: Exploiting vulnerable routers and IoT devices
Execution: DDoS botnet attacks
Persistence: Use of botnet infrastructure and proxies
Command and Control (C2): Telegram channels, IP-based botnet traffic
Impact: Service disruption, internet outages, reputation damage

---

Notes & Analyst Assessment

Summary:
Dark Storm Team has established itself as a persistent pro-Palestinian hacktivist group leveraging opportunistic exploitation of vulnerable devices and botnets to execute

disruptive DDoS campaigns. While not technically elite, their operations have demonstrated impactful and coordinated targeting against critical infrastructure.

Potential Threat Level: Medium → based on moderate skill level but high intent and disruptive potential

Recommendations:

- Monitor public Telegram channels for activity
- Block known IPs and domains in security appliances
- Educate org staff on DDoS mitigation

Appendices

- Links to OSINT sources:
    - ThreatFox: https://threatfox.abuse.ch
    - MalwareBazaar: https://bazaar.abuse.ch
    - Telegram Channel (Primary): https://t.me/DarkStormTeams
    - Telegram Channel (Backup): https://t.me/darkstormteambackup2
    - Telegram Channel Search OSINT Tools:
        - https://telegramchannels.me
        - https://tgstat.com
        - https://telemetr.io/en
    - VirusTotal (for malware analysis): https://www.virustotal.com
    - MITRE ATT&CK Framework: https://attack.mitre.org