KASABLANKA

[/ˌkæz.əˈblæŋ.kə/]

Kasablanka is a medium-to-high-risk threat actor active since 2021, suspected to be linked to North African or Middle Eastern networks. Driven by financial gain, hacktivism, and regional intelligence interests, the group has evolved from basic defacements to sophisticated phishing and credential-harvesting operations targeting governments, energy firms, and media across North Africa, Europe, and the Middle East.

IDENTITY

Attribution	: Suspected North African or Middle Eastern threat actor with indicators pointing to Morocco-based or Morocco-affiliated cyber operators. Potential mix of hacktivist and financially motivated individuals.
Active Since	: -2021
Aliases	: None officially confirmed.
Motivation	: Financial gain, political hacktivism, and cyber-espionage aligned with regional geopolitical narratives and influence operations.

TTPs

Initial Access	: Spearphishing emails, social media impersonation, and malicious websites imitating government portals; use of credential-harvesting pages hosted on cloud platforms.
Persistence	: Credential reuse, use of commercial remote administration tools (RATs), and cloud-based persistence through compromised accounts.
Command & Control (C2)	: HTTP/HTTPS-based C2 via cloud services, Telegram bots, and public file-sharing platforms.
Tools & Malware	: Open-source tools (QuasarRAT, njRAT), credential stealers, and malicious scripts embedded in phishing pages.
Techniques	: Credential theft, data exfiltration via encrypted channels, defacement, and disinformation distribution through social media.

TARGET PROFILE

Target Sectors	: Government, Energy, Telecommunications, Financial, Media, and NGOs.
Geographies Targeted	: North Africa (Morocco, Algeria, Tunisia), Western Europe (France, Spain), and the Middle East.

THREAT ASSESSMENT

Risk Level	: Medium to High (Regional Influence and Emerging Espionage Capability)
Most Recent Activity	: 2025 operations focused on targeting European energy suppliers and North African government ministries via phishing and fake Microsoft 365 login portals.
Evolution	: Progressed from hacktivist-style attacks and defacements to organized cyber-espionage campaigns. Increasing technical maturity with adoption of cloud-based C2 and encrypted communications.

NOTABLE OPERATIONS

- **2021 – Website Defacement Campaigns:** Conducted ideological defacements of government and media portals in Algeria and Tunisia.
- **2023 – Phishing Against Energy Firms:** Launched credential theft campaigns against European and North African energy companies using fake Microsoft login portals.
- **2024 – Regional Disinformation Drive:** Coordinated social media operations spreading false narratives about North African political movements.
- **2025 – Espionage on Government Networks:** Conducted multi-stage phishing attacks against North African ministries and diplomatic entities for intelligence collection.