Cyber Insight

Hider_Nex Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.
This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

Hider Nex Group

- **Creation date:**
  The "Hider_Nex" group, also known as "Tunisian Maskers Cyber Force," was first publicly identified in mid-2025, with significant activity noted around July 2025. Its origins are tied to Tunisia, emerging in response to regional geopolitical tensions, particularly with Morocco and in support of pro-Palestinian causes. No clear evidence of Russian leadership or founding members. However, their alliances with groups like ANONYMOUS RUSSIA and KGB, announced on X, suggest possible Russian influence or collaboration.

- **Probable Origin**:
  The "Hider_Nex" group, also known as "Tunisian Maskers Cyber Force," originated in Tunisia, emerging in mid-2025 amid escalating cyber tensions with Morocco. It was formed to support pro-Palestinian causes and counter perceived Moroccan cyber operations, as evidenced by its public activities starting in July 2025.

- **Main strategies:**
  The "Hider_Nex" group employs a "hack-and-leak" strategy, combining DDoS attacks with data breaches to disrupt and expose sensitive information from targeted government, financial, and infrastructure sectors. They leverage public platforms like X and Telegram for coordinated propaganda and alliance-building to amplify the geopolitical impact of their pro-Palestinian and anti-Moroccan campaigns.

- **Geopolitical Motivation:**
  The "Hider_Nex" group is driven by geopolitical motivations, aiming to counter Moroccan influence and oppose nations supporting Israel, particularly targeting the United States, France, and Israel.

- **Targeted business sectors:** The "Hider_Nex" group primarily targets government, financial, educational, and telecommunications sectors, focusing on entities in Morocco, France, the United States, and Israel to disrupt operations and expose sensitive data. Their attacks, such as DDoS and data breaches, aim to impact critical infrastructure and businesses like banks (e.g., BNP Paribas, BMCI) and telecom providers (e.g., Orange Tunisia) to advance their pro-Palestinian and anti-Moroccan agenda.

Identification

The "Hider_Nex" group, also known as "Tunisian Maskers Cyber Force," was first publicly identified in mid-2025 as a pro-Tunisian and pro-Palestinian hacktivist collective. Motivated by geopolitical tensions, particularly opposition to Morocco and support for Palestinian causes, the group targets entities aligned with Israel and Western interests. Since July 2025, Hider_Nex has executed cyberattacks, including DDoS and data breaches, against government, financial, and infrastructure sectors in Morocco, France, the United States, and Israel.

Main collaborating

Keymous Plus:

Targets Moroccan institutions with DDoS and leaks.

Likely Tunisian, anti-Morocco focus.

Boosts regional cyber campaigns.

HEZI RASH:

Attacks Western/pro-Israeli targets.

Likely Middle Eastern, pro-Palestinian.

Provides technical support.

DieNet:

Joins #OPMorocco with DDoS/breaches.

Possibly russophone, anti-Western.

Shares resources for scale.

KGB:

Supplies tools for Western-targeted attacks.

Likely Russian, anti-Western stance.

Enhances attack capabilities.

Dark Storm:

Hits U.S. infrastructure with DDoS.

Likely Middle Eastern, pro-Palestinian.

Amplifies joint operations.

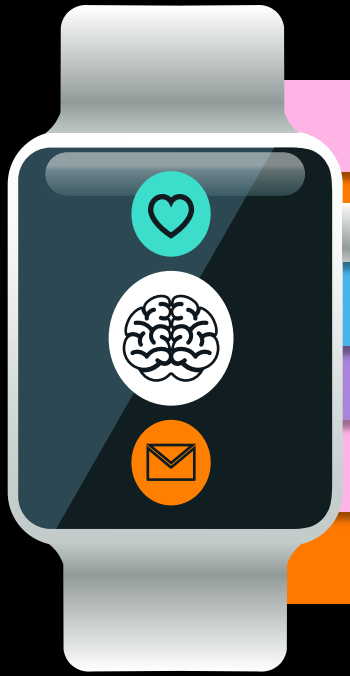
ANONYMOUS RUSSIA:

Uses botnets for U.S./French attacks.

Russian, anti-Western hacktivist.

Expands global reach.

Key Points



1
2
3
4
5
6

Structure

Hider_Nex operates as a decentralized hacktivist collective, coordinating with international allies like ANONYMOUS RUSSIA to execute large-scale cyberattacks across multiple regions.

Platform

The group leverages platforms like X and Telegram to publicly claim attacks, coordinate with partners, and amplify their pro-Palestinian and anti-Moroccan propaganda.

Financing

Hider_Nex likely sustains operations through anonymous cryptocurrency donations from ideological supporters and by accessing low-cost or cracked cyber tools from underground markets.

Associated projects/tools

They utilize DDoS tools for widespread disruptions and advanced malware like VIP RAT v7.6 for data breaches, often integrating these into hack-and-leak campaigns targeting critical systems.

Motivations

Motivated by pro-Tunisian and pro-Palestinian ideologies, Hider_Nex seeks to undermine nations like Morocco and Western supporters of Israel through disruptive cyber operations.

Targets

Hider_Nex attacks government agencies, financial institutions like BNP Paribas, and critical infrastructure such as French power grids and Moroccan telecoms to maximize geopolitical and economic impact.

Vectors of Influence

1

Social Media Framing

Hider_Nex uses platforms like X to spread pro-Palestinian messages, intimidating victims by publicizing attacks. This draws in recruits who share their views and strengthens alliances through viral calls for support.

2

Cognitive Overload via Disruptions

Through DDoS attacks, the group overwhelms victims' systems to induce confusion and decision fatigue, exploiting mental exhaustion. This tactic recruits by showcasing "wins" that appeal to those frustrated with systems, fostering alliances based on perceived intellectual superiority

3

Emotional Gaslighting

Hider_Nex uses appeals to victimhood, like "child victims" rhetoric, to question targets' moral judgments and create self-doubt. Recruits are drawn in by this intellectual reframing of conflicts as black-and-white, building coalitions with groups swayed by similar manipulative empathy.

4

Ideological Indoctrination

Hashtags like #FreePalestine embed subtle cognitive biases, reshaping victims' worldviews to align with the group's agenda. This draws recruits through intellectual persuasion disguised as activism, solidifying coalitions via collective delusion of moral high ground.

5

Alliance Echo Chambers

Public partnership announcements create illusions of overwhelming support, pressuring victims intellectually to concede powerlessness. Recruits join these echo chambers for validation of their beliefs, while alliances form around mutually reinforced manipulative ideologies.

Emotional Intelligence

1

Hider_Nex justifies cyberattacks as moral acts to defend Palestine, making victims like banks or governments seem like villains. This manipulation, based on Bandura's research, recruits supporters by easing guilt and paints targets as deserving of disruption.

2

Hider_Nex uses threats of leaks or outages to scare targets like French infrastructure into compliance or panic. Psychology research on fear priming explains how this recruits followers seeking control and pressures victims to doubt their security.

3

By sharing only partial data from breaches, the group shapes perceptions to make targets question their own systems' integrity. PhD work on selective exposure bias highlights how this recruits by offering "exclusive" insights and sways allies with curated truths.

4

Hider_Nex fosters a sense of unity on Telegram, pushing members to conform to their anti-Western agenda without questioning. Janis's groupthink studies show this strengthens alliances by suppressing dissent and manipulates victims through collective pressure.

5

The group offers "protection" or ceasefire promises to compliant targets, creating a false sense of obligation to align with their cause. Cialdini's persuasion research notes this recruits supporters expecting rewards and coerces victims into negotiation traps.

6

Hider_Nex spreads conflicting messages about geopolitical events to confuse targets and make them doubt their own beliefs. Doctoral theses on cognitive dissonance reveal this recruits by exploiting uncertainty and influences allies by aligning them with the group's narrative.

orange Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

Infrastructure

Technology

Finance

Government

Education

Telecommunications

Transportation

Note on Surveillance Countermeasures

To counter the "Hider_Nex" group, organizations should implement real-time monitoring of platforms like X and Telegram to detect threats and track alliances, using OSINT tools to identify attack patterns early. Deploy robust cybersecurity measures, including firewalls, intrusion detection systems, and regular audits to mitigate DDoS and data breach attempts targeting government, financial, and infrastructure sectors. Educate employees on phishing prevention and enforce multi-factor authentication to protect against potential malware like VIP RAT v7.6, which could be used for espionage or credential theft..

Credits Orange Cyberdefense

Targeted Countries

Tunisia

Cyprus

Morocco

France

United States

Israel

Philippines

Credits Orange Cyberdefense

Most Likely Hypothesis

Targeting Strategies:

- The group would focus on European nations like France, Germany, Italy, and Spain with strong EU ties to Israel for symbolic and disruptive impact.
- They might use OSINT to identify weak OT/ICS endpoints in utilities and transport, prioritizing those with outdated SCADA systems.
- Alliances such as ANONYMOUS RUSSIA could provide intel on high-value targets to coordinate multi-country strikes.

Attack Methods:

- Initial phishing or supply-chain compromises to deploy malware like custom RAT variants into ICS environments.
- Exploitation of zero-day vulnerabilities in protocols for persistent access and command injection.
- Hybrid tactics blending ransomware with DDoS to lock systems and overwhelm monitoring tools simultaneously.

Systemic Impacts:

- Disruptions could cause widespread blackouts or train delays, leading to economic losses in billions across Europe.
- Heightened public panic and regulatory scrutiny might force EU governments to reassess foreign policies.
- Long-term erosion of trust in critical infrastructure could inspire copycat attacks from other hacktivists.

Credits Orange Cyberdefense

The most dangerous hypothesis

Feared Scenario:
Hider_Nex launches a coordinated ransomware attack on OT/ICS systems, crippling operations across multiple countries.
- This could shut down factories and utilities in real time.
- Allies like ANONYMOUS RUSSIA amplify the scale for maximum chaos.

Main Targets:
Energy firms like power grids in Germany and transportation hubs like ports in France.
- Focus on interconnected EU infrastructure for widespread effects.
- Prioritize companies with weak cybersecurity to exploit easily.

Methodology:
Trick employees into clicking fake emails to install malware, then lock systems and demand ransom.
- Use simple tools to spread virus through networks like a chain reaction.
- Leak stolen data online if unpaid to embarrass victims.

Potential Consequences:
Billions in economic losses from halted production and supply chain breakdowns.
- Public panic leads to stock market drops and regulatory fines.
- Heightened geopolitical tensions prompt EU-wide cyber defense reforms.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense