Cyber Insight

LunarisSec Group

Cyber Intelligence Bureau

Cyberdefense

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

Credits Orange Cyberdefense

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.

LunarisSec Group

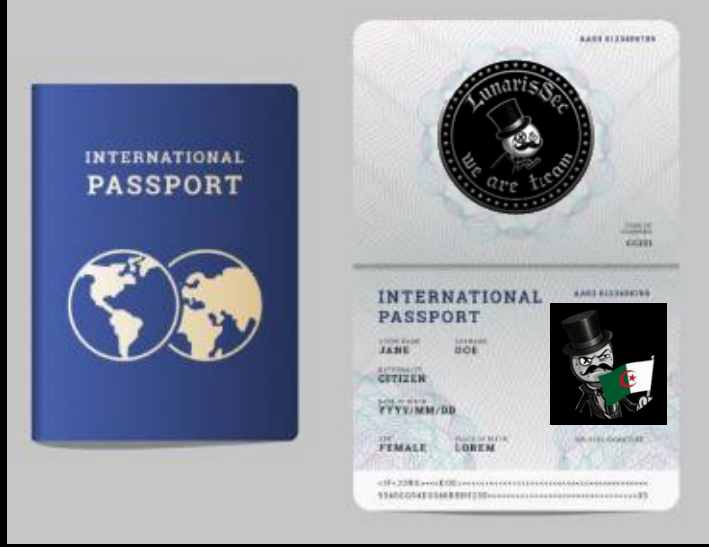
- **Creation date:**
  LunarisSec's founding date is estimated to fall between late 2025 and early 2026. While their first traces date back to late 2025, their public activity and visibility saw a significant peak during the spring and summer of 2026

- **Probable Origin**:
  The group's geographic origin is formally linked to Algeria, as shown by their systematic use of the Algerian flag and national hashtags in their communications. Their operations focus almost exclusively on French targets, suggesting the existence of a network operating from Algeria or through its diaspora

- **Main strategies:**
  LunarisSec favors the exploitation of common web vulnerabilities, such as exposed APIs, SQL injection, and database misconfigurations, rather than sophisticated malware. Their tactic is to alternate between "responsible disclosure" to gain credibility and public data leaks to erode trust in the targeted institutions

- **Geopolitical Motivation:**
  LunarisSec's motivations are deeply rooted in Algerian nationalism and anti-French sentiment, often framed around post-colonial grievances. The group seeks to pressure French diplomacy while highlighting the systemic weaknesses of the French state's digital security.

- **Targeted business sectors:**
  Higher education is their primary target, with numerous claimed intrusions against French and international universities. They also intensively target government services, including taxation and municipal systems, as well as the legal sector, in order to maximize the symbolic impact of their operations

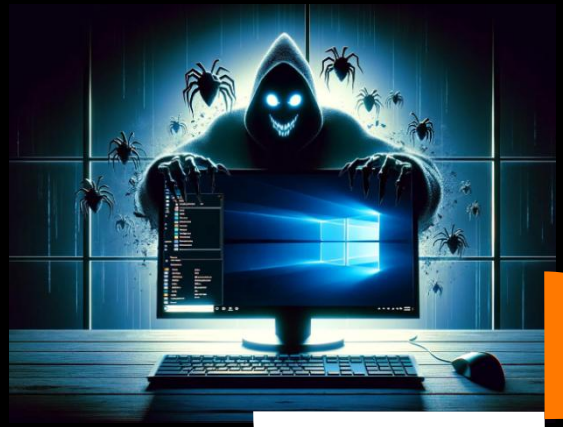


Identification

LunarisSec is an emerging hacktivist collective that presents itself as a team of vulnerability researchers blending technical disclosures with nationalist messaging. The group cultivates a "white-hat" activist image, using the publicity around its findings to increase its visibility within the cyber community

Credits Orange Cyberdefense

Associated Adversary Groups & Alliances



- TEAM BD DARK FORCE
- Anonymous Switzerland
- French Hackers Squad
- konco #INDO (Indonesian)
- NullSec Philippines (NullSec #PH)
- ZEc0n
- AKATSUKI CYBER TEAM
- LolForum
- FINIX CYBER TEAM
- 404 Crew (404 CREW CYBER TEAM)
- Dark Storm Team
- BD Anonymous Team (Anonymous BD)
- BontenSec
- IHS
- Order403
- KEYMOUS+
- Terminal 404
- HxH
- HawkSec (formerly LazurGroup)
- X-VDP-X
- VexOs Team
- KillServer Team
- Hydra France
- The Legion
- SnowSec Alliance
- Security Team
- 0wnzSec (0wnzS3c)
- NullSec Brazil (NullSec BR)

Credits Orange Cyberdefense

Vectors of Influence

1

Responsible Disclosure Framing

LunarisSec uses Robert Cialdini's principles of reciprocity and authority to legitimize its actions by presenting them as a public cybersecurity service.

2

Nationalist Shaming on Social Media

LunarisSec relies on emotional appeals and propaganda to radicalize its audience and demoralize its opponents on social media.

3

Alliance Signaling

By publicly highlighting its international cooperation, the group practices Erving Goffman's "impression management" to amplify the perception of its real power.

4

Rhetorical Activation of Biases

The group saturates the information space to trigger preexisting cognitive biases in its targets, a method of influence documented by Douglas S. Wilbur.

5

Public Shaming for Reputation Damage

The public exposure of web vulnerabilities is meant to create a strong negative reputational effect and erode trust in French institutions.

Emotional Intelligence

Cognitive Framing:
The group uses Daniel Kahneman's prospect theory to frame its intrusions as acts of justice in response to the French state's negligence.

1

HOOK Patterns (Hooking):
This hooking technique uses specific language structures, such as suggested commands ("join the light"), to capture emotional interest and recruit new members by building subtle persuasive rapport.

2

Pacing & Leading:
This neuro-linguistic programming method allows the group to align itself with its audience's values before guiding them toward ideological claims.

3

4

Propaganda Symbiosis:
LunarisSec merges technical claims with appeals to pan-Islamic or Algerian solidarity to encourage symbiotic radicalization.

5

S.T.O.P. Patterns:
These communication patterns are adapted to interrupt the target's critical thinking and encourage immediate acceptance of the group's narrative.

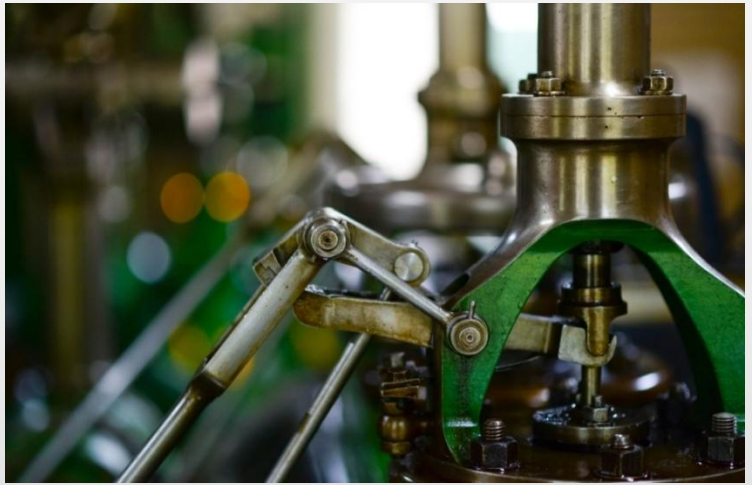
6

S.W.I.F.T. Patterns:
These rapid emotional influence models are deployed during data leaks to trigger panic or urgency in targeted users.

Professional Sectors

List of targeted sectors

- Education / Higher Education (universités françaises et internationales)
- Government / Public Services (services fiscaux, administrations nationales et municipalités)
- Legal / Law Firms
- Defense / Military Industry
- Commerce / Retail
- Social Media / Communication
- Online Services / Associations



Note

More than just a hacker collective, LunarisSec has established itself as a true “pirate of minds,” capable of manipulating public perception by combining targeted cyberattacks with psychological persuasion strategies. This group, believed to originate from Algeria, targets French institutions not only to extract data, but above all to influence minds through sophisticated techniques such as neuro-linguistic programming and the activation of cognitive biases.

Targeted Countries

Credits Orange Cyberdefense

High-Probability Future Targets Countries

Western Countries

Mexico

France

Israel

European Union

Most Probable Hypothesis on LunarisSec Group Future Activities

Future Targets

France remains the group's primary and permanent target, with continued focus on public administration, education, and mid-sized private-sector organizations. The group has explicitly announced imminent attack intentions against Mexico ("Soon Mexico"), while also planning to expand its activity toward France's European allies.

Hybrid Methods

LunarisSec combines "responsible disclosure" to gain media legitimacy with selective data leaks aimed at eroding trust in institutions.

Their operations rely on a synergy between the technical exploitation of web vulnerabilities (APIs, SQL) and the use of psychological persuasion tactics such as neuro-linguistic programming.

Systemic Impacts

These attacks generate rising regulatory costs and widespread fatigue toward hacktivism, thereby normalizing digital insecurity.

In the long term, they reinforce the narrative of a systemic weakness in the French state, without triggering major state retaliation.

Credits Orange Cyberdefense

The most dangerous hypothesis

The Most Dangerous Scenario
The most critical scenario envisions a massive coordinated campaign named “Lunaris Eclipse,” involving a supply-chain compromise through critical service providers.

Targets and Sectors Targeted
The targeted sectors would include software providers for defense and the legal sector, as well as operators managing national infrastructure essential to the country’s functioning.

Methodologies
The group would use zero-day vulnerabilities in common web configurations, carrying out stealthy exfiltration followed by timed data releases to saturate the media space.

Potential Consequences
The consequences would include a massive privacy crisis affecting millions of citizens, economic losses, social destabilization, and the potential escalation into interstate cyber tensions.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

Build a safer digital society

Cyberdefense

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

Credits Orange Cyberdefense