Cyber Insight

Al Ahad Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

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.

Al Ahad Group

- Creation date: Al Ahad is described as an emerging hacktivist group, reportedly active since at least 2024. The first public mention dates to September 2024, when the group announced it would maintain operations on Telegram while prioritizing activity on Signal. By December 2024, Al Ahad had formed a confirmed alliance with Anonymous Guys and DXPLOIT while aligning with the Holy League-a collective targeting Western interests and NATO. The group has demonstrated verified collaboration with NoName057(16) on anti-Israel operations and likely coordinates with the Pro-Palestine Hackers Movement (PPHM) to amplify the media impact of attacks. Evidence also suggests partnerships with CyberVolk and KillNet for hybrid operations, combining cyberattacks with disinformation campaigns while sharing techniques and logistical resources.

- Probable Origin: While Al Ahad's precise geographic origins are generally considered unknown, a moderately reliable source specifically describes it as an Iraqi entity, operating within the geopolitical context of the Middle East.

- Main strategies: Website defacement, DDoS attacks, exploitation of software vulnerabilities (particularly in CMS like WordPress and SCADA systems), intrusion into critical systems, exploitation of technical flaws, and identity spoofing.

- Geopolitical Motivation:
  Al Ahad is driven by pro-Palestinian activism and opposition to Israel, targeting governments and organizations backing Israeli interests while promoting an anti-Western agenda. The group collaborates with pro-Russian hacktivists within the Holy League alliance to attack Western and NATO interests, united by an anti-establishment ideology that rejects perceived oppressive institutions and regimes.

- Targeted business sectors:
  Education, Finance (banks and financial institutions), Healthcare, attacks against industrial systems.

Identification

"Al Ahad" is an emerging hacktivist group, believed to have been active since late 2024, positioning itself as a defender of geopolitical and social causes connected to the Middle East. Although direct information about the group is limited, their tactics and public statements indicate ideological ties to pro-Palestinian and anti-imperialist movements. Our sources indicate that Al Ahad is aligning with the Holy League alliance while also partnering with groups like CyberVolk, KillNet, and PPHM.

Credits Orange Cyberdefense

Al Ahad Group: Main collaborating

Alliance Names

- Holy League
- Cyber Axis

Hacktivist Group Names

- Pro-Palestine Hackers Movement (PPHM)
- RipperSec DarkStorm Team
- Mr. Hamza
- SECTOR 16
- Z-Pentest Alliance
- KillNet
- NoName057(16)
- Anonymous Guys
- DXPLOIT
- UserSec
- Hunt3r-Kill3rs
- CyberVolk
- Fatemiyoun Electronic Team
- AnonGhost
- ThreatSec
- CyberAv3ngers

Cybercriminal Group Names

- CL0P
- Rhysida
- Medusa
- REvil (indirect ties through tactical cooperation)

Underground Network Names

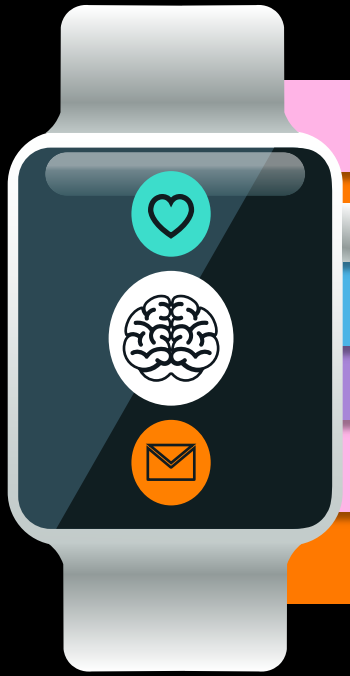
- XSS Forum (recruitment and information-sharing platform)
- Exploit.in (clandestine operations coordination)

Mercenary Names

- CyberBerkut (pro-Russian digital mercenaries)
- Black Shadow (hired actors for targeted operations)

Credits Orange Cyberdefense

Key Points



1
2
3
4
5
6

Structure

Al Ahad operates with a decentralized structure to maintain anonymity and resilience. The group relies on collaboration and flexible partnerships with other hacktivist organizations rather than maintaining a strict hierarchical framework

Platform

Al Ahad announces attacks and propaganda publicly through platforms like Telegram and Twitter (X) to reach media and audiences. For private coordination, they use encrypted channels like Signal to protect anonymity and avoid detection.

Financing

Al Ahad's exact funding sources remain undocumented, but they are suspected to potentially receive cryptocurrency donations or funds from cybercriminal activities.

Associated projects/tools

The group develops or adapts its own tools and collaborates with allies to enhance its technical capabilities.

Motivations

Al Ahad's motivations are primarily ideological and geopolitical, anchored in advocating for the Palestinian cause and opposing entities viewed as pro-Israel or aligned with Western interests

Targets

A wide range of sectors, notably Education, Finance (banks and financial institutions), Healthcare, attacks against industrial systems.

Vectors of Influence

1 Anger

Al Ahad taps into strong emotions linked to the Israeli-Palestinian conflict and uses stories of oppression to rally support and legitimize their actions. This approach attracts people who feel similar frustrations or share the same political views.

2 Fear

The group issues public threats, sometimes targeting political leaders, to spread fear among individuals and communities. This psychological pressure is designed to intimidate and unsettle their targets.

3 Geopolitical Conflicts

Al Ahad frames its actions within the context of geopolitical conflicts, particularly supporting the Palestinian cause and opposing entities perceived as supporting Israel. This ideological messaging is used to mobilize potential supporters and recruit affiliates by appealing to shared religious or political beliefs and narratives.

4 Guilt

Al Ahad runs campaigns accusing their targets of being complicit in geopolitical conflicts. Their messages use emotional language to make adversaries feel responsible and pressured to act.

5 Leveraging Alliances

Al Ahad forms partnerships with other hacktivist groups and alliances. These collaborations allow for the sharing of techniques, logistical support, and potential infrastructure, enhancing their collective ability to conduct transnational attacks and increase pressure on targets.

Emotional Intelligence

1

Al Ahad employs "Guilt-Tripping" campaigns, accusing their targets of complicity in geopolitical conflicts. They utilize emotionally charged messages, such as appeals for justice for Palestine, to mobilize supporters and gain media attention.

2

The group uses psychological blackmail tactics, including making public threats against individuals like political leaders. This strategy aims to generate fear and pressure perceived opponents to their cause.

3

Al Ahad leverages cognitive intelligence by identifying and exploiting technical vulnerabilities in targeted systems, such as flaws found in content management systems like WordPress. They also analyze target systems to maximize the effectiveness of their cyberattacks.

4

Al Ahad demonstrates SWITCH tactics through rapid adaptation, notably by changing communication platforms from Telegram to Signal. This rapid shift is designed to help them avoid detection and maintain operational security during their activities.

5

Their actions are framed within ideological justification narratives, positioning themselves as defenders of causes such as pro-Palestinian and anti-imperialist movements. These ideological underpinnings serve to legitimize their cyberattacks against entities they perceive as oppressive.

6

Al Ahad exploits emotional connections to conflicts, using messages that appeal to feelings like anger or a sense of injustice related to the Israeli-Palestinian conflict. This manipulation of sentiment helps them recruit sympathizers and garner broader support for their actions.

Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Western Governments & NGO
- NATO and Western Allies
- Defense, Military, Security Agencies
- Critical Infrastructure
- Ports
- Banking and Financial Services
- Telecommunications
- Media
- Health and Healthcare
- Social Services
- Education
- Religious Institutions
- Software (including Supply Chain)

Note

Al Ahad primarily targets organizations in Israel and Australia, focusing on government, education, and financial sectors. They also potentially attack critical infrastructure such as energy or transportation systems to disrupt services and amplify their political messaging. Their specific targets often shift with geopolitical developments and collaborations, such as alliances with other groups.

Credits Orange Cyberdefense

Targeted Countries

United Kingdom

Australia

Israel and Allies of Israel

United States (Hypothesis)

France

NATO

Credits Orange Cyberdefense

Most Likely Hypothesis

Strategic Targeting - Geopolitical Alignment with Pro-Russian Agendas:

Al Ahad may target European nations supporting Ukraine or opposing Russian interests to destabilize NATO cohesion. Attacks on critical infrastructure-such as energy grids in Europe could aim to weaken Western resolve to aid Ukraine. Their affiliation with the Holy League suggests alignment with Russian hybrid warfare tactics to fragment EU unity.

Hybrid Attack Methods - Coordinated Operations with Allied Groups:

Collaboration with groups like Killnet could enable Al Ahad to execute multi-vector attacks (e.g., DDoS + disinformation) to overwhelm defenses. For example, disrupting EU government portals while spreading propaganda about institutional corruption. Shared tools and intelligence within alliances like Holy League amplify their disruptive capacity

Systemic & Psychological Impact - Undermining Public Trust:

Attacks targeting healthcare systems or transport networks (e.g., UK railways) might trigger panic and erode confidence in state institutions. Leaks of sensitive data, such as voter records, could fuel conspiracy theories and deepen societal divisions. This psychological warfare aims to destabilize democracies.

The most dangerous hypothesis

Target Hypothesis - Critical National Infrastructure:

Al Ahad could prioritize attacks on energy grids or transportation systems, crippling essential services. Such targets maximize chaos, disrupt economies, and expose state vulnerability. Infrastructure breaches also invite public backlash against governments for perceived incompetence.

Methods Hypothesis - Hybrid Cyber-Physical Sabotage:

Combining ransomware attacks on industrial control systems (ICS) with physical disruptions (e.g., tampering with grid sensors) could trigger cascading failures. Collaboration with groups like KillNet or Conti might provide access to advanced malware (e.g., Industroyer2). Decentralized operations via encrypted platforms like Session would complicate attribution and countermeasures.

Impact Hypothesis - Societal Fracturing and Panic:

A successful attack could paralyze hospitals, trigger fuel shortages, or halt public transit, leading to civilian casualties and mass unrest. Long-term, recovery costs and eroded confidence might destabilize EU unity, aligning with Al Ahad's anti-Western agenda.

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