Cyber Insight

Keymous+ Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

orange 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.

Credits Orange Cyberdefense

Keymous+ Group

- **Creation date:**
  The Keymous+ hacktivist group officially traces its origins to **late 2023**, with its earliest public activity documented in November of that year. This debut was marked by an inaugural claim of a DDoS attack targeting a Moroccan e-Visa portal.

- **Probable Origin**:
  The Keymous+ group originated in North Africa, primarily Algeria, in late 2023, growing from a small collective of disaffected coders. This emergence was directly fueled by heightened cyber tensions between Algeria and Morocco and the opportunistic hacktivist mobilization spurred by the Gaza crisis.

- **Main strategies:**
  The Keymous+ group primarily launches high-volume distributed denial-of-service (DDoS) attacks, often utilizing commercially available DDoS-for-hire platforms like EliteStress. Their targeting extends deliberately to critical industrial and manufacturing sectors (such as Israeli manufacturing targets), aiming to cause industrial process delays and operational bottlenecks. They supplement these disruptive technical attacks with occasional data exfiltration and website defacements to maximize media visibility and psychological impact.

- **Geopolitical Motivation:**
  The group's core ideological driver is pan-Arab solidarity, often operating under the "Hack for Humanity" banner to support the Palestinian cause and opposing perceived Western influence. Geopolitically, Keymous+ also focuses heavily on retaliatory strikes against regional rivals like Morocco, framing these as assertions of digital sovereignty. However, analysts believe that the group's publicly stated causes are often opportunistic, masking underlying commercial objectives related to DDoS-as-a-Service operations.

- **Targeted business sectors:**
  Keymous+ consistently targets European government, education, and telecommunications sectors, notably focusing on French infrastructure and Danish academic systems. Additionally, the group occasionally strikes other European sectors, including media, finance, and manufacturing, particularly in countries like Sweden and Germany. Furthermore, the group strikes critical infrastructure in Europe, including the French energy sector (RTE electricity network), as well as media, finance, and manufacturing targets in countries like Sweden and Germany

Identification

Keymous+ is a highly visible North African hacktivist collective that focuses high-volume Distributed Denial-of-Service (DDoS) attacks against European assets. The group specifically targets critical infrastructure across the continent, notably attacking French energy networks (RTE), telecommunications providers, and local government portals in France and Germany. Keymous+ consistently disrupts public services by striking the European education sector, including university networks in Denmark and Sweden, often timed to global political tensions. Their operations also extend to European media, finance, and manufacturing sectors in countries like Sweden and Germany, aiming for maximum visibility and localized service disruption.

Credits Orange Cyberdefense

Associated Adversary Groups of Keymous+

- **NoName057(16)**

This group primarily focuses on pro-Russian operations, specifically attacking the internet infrastructure of Ukraine. They frame their actions as fighting against the "criminal regime" of Zelensky and ensuring the maintenance of peace and security by acting as a "peacemaker country".

- **MR M44Z (aka Mr. Hamza)**

This entity is described as a close tactical ally that amplifies DDoS attacks and provides joint reconnaissance, particularly in pro-Palestine operations. Their motivations are rooted in nationalist revenge against "traitorous neighbors" and leveraging regional intelligence for Keymous+'s broader reach.

- **AL-MUJAHIDEEN FORCE 313 (aka 313 Team)**

This Pakistan-based cell is an integrated partner in Keymous+'s "Holy League" alliance, focusing on leak amplification and defacements. Their motivations fuse Islamism with explicit anti-Zionism, utilizing shared proxies and resources to rally forces against common "infidel" foes.

- **Hunter Killerz**

This group engages in direct collaboration with Keymous+, typically sharing attack infrastructure. They are frequently listed as participants in large alliance operations, such as the extensive "Holy League" campaigns.

- **Moroccan Dragons**

This entity provides regional cover and information exchange for Keymous+'s operations, acting as a hub for Morocco-North Africa activities. Their primary motivations are centered on supporting regional operations and aligning with broader Arab-aligned hacktivism.

- **Fire Wire**

This European anarchist collective aids Keymous+ opportunistically in European strikes, particularly in France and Germany, by providing reconnaissance and proxy support. They are motivated by anti-surveillance anarchy and bond with allies over a shared desire for "chaos for justice" within EU protest contexts.

- **Shadow Cyber Security**

This group formed a formal alliance with Keymous+ in August 2025, primarily focused on intelligence sharing. Their operations are mutually supportive within North African contexts, indicating motivations tied to regional influence and information warfare.

- **CYBER TEAM INDONESIA**

Keymous officially announced an alliance with CYBER TEAM INDONESIA in October 2024 to strengthen their collaborative efforts. The purpose of this alliance is to coordinate operations, with Keymous encouraging supporters to join the newly formed team

Credits Orange Cyberdefense

Vectors of Influence

1

Hybrid Financial and Ideological Masking

The group disguises potential commercial objectives, such as operating as a DDoS-as-a-Service (DaaS) provider, behind hacktivist banners like "Hack for Humanity." This dual strategy allows Keymous+ to profit financially from its technical services while recruiting members through compelling, altruistic narratives.

2

Strategic Alliance Amplification

Keymous+ consistently forms alliances with other groups, such as NoName057(16) and MR M44Z, to instantly scale its operations and amplify attack volume. These partnerships provide shared botnets and tactical resources, significantly increasing the collective's global operational reach and media visibility.

3

Targeting Critical Infrastructure for Systemic Impact

The group deliberately strikes sensitive national infrastructure, including the French energy networks and Israeli manufacturing facilities. By causing operational bottlenecks and interruptions in critical services, Keymous+ exerts technical pressure designed to erode public trust and destabilize governments.

4

Recruitment and Cohesion through Social Proof

The group rapidly grows its ranks by sharing joint operations and displaying extensive member lists on platforms like Telegram to foster a strong sense of belonging and support the recruitment of future attackers.

5

Propaganda through Data Exfiltration and Shock Value

While primarily a DDoS group, Keymous+ incorporates data leaks—such as exposing student records or internal documents—to increase media outrage and psychological leverage. These leaks are strategically framed to expose perceived government oppression or complicity, fueling social discord among the victims.

orange Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

1 Cognitive Reframing (Framing Effects). They recast destructive DDoS attacks as acts of "heroic resistance" or "victories for humanity" to minimize ethical dissonance among members. This psychological technique bypasses moral guilt and is used to increase public support.

2 Exploitation of Social Proof: Keymous+ leverages massive alliance lists and boasts of "70+ groups" to generate a sense of irresistible collective power and legitimacy. This tactic triggers conformity and dramatically speeds up recruitment by assuring potential members they are joining a powerful, successful movement.

3 Grooming through Empathy and Belonging: They actively identify and mirror the personal grievances and traumas of potential recruits in private Telegram chats to establish deep rapport and the illusion of a "family." This emotional connection significantly reduces the defection rate and channels personal anxieties into high-loyalty collective action.

4 Structured Narrative Control (SWIFT Model): The group utilizes the SWIFT template (Stop, Watch, Investigate, Find, Tell) as a structured process for claiming operations and quickly shaping the public narrative. This approach allows Keymous+ to issue rapid, structured responses that control information flow and enhance their social influence immediately following an attack.

5 Neuro-Linguistic Programming (NLP) Tactics: Keymous+ employs persuasive and targeted language patterns in its manifestos and recruitment messages to enhance conversion rates among prospects. By subtly mirroring the language and emotional tone of potential recruits, they establish rapid rapport, facilitating their grooming into the movement.

6 Reinforcement of Confirmation Bias: Keymous+ meticulously curates social media feeds and reposts biased "proof" of perceived atrocities or government complicity to reinforce followers' existing radicalized beliefs. This echo chamber strategy locks in member loyalty and ensures they remain blind to counter-narratives or defensive communications from victim organizations.

Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Government (Public Portals, Ministries, Local Administration)
- Telecommunications
- Financial Services (Banks, Fintech Platforms)
- Education (Universities, Academic Systems)
- Manufacturing (Industrial Targets)
- Healthcare (Medical Centers, Ministry of Health)
- Energy and Critical Infrastructure (Electricity Networks, Network Monitoring)
- Media and Press Agencies
- Commerce and Business Services
- International Development

Note

Keymous+ is accurately profiled as a hybrid threat actor because it strategically blends politically motivated hacktivism, often using pan-Arab solidarity slogans, with underlying commercial objectives like operating a DDoS-as-a-Service brand. The group employs an asymmetric model by achieving high-volume disruption against critical infrastructure and high-value government entities using easily scalable, lsophistication technical tools. This threat is further amplified by sophisticated psychological manipulation and rapid alliance formation, maximizing the group’s social and political impact globally.

Credits Orange Cyberdefense

Targeted Countries

Netherlands

Belgium

United States

Sweden

United Arab Emirates

Morocco

France

Israel

India

Denmark

Germany

United Kingdom

Italy

Spain

Ukraine

Iraq

United Kingdom (UK)

Denmark

EU countries

Sueden

Germany

China

Iran

- Hypothetical - Countries at Risk

Credits Orange Cyberdefense

Most Probable Hypothesis on Keymous+'s Future Activities

Future Targets

The group’s targeting logic increasingly follows political flashpoints to maximize media exposure and online influence.

Likely focus on European countries such as France and Germany, as well as high-visibility sectors like finance and education in the US and Israel, aligning their actions with global conflicts to maximize symbolic impact.

Hybrid Methods

Their strategy shows a growing shift from regional hacktivism to transnational operations with ideological alignment.

Expected to merge DDoS and data-leak tactics for both disruption and reputational harm, collaborating with groups like MR HAMZA (M44Z) and DDoS54 to boost attack power beyond 44 Gbps. Increasing use of simple AI for target scouting, automation, and propaganda coordination.

This evolution signals a transition toward a more professionalized structure mimicking advanced cyber-collectives.

Systemic Impacts

Potential large-scale economic disruption through repeated financial and telecom sectors’ attacks; social polarization heightened by online narratives; overall strain on global cybersecurity, possibly leading to wider cyber confrontations.

These cascading impacts could pressure states to increase cyber defense spending and tighten international counter-hacktivist cooperation.

Credits Orange Cyberdefense

The most dangerous hypothesis

The Most Dangerous Scenario

Keymous+ could coordinate a multi-allied cyber offensive across Europe during a potential Middle East crisis in 2026, aligned with protest waves such as #BloquonsTout in France.

This operation would mix large-scale DDoS campaigns (up to 44 Gbps) and propaganda efforts to cause prolonged blackouts and paralyze governmental response.

Targets and Sectors Targeted

Likely primary targets include government and telecom infrastructures in France and Germany, exploiting internal unrest for maximum disruption.

Energy and financial institutions across Europe and North Africa could be hit to generate economic damage and raise global visibility through coordinated online narratives.

Methodologies

Attacks would blend high-volume DDoS floods with selective data leaks, supported by alliances like MR M44Z for botnet sharing and anonymity.

Use of public booters, Telegram, and X coordination tools enables scalable, low-skill yet high-impact assaults across multiple countries.

Potential Consequences

Extended service outages could lead to billions in losses and worsen social instability, especially in volatile regions like France.

These campaigns might deepen geopolitical divides, spark imitation by other hacktivists, and accelerate the shift toward state-level cyber conflicts and resilience measures.

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