Cyber Insight

Mr.Hamza 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.

Mr.Hamza Group

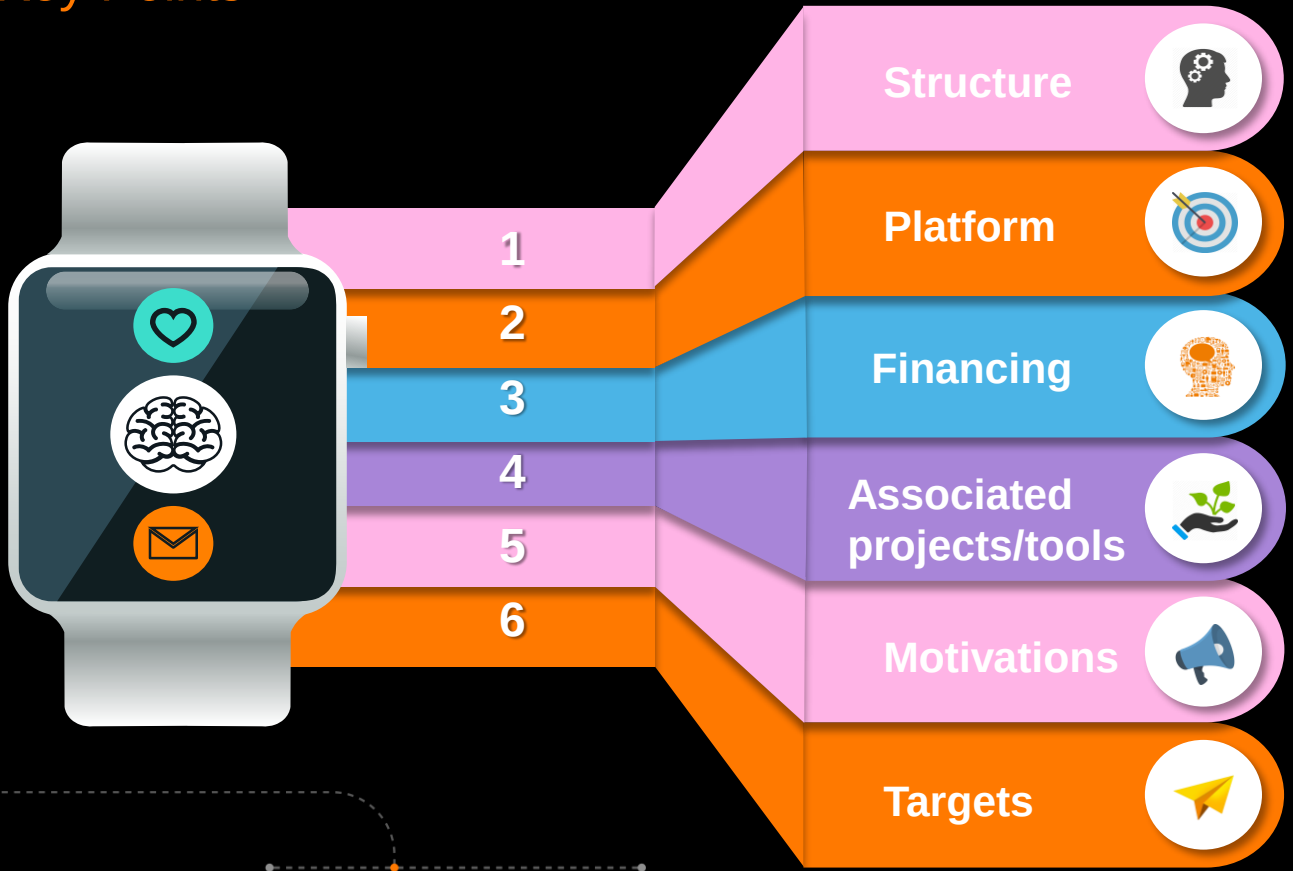
- Creation date: first appeared in October 2024
- Probable Origin: suspicions that Mr.Hamza is managed by actors of Moroccan origin
- Main strategies:
  Mr.Hamza carries out DDoS attacks against government targets and critical infrastructure, claims data leaks on social media
- Geopolitical Motivation:
  Primarily focused on an anti-Israel and pro-Palestinian agenda, as part of a broader context of ideological and religious digital activism
- Characteristic:
  Mr.Hamza is known for conducting DDoS attacks, data leaks, selling malicious tools, and collaborating with other hacktivist groups
- Targeted business sectors:
  Mr.Hamza primarily targets government institutions, intelligence and cybersecurity agencies, energy infrastructure (including nuclear facilities), financial services, and military sectors of countries considered to be supporting Israel or Western countries.

Identification

Mr.Hamza Group: Main collaborating groups

- Holy League
- NoName057(16)
- Anonymous Guys
- Anonymous Arab-Team
- Anonymous Morocco
- Velvet Team
- Z-Pentest
- Actors of Moroccan origin (suspected)

Key Points



Mr.Hamza's organization is a primarily decentralized structure at the operational level, with a centralized leadership of Moroccan origin, coordinated via Telegram and collaborating with other groups within the Holy League alliance

Telegram as a communication platform, but also other platforms such as Mega and Pastebin to disseminate information and strategies

Primarily come from the sale of malicious tools, from donations and crypto funding, and from the sale of leaks obtained during their attacks

Developing tools such as DDoS stressers, botnets, Communications C2 tools.

Ideological, with a strong anti-Israel sentiment and support for the Palestinian cause

Government institutions, intelligence and cybersecurity agencies, energy infrastructure (including nuclear facilities), financial services, and military sectors

Vectors of Influence

1

Ideology

Mr. Hamza uses strong ideological messages to attract members who share their political or religious views. This serves to recruit individuals passionate about their cause. For the victims, it justifies the attacks, aiming to create fear or submission through public declarations of their motives.

2

Communication

The group uses social media and messaging apps not only for recruitment, but also to amplify its message globally. This helps to raise awareness among potential recruits while intimidating targets with wide visibility of their actions. Communication platforms are Telegram and platforms such as Mega, Pastebin.

3

Training Sessions

Offering training sessions or providing access to advanced hacking tools is another vector used by Mr. Hamza to strengthen the technical skills of new members. Such support helps less experienced hackers to contribute effectively, thus strengthening the group's capabilities.

4

Peer Pressure

Creating a sense of community within the group fosters loyalty and commitment among members through peer pressure and shared goals. Regular interactions via forums or chats help maintain morale and cohesion, thus encouraging continued participation.

5

Psychological Operations

Conducting psychological operations (PsyOps) against adversaries and potential insiders involves the dissemination of disinformation or false narratives tailored specifically to manipulate perceptions or behaviors. Mr. Hamza refines these tactics further, targeting either conversion or deterrence.

Emotional Intelligence

1

NLP (Neuro-Linguistic Programming): The NLP principles to influence or manipulate online behaviors to facilitate sensitive information gathering or convince individuals to disclose critical data.

2

SWICH (Rapid Change Strategy): By quickly changing their targets and methods of attack, such as switching from DDoS attacks to data leaks, Mr. Hamza can avoid detection and adapt strategies to stay one step ahead of cyber defenses.

3

Cognitive Intelligence: The group applies a deep understanding of computer systems and networks to identify and exploit technical vulnerabilities, such as using IoT botnets to amplify their DDoS attacks against important websites.

4

The group uses emotional intelligence to understand and exploit the emotions of its targets, adapting its messages and tactics to elicit specific reactions, such as fear or anger, to achieve its objectives.

5

Exploitation of Vulnerabilities: The group actively identifies software and hardware flaws in the digital infrastructures of their targets, exploiting these weaknesses to infiltrate secure networks and exfiltrate sensitive data.

6

Exploitation of Ransomware and Data Exfiltration: In addition to DDoS attacks, Mr. Hamza also uses ransomware to lock critical systems and exfiltrate data before demanding a ransom, combining multiple threats to increase pressure on victims.

Cyberdefense

Credits Orange Cyberdefense

Tools used

Elite Botnet

Rebirth Botnet

Nova Botnet

Sapphire C2

Cindy Network

Ryzer Stresser

Email-Tracker

Chiasmodon

Doxing Tools

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Government institutions
- Intelligence agencies
- Cybersecurity agencies
- Energy infrastructures (including nuclear facilities)
- Financial services
- Military sectors
- Healthcare
- Agriculture and food
- Urban planning
- Oil and gas
- Industrial control systems (ICS/SCADA)
- Automotive sector
- Hospitality
- Law enforcement agencies
- Communication services

Note

Mr.Hamza is an ideologically motivated and anti-Israel group, targeting various sectors such as government institutions, energy infrastructure, financial services, military sector, and health, agriculture, and transportation sectors, which can lead to serious disruptions, financial losses, and even risks to the security and lives of citizens.

Targeted Countries

Credits Orange Cyberdefense

Most Likely Hypothesis

Targets

- Western government agencies, particularly those supporting Israel or Ukraine
- Critical infrastructure in European countries, especially France
- High-profile cybersecurity organizations (e.g., ENISA)

Methods

- Coordinated Distributed Denial-of-Service (DDoS) attacks
- Website defacements
- Data exfiltration and leaks

Impacts

- Temporary disruption of government services and websites
- Reputational damage to targeted organizations
- Increased public awareness of the group's capabilities and ideology

The most dangerous hypothesis

Targets

- Industrial control systems (SCADA) of nuclear power plants
- Critical national infrastructure (e.g., energy sector, water treatment facilities)
- Military development networks and command systems

Methods and knowledges shared with Holy League Alliance

- Sophisticated malware deployment using tools sold on their Telegram channel
- Coordinated, large-scale attacks involving multiple hacktivist groups
- Exploitation of zero-day vulnerabilities in industrial systems

Impacts

- Prolonged disruption of essential services
- Potential safety risks at compromised facilities (e.g., nuclear power plants)
- Significant economic damage due to widespread infrastructure failures
- Escalation of geopolitical tensions

This analysis examines Mr. Hamza's proven abilities, ideological drivers, and collaborative tendencies within the "Holy League" alliance.
The Most Dangerous Hypothesis considers the group's potential to exploit its tool distribution network and partnerships to launch more advanced and high-impact attacks compared to those seen so far.

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