Cyber Insight

Pro-Palestine Hackers Movement Collective

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.

Pro-Palestine Hackers Movement (PPHM)

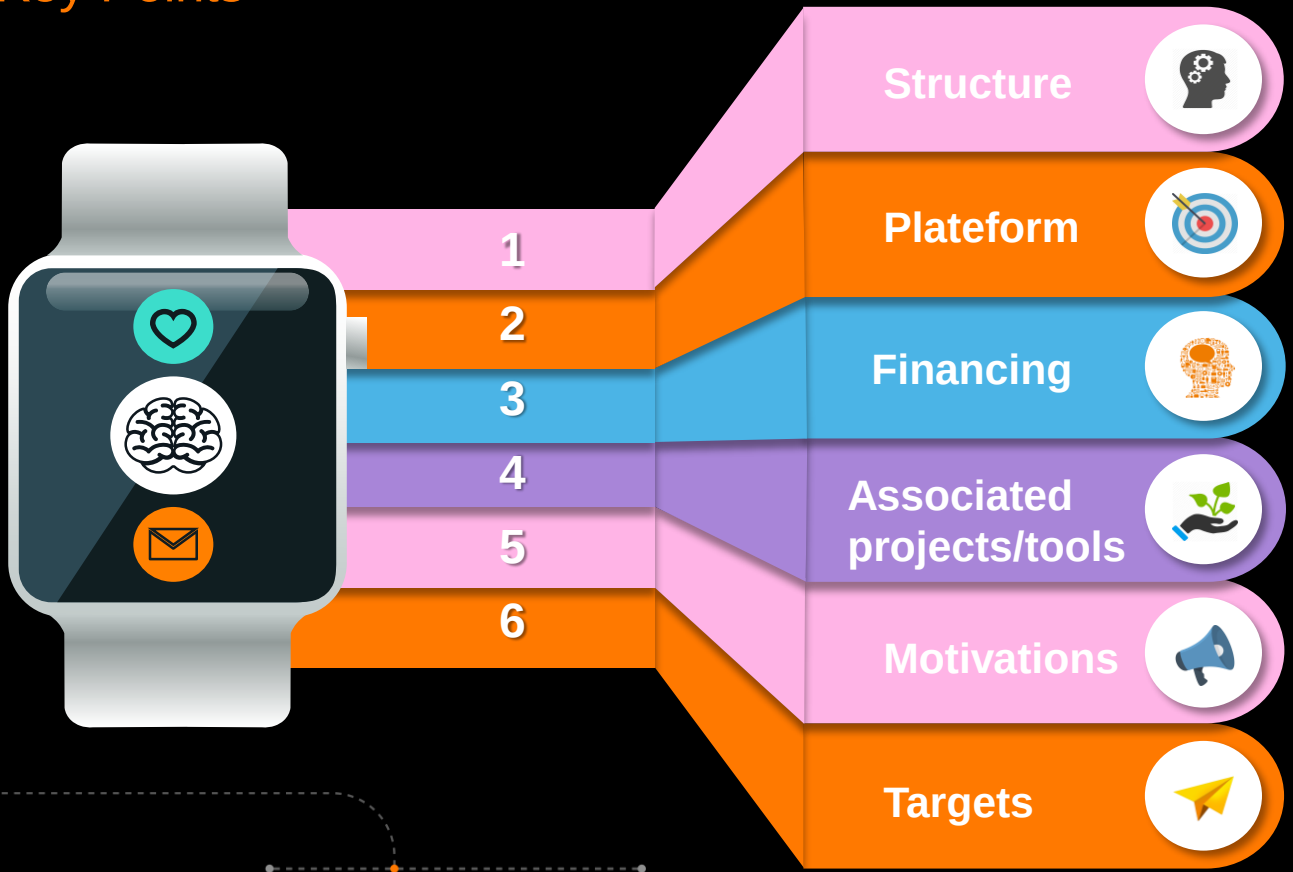
- Creation date: active since October 2023
- Probable Origin: It's a hacktivist collective with unclear exact geographical origins, but it's strongly associated with international pro-Palestinian hacker networks.
- Main strategies:
  A combination of advanced techniques, a strong symbolic dimension, and collaboration with other hacktivist groups.
- Geopolitical Motivation:
  The Pro-Palestine Hackers Movement (PPHM) is geopolitically motivated to support the Palestinian cause, oppose nations seen as backing Israel, and disrupt critical infrastructure to sway international policies in Palestine's favor.
- Characteristic:
  Capabilities to disrupt critical infrastructure while spreading pro-Palestinian political messages
- Targeted business sectors:
  Critical infrastructure (energy, telecommunications), government websites, media and financial institutions

Identification

Pro-Palestine Hackers Movement: Main collaborating groups

- Holy League
  - Anonymous Sudan
  - Killnet
  - NoName057(16)
- Cyber Operations Alliance (C.O.A)
  - LulzSec Muslims
  - Team 1916
  - Ghosts of Palestine
  - AnonGhost
  - Moroccan Black Cyber Army
  - BhinnekaSec1337

Key Points



It's a decentralized collective without a rigid hierarchical structure. It consists of geographically dispersed members and affiliated groups bound together by a shared ideology

Coordination of attacks on Telegram and Private Forums. Propaganda, amplification of the impact of its operations and influences on X (Twitter)

PPHM primarily funds its activities through the sale of leaked data and cryptocurrency transactions, potentially supported by state or organizational backers, while maintaining anonymity.

Phishing kits like IronWind, malware like Donut, DDoS tools like DDoSia, exfiltration tools like Mimikatz, OT implementations like EMP-OT, and C2 frameworks like Havoc.

The group driven by their support for the Palestinian cause and their opposition to the actions of Israel and its allies.

PPHM is not limited to individual attacks; they are part of a larger coalition called the Holy League, which includes approximately 70 anti-Western hacktivist groups

Credits Orange Cyberdefense

Vectors of Influence

1 Political Goals

Deeply motivated ideology and political goals aimed at supporting the Palestinian cause and denouncing perceived injustices against Palestinians. Their actions are often a direct response to political events and ongoing conflicts.

2 Alliances

The PPHM is part of a broader coalition called the Holy League, which brings together anti-Western hacktivist groups. They also collaborate with other hacktivist groups, such as Anonymous Sudan and Killnet, to amplify their impact and coordinate attacks.

3 Economic Pressure

PPHM targets businesses and organizations perceived as supporting Israel, using cyberattacks to disrupt their operations and exert economic pressure. They aim to encourage these entities to reconsider their ties to Israel.

4 Perception of Conflicts

By spreading pro-Palestinian messages and disrupting online services, the PPHM seeks to influence public opinion and shape the perception of Israeli-Palestinian conflicts.

5 Expertise

PPHM possesses technical skills to carry out cyberattacks such as DDoS attacks, website defacements, phishing campaigns, and exploitation of vulnerabilities on sensitive OT/ICS systems. They utilize sophisticated Android and IoS tools and softwares developed by programmers allied to their cause to achieve their goals

Emotional Intelligence

1 Emotional Communication: The group uses strong emotional communication in its messages and propaganda to mobilize support and influence public opinion. They exploit feelings of injustice and solidarity to rally sympathizers to their cause.

2 PPHM uses empathy to understand the reactions and weaknesses of their targets. This understanding allows them to create more convincing phishing campaigns or exploit the emotional vulnerabilities of their victims.

3 Emotional Decision-Making: The group considers the emotional impact of its attacks on the public and victims. They choose strategic targets and timing to maximize the impact of their message and evoke sympathy for the Palestinian cause.

4 Cognitive Reasoning: PPHM uses logical reasoning to analyze security systems and identify vulnerabilities to exploit. This cognitive ability is essential for planning sophisticated attacks and bypassing security measures.

5 Modeling Excellence: PPHM studies the tactics of hacktivist groups recognized for their effectiveness, such as Anonymous Sudan or Killnet, to improve their own methods. They analyze the success patterns of these groups to replicate them and maximize the impact of their attacks.

6 SWIFT Visualization: PPHM members use SWIFT to quickly enter an optimal state of concentration before launching a cyberattack. By visualizing the success of their operation, they boost their confidence and reduce stress related to the act of hacking.

Credits Orange Cyberdefense

Techniques and Capabilities

PPHM uses spyware to monitor victims' activities, collect sensitive data, and exfiltrate confidential information. They can deploy spyware through phishing emails or malicious applications.

Vulnerability Exploitation: PPHM uses tools like Metasploit to exploit known vulnerabilities in SCADA, ICS, and OT systems to disrupt industrial operations and critical infrastructure.

Website Defacement: PPHM modifies the content of targeted websites to display political messages or propaganda, often in support of the Palestinian cause. They replace the original content with their own messages to promote their cause.

PPHM targets media outlets perceived as pro-Israeli or those that do not cover the Israeli-Palestinian conflict in a manner deemed satisfactory by the group.

Credits Orange Cyberdefense

IoS and Android Techniques and Capabilities

Pro-Palestine Hackers Movement uses social engineering tactics, such as posing as journalists, to build trust with targets and convince them to install malicious apps or share sensitive information .

PPHM distributes malware through third-party app stores or websites, bypassing official app store security checks and tricking users into downloading infected apps .

PPHM creates fake apps (e.g., Golden Cup) that appear legitimate but contain hidden malware, allowing them to gain control over the victim's smartphone .

PPHM develops custom spyware like Phenakite for iOS, which can remotely jailbreak devices, monitor activities, and exfiltrate sensitive data such as messages, contacts, and location

The group uses malware to execute remote code on smartphones, enabling them to take full control of the device, including accessing cameras, microphones, and files .

PPHM extracts sensitive data such as call logs, SMS messages, and device metadata, which can be used for further attacks or intelligence

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Government
- Energy
- Telecommunications
- Finance
- Media
- Healthcare
- Education
- Transportation
- Public Services
- Mobile Applications

Note

PPHM is able to adapt and evolve constantly. They master DDoS attacks, website defacements, and sophisticated techniques such as the exploitation of zero-day vulnerabilities, the development of mobile malware, and advanced offensive security tools to target OT infrastructures.

Targeted Countries

Canada

Australia

Israel

France

United States

India

United Kingdom

Ukraine

Credits Orange Cyberdefense

The most Probable Hypotheses

1. Exploitation of OT Vulnerabilities in the Sensible Sectors

Targeted Sectors: Energy, Telecommunications.

Method: PPHM could exploit vulnerabilities in OT systems (e.g., power plant controls) via ZeroDay exploits or malware, already used to disrupt critical infrastructure in Israel and Europe.

Likely Impact: Temporary disruptions to power grids or communications, with the symbolic goal of destabilizing countries supporting Israel.

2. Payload deployments

Targeted Sectors: Departments of Foreign Affairs, intelligence agencies, defense organizations, and think tanks related to the Israeli-Palestinian conflicts

Method: via Donut or ScareCrow malwares to establish persistent access and exfiltrate data through encrypted channels (e.g., HTTPS protocols or DNS tunnels).

Likely Impact: Theft of sensitive data: Exfiltration of diplomatic communications, national security plans, or strategic information, which could be used for geopolitical blackmail or sold to hostile state actors.

Credits Orange Cyberdefense

The most Dangerous Hypotheses

1. OT Attacks on Industrial Control Systems (ICS) in Transportation

Targeted Sectors: Transportation, Ports, Airports.

Method: Collaboration with groups like Killnet to infiltrate SCADA/ICS systems and disrupt logistics (e.g., blocking ports like Trieste or Taranto).

Dangerous Impact: Prolonged supply chain shutdowns, industrial accidents, or major economic disruptions in countries supporting Israel.

2. Smartphone Hacking in the Healthcare Sector

Targeted Sectors: Healthcare, Hospitals.

Method: Spreading malware via fraudulent mobile apps (e.g., fake vaccination or medical tracking apps), paralyzing devices or data.

Dangerous Impact: Disruption of emergency care, leaks of sensitive medical data, or loss of life if critical systems become unavailable.

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