Cyber Insight

RipperSec

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.

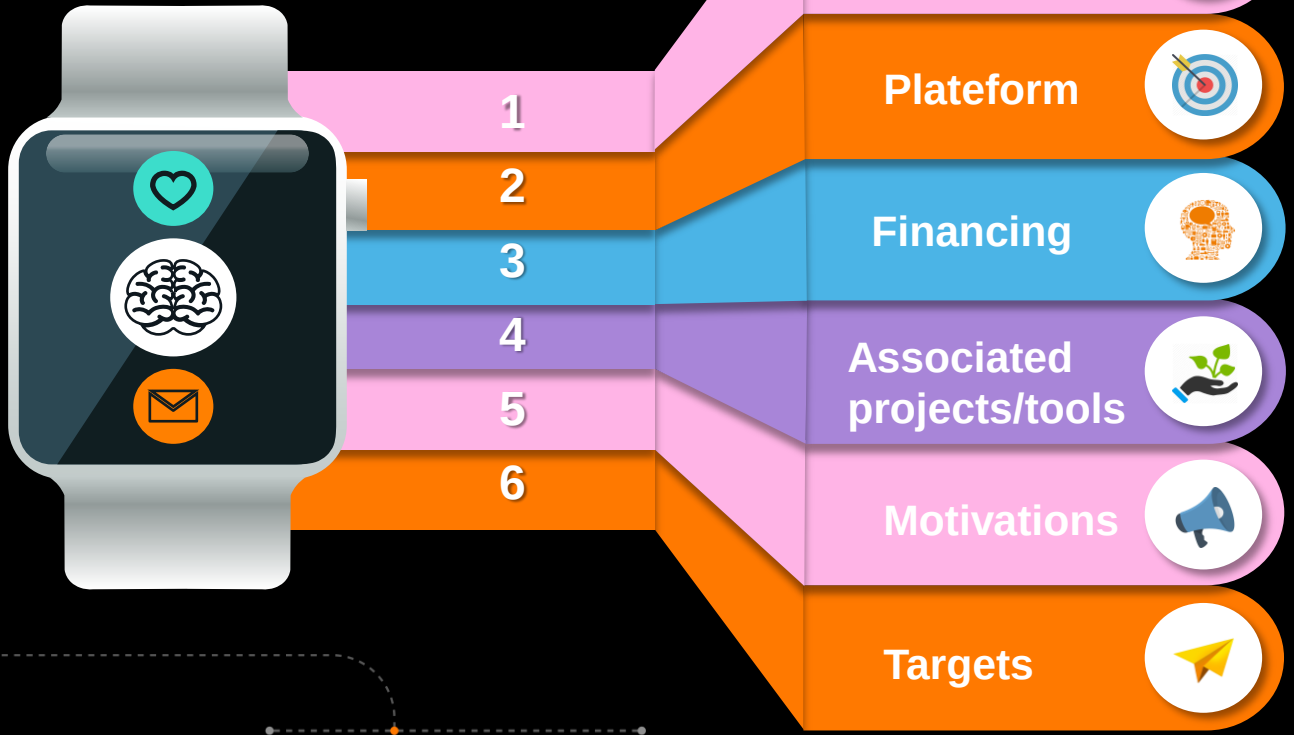
The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

RipperSec

- Creation date: June 2023(not confirmed)
- Strategies : Leaks, DDoS, MegaMedusa tool, proxies to mask the origin of attacks, bypass CAPTCHAs, ZeusAPI to bypass DDOS protections, Coalitions with other groups
- Géopolitical Motivation: Support for the Palestinian cause, Opposition to Israel's allies, Social justice and denunciation of injustices
- Characteristics: Pro-Palestinian and pro-Muslim, based in Malaysia. Aggressive targeting of France: France is a preferred target, collaboration with pro-Russian groups: their alliances reveal broader geopolitical connections.
- Sectors: Government institutions, public services, International organizations Businesses, private sectors, Research and education institutions, Health sector, Media, Technology, Finance

Identification

Key Points



Decentralized network of cells collaborating on common goals, including support for the Palestinian cause

Telegram, secure messaging services on the deepweb, darknet, Facebook, X-Twitter and e-media

Adopts a hybrid financial model, combining collaboration with other groups, and the sale of stolen information on the dark web

Uses a range of tools and techniques such as ZeusAPI PRO and MegaMedusa

Pro-Palestinian and pro-Muslim ideology, which pushes them to target entities perceived as supporting Israel or oppressing Muslims.

European Court of Human Rights, transport, energy, health, finance, and information technology

Credits Orange Cyberdefense

Vectors of Influence

1

Ideology

The group leverages this shared conviction to mobilize sympathizers and rationalize its actions. They target organizations and countries perceived as supporting Israel's oppression of Palestinians, framing their cyberattacks as a form of digital resistance.

2

Injustice

Resentment felt by many toward perceived Western bias and intervention in the Middle East. They present themselves as defenders of the oppressed, seeking to expose and disrupt those they deem complicit in these injustices.

3

Propaganda

The group leverages platforms like Telegram to disseminate propaganda, coordinate actions, and cultivate a sense of community among its members. Their online presence allows them to rapidly disseminate information, recruit new members, and incite action on a global scale.

4

Attractive

RipperSec attracts individuals who want to be actively involved, using their technical skills to support a cause. The group utilizes Telegram and other platforms to maximize recruitment and coordinate attacks.

5

Romanticization of hacking

The "hacker" image: RipperSec capitalizes on the popular perception of hackers as skilled and rebellious figures challenging the status quo. They cultivate this image to attract recruits, romanticizing their actions as a form of digital activism against powerful institutions.

Emotional Intelligence

1 Exploitation of cognitive dissonance: By exposing contradictions, they push individuals to question their beliefs and open up to the group's influence.

2 The group is creating a sense of urgency: The use of alarmist language and shocking images pushes individuals to act quickly without critical thinking.

3 Use of social proof: RipperSec highlights its importance and effectiveness to encourage individuals to conform and join the movement.
The group uses inclusive language and strong symbols to create a sense of belonging and solidarity.

4 Manipulation of emotions: RipperSec exploits anger, fear, and indignation to mobilize its supporters and justify its actions.

5 Use of simplification and polarization: Simplistic and Manichean arguments facilitate understanding and fuel frustration. The group disseminates information that confirms the prejudices of its supporters to reinforce adherence and resistance to opposing arguments.

6 Use of storytelling: Poignant stories and moving testimonials create empathy and humanize the cause, thereby justifying the RipperSec's actions.

Cyberdefense

Credits Orange Cyberdefense

Techniques and Capabilities

RipperSec primarily uses two cyber techniques to enable and launch cyberattacks:

- **Distributed Denial of Service (DDoS) attacks:**

  These attacks aim to saturate a server with artificial traffic, making it inaccessible to legitimate users.
  The group utilizes the MegaMedusa tool (open source), developed in Node.js, to orchestrate these DDoS attacks, exploiting its capability to handle multiple simultaneous connections to amplify traffic volume.

  MegaMedusa can bypass anti-DDoS protections and specifically target the application layer of web services, rendering websites unavailable to users.

- **Data leaks:**

  The group exfiltrates and discloses sensitive information from targeted organizations to discredit them, disrupt their operations, and attract media attention.
  RipperSec utilizes this technique to create psychological and media impact, exposing confidential or embarrassing information to damage the reputation of its targets and garner public attention.

  The disclosed data may include personal information, trade secrets, or sensitive correspondence, potentially leading to financial and legal consequences for the victims.

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Government institutions
- Public services
- International organizations
- Businesses and private sectors
- Research and educational institutions
- Healthcare sector
- Media
- Technology
- Finance

Note

RipperSec's primary motivation is ideologically driven by support for Palestine and alliances with other hacktivist groups. Their targets are not limited to France, and future attacks could target NATO countries or companies perceived as enemies of their cause.

Targeted Countries

Australia

Thailand

India

Israel

United States

United Kingdom

France

Credits Orange Cyberdefense

The most dangerous hypothesis

Most Likely Scenario:

RipperSec will likely continue to target French organizations related to the technology sector, media, and finance with DDoS attacks and data leaks. The main objective will remain to disrupt operations, gain media attention, and exert pressure for political change in favor of Palestine. These attacks could intensify in frequency and sophistication, exploiting new vulnerabilities and bypassing existing protections. The group could also target European companies perceived as supporting Israel, thereby expanding its scope of action.

Most Dangerous Scenario:

RipperSec might attempt a coordinated attack against critical infrastructure in France and/or other European NATO countries. By targeting sectors like energy, telecommunications, or transportation, the group would aim to cause massive disruption and sow panic. This scenario, although less likely, represents a significant danger due to its potential impact on national security and the well-being of citizens.

It is crucial to note that RipperSec has already demonstrated its ability to collaborate with other hacktivist groups, including those based in Russia. This collaboration could provide the group with additional resources, technical skills, and potential targets, thereby increasing the risk of more sophisticated and damaging attacks.

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