Cyber Insight

NoName057(16)

Cyber Intelligence Bureau

a division of Epidemiology Labs OCD

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.

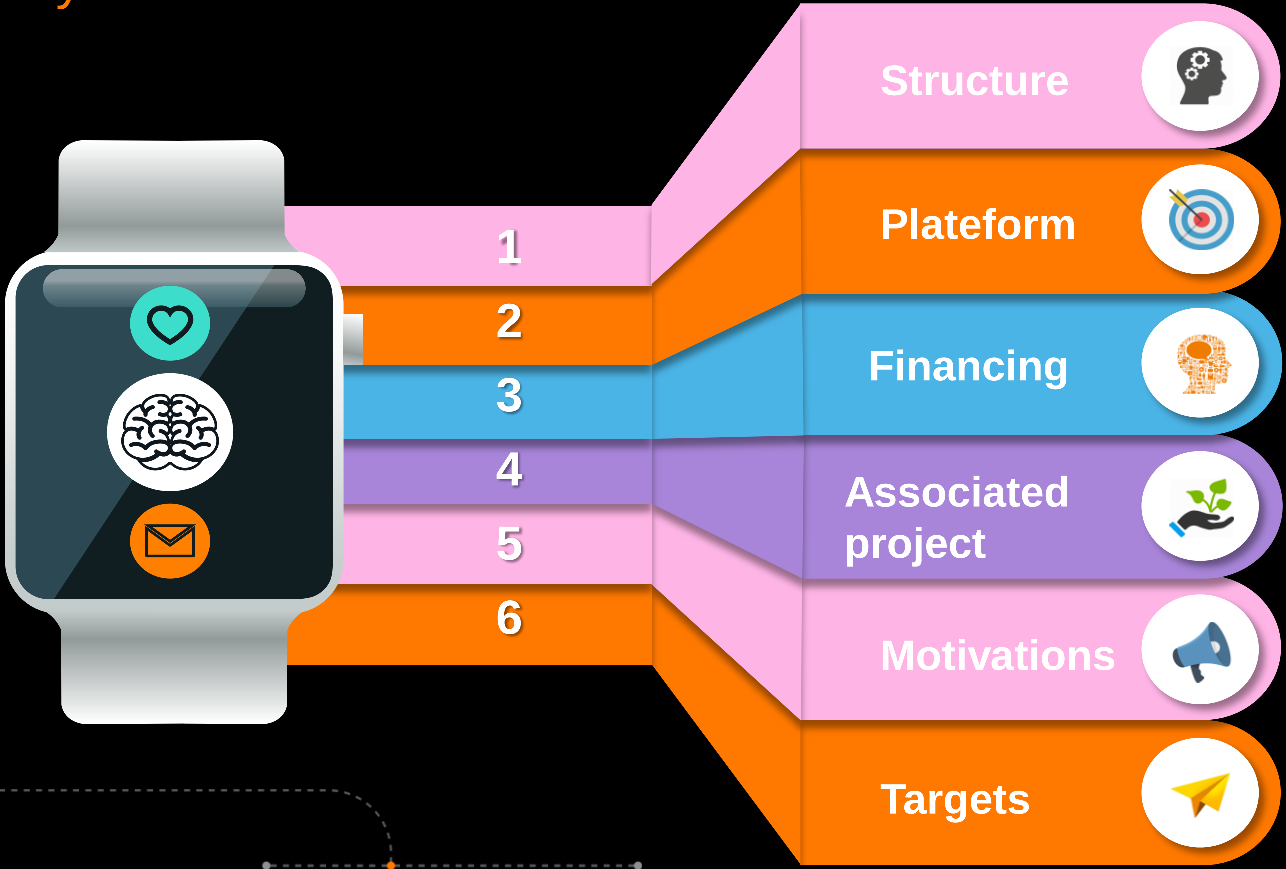
NoName057(16)

- Creation date: March 2022
- Strategies : DDoS attacks via their DDOSIA project
- Motivation: Geopolitical, mainly pro-Russian
- Characteristics: Community threat, based on paid individuals
- Sectors: State organizations, media and private companies linked to political events or decisions perceived as hostile to Russia
- Number of Telegram followers - September 2024: 76600

Identification

Credits Orange Cyberdefense

Key Points



1 **Structure**

Horizontal organizational structure (unconfirmed)

2 **Plateform**

Telegram: coordination and communication in Russian and English

3 **Financing**

Remuneration of “hero” participants in attacks - Crypto currency TON via CryptoBot

4 **Associated project**

DDoS attacks with DDoSia software daily updates

5 **Motivations**

Pro-Russian geopolitics, player in the “information war” against Russia

6 **Targets**

Targeting of state organizations in Ukraine, NATO and EU countries

Credits Orange Cyberdefense

Vectors of Influence

1

Sentiment

Nationalism and pro-Russian patriotism.
The group exploits these sentiments to recruit, justify its actions and mobilize online support

2

Resistance

Anti-Western resistance
Demonization of the West, as a hostile force seeking to weaken Russia, justifying its cyberattacks

3

Greed

Financial incentive via the DDosia project
Offers cryptocurrency rewards to participants based on their contribution to DDoS attacks, attracting individuals motivated by gain.

4

Strategies

Strategies around Telegram.
Using this platform to spread propaganda, coordinate attacks, recruit members, make announcements and claim responsibility for its actions to a wide audience.

5

Visibility

Seeking media visibility.
Targets leading institutions.
The group secures media coverage to spread its message and influence public opinion..

Credits Orange Cyberdefense

Emotional Intelligence

Creating fear and uncertainty among victims DDoS attacks disrupt essential services, creating a climate of anxiety and worry 1

Nurturing ego and a sense of belonging:
NoName's “hero” members are encouraged to share their exploits and feel valued within the group. 2

Stirring up anger and resentment among adherents.
The group exploits nationalism and frustration at perceived anti-Russian stances. 3

4 Exploiting feelings of injustice and the desire for revenge. The group's propaganda presents the cyberattacks as a legitimate response to anti-Russian actions.

5 Promising financial rewards to fan the flames of greed. DDosia's payment program encourages greed-driven individuals to join the attacks.

6 Reinforcing ideology by presenting it as an identity. NoName promotes a vision of the world where support for Russia transcends geographical and cultural boundaries.

Credits Orange Cyberdefense

Tools and services used

DDoSia:
Easy-to-use DDoS client. Tool compiled daily new features

CryptoBot:
Telegram bot used to pay participants (“heros”) in TON cryptocurrency, based on their “performance”.

Telegram:
Platform for centralizing communication, coordinating attacks, disseminating propaganda, recruiting members and publishing claims.

Check-Host.net:
Checks the effectiveness of attacks and publishes “trophy” screens.

Virtual Private Networks (VPN):
For Russian-based “heroes” and participants to mask themselves.

Strategic partnerships :
Collaboration with groups and the RCAT project

Credits Orange Cyberdefense

Sectors of Activities

Targeted Sectors

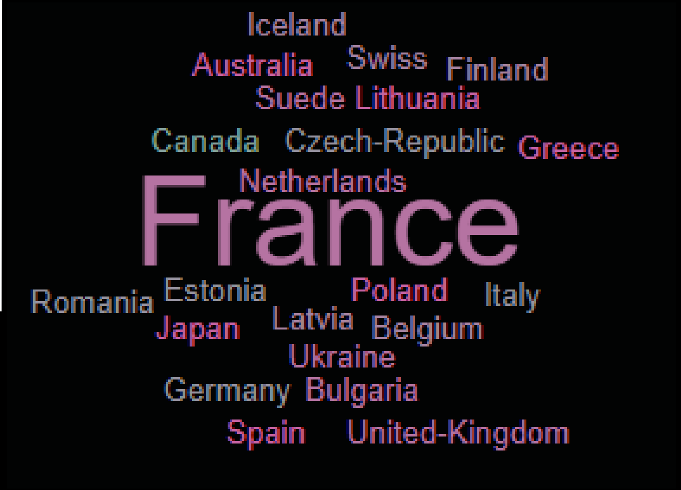
- Government
- Banking
- Transportation
- Technology
- Energy
- Defense

Note

NoName057(16) targets sectors of activity essential to the functioning of states and the economy, the daily lives of citizens, commercial operations and national security.

Credits Orange Cyberdefense

Targeted Countries



Credits Orange Cyberdefense

The most dangerous hypotheses

- Large-scale, coordinated DDoS attacks against French critical infrastructures, such as the energy sector, transport or telecommunications
- Dissemination of false information targeting French public opinion via social media platforms and falsified news sites, with the aim of influencing confidence in the government or stirring up social tensions
- Ransomware attacks targeting French hospitals, businesses and government agencies
- Exploitation of security flaws in critical software and information systems used in France, enabling attackers to take control of critical infrastructures and cause major damage.
- Destabilization campaigns by pro-Russian groups seeking to exploit political and social divisions in France.

orange Cyberdefense

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Laboratoire d'Epidémiologie OCD

Build a safer digital society

orange™ Cyberdefense

Credits Orange Cyberdefense