



Cyber Insight

Shadow ClawZ 404 Group

Cyber Intelligence Bureau

a division of Epidemiology Labs



Cyberdefense

<https://www.orange cyberdefense.com/global/insights/research-intelligence/epidemiology-labs>



Cyberdefense

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.

Shadow ClawZ 404 Group

- **Creation date:**
Early December 2025: Shadow ClawZ 404 publicly emerged during this period, marked by the creation of its Telegram channels and the release of its initial identity-related messages. Its emergence fits within the broader global expansion of hacktivism fueled by nationalist narratives reacting to the conflict in Ukraine and to European support for Ukraine
- **Probable Origin:**
The target selection, the use of English communications containing Russian-language elements, and the alliances established suggest that the group originated within pro-Russian volunteer hacktivist networks.
- **Main strategies:**
The group uses repeated DDoS attacks while also exploiting poorly secured IoT/CCTV devices, claiming intrusions into industrial and banking systems.
- **Geopolitical Motivation:**
Shadow ClawZ 404 seeks to support Russia's strategic objectives and counter the narrative promoted by Kyiv's allies, while aiming to penalize European countries supporting Ukraine, undermine public confidence in the security of critical infrastructure, and establish its presence within the hacktivist landscape.
- **Targeted business sectors:**
Shadow ClawZ 404 has claimed intrusions into and access to photovoltaic power plants and associated SCADA systems, as well as pumping systems and PLC automation equipment within industrial environments. It has also targeted public-sector and ministerial web services through DDoS attacks, while claiming the exfiltration of banking and investment data. In addition, it has reported infiltrating CCTV and DVR surveillance systems at commercial, construction, and rural sites, reflecting a broad focus on energy, industrial, governmental, financial, and IoT-related targets.



Identification

Shadow ClawZ 404, a pro-Russian hacktivist collective that emerged in late 2025 to execute low-to-mid complexity cyber operations against European and Ukrainian infrastructure. Operating primarily through Telegram networks, the group utilizes commodity denial-of-service tools and opportunistic exploitation of default credentials to target energy, industrial, financial, and surveillance systems. Rather than relying on advanced technical capabilities, the organization strategically amplifies its impact through psychosocial influence techniques, drawing on established behavioral frameworks to foster internal cohesion and project an exaggerated sense of capability.

Associated Adversary Groups of Shadow ClawZ 404

NoName057(16) (and the DDoSia network)

- Profile: A major, leading pro-Russian collective.
- Role: Leverages the participatory DDoSia platform to recruit volunteer participants into distributed denial-of-service (DDoS) attacks.

Russian Legion

- Profile: A nationalist, pro-Russian cyberactivist group.
- Role: Conducts service-disruption operations and participates in formal announcements of unified force.

Dark Storm (DarkStormTeam)

- Profile: A unit specializing in web disruption and amplification.
- Role: Forms opportunistic coalitions to co-sign attacks and increase their visibility on Telegram.

BD Anonymous

- Profile: A collective reusing Anonymous' visual codes for pro-Russian purposes.
- Role: Conducts cross-promotion and joint actions through the co-branding of operations.

Monarch (aka Monarc / Cardinal)

- Profile: Founding collective and driving force behind the "Russian Legion" alliance.
- Role: Coordinates multiple hacktivist cells (including Shadow ClawZ 404) in cyber-sabotage campaigns and targeted influence operations.



Vectors of Influence

1

Identity & Belonging

Shadow ClawZ 404 builds a strong visual and theatrical identity on Telegram to give isolated members a feeling of power and community. This striking image draws in volunteers who want to join a shared cause without any financial reward.

2

Social Proof

The group has publicly claimed control of CCTV systems, photovoltaic plant SCADA systems in Northern Europe, banking data, and Japanese logistics networks, using these posts as proof of ongoing capability.

3

Moral Legitimacy

The collective presents its cyberattacks as simple, legitimate responses against an opponent portrayed as aggressive. This role reversal lets participants target critical infrastructure without feeling moral guilt.

4

Psychological Pressure

By repeatedly spreading warning slogans, Shadow ClawZ 404 keeps its targets in constant fear of an imminent attack. This permanent threat exhausts security teams who must stay on continuous high alert.

5

Alliance Authority

Shadow ClawZ 404 publicly displays partnerships with other recognized collectives to create the impression of major force. This show of strength impresses observers and convinces recruits of the network's solidity.

Emotional Intelligence

1

Emotional contagion: Shadow ClawZ 404 spreads messages heavily charged with anger and indignation across its networks so these feelings instantly pass to its followers. This automatic emotional transfer pushes supporters to share the resentment and react impulsively.

2

Collective moral indignation : The collective instrumentalizes the feeling of injustice by pointing to specific targets as responsible for geopolitical tensions. This shared anger turns individual discontent into motivated action driven by the desire to punish the adversary.

3

Hijacking of emotional regulation: By repeatedly triggering emotional shocks through spectacular announcements, the attackers disrupt their targets' ability to think calmly. This blockage of logical reasoning pushes victims and observers to react under stress rather than reason.

4

Selective empathy and dehumanization: The group limits its members' compassion strictly to their own community while portraying European targets as mere hostile entities. This neutralization of human feeling makes attacks on civilian infrastructure fully acceptable in the militants' eyes.

5

Collective narcissism and the appeal to pride: Communications constantly highlight the collective's exaggerated technical superiority and invincibility to flatter recruits' egos. This boosting of group pride strengthens the loyalty of supporters who identify with this image of power.

6

Emotional exhaustion and decision fatigue: The uninterrupted stream of small claims and threats creates an anxiety-inducing background noise that saturates the attention of crisis managers. This progressive emotional numbing lowers defenders' vigilance and slows their ability to respond.



Professional Sectors

List of targeted sectors

- Energy & Renewable Energy
- Industrial Control Systems (ICS/SCADA) & Manufacturing
- Government & Public Sector
- Financial & Banking Services
- Healthcare & Public Infrastructure
- Commercial Facilities & Video Surveillance



Note

Shadow ClawZ 404 is a pro-Russian hacktivist collective targeting critical infrastructure across European professional sectors, including energy, manufacturing, finance, and public services. The group combines low-to-medium complexity DDoS attacks with the opportunistic exploitation of internet-exposed IoT devices, CCTV networks, and default credentials. It actively asserts compromise over SCADA/ICS operational technology, such as photovoltaic plants and industrial pumping systems, to maximize geopolitical leverage. By pairing technical disruption with strategic Telegram propaganda, the collective weaponizes narrative influence to impose continuous psychological pressure on sector defenders.

Targeted Countries



Northern European countries

Ukraine

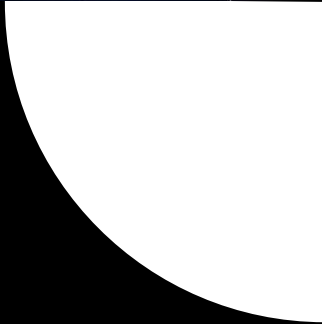
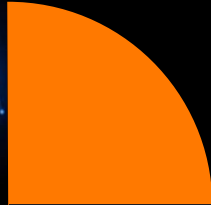
France

Belgium

Poland

European Union (EU) member states

High-Probability Future Targets Countries



Czech Republic

Netherlands

Norway

Denmark

Germany

Poland

Ukraine

Belgium

France

Estonia

Finland

Sweden

Romania

Spain

Italy

Most Probable Hypothesis on Shadow ClawZ 404's Future Activities

Strategy & Anticipated Tactics

- Ongoing DDoS campaigns: Continued medium-volume attacks on government, institutional, and commercial websites.
- Opportunistic IoT & SCADA targeting: Automated scanning and exploitation of default credentials on Internet-exposed CCTV/DVR and SCADA/ICS systems.
- Telegram information warfare: Claims of industrial compromises and data exfiltration to boost visibility and credibility.

Targeted Sectors & Regions

- Sectors: Public services, banking and finance, energy infrastructure (especially solar/renewables), industrial automation, and video surveillance.
- Regions: Ukraine, Belgium, Poland, France, and Northern/Western Europe.

Impact & Strategic Goals

- Psychological pressure: Create temporary outages and sustain anxiety among infrastructure operators.
- Coalition building: Reinforce alliances through the DDoSia network and attract volunteer recruits.



The most dangerous hypothesis



Attack Nature

- Combined attack: ICS/SCADA compromise + mass DDoS.
- Targets: Public services and transportation.
- Timing: Major geopolitical or diplomatic tension in Europe.

Vectors & Tactics

- Exploitation: Default credentials on PLCs, SCADA portals, solar plants.
- Disruption: Water pumping and local power grids.
- Amplification: Theatrical claims on Telegram and in the media.

Targets

- Sectors: Energy, renewables, ICS/SCADA, public services, transport, IoT surveillance.
- Regions: Ukraine, Poland, Belgium, France, Germany, Baltics, Northern Europe.

Feared Impacts

- Operational: Equipment downtime; disruption of essential services.
- Economic: Production losses; emergency response costs.
- Psychosocial: Public panic; systemic insecurity; political pressure.



Cyber Intelligence Bureau

a division of Epidemiology Labs



Build a safer digital society



Cyberdefense

<https://www.orange cyberdefense.com/global/insights/research-intelligence/epidemiology-labs>

Credits Orange Cyberdefense