SHUM

CYBER THREAT INTELLIGENCE REPORT

NoName057(16)
Pro-Russian Hacktivist DDoS Collective

NoName057(16) is a pro-Russian hacktivist collective engaged in large-scale Distributed Denial-of-Service (DDoS) campaigns targeting government institutions, financial systems, transportation infrastructure, and media organizations across Europe and NATO-aligned countries.

Since its emergence in 2022, the group has developed into a persistent and scalable disruption actor. It operates using a volunteer-based attack model supported by the DDoSia platform and coordinated primarily through Telegram.

Recent intelligence indicates a renewed and sustained level of activity, suggesting that the group has successfully maintained operational resilience despite law enforcement pressure and disruption attempts.

Unlike traditional Advanced Persistent Threat (APT) groups, NoName057(16) does not focus on persistence or espionage. Its primary objective is disruption through high-volume DDoS attacks aligned with geopolitical triggers.

Key Judgments

- NoName057(16) is a high-impact hacktivist disruption actor.
- Operations are event-driven and aligned with geopolitical developments.
- Volunteer-based participation significantly increases scalability.
- The group demonstrates strong resilience and adaptability.
- Recent activity indicates sustained or renewed operational tempo.

Support the organization’s activities: https://donate.shum-ng.org/

Recent Activity (March 2026):

In March 2026, there is a notable surge in hacktivist-driven DDoS activity affecting government, corporate, and event-related online services across multiple regions. This increase aligns with heightened geopolitical tensions and reflects broader hacktivist mobilization trends. Pro-Russian hacktivist collectives, including NoName057(16), have been associated with attempts to disrupt high-profile targets, such as the Milano-Cortina 2026 Winter Olympics web infrastructure and various European organizational sites. Although direct public attribution for specific March attacks is limited, the pattern of elevated DDoS campaigns is consistent with the group's historical behavior and operational profile, indicating continued operational activity in 2026.

Recent observations indicate renewed operational activity following temporary fluctuations.

Indicators include:

- Increased frequency of coordinated DDoS campaigns
- Continued targeting of NATO-aligned countries
- Reappearance of multi-wave attacks
- Sustained Telegram-based coordination
- Continued use of the DDoSia platform

Analytical Implication

This activity suggests:

- Reconstitution of operational capabilities
- Continued recruitment and engagement
- Adaptation to disruption efforts

Threat Actor Overview

- **Type**: Hacktivist / Cybercrime Collective
- **Motivation**: Political / Ideological (Pro-Russian alignment)
- **First Observed:** 2022

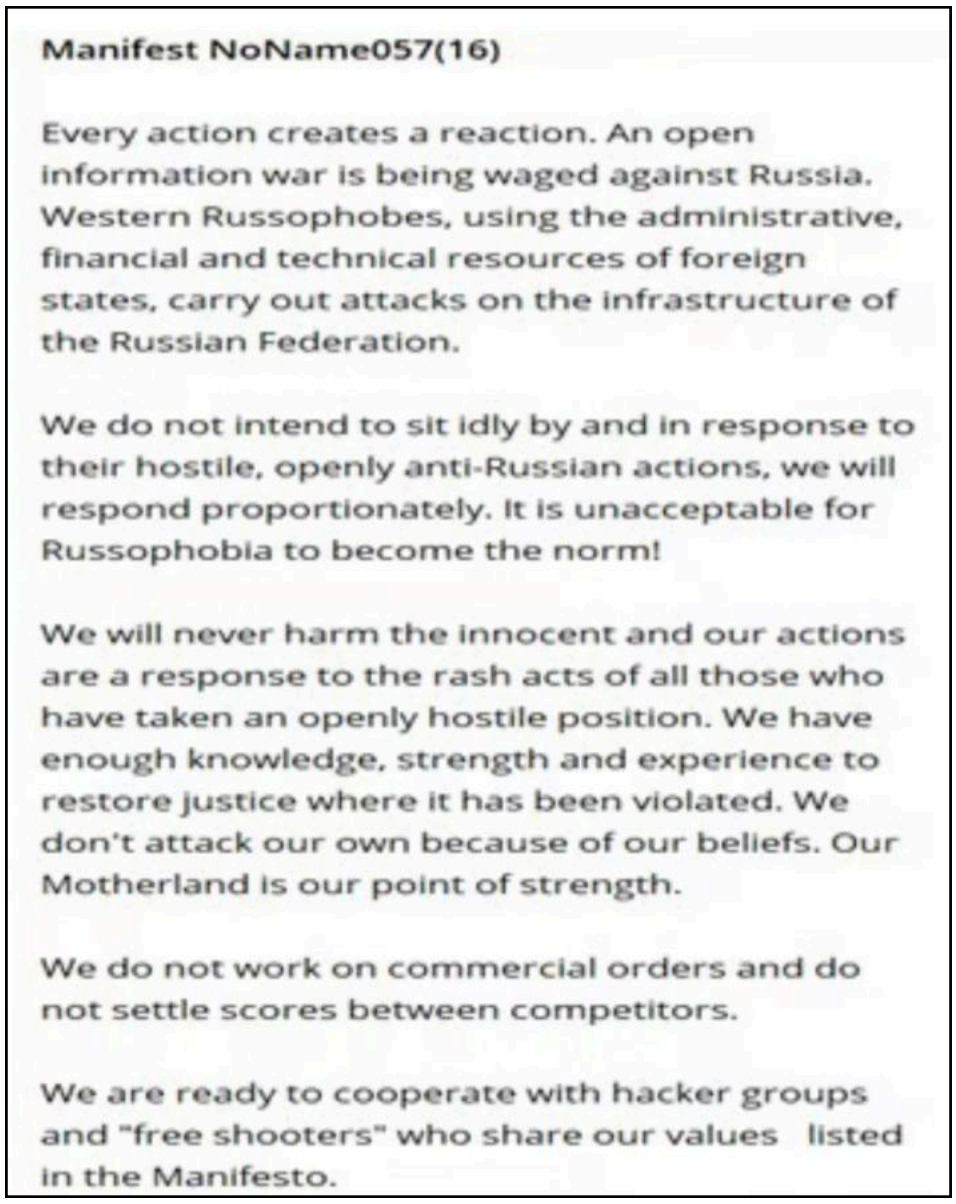
Affiliated Actors

- ServerKillers
- 404CREWCYBERTEAM
- DarkStormTeam
- BDAnonymous

Support the organization's activities: https://donate.shum-ng.org/

Shortly after the Russo-Ukrainian conflict began, a new threat actor announced their formation on Telegram along with their manifesto.

Their self-declared mission statement was to counter-act open hostility towards Russia, targeting NATO-aligned countries. Additionally, they stated an openness to collaborate and would not target innocent people, though the latter part of that statement has not held true.



Manifest NoName057(16)

Every action creates a reaction. An open information war is being waged against Russia. Western Russophobes, using the administrative, financial and technical resources of foreign states, carry out attacks on the infrastructure of the Russian Federation.

We do not intend to sit idly by and in response to their hostile, openly anti-Russian actions, we will respond proportionately. It is unacceptable for Russophobia to become the norm!

We will never harm the innocent and our actions are a response to the rash acts of all those who have taken an openly hostile position. We have enough knowledge, strength and experience to restore justice where it has been violated. We don't attack our own because of our beliefs. Our Motherland is our point of strength.

We do not work on commercial orders and do not settle scores between competitors.

We are ready to cooperate with hacker groups and "free shooters" who share our values listed in the Manifesto.

Operational Model

NoName057(16) operates as a semi-decentralized, volunteer-driven collective.

Key elements:

- Central coordination via Telegram
- Distributed execution by volunteers
- Gamified participation (leaderboards, rewards, badges)
- Cryptocurrency-based incentives

The group maintains ideological alignment with pro-Russian narratives but operates without confirmed direct state control.

Support the organization’s activities: https://donate.shum-ng.org/

Strategic Objectives

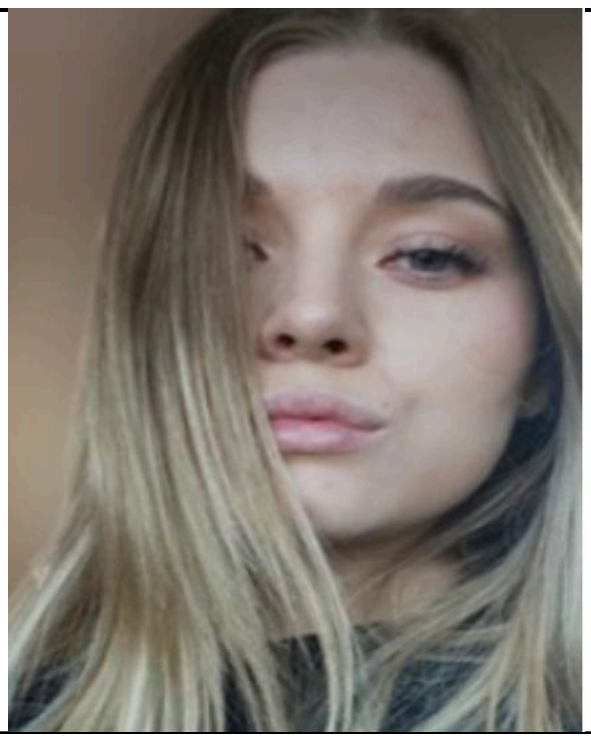
- Disruption of digital services
- Psychological and informational impact
- Demonstration of cyber capability
- Undermining trust in infrastructure
- Amplification of geopolitical narratives

Key Individuals (Attribution)

Mikhail Evgenyevich Burlakov

- Technical leader
- Responsible for development and optimization of attack tooling
- Manages infrastructure-related operations

Olga Evstratova

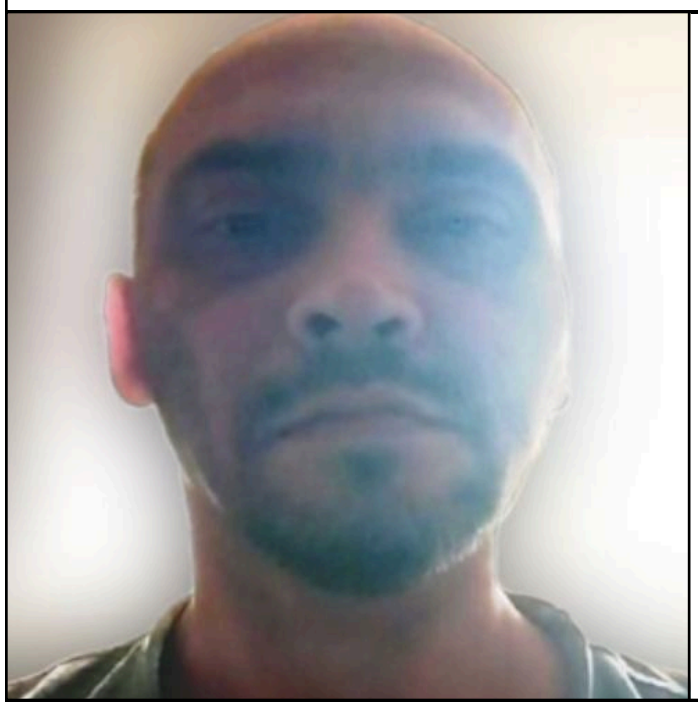


- Software developer
- Key contributor to DDoSia platform
- Supports automation and scalability of attacks

Support the organization’s activities: https://donate.shum-ng.org/

SHUM

Andrey Stanislavovich Avrosimov



- Operational participant
- Associated with execution of cyberattacks

Maxim Nikolaevich Lupin

- Coordinator
- Supports operational and infrastructure management

Andrey Muravyov

- Support actor
- Contributes to infrastructure and operational execution

Support the organization’s activities: https://donate.shum-ng.org/

Summary of Roles

Name	Nationality	Role	Main Responsibilities
Mikhail Burlakov	Russian	Technical leader	Software development/optimization, server infrastructure payments
Olga Evstratova	Russian	Technical member	Optimization of DDoSia, software development
Andrey Avrosimov	Russian	Operational participant	Cyber sabotage, conducting attacks
Andrey Muravyov	Russian	Support participant	DDoSia operation, promotion and support

Targeting and Geographic Scope

Primary Targets:

- Government institutions
- Financial systems
- Transportation infrastructure
- Media organizations
- Energy sector

Geographic Focus

- Poland
- Baltic States
- Germany
- Italy
- Spain
- Czech Republic
- Ukraine
- Other NATO-aligned entities

Operational Characteristics

- Heavy reliance on DDoS attacks (T1498)
- Event-driven campaigns
- Telegram-based coordination
- Volunteer-driven botnet model
- Rapid deployment capability
- Low technical sophistication

Indicators of Activity (IOAs)

- Increased Telegram activity
- Frequent target publication
- Multi-country coordinated attacks
- Continued DDoSia usage
- Repeated targeting of sectors
- Alignment with geopolitical events

Support the organization’s activities: https://donate.shum-ng.org/

References (Real Sources)

- Europol – Most Wanted Fugitives (Cybercrime)
  https://www.europol.europa.eu/most-wanted
- Europol (EC3) – Internet Organised Crime Threat Assessment (IOCTA)
  https://www.europol.europa.eu/publications-events/main-reports
- ENISA – Threat Landscape Reports
  https://www.enisa.europa.eu/publications/enisa-threat-landscape
- CERT-EU – Threat Intelligence Reports
  https://cert.europa.eu/publications/
- Microsoft Threat Intelligence Blog
  https://www.microsoft.com/en-us/security/blog/
- Mandiant (Google Cloud) – Threat Intelligence Reports
  https://www.mandiant.com/resources
- CrowdStrike – Threat Intelligence Reports
  https://www.crowdstrike.com/resources/reports/
- Flashpoint – Intelligence Reports on Hacktivism
  https://flashpoint.io/blog/
- Recorded Future – Intelligence Reports
  https://www.recordedfuture.com/resources
- BKA (Germany Federal Criminal Police) – Cybercrime statements
  https://www.bka.de/EN/
- Spanish National Police – Cybercrime operations
  https://www.policia.es/
- Open-source intelligence from publicly available Telegram channels and news reporting on DDoS campaigns

Tactics, Techniques, and Procedures (MITRE ATT&CK)

Tactic	Technique
Impact	T1498 – Network Denial of Service
Impact	T1499 – Endpoint Denial of Service
Resource Development	T1584 – Infrastructure via volunteers
Command & Control	T1071 – Application Layer Protocol (Telegram)
Reconnaissance	T1590 – Open-source targeting

Threat Assessment

- Threat Level: **Medium–High**
- Impact: **High**
- Likelihood: **High**
- Persistence: **High**
- Confidence: **Medium**

Hypothesis

The renewed activity of NoName057(16) may indicate:

- Reconstitution of operational infrastructure
- Increased recruitment of participants
- Adaptation to law enforcement pressure
- Continued geopolitical alignment
- Sustained operational relevance

Key Findings

1. Persistent multi-country targeting
2. Telegram-centric coordination
3. Standardized DDoS methodology
4. Psychological and propaganda component
5. Limited technical sophistication

Conclusion

NoName057(16) continues to represent a resilient and active hacktivist threat actor capable of executing large-scale DDoS campaigns.

Despite disruption efforts, the group maintains:

- operational continuity
- participant engagement
- adaptive capabilities

It remains a significant cyber disruption threat to European and NATO-aligned infrastructure.

Lockheed Martin Cyber Kill Chain Mapping

The operations of NoName057(16), while less technically sophisticated than traditional APT actors, can still be effectively mapped to the Lockheed Martin Cyber Kill Chain model, highlighting a structured and repeatable attack lifecycle.

Attack Chain Table

Phase	Activity	Techniques Used	Tools / Methods	Observed Behavior
Reconnaissance	Target identification	Open-source intelligence	Public data, news monitoring	Selection of politically relevant targets
Weaponization	Preparation of attack vectors	DDoS payload configuration	DDoSia scripts	Pre-configured traffic patterns
Delivery	Distribution of attack instructions	Telegram channels	Target lists, attack commands	Mass coordination
Exploitation	Initiation of attack	Network flooding	HTTP / TCP floods	Immediate service disruption attempts
Installation	Botnet activation	Volunteer node engagement	DDoSia clients	No persistence (stateless attacks)
Command & Control	Coordination of attack waves	Application-layer comms	Telegram	Real-time updates
Actions on Objectives	Service disruption	DDoS impact	Traffic saturation	Website downtime / latency

Repetition & Pattern Table

Pattern Type	Description	Evidence
Re-targeting	Same country attacked multiple times	Poland, Germany
Sector rotation	Gov → Finance → Media	Observed across campaigns
Event-driven spikes	Attacks after political events	Consistent timing
Multi-country waves	Simultaneous targeting	Coordinated campaigns

Geopolitical Correlation Analysis

Event Type	Observed Response	Time Delay	Target Shift
Military aid to Ukraine	Immediate DDoS campaigns	24–48h	Poland, Germany
Sanctions announcements	Financial sector attacks	24h	Banks
NATO activity	Government targeting	24–72h	EU states
Media narratives	Media site attacks	Same day	News platforms

Conclusion

NoName057(16) continues to operate as a persistent and adaptive hacktivist collective capable of executing large-scale Distributed Denial-of-Service (DDoS) campaigns. Despite international law enforcement pressure and disruption attempts, the group has demonstrated an ability to maintain operational continuity and rapidly reconstitute its capabilities.

The group’s reliance on a volunteer-driven model, combined with centralized coordination via Telegram and the use of the DDoSia platform, enables high scalability and low entry barriers for participants. This structure significantly enhances its resilience and allows it to quickly mobilize resources in response to geopolitical triggers.

Recent activity indicates that NoName057(16) remains operationally active and continues to target NATO-aligned countries, suggesting sustained motivation and access to resources. The observed patterns confirm that the group prioritizes disruption over persistence, focusing on high-impact, short-duration attacks designed to degrade services and generate visibility.

From an analytical perspective, the group represents a **persistent cyber disruption threat** rather than a sophisticated intrusion actor. Its strength lies in coordination, scalability, and ideological alignment rather than technical complexity.

Final Analytical Takeaways

- The group is **resilient and difficult to fully disrupt** due to its decentralized volunteer model.
- Operational activity is **event-driven and geopolitically motivated.**
- The use of **automation platforms (DDoSia)** enables rapid scaling of attacks.
- Telegram remains the **core coordination and command infrastructure.**
- NoName057(16) should be assessed as a **continuing medium-to-high threat to digital infrastructure stability,** particularly within NATO-aligned regions.

Support the organization’s activities: https://donate.shum-ng.org/