ЗВІТ З КІБЕРРОЗВІДУВАЛЬНОЇ АНАЛІТИКИ ЗАГРОЗ

NoName057(16)

Проросійське хактивістське угруповання, орієнтоване на DDoS-атаки

NoName057(16) — це проросійське хактивістське угруповання, яке проводить масштабні кампанії Distributed Denial-of-Service (DDoS), спрямовані проти державних установ, фінансових систем, транспортної інфраструктури та медіаорганізацій у країнах Європи та державах, орієнтованих на НАТО.

З моменту появи у 2022 році група перетворилася на стійкого та масштабованого актора, що спеціалізується на деструктивній діяльності. Вона працює за моделлю атак на основі волонтерської участі, яку підтримує платформа DDoSia, а координація здійснюється переважно через Telegram.

Останні розвідувальні дані вказують на відновлення та стабільно високий рівень активності, що свідчить про здатність групи підтримувати операційну стійкість попри тиск з боку правоохоронних органів та спроби її нейтралізації.

На відміну від традиційних груп класу Advanced Persistent Threat (APT), NoName057(16) не фокусується на довготривалому закріпленні чи кібершпигунстві. Її основна мета — створення перебоїв через високонавантажені DDoS-атаки, синхронізовані з геополітичними подіями.

Ключові висновки

- NoName057(16) є хактивістським актором із високим рівнем деструктивного впливу.
- Операції мають подієво-орієнтований характер і узгоджуються з геополітичними подіями.
- Модель участі на основі волонтерів суттєво підвищує масштабованість діяльності групи.
- Група демонструє високий рівень стійкості та адаптивності.
- Остання активність свідчить про збереження або відновлення високого операційного темпу.

Підтримати діяльність організації: https://donate.shum-ng.org/

Остання активність (березень 2026):

У березні 2026 року спостерігається помітне зростання активності DDoS-атак, організованих хактивістськими угрупованнями, які впливають на державні, корпоративні та пов’язані з подіями онлайн-сервіси в різних регіонах. Це зростання збігається з посиленням геополітичної напруги та відображає ширшу тенденцію мобілізації хактивістських груп. Проросійські хактивістські угруповання, включно з NoName057(16), пов’язують зі спробами порушити роботу високопрофільних цілей, таких як вебінфраструктура зимових Олімпійських ігор Milano-Cortina 2026 та вебресурси різних європейських організацій. Хоча прямої публічної атрибуції щодо конкретних атак у березні небагато, патерн посилення DDoS-кампаній відповідає історичній поведінці та операційному профілю групи, що вказує на продовження її активної діяльності у 2026 році.

Останні спостереження також вказують на відновлення операційної активності після тимчасових коливань.

Індикатори включають:

- Збільшення частоти скоординованих DDoS-кампаній
- Продовження атак проти країн, орієнтованих на НАТО
- Повторну появу багатоетапних хвиль атак
- Постійну координацію через Telegram
- Подальше використання платформи DDoSia

Аналітичний висновок

Ця активність може свідчити про:

- Відновлення операційних можливостей
- Продовження залучення та активності учасників
- Адаптацію до заходів із протидії та спроб нейтралізації

Огляд загрозливого актора

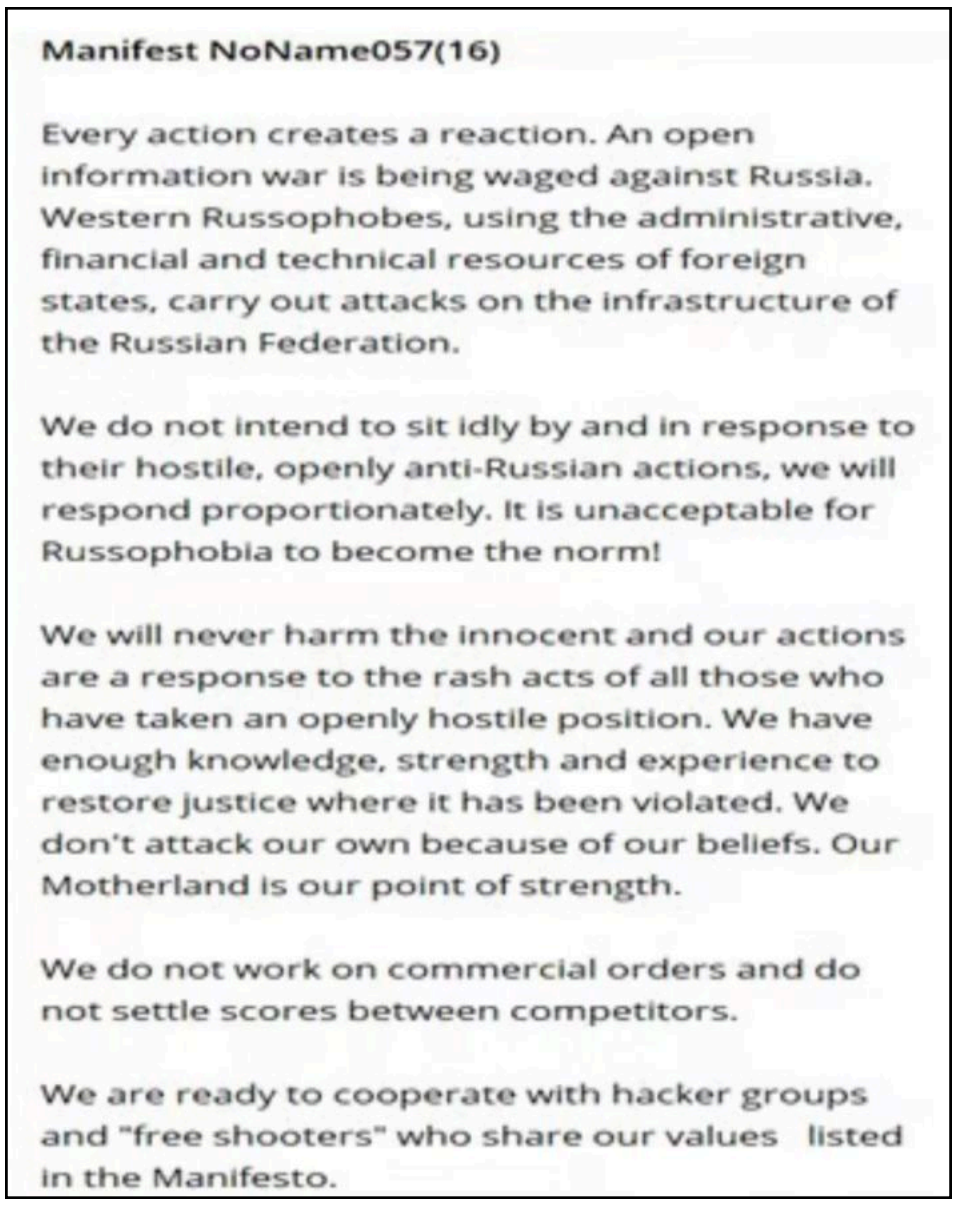
- **Тип:** хактивістське / кіберзлочинне угруповання
- **Мотивація:** політична / ідеологічна (проросійська орієнтація)
- **Перше виявлення:** 2022 рік

Афілійовані актори

- ServerKillers
- 404CREWCYBERTEAM
- DarkStormTeam
- BDAnonymous

Невдовзі після початку російсько-української війни новий загрозливий актор оголосив про своє створення в Telegram, одночасно опублікувавши власний маніфест.

Згідно із заявленою ними місією, метою було протидіяти відкритій ворожості до Росії, націлюючись на країни, орієнтовані на НАТО. Крім того, вони заявляли про готовність до співпраці та стверджували, що не атакуватимуть невинних людей, хоча остання частина цієї заяви згодом не підтвердилася.



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.

Операційна модель

NoName057(16) працює як напівдецентралізоване угруповання, діяльність якого базується на волонтерській участі.

Ключові елементи:

- Централізована координація через Telegram
- Розподілене виконання атак волонтерами
- Гейміфікована участь (рейтинги, винагороди, бейджі)
- Стимулювання через криптовалютні винагороди

Група дотримується ідеологічної орієнтації на проросійські наративи, однак наразі немає підтверджень її прямого контролю з боку держави.

Підтримати діяльність організації: https://donate.shum-ng.org/

Стратегічні цілі

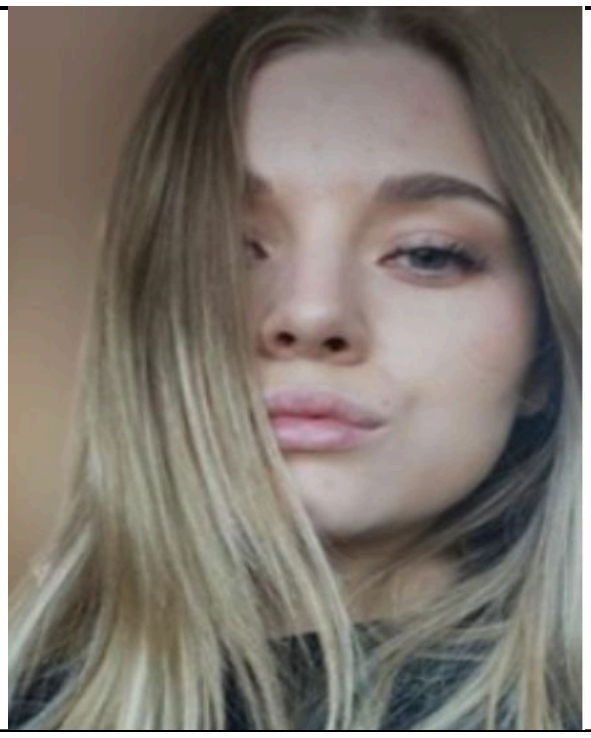
- Порушення роботи цифрових сервісів
- Психологічний та інформаційний вплив
- Демонстрація кіберможливостей
- Підрив довіри до інфраструктури
- Посилення геополітичних наративів

Ключові особи (атрибуція)

Бурлаков Михайло Євгенійович

- Технічний керівник
- Відповідає за розробку та оптимізацію інструментів для атак
- Керує операціями, пов’язаними з інфраструктурою

Ольга Євстратова

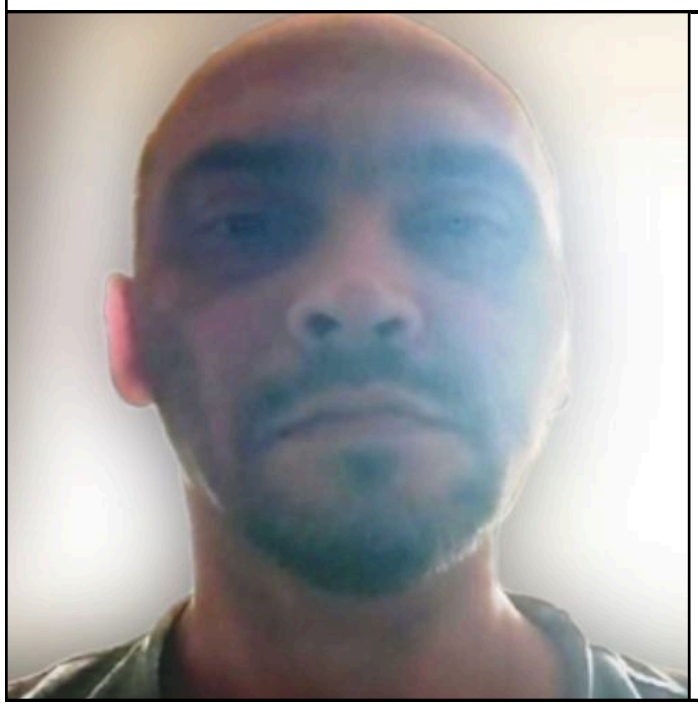


- Розробниця програмного забезпечення
- Ключова учасниця розробки платформи DDoSia
- Підтримує автоматизацію та масштабованість атак

Підтримати діяльність організації: https://donate.shum-ng.org/

SHUM

Авросимов Андрій Станіславович



- Операційний учасник
- Пов’язаний із безпосереднім проведенням кібератак

Лупін Максим Миколайович

- Координатор
- Підтримує операційне та інфраструктурне управління

Андрій Муравйов

- Допоміжний учасник
- Залучений до підтримки інфраструктури та виконання операцій

Підтримати діяльність організації: https://donate.shum-ng.org/

Підсумок ролей

Ім’я	Національність	Роль	Основні обов’язки
Михайло Бурлаков	Російська	Технічний керівник	Розробка та оптимізація програмного забезпечення, оплата серверної інфраструктури
Ольга Євстратова	Російська	Технічний учасник	Оптимізація DDoSia, розробка програмного забезпечення
Андрій Авросимов	Російська	Операційний учасник	Кіберсаботаж, проведення атак
Андрій Муравйов	Російська	Допоміжний учасник	Підтримка роботи DDoSia, просування та супровід

Цілі та географічне охоплення

Основні цілі:

- Державні установи
- Фінансові системи
- Транспортна інфраструктура
- Медіаорганізації
- Енергетичний сектор

Географічний фокус:

- Польща
- Країни Балтії
- Німеччина
- Італія
- Іспанія
- Чехія
- Україна
- Інші держави, орієнтовані на НАТО

Операційні характеристики

- Сильна залежність від DDoS-атак (T1498)
- Кампанії, прив’язані до подій
- Координація через Telegram
- Модель ботнету на основі волонтерської участі
- Можливість швидкого розгортання
- Низький рівень технічної складності

Індикатори активності (IOA):

- Зростання активності в Telegram
- Часте публікування цілей
- Скоординовані атаки одночасно в кількох країнах
- Постійне використання DDoSia
- Повторне націлювання на окремі сектори
- Прив’язка активності до геополітичних подій

Джерела

- Europol – Найбільш розшукувані особи (кіберзлочинність)
  https://www.europol.europa.eu/most-wanted
- Europol (EC3) – Оцінка загроз організованої кіберзлочинності в Інтернеті (IOCTA)
  https://www.europol.europa.eu/publications-events/main-reports
- ENISA – Звіти щодо ландшафту кіберзагроз
  https://www.enisa.europa.eu/publications/enisa-threat-landscape
- CERT-EU – Звіти з threat intelligence
  https://cert.europa.eu/publications/
- Microsoft Threat Intelligence Blog
  https://www.microsoft.com/en-us/security/blog/
- Mandiant (Google Cloud) – Звіти з threat intelligence
  https://www.mandiant.com/resources
- CrowdStrike – Звіти з threat intelligence
  https://www.crowdstrike.com/resources/reports/
- Flashpoint – Аналітичні звіти щодо хактивізму
  https://flashpoint.io/blog/
- Recorded Future – Аналітичні звіти
  https://www.recordedfuture.com/resources
- Федеральне управління кримінальної поліції Німеччини (BKA) – заяви щодо кіберзлочинності
  https://www.bka.de/EN/
- Національна поліція Іспанії – операції у сфері кіберзлочинності
  https://www.policia.es/
- OSINT з відкритих Telegram-каналів та новинних матеріалів щодо DDoS-кампаній.

Тактики, техніки та процедури (MITRE ATT&CK)

Тактика	Техніка
Вплив	T1498 – Network Denial of Service
Вплив	T1499 – Endpoint Denial of Service
Розвиток ресурсів	T1584 – Infrastructure via volunteers
Командування та управління	T1071 – Application Layer Protocol (Telegram)
Розвідка	T1590 – Open-source targeting

Оцінка загрози

- Рівень загрози: **середній–високий**
- Вплив: **високий**
- Ймовірність: **висока**
- Стійкість: **висока**
- Рівень впевненості: **середній**

Гіпотеза

Відновлення активності NoName057(16) може свідчити про:

- Відновлення операційної інфраструктури
- Посилене залучення нових учасників
- Адаптацію до тиску з боку правоохоронних органів
- Збереження геополітичної орієнтації
- Підтримання операційної актуальності

Ключові висновки

1. Координація, зосереджена навколо Telegram
2. Стандартизована методологія DDoS-атак
3. Наявність психологічної та пропагандистської складової
4. Обмежений рівень технічної складності

Висновки

NoName057(16) продовжує залишатися стійким та активним хактивістським загрозливим актором, здатним проводити масштабні DDoS-кампанії.

Попри спроби протидії, група зберігає:

- операційну безперервність
- залучення учасників
- адаптивні можливості

Вона й надалі становить суттєву кіберзагрозу у сфері дестабілізації для європейської інфраструктури та структур, орієнтованих на НАТО.

Мапування за моделлю Lockheed Martin Cyber Kill Chain

Операції NoName057(16), хоча й мають нижчий рівень технічної складності порівняно з традиційними APT-акторами, все ж можуть бути ефективно співвіднесені з моделлю Lockheed Martin Cyber Kill Chain, що демонструє структурований та повторюваний життєвий цикл атак.

Таблиця ланцюга атаки

Фаза	Активність	Використані техніки	Інструменти / методи	Спостережувана поведінка
Розвідка	Визначення цілей	Розвідка з відкритих джерел	Публічні дані, моніторинг новин	Вибір політично значущих цілей
Підготовка засобів атаки	Підготовка векторів атак	Налаштування DDoS-навантаження	Скрипти DDoSia	Попередньо налаштовані патерни трафіку
Доставка	Поширення інструкцій для атак	Telegram-канали	Списки цілей, команди для атак	Масова координація
Експлуатація	Ініціювання атаки	Перевантаження мережі	HTTP / TCP flood-атаки	Негайні спроби порушення роботи сервісів
Встановлення	Активація ботнету	Залучення волонтерів	Клієнти DDoSia	Відсутність закріплення (атаки без збереження стану)
Командування та управління	Координація хвиль атак	Комунікація прикладного шару	Telegram	Оновлення в режимі реального часу
Досягнення цілей	Порушення роботи сервісів	Вплив DDoS-атак	Насичення трафіком	Недоступність вебсайтів / затримки в роботі сервісів

Таблиця повторюваності та патернів

Тип патерну	Опис	Докази
Повторне націлювання	Багаторазові атаки на одну й ту саму країну	Польща, Німеччина
Ротація секторів	Державний сектор → фінансовий сектор → медіа	Різні кампанії
Події як тригер активності	Атаки після політичних подій	Стабільна закономірність
Кампанії у кількох країнах	Одночасне націлювання на різні держави	Скоординовані кампанії

Аналіз геополітичної кореляції

Тип події	Реакція	Часова затримка	Зміна цілі
Військова допомога Україні	Негайні DDoS-кампанії	24–48 годин	Польща, Німеччина
Оголошення санкцій	Атаки на фінансовий сектор	24 години	Банки
Активність НАТО	Дерржавні структури	24–72 години	Країни ЄС
Медійні наративи	Атаки на медіаресурси	Того ж дня	Новинні платформи

Висновки

NoName057(16) продовжує діяти як стійке та адаптивне хактивістське угруповання, здатне проводити масштабні кампанії Distributed Denial-of-Service (DDoS). Попри міжнародний тиск з боку правоохоронних органів та спроби протидії, група демонструє здатність підтримувати операційну безперервність і швидко відновлювати свої можливості.

Модель діяльності групи базується на волонтерській участі, поєднаній із централізованою координацією через Telegram та використанням платформи DDoSia, що забезпечує високу масштабованість і низький поріг входу для учасників. Така структура суттєво підвищує її стійкість та дозволяє швидко мобілізувати ресурси у відповідь на геополітичні події.

Остання активність свідчить про те, що NoName057(16) залишається операційно активною та продовжує націлюватися на країни, орієнтовані на НАТО, що вказує на збереження мотивації та доступу до ресурсів. Спостережувані патерни підтверджують, що група надає перевагу деструктивному впливу, а не довготривалому закріпленню, зосереджуючись на короткотривалих атаках із високим рівнем впливу, спрямованих на порушення роботи сервісів і створення інформаційного ефекту.

З аналітичної точки зору група становить постійну загрозу кібердестабілізації, а не є високотехнологічним актором проникнення. Її сила полягає не у технічній складності, а в координації, масштабованості та ідеологічній узгодженості.

Фінальні аналітичні висновки

- Група демонструє високий рівень стійкості, а її повна нейтралізація є складною через децентралізовану модель, засновану на волонтерській участі.
- Операційна активність має подієвий характер та мотивується геополітичними чинниками.
- Використання автоматизованих платформ, таких як DDoSia, забезпечує швидке масштабування атак.
- Telegram залишається основною інфраструктурою для координації та управління операціями.
- NoName057(16) слід оцінювати як постійну загрозу середнього–високого рівня для стабільності цифрової інфраструктури, особливо в регіонах, орієнтованих на НАТО.