ZEROFOX INTELLIGENCE

# Flash

## DDoS Attacks Target Spanish Government Websites

F-2026-02-17a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: DDoS, Critical Infrastructure, Hacktivism

February 17, 2026

### Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EST) on February 17, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# | Flash | DDoS Attacks Target Spanish Government Websites

## | Key Findings

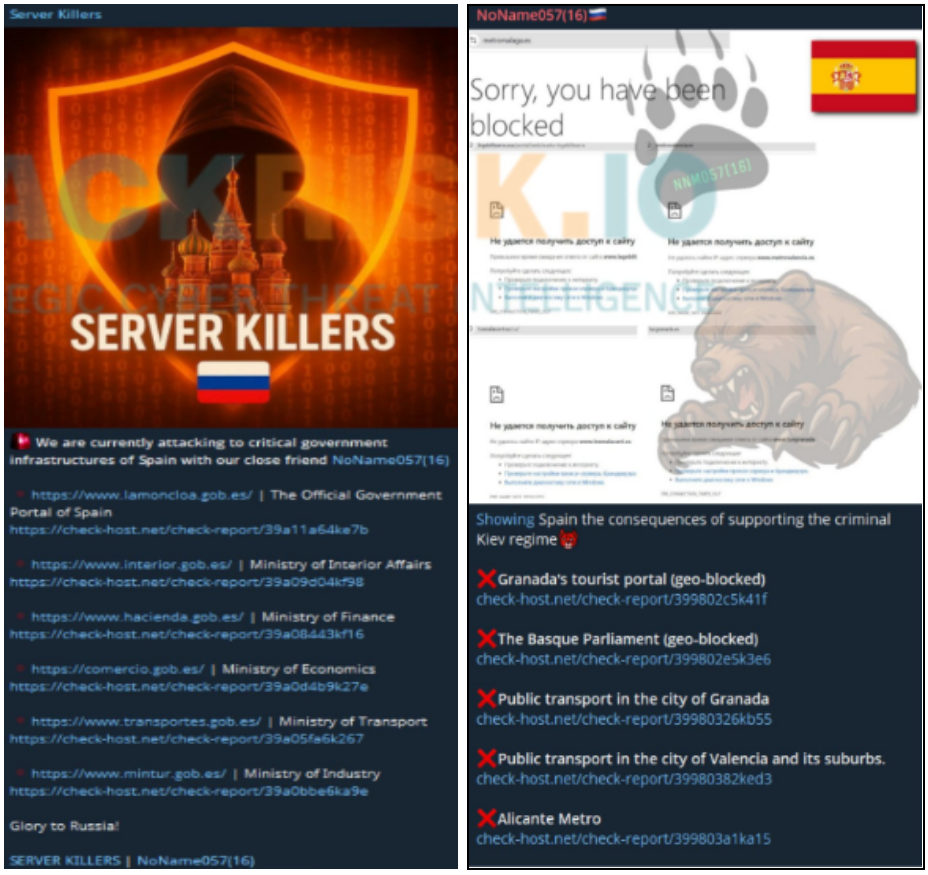
- Over the period of February 16-17, 2026, pro-Russia threat collectives NoName057(16) and Server Killers alleged they were responsible for coordinated distributed denial-of-service (DDoS) attacks against multiple Spanish government websites and provided check-host links to verify their claims. The alleged motivation behind their attacks was the Spanish government's perceived support of Ukraine and its participation in Operation Eastwood.
- On January 19, 2026, the National Cyber Security Centre (NCSC)—a part of the United Kingdom's Government Communications Headquarters (GCHQ)—issued an alert highlighting the persistent targeting of UK organizations by Russian state-aligned hacktivist groups aiming to disrupt networks.
- This recent coordinated string of DDoS attacks demonstrates the ongoing threat faced by NATO members and organizations perceived as pro-Ukraine posed by collectives who are considered pro-Russia.
- ZeroFox assesses it is very likely that pro-Russia and anti-West hacktivist collectives will continue to target Western institutions throughout 2026 and that

NoName057(16) will collaborate with other pro-Russia collectives to conduct DDoS attacks against perceived pro-Western targets in the coming months.

## Details

Over the period of February 16-17, 2026, pro-Russia threat collectives NoName057(16) and Server Killers alleged they were responsible for coordinated DDoS attacks against multiple Spanish government websites and provided check-host links to verify their claims.

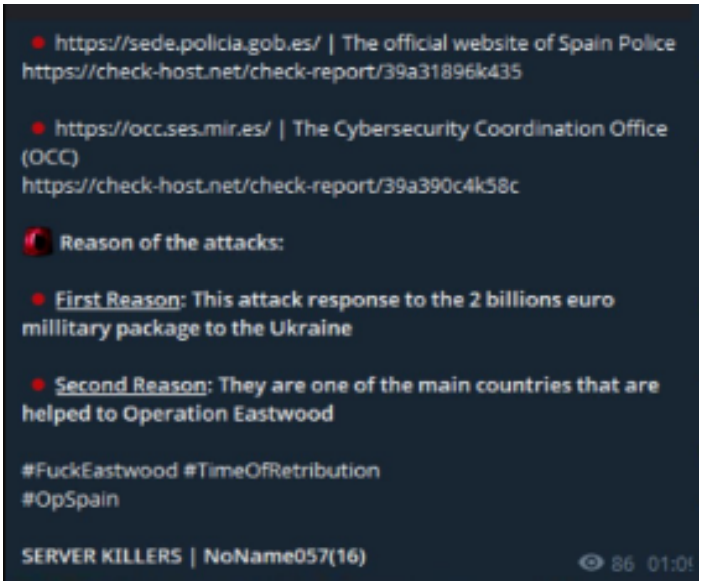
- Both threat collectives posted a list on their respective Telegram channels of all the Spanish government-associated websites that they allegedly conducted DDoS attacks against, which were primarily ministries and security forces.




**Server Killers' (left) and NoName057(16)'s (right) Telegram posts**
*Source: ZeroFox Intelligence*

The alleged motivation behind their attacks was the Spanish government's perceived support of Ukraine and its participation in Operation Eastwood.

- Operation Eastwood is a joint international operation coordinated by Europol and Eurojust that targeted NoName057(16)'s network from July 14-17, 2025.[1]
- NoName057(16) is a pro-Russia threat collective that has claimed responsibility for multiple attacks against the United States, Ukraine, and other European entities.
- Server Killers is a pro-Russia threat collective that has claimed responsibility for multiple attacks against the United Kingdom, Poland, and Denmark.
- In early January 2026, NoName057(16) and Server Killers claimed responsibility for multiple DDoS against UK government entities for their perceived support of Ukraine.




**Telegram post by Server Killers stating motivations**
*Source: ZeroFox Intelligence*

[1] hXXps://www.europol.europa[.]eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

On January 19, 2026, the NCSC issued an alert highlighting the persistent targeting of UK organizations by Russian state-aligned hacktivist groups aiming to disrupt networks.[2] The alert urges UK organizations—particularly local authorities and operators of critical national infrastructure (CNI)—to strengthen their resilience against denial-of-service (DoS) attacks.

- DoS and DDoS attacks—the most commonly used by Russian hacktivist collectives to cause disruption—typically require relatively low technical skill to conduct. However, they often cause severe financial and operational losses.
- The alert notes that Russian-aligned hacktivist collectives are largely targeting victims whom they perceive support Ukraine and are operating independently of direct state control.
- On January 12, 2026, ZeroFox observed that NoName057(16) and DarkStorm Team claimed on their respective official Telegram channels to have conducted DDoS attacks targeting multiple organizations based in Poland.

This recent coordinated string of DDoS attacks demonstrates the ongoing threat faced by NATO members and organizations perceived as pro-Ukraine posed by collectives who are considered pro-Russia. As tensions between Russia and the West remain, it is very likely that pro-Russia and anti-West hacktivist collectives will continue to target Western institutions throughout 2026. It is also very likely that NoName057(16) will collaborate with other pro-Russia collectives to conduct DDoS attacks against perceived pro-Western targets in the coming months.

[2] hXXps://www.ncsc[.]gov[.]uk/news/ncsc-issues-warning-over-hacktivist-groups-disrupting-uk-organisations-online-services

## Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

# Appendix A: Traffic Light Protocol for Information Dissemination

| | Red | Amber |
|---|---|---|
| WHEN SHOULD IT BE USED? | **Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | **Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved. |
| HOW MAY IT BE SHARED? | **Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed. | **Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only. |

| | Green | Clear |
|---|---|---|
| WHEN SHOULD IT BE USED? | **Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector. | **Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release. |
| HOW MAY IT BE SHARED? | **Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels. | **Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls. |

## Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|---|---|---|---|---|---|---|
| 1-5% | 5-20% | 20-45% | 45-55% | 55-80% | 80-95% | 95-99% |