



| Flash |

Hacktivists Claim Responsibility for Recent Power Outages

F-2025-05-01a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Threat Actor, Dark Web, DDoS

May 1, 2025

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 8:30 AM (EDT) on May 1, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Hacktivists Claim Responsibility for Recent Power Outages

| Key Findings

- On April 28, 2025, hacktivist collective “Dark Storm” posted on the social media platform X (formerly Twitter) claiming that—in conjunction with fellow hacktivist group “NoName057”—it was responsible for a recent power outage that affected Spain, Portugal, and parts of Southern France.
- Several subsequent posts have been observed within both Dark Storm’s Telegram channel and X account referencing the outages and claiming additional attacks targeting the infrastructure of European nations.
- As of this writing, the Spanish government is continuing to investigate the cause of these outages and has publicly denied they are the result of a cyberattack.
- While the exact cause of the power outage is currently unclear, it is unlikely that it was caused by a Dark Storm-led distributed denial-of-service (DDoS) attack, as the group very likely lacks the capabilities to conduct such an attack.

Details

On April 28, 2025, hacktivist collective Dark Storm posted on X claiming that, in conjunction with fellow hacktivist group NoName057, it was responsible for a recent power outage that affected Spain, Portugal, and parts of Southern France. The X post stated, “Today, we and the noname057 team succeeded in cutting off the electricity in some NATO countries.”¹

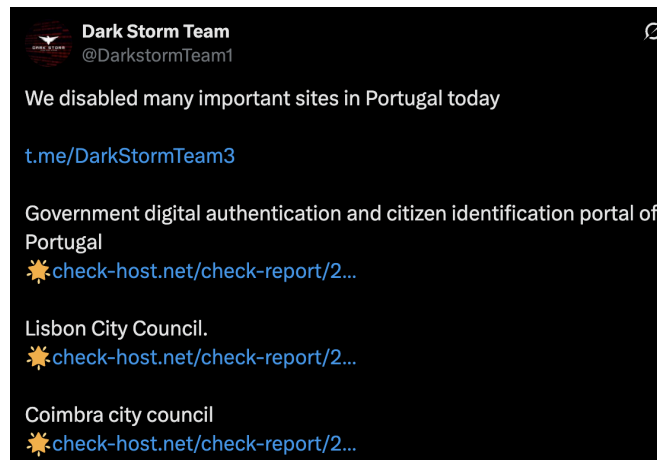


Dark Storm X post claiming responsibility for the power outages

Source: X

Several subsequent posts have been observed within both Dark Storm’s Telegram channel and X account referencing the outages and claiming additional attacks targeting the infrastructure of European nations. As of the writing of this report, NoName057 has not claimed any involvement through its own channels.

¹ [hXXps://x\[.\]com/DarkstormTeam1/status/1916830963855732761](https://x.com/DarkstormTeam1/status/1916830963855732761)



Dark Storm X post alleging attacks against Portuguese government entities

Source: [hXXps://x\[.\]com/DarkstormTeam1/status/1917304173646819385](https://x.com/DarkstormTeam1/status/1917304173646819385)

Dark Storm is a hacktivist collective primarily known for conducting politically and socially motivated DDoS attacks. The group was first observed in approximately mid-2023 and has historically been vocally pro-Palestine and anti-Israel. The majority of the collective's attacks have targeted Israel-based entities, particularly military targets and critical national infrastructure (CNI.)

- On March 10, 2025, Dark Storm claimed responsibility for the DDoS attack that resulted in X being taken offline with multiple service outages that affected millions of the platform's users.
- Dark Storm has also been implicated in attacks against various government and CNI entities, such as Finland's Central Bank, the Hungarian Defense Ministry, airports, and the North Atlantic Treaty Organization (NATO).²³
- In a March 2025 X post, Dark Storm threatened to increasingly target NATO-based entities.⁴

NoName057 is a pro-Russia hacktivist collective that primarily operates on Telegram, most often targeting perceived political opponents of Russia. Less is known about this

² [hXXps://thecyberexpress\[.\]com/dark-storm-team-announces-cyberattack/](https://thecyberexpress[.]com/dark-storm-team-announces-cyberattack/)

³ [hXXps://cybernews\[.\]com/news/breachforums-dark-storm-ddos-cyberattack-fbi-hackers/](https://cybernews[.]com/news/breachforums-dark-storm-ddos-cyberattack-fbi-hackers/)

⁴ [hXXps://x\[.\]com/DarkstormTeam1/status/1906919037000388964](https://x[.]com/DarkstormTeam1/status/1906919037000388964)

collective, due in part to its limited social media presence in comparison to many other hacktivist collectives.

- NoName057 has previously been observed conducting disruptive cyberattacks against targets based in Ukraine, the Baltic States, and other European countries.

On April 28, 2025, the Spanish government reported significant power outages across the country, with Portugal and parts of Southern France also affected. Approximately 55 million people were reportedly affected in these regions, most of which were without power for at least 20 hours. Mobile networks, internet access, travel infrastructure, and electronic payment devices were also purportedly affected, resulting in damage to critical infrastructure and confusion among the populace.⁵

As of this writing, the Spanish government is continuing to investigate the cause of these outages and has publicly denied they are the result of a cyberattack, despite Dark Storm's claims.⁶ Other avenues of likely causes are being pursued, such as an "atmospheric event" or renewable energy failures.⁷

- ZeroFox observed several responses from threat actors such as "CyberKnow", that expressed significant doubt about the prospect of Dark Storm and NoName057 being responsible for the power outage.

While the exact cause of the power outage is currently unclear, it is unlikely that it was caused by a Dark Storm-led DDoS attack, as the collective very likely lacks the capabilities to conduct such an attack.

ZeroFox has observed, on numerous occasions, statements from Dark Storm that allude to likely false attack attribution, as well as significantly exaggerated claims. This behavior is typical of Telegram-based hacktivist collectives, many of which seek notoriety in the pursuit of politically driven agendas. Furthermore, subsequent Dark Storm posts

⁵

[hXXps://www.theguardian\[.\]com/environment/2025/apr/29/what-caused-the-blackout-in-spain-and-portugal-and-did-renewable-energy-play-a-part](https://www.theguardian.com/environment/2025/apr/29/what-caused-the-blackout-in-spain-and-portugal-and-did-renewable-energy-play-a-part)

⁶

[hXXps://www.reuters\[.\]com/world/europe/spanish-grid-operators-first-assessment-rules-out-cyberattack-behind-blackout-2025-04-29/](https://www.reuters.com/world/europe/spanish-grid-operators-first-assessment-rules-out-cyberattack-behind-blackout-2025-04-29/)

⁷ [hXXps://www.bbc\[.\]com/news/articles/c209yr13258o](https://www.bbc.com/news/articles/c209yr13258o)

advertised a discount on its “DDoS services”—seemingly in an attempt to profit from any publicity surrounding the incident.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- 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).
- Utilize ZeroFox Intelligence and our proprietary platform to understand potential exposure in stealer logs.

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%