



| Flash |

Cyberattack Suspected in Worldwide X Outage

F-2025-03-11a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: DDoS, Hacktivist, Threat Groups

March 11, 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 4:00 AM (EDT) on March 11, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cyberattack Suspected in Worldwide X Outage

| Key Findings

- On March 10, 2025, social media platform X (formerly Twitter) experienced multiple service outages affecting a reported 1.6 million users worldwide and lasting several hours. As of the writing of this report, X services appear to be functional.
- Several hours later, the “Dark Storm” threat collective posted on its Telegram channel, claiming to have conducted a distributed-denial-of-service (DDoS) attack which resulted in X being “taken offline.”
- Ideologically motivated hackers, particularly pro-Russia hacktivist collectives, almost certainly view Elon Musk—and his high-profile government appointment and assumed political allegiances—as an acceptable and in-bounds target for disruptive cyberattacks.
- There is a likely chance that Dark Storm is responsible for a DDoS attack targeting X infrastructure as claimed. Although the collective offered no evidence to support its involvement, there is a robust correlation between the chosen target, Dark Storm’s publicly stated allegiances and motivations, and the historic tactics, techniques, and procedures (TTPs) of other pro-Russia, anti-Western hacktivist collectives.

Details

On March 10, 2025, social media platform X experienced multiple service outages affecting a reported 1.6 million users worldwide.¹² Elon Musk, the organization's Chairman and Chief Technology Officer (CTO), posted to the platform claiming that services had been and continue to be disrupted by a "massive" cyberattack, adding that the activity was conducted with "a lot" of resources by either "a large group and/or a country."³ As of the writing of this report, X services appear to be functional.

Several hours later, the Dark Storm threat collective posted in its Telegram channel, claiming to have conducted a DDoS attack that resulted in "Twitter" (X) being "taken offline."

- Dark Storm is a hacktivist threat collective first observed in mid-2023. The group is vocal about its support for Palestine and its contempt for Israel and its allies—both national governments and private organizations. The collective is very likely primarily politically and ideologically motivated.
- Dark Storm primarily operates in the messaging app Telegram, where intermittent posts claim responsibility for attacks, make threats, and also offer DDoS-for-hire services, indicating some extent of financial motivation.
- During 2023 and 2024, Dark Storm claimed responsibility for numerous disruptive attacks against Western targets, including airports and other critical national infrastructure.⁴ The collective has also made threats against the North Atlantic Treaty Organization (NATO).⁵
- Like other hacktivist collectives, Dark Storm has previously been observed falsely claiming responsibility for disruptive DDoS attacks. This behavior is almost certainly intended to gain notoriety (both within public discourse and amongst peers), market malicious services, and draw attention to Dark Storm's political and ideological affiliations.

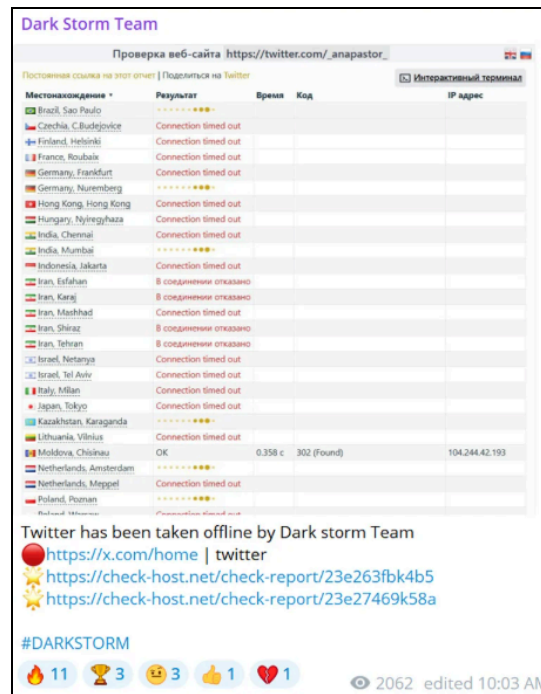
¹ <https://www.bbc.com/news/articles/c62x5k44rl0o>

² <https://downdetector.com/status/twitter/>

³ https://x.com/elonmusk?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

⁴ <https://www.techmonitor.ai/technology/cybersecurity/opfrance-cyberattack-charles-de-gaulle-airport?cf-view>

⁵ <https://thecyberexpress.com/dark-storm-team-announces-cyberattack/>

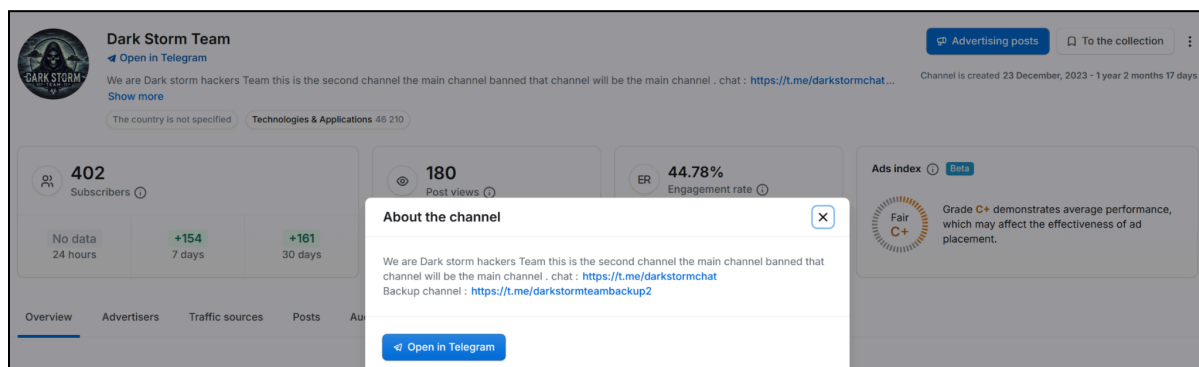


Dark Storm Telegram post claiming responsibility for X outage

Source: Telegram

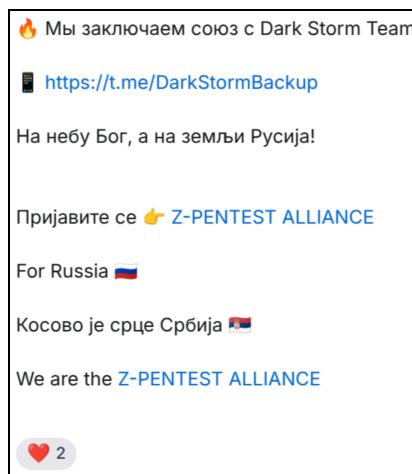
As of the writing of this report, several channels seemingly associated with Dark Storm have been removed from the Telegram platform. It is unclear if they were deleted by the collective or removed by platform moderators, though other channels associated with Dark Storm have been removed in the past.

- ZeroFox has previously observed other primarily pro-Russian hacktivist collectives proclaiming allegiance to and cooperation with Dark Storm.



Dark Storm Telegram post alluding to removed channels

Source: Telegram



“z-pentest-beograd” Telegram post claiming allegiance to Dark Storm

Source: Telegram

Elon Musk is currently serving as a senior advisor to U.S. President Donald Trump, as well as undertaking a leadership role within the Department of Government Efficiency (DOGE). Due to his assumed allegiances, politically and ideologically motivated pro-Russia hacktivist collectives almost certainly deem Musk and his associated government departments and private organizations as high-value targets for disruptive cyberattacks.

- On March 10, 2025, pro-Russia hacktivist collective “keymous+” posted in its Telegram channel claiming responsibility for unspecified cyberattacks against Tesla, an automotive organization owned by Musk. No further detail was given, but Musk appeared to confirm the incident. Any attack that occurred is likely to have been DDoS targeting of digital infrastructure.



X post alluding to cyberattacks targeting Tesla stores, shared by Elon Musk

Source: ZeroFox Intelligence



keymous+ Telegram post claiming responsibility for Tesla cyberattack

Source: Telegram

Shortly after the X outage, Musk alleged that internet protocol (IP) addresses “originating in the Ukraine area” were involved in the attack, though no further detail was offered.⁶ The full extent of any basis for these claims is unclear, though Musk and other entities within the U.S. government have recently been overtly critical of both NATO and Ukrainian state decision-making in relation to the ongoing Russia-Ukraine war.⁷⁸ Threat collective Dark Storm responded to this statement in a Telegram post, denying any association with Ukraine.

Dark Storm Team

According to what Elon Musk said about the cyber attack on the X platform, its source is Ukraine. It is an accusation without any evidence, and we have no relationship with Ukraine.

#DARKSTORM



207 edited 5:08 AM

Dark Storm Telegram post denying association with Ukraine

Source: Telegram

⁶ [hXXps://news.sky\[.\]com/story/elon-musk-says-x-hit-by-massive-cyber-attack-as-users-unable-to-log-in-13325939](https://news.sky.com/story/elon-musk-says-x-hit-by-massive-cyber-attack-as-users-unable-to-log-in-13325939)

⁷ [hXXps://www.bbc\[.\]com/news/articles/cy87vg38dnpo](https://www.bbc[.]com/news/articles/cy87vg38dnpo)

⁸ [hXXps://x\[.\]com/elonmusk?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor](https://x[.]com/elonmusk?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor)

There is a likely chance that Dark Storm is responsible for a DDoS attack targeting X infrastructure as claimed. While the collective offered no evidence to support its involvement, there is a robust correlation between the chosen target, Dark Storm's publicly stated allegiances and motivations, and the historic TTPs of other pro-Russia, anti-Western hacktivist collectives. If Dark Storm was indeed responsible, it is almost certain that the collective's intent was to undermine Elon Musk—and the West by extension—as well as gain notoriety through publicity.

ZeroFox can neither confirm nor deny the public allegation regarding the use of Ukraine-based IP addresses involved in the suspected X cyberattack. Additionally, ZeroFox notes that their presence does not necessarily imply Ukraine state involvement or that those responsible were physically located in Ukraine. Threat actors (including nation-state sponsored actors) regularly use spoofing, virtual private networks (VPNs), and previously compromised servers to falsify and obfuscate associated IP addresses.

Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of ransomware and digital extortion (R&DE) threats, their associated TTPs, and Indicators of Compromise (IOCs).
- 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.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.

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%