Graphika

ATLAS

GRAPHIKA HIGHLIGHTS REPORT

Global Hacktivist Threats

Selected Insights From Graphika's ATLAS Intelligence Reporting on Hacktivist Groups and Adjacent Communities

03.2025

ATLAS Highlights Report | Global Hacktivist Threats

Overview

This report contains selected insights from Graphika's ATLAS intelligence reporting on hacktivist actors and adjacent communities from February and March 2025. Graphika subscribers can access a full set of insights, as well as accompanying data and signals. Please visit the Graphika website for more information. Below is a summary of our key findings.

- Dark Storm Team, which claimed responsibility for a global X outage allegedly caused by cyberattacks on March 10, is a self-described pro-Palestine and anti-NATO hacktivist group that first emerged in 2023. The group regularly claims to conduct distributed denial of service (DDoS) attacks on targets that align with its declared political agenda, such as the websites of hospitals and transportation infrastructure in Israel and allied countries. The group has also cooperated with pro-Russia hacktivist groups in attack campaigns against Western countries.

- Illustrating a key feature of the current hacktivist ecosystem, Dark Storm is very likely motivated by financial gain as well as politics. The group often uses claims of cyberattacks on high-profile targets to advertise its DDoS-for-hire services and attempt to monetize mainstream social media attention. After Dark Storm's unverified claims of responsibility for the X outage, the group launched its DARKSTORM Solana cryptocurrency coin.

- We've previously observed Dark Storm overstating the impact and significance of its claimed attacks. In this case, other hacktivist groups highlighted that a screenshot of website monitoring tool Check-Host – which Dark Storm posted as evidence of its claimed attack on X – showed targeting of a single X account, not the platform itself. In February, we also observed Dark Storm mischaracterizing targets in what the group called a series of disruptive cyberattacks on international airports and the U.S. healthcare system.

- Dark Storm and other hacktivist groups will almost certainly continue attacking high-profile commercial and government targets to gain online and mainstream media attention for their political agendas. Some will almost certainly additionally seek to exploit public attention for financial gain, such as by advertising commercial hacking services, selling cryptocurrencies and other online products, or soliciting donations.

Insights

Dark Storm Team Claims Attacks Against X, Promoting Hacking Services and New Cryptocurrency Coin

Published on March 11, 2025

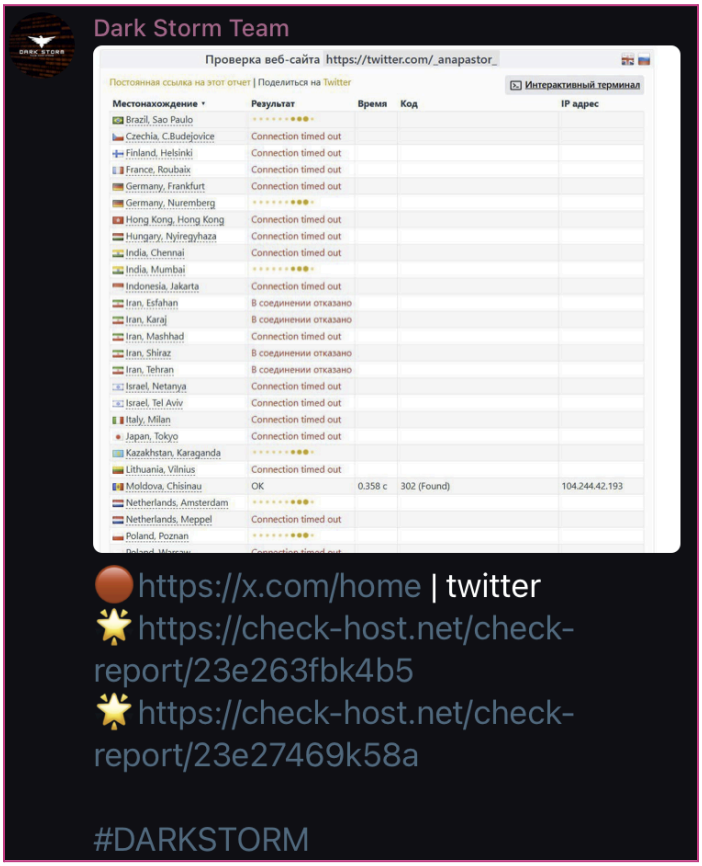
Key Finding: Pro-Palestine hacktivist group Dark Storm Team has gained mainstream media attention after claiming responsibility for a global X outage allegedly caused by cyberattacks on March 10. Shortly after making the claims, Dark Storm launched a cryptocurrency coin and promoted its commercial website disruption and database compromise services on Telegram.

Why It Matters: Although we were unable to verify Dark Storm's involvement in the X outage, we assess the group very likely claimed involvement to increase its public profile through mainstream media attention, which it then attempted to monetize via the launch of a cryptocurrency coin and advertising its commercial services. The activity highlights how some hacktivist groups partially operate as financially-motivated actors, despite adopting political online personas.

Online Activity:

- Dark Storm is a pro-Palestine and anti-NATO hacktivist group that performs distributed denial of service (DDoS) attacks. The group emerged in 2023, offers a DDoS-for-hire service, and has previously cooperated with pro-Russia hacktivist actors.
- On March 10 at 10:03 a.m. EDT, Dark Storm claimed on Telegram to have "taken down" X via DDoS. Shortly thereafter, the group launched the DARKSTORM Solana cryptocurrency coin and advertised their DDoS-for-hire services on Telegram.
- Political commentator Ed Krassenstein said on X the leader of Dark Storm had told him the attack was "a demonstration of our strength" with no political motives. Krassenstein posted screenshots of an apparent private conversation with Dark Storm, in which the group says it may attack Musk-owned carmaker Tesla for financial purposes.
- Pro-Palestine social media users shared Dark Storm's claims of responsibility as evidence that the attacks were a protest against the U.S. arrest of Palestinian activist Mahmoud Khalil. Some U.S. users claimed the attacks were a demonstration against X CEO Elon Musk and U.S. President Donald Trump over events in Ukraine.
- Pro-Palestine hacktivist groups such as Moroccan Ghosts expressed doubt over Dark Storm's involvement in the X outage, highlighting that an X availability report from website monitoring tool Check-Host showed Dark Storm attacking one X account, not the platform itself.

The pro-Palestine, anti-NATO hacktivist group Dark Storm Team claimed responsibility for alleged cyberattacks disabling X on March 10, but denied any political motive.



Dark Storm's claim of the first attack on March 10, with a Check-Host screenshot showing that the group had targeted the X account of a Spanish journalist, rather than X's main page. This screenshot led other hacktivist groups to claim that Dark Storm was not behind the attacks.

Pro-Palestine Hacktivist Groups Target Bosnia's Government, Banks Over Alleged Ties to Israel

Published on Feb. 27, 2025

Key Finding: Pro-Palestine hacktivist groups attacked a series of targets in Bosnia while posting years-old images of meetings between government officials from Israel and Bosnia. The groups launched the campaign with unclear motivations and struck Bosnia's government ministries, banks, and a media website.

Why It Matters: The activity shows how hacktivist groups can use decontextualized media to insert a political narrative into their activities. In this case, the actors shared publicly available photos of meetings between Bosnian and Israeli officials from 2017 and 2018 to suggest the attacks were tied to events in the Middle East.

Online Activity:

- On Feb. 23, the pro-Palestine Moroccan group Mr Hamza announced in a Telegram post that Bosnia would be targeted by a "massive cyber attack" alongside images showing meetings between Bosnian and Israeli officials from 2017 and 2018. The group did not provide a rationale for the attack outside of the posted images.

- The group later claimed an "unstoppable" series of distributed denial of service (DDoS) attacks on the presidential website, the Council of Ministers, and the ministries of defense, foreign affairs, and security. Other targets included the major news website Klix and the e-services portal for Bosnian Bank International and the Central Bank.

- Shortly after, the Bangladeshi group Mysterious Team – who had announced its alliance with Mr Hamza on Feb. 22 – joined the campaign with DDoS attacks on the Bosnian national railways websites. The pro-Palestine Dark Storm Team also claimed to have sabotaged the website of the Bosnian government's secretariat.

- The activity gained little traction on social media, only receiving attention from a small number of users on X. The last attack of the campaign was announced on Feb. 24.

On Feb. 23, the pro-Palestine group Mr Hamza announced in a Telegram post that Bosnia would be targeted by a "massive cyber attack."

Mr Hamza shared publicly available photos of meetings between Bosnian and Israeli officials from 2017 and 2018 to suggest the attacks were tied to events in the Middle East.

Pro-Palestine Hacktivist Group Dark Storm Team Overstates Attacks on Airports, U.S. Healthcare System

Published on Feb. 21, 2025

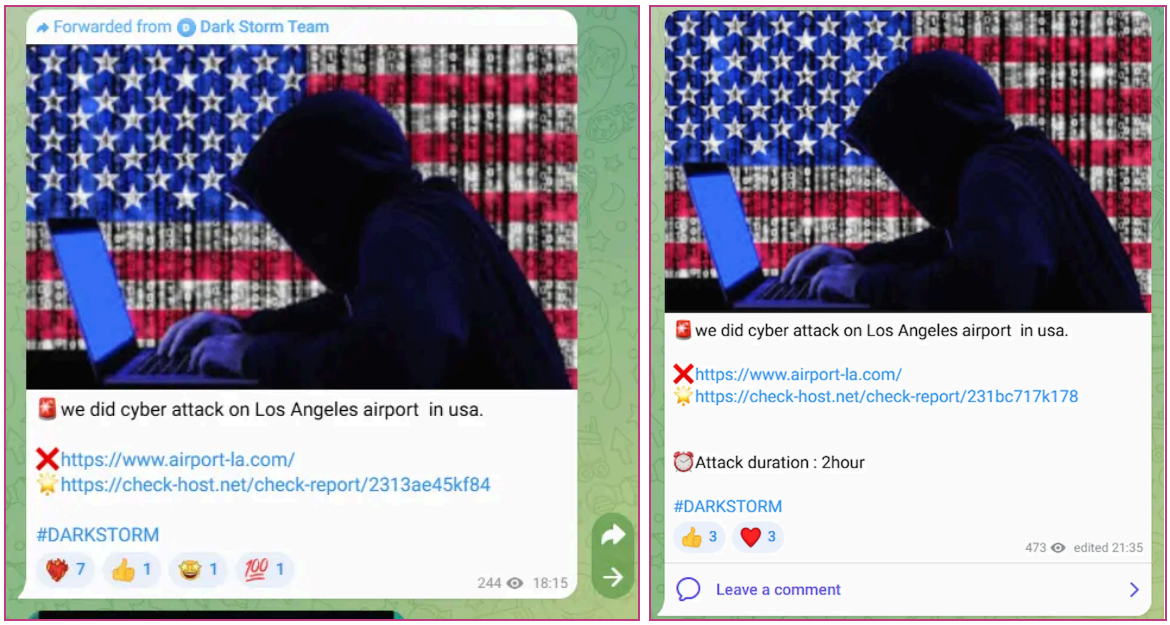
Key Finding: The pro-Palestine hacktivist group Dark Storm Team launched what it said was a series of disruptive cyberattacks on U.S. and international airports, as well as the U.S. healthcare system, while providing at times inaccurate information to support its claims.

Why It Matters: The activity shows how Dark Storm and other hacktivist groups can overstate the significance and impact of their attacks, sometimes posting inaccurate information about the identity or nature of the target. Dark Storm, for instance, framed its targeting of a U.S. university-run healthcare system as an attack on the "USA health system official website".

Online Activity:

- On Feb. 13, Dark Storm Team claimed on Telegram that it had conducted a cyberattack on a website for Los Angeles airport. It provided a Check-Host link indicating a disruption, though the extent of any impact was unclear.
- The same day, Dark Storm Team said Telegram had banned its main channel. The group quickly created a new channel, which Telegram took down the next day. The group then made another channel, stating, "They want us to give up, but that's impossible."
- Dark Storm Team intensified its campaign against U.S. targets, including posting again about its alleged attack against the LA airport website and sharing a new Check-Host link. It also claimed attacks on South Dakota's Grand Forks International Airport and one on a "USA health system official website" but listed a website for a University of South Alabama-run hospital system.
- The group expanded to international targets, claiming DDoS attacks against Paris Charles de Gaulle airport – but listing an unofficial airport website as the target – a Cameroon-based airline, and the German Ministry of Transport and Digitalization.

The logo for the pro-Palestine hacktivist group Dark Storm Team, as shared on its Telegram channel.



Dark Storm Team's Feb. 13 Telegram post from its now-banned channel, in which it claimed it attacked a website for Los Angeles International Airport (left). The hacktivist group posted a similar message on Feb. 15 on a new channel it created after Telegram banned its original one (right).

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as "suggest."

Almost No Chance	Very Unlikely	Unlikely	Real Chance	Likely	Very Likely	Almost Certain(ly)
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	Medium Confidence	High Confidence
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika *is the most trusted provider of actionable open-source intelligence to help organizations stay ahead of emerging online events and make decisions on how to navigate them. Led by prominent innovators and technologists in the field of online discourse analysis, Graphika supports global enterprises and public sector customers across trust & safety, cyber threat intelligence, and strategic communications spanning industries including intelligence, technology, media and entertainment, and global banking. Graphika continually integrates new and emerging technologies into our proprietary intelligence platform and analytic services, empowering our customers with high-precision intelligence and confidence to operate in a complex and continuously evolving information environment.*

For more information or to request a demo, visit our website.