



Graphika

ATLAS

GRAPHIKA REPORT

Keeping Up With The ~~Kardas~~ Hacktivists

Examining How International
Hacktivist Groups Pursue
Attention, Select Targets, and
Interact in an Evolving
Online Landscape

07.2025

Keeping Up With The ~~Kardas~~ Hacktivists

Examining How International Hacktivist Groups Pursue Attention, Select Targets, and Interact in an Evolving Online Landscape

Quick Find

- [Overview](#)
 - [Clout is the Currency](#)
 - [Monetization](#)
 - [Community Dynamics: Alliances & Feuds](#)
 - [Platform Moderation & Hacktivist Persistence](#)
 - [Appendix: Estimative Language Legend](#)
-

Overview

Through our [ATLAS intelligence reporting](#), Graphika has monitored close to 700 active and inactive hacktivist groups since 2022. The groups include state-sponsored hacktivist personas, pro-Russia and pro-Ukraine groups, and groups based in the Middle East, North Africa, and South and Southeast Asia.

In the first half of 2025, we observed hacktivist groups across the ideological spectrum claim attacks against or [threaten social media platforms](#), including LinkedIn, Pinterest, TikTok, Truth Social, and X, forums like [4chan](#), the music streaming platform Spotify, as well as banks, [airports](#), and [government websites](#) in the U.S. and dozens of other countries. Smaller companies and entities with older, more vulnerable cybersecurity systems are also common targets as hacktivists seek out relatively easy-to-exploit defenses.

As [Mandiant](#) and [other cybersecurity firms](#) have noted, before 2022, hacktivists were primarily ideologically motivated. Since then, however, the structure of the hacktivist landscape has shifted largely in response to two events: Russia's full-scale invasion of Ukraine in 2022, which continues to be a source of motivation for pro-Russia and pro-Ukraine groups, and Israel's response to the

Oct. 7, 2023, Hamas attacks, which resulted in an ongoing conflict that hacktivist groups routinely cite as justification for their actions. Other high-traction events, such as elections, regional tensions, and emerging conflicts, like the collapse of the [Assad regime](#) in Syria, the May 2025 [India-Pakistan crisis](#), or the recent [Israel-Iran conflict](#), also often trigger spikes of activity.

The hacktivist landscape has grown increasingly complex, with groups participating in a highly active online community that displays social dynamics observed in other, benign online communities. While driven by ideological and geopolitical motivations, the hacktivists we monitor are also heavily influenced by a pursuit of attention, building their brand as effective cyber threat actors, and monetizing their activity, often using the attention they have received as marketing opportunities. Hacktivism has also become more globalized, with groups with traditionally disparate ideological or geopolitical motivations joining forces to collaborate on attacks.

This report identifies and explains some of these dynamics to help organizations targeted by these groups better understand the online hacktivist landscape. Most notably:

- Due to their motivations, hacktivist groups regularly pick high-profile targets to attack or disrupt, such as banks, social media platforms, and government agencies. They also seek multiple means of promoting themselves, including using dedicated hashtags and logos, and celebrating mentions of their activities in the press.
- These groups engage in what we consider to be a form of perception hacking, often claiming without sufficient evidence that they have attacked high-profile targets or caused significant disruptions to bolster their name recognition and present their targets as easily compromised or lacking security.
- The hacktivists we monitor display an acute interest in developing new, more disruptive capabilities, signaling that the threat this community poses will almost certainly grow and that their attacks will become [more complex and disruptive](#).
- Hacktivists attempt to monetize their online activities, using the publicity around their attacks to promote and sell external or self-made tools, services, and hacking courses.
- The hacktivist landscape includes more active and public members who set the tempo for attacks and hacking campaigns by naming specific targets and rallying others to their cause. Aligned groups often partner together to amplify claims or a campaign's impact. However, they also engage in inter-community feuds, targeting each other and using their fights to generate even more content and garner attention.
- While hacktivist groups are most active on Telegram, some maintain accounts on mainstream social media platforms like Facebook, Instagram, and X. Even so, these groups have had to contend with increases in platform moderation. Some regularly re-emerge with new usernames and handles, while others stop posting publicly for months at a time.

Clout is the Currency

Hactivist activity holds a unique position in the online threat landscape, falling between traditional cybersecurity threats and operations that seek to influence public views. Hacktivists claim to conduct cyberattacks against public and private sector targets but often overstate their impact. They hijack major cybersecurity incidents for their own gain and leverage several means to amplify their messaging and activities. Graphika views these tactics as a form of [perception hacking](#) that reflects an effort to present their attacks as more destructive than they are, depict a targeted country's cyberspace as compromised, and suggest that their victims – whether they be banks, government agencies, airports, or others – are weakly protected and will face further attacks due to their connection to the targeted country.

Ideological Motivations

The hactivist groups Graphika routinely tracks are primarily ideologically and geopolitically motivated. They pick targets based on their perceived connections to the hactivists' adversaries or to support the goals of the nation or sociocultural group they align with.

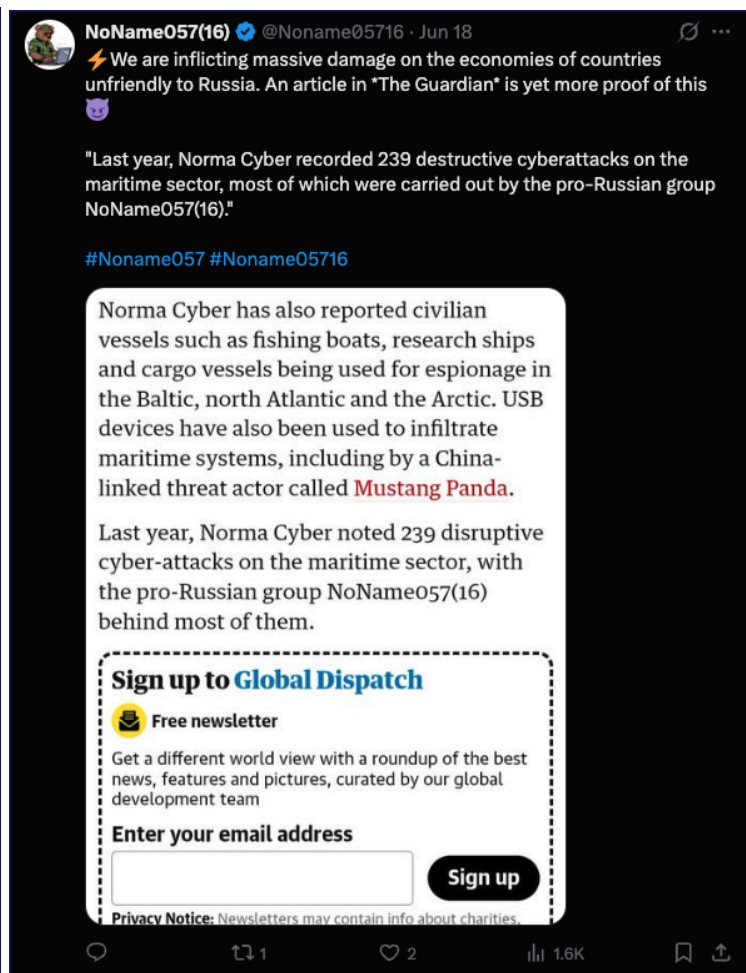
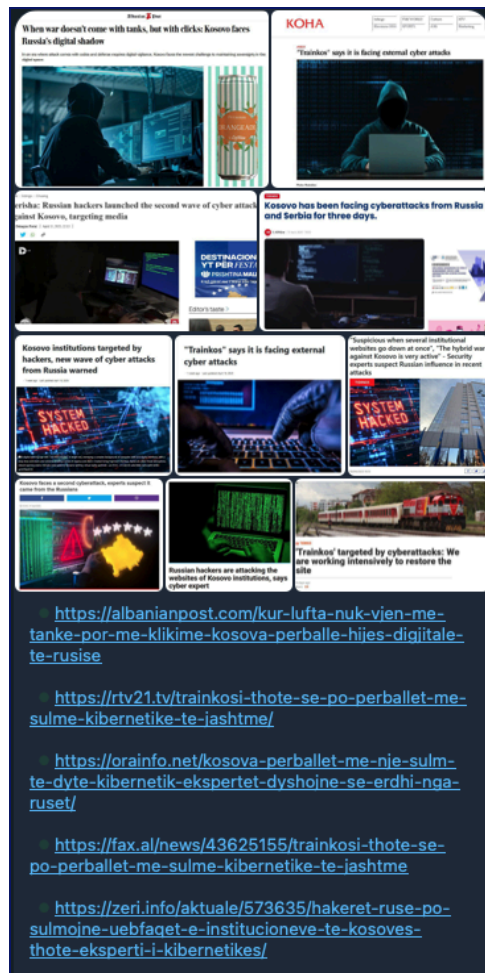
- Pro-Russia hactivist groups, such as NoName057(16) and its allies, regularly target public and private sector entities in Ukraine and NATO countries. For example, just this year, NoName057(16), the [recently re-emerged](#) Killnet, and others have claimed attacks against targets in [Belgium](#), [Finland](#), [France](#), [Germany](#), [Lithuania](#), [the Netherlands](#), and [Poland](#), among others, citing their support for Ukraine or alleged Russophobia.
- Muslim or pro-Palestine hactivist groups, such as members of the [Holy League collective](#), commonly go after targets in countries that they perceive as Zionist, allied with Israel, or Islamophobic.
- More regionally focused groups will target entities based in the country they oppose. For example, during the May 2025 India-Pakistan crisis, hactivist groups that supported Pakistan [conducted attacks](#) against Indian entities, while those supporting India attacked Pakistani targets.
- After Israel conducted military strikes against Iran in June 2025, the pro-Israel group [Predatory Sparrow](#), which has [suspected ties](#) to the Israeli government, [claimed](#) it "destroyed the data" of Bank Sepah in Iran. A Telegram channel claiming to be Cyber Av3ngers, a [hactivist group](#) that the U.S. government has said is [affiliated](#) with the Islamic Revolutionary Guard Corps, also [promoted](#) a list of allegedly hacked email addresses from an Israeli defense company that another group claimed it obtained. Similarly, the pro-Iran group Handala [promoted](#) a series of hack-and-leaks against Israeli defense and petroleum companies, among others.

Attention Seeking

The hacktivist groups we monitor also have a desire to be noticed. As a result, they often target or take credit for attacks on high-profile companies, government agencies, banks, hospitals, or other critical infrastructure assets, where even the threat of attack or fear of disruption may result in traditional and social media attention. For example, the pro-Palestine hacktivist group DieNet has repeatedly [claimed responsibility](#) for attacks on Spotify. In May 2025, during elections in [Poland](#) and [Romania](#), pro-Russia hacktivist groups targeted the websites of government agencies and political parties in both countries, which [international](#) and [local media](#) outlets [covered](#).

Hacktivism also attempt to hijack or co-opt attention around cybersecurity incidents or service outages that receive widespread media attention, such as when several groups [took responsibility](#) for an [outage](#) of OpenAI's ChatGPT in January 2025.

We've also observed activity from pro-Russia or Russian state-sponsored hacktivist groups that suggests they cooperate or coordinate with state-owned or -aligned media sources to produce coverage of their attacks. The popular Russian news Telegram channel Mash, which has [reported links](#) to Russian security services, announced the [re-emergence](#) of the pro-Russia group Killnet in May. Mash has [served](#) as a primary source of promotion for Killnet's attacks against Ukraine. In 2024, Russian state media outlets often [reported](#) within minutes [attacks against Ukraine](#) by the hacktivist group RaHDit, the leader of which the U.S. Department of the Treasury has [linked](#) to Russia's Federal Security Service (FSB).



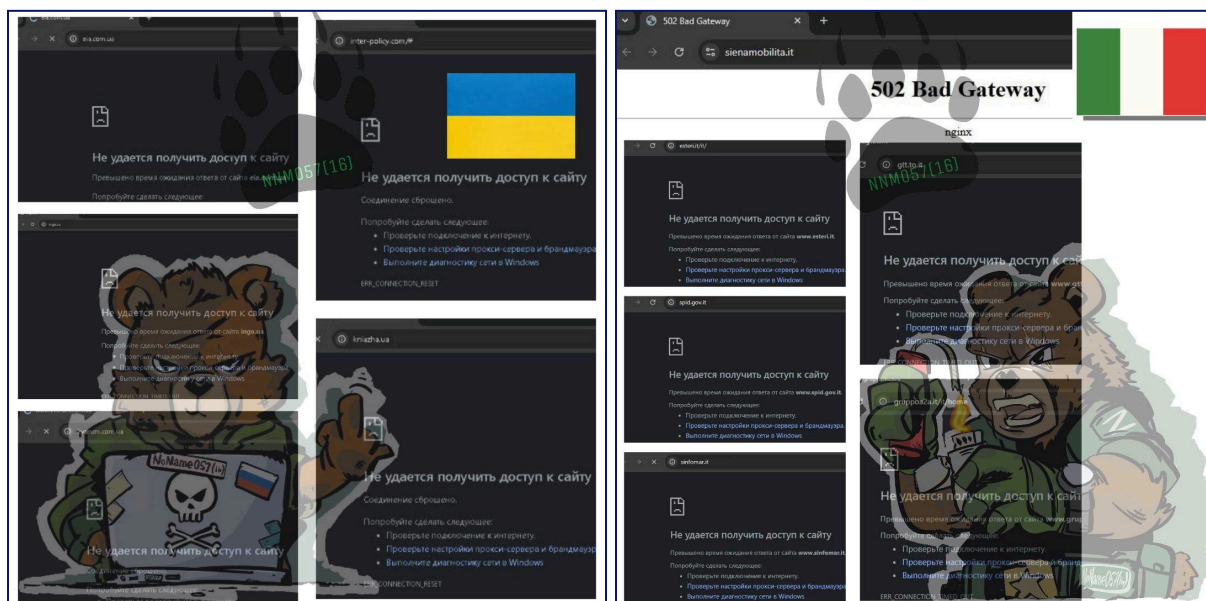
An April 19, 2025, Telegram post from the pro-Russia hacktivist group Server Killers sharing news coverage about cyberattacks against websites in Kosovo, which it claimed to have participated in (left). A June 18, 2025, X post from the pro-Russia group NoName057(16) claiming that an article from The Guardian is "proof" that it is "inflicting massive damage" on nations adversarial to Russia (right).

Branding

Most hacktivist groups we monitor attempt to cultivate specific brands by leveraging distinct logos and imagery (often likely AI-generated), posting styles, taglines, and hashtags. These brands are displayed prominently across their social media accounts, primarily on Telegram. Some groups, such as NoName057(16), post the same style of image with almost every post claiming an attack, making their social media activity instantly recognizable.



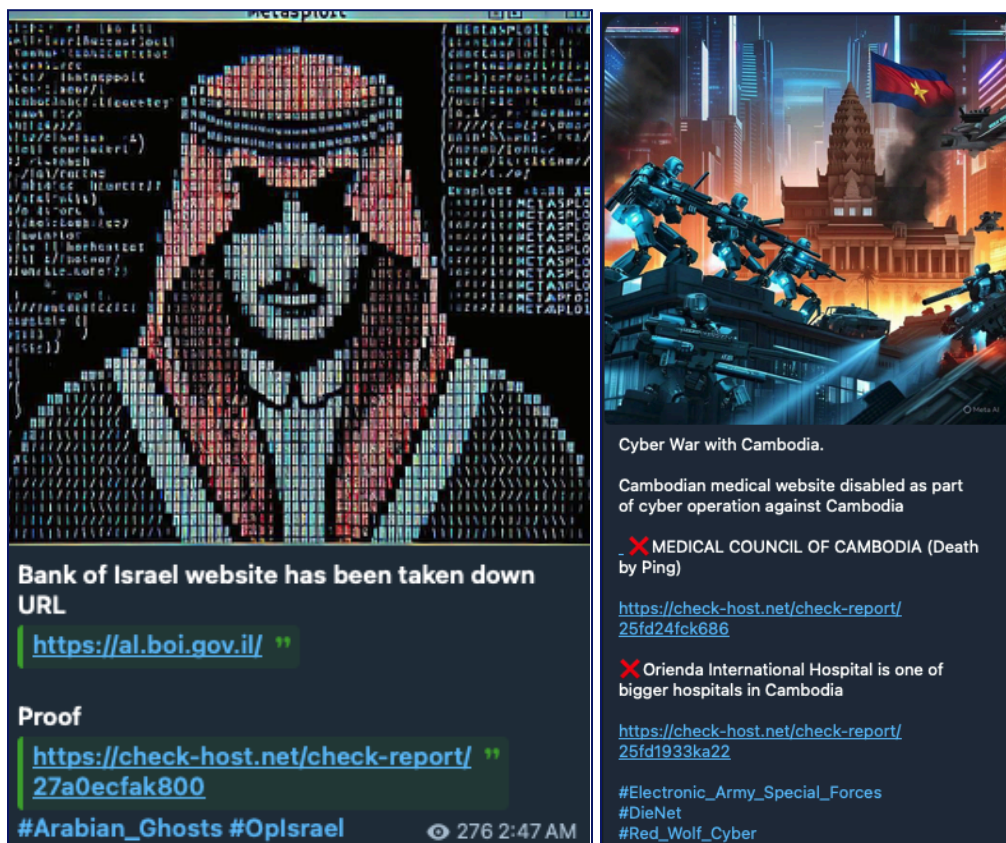
Examples of logos and profile images that various hacktivist groups have used in their social media profiles. From top left, the images are for the pro-Russia groups NoName057(16), Killnet, Server Killers, and Z-Pentest, and the pro-Palestine groups Keymous+ and Dark Storm Team.



Examples of images the pro-Russia hacktivist group NoName057(16) has posted with its Telegram messages announcing attacks against Ukrainian and Italian targets.

Overstating the Impact, Looking to Learn

Hactivist groups also very likely overstate the real effects of their attacks to attract social and traditional media attention. Groups often claim to disrupt major social media platforms and targets that are considered critical infrastructure – for example, websites for government agencies, transportation services, and bank login pages – and depict their attacks as disruptive and destructive, while they very likely only have a limited impact. They attempt to provide evidence, even if thin, that their attacks were successful, such as sharing screenshots or links to the connection status website check-host.net to show that they disrupted a specific website.



Examples of Telegram posts from the pro-Palestine hactivist group Arabian Ghosts (left) and the Vietnamese hactivist group Special Forces Electronic Army (right) that shared links to the connection status website check-host.net as alleged evidence that they had successfully disrupted a target's website.

We have also observed some groups claim they hacked and accessed sensitive databases, only to share publicly available or repackaged, previously leaked documents as alleged proof, as well as documents from completely different, low-security targets that are passed as government or confidential material.

Groups also make unverifiable or false claims about their attacks or attempt to co-opt attention around real disruptions to promote themselves. For example, the pro-Palestine Dark Storm Team claimed in March and April 2025 that it was responsible for disruptions of [X](#) and [4chan](#), respectively. Dark Storm Team launched its own cryptocurrency shortly after its claims about X.

In late May, DieNet used its claims that it took down Spotify's website as an opportunity to [promote](#) the [third version](#) of its distributed denial of service (DDoS) tool.

Even so, groups with varying technical capabilities have shown an interest in developing new skills, working with more prominent or skilled hacktivist groups, and recruiting members to bolster their capabilities. Graphika routinely witnesses hacktivist groups seeking to recruit users with cybersecurity skills, such as intrusion, pentesting, or malware development, to join their teams. Some also advertise their own services or tools, discussed further below.

Others have partnered with external providers of botnets, stress-testing services ("[stressers](#)"), or [command-and-control](#) (C2) tools to increase the intensity of their attacks in exchange for promoting the tool used. Some groups have explored new attack pathways, such as conducting DDoS attacks against website login pages, servers, or APIs rather than focusing on disrupting a target website's homepage. Based on this, we assess that the overall threat from the international hacktivist community will almost certainly grow as groups work to improve their skills, eventually leading to more complex and sophisticated attacks and operational techniques.

Monetization

In addition to promoting their ideologies, a significant share of the hacktivist groups we monitor also attempt to use their clout to make money. When we began monitoring this community, hacktivist groups, mainly pro-Russia ones, directly asked for donations and shared their cryptocurrency wallet or bank account numbers. Since then, however, monetization activities have diversified notably.

Now, we commonly see these groups attempt to monetize their activities by selling access to products, tools, or services, and access to data they allegedly obtained.

Products & Tools

Several hacktivist groups have launched specific products, tools, or other offerings that rely on their brands, including hacktivist-developed botnets to initiate DDoS attacks and C2 tools.

- In May 2025, the Moroccan hacktivist group Mr Hamza announced that it had developed its own DDoS tool, Abyssal DDoS. The group presented it as a tool with "advanced technology and attack techniques" and an "invincible system to hack any website."
- As mentioned above, the pro-Palestine hacktivist group DieNet has started using and promoting its own eponymous DDoS tool, claiming it is capable of launching attacks "so massive it is like a black hole swallowing everything." It has also started teasing its own ransomware, LockNet.


- The Italian pro-Palestine group AzzaSec, which also calls itself APT-ITA, launched its own C2 service, Azza-C2, in April 2025. The group also [claims](#) to operate ransomware with “military-grade encryption methods.”
- As mentioned above, Dark Storm Team launched a cryptocurrency coin, \$DARKSTORM, earlier in 2025.
- NoName057(16) has partnered with the Russian artist [DaZbastaDraw](#) to produce merchandise, such as [T-shirts](#), hoodies, stickers, and [patches](#). The artist has [claimed](#) that money raised from these sales will support Russian frontline soldiers.

Services & Subscriptions

Since 2024, hacktivist groups have increasingly launched or promoted services-for-hire, including ransomware-as-a-service (RaaS), DDoS-as-a-service, and hack-and-leak services.

- Dark Storm Team and the Yemeni group R70 have each advertised DDoS-as-a-service offerings, typically alongside claims that they’ve attacked high-profile targets, like Western social media platforms or airports.
- The Indian hacktivist group CyberVolk began promoting its own RaaS in 2024, claiming it features “a unique encryption algorithm.”
- The pro-Palestine group Cyber Islamic Resistance offers its followers a \$45/year “VIP subscription” for “web hacking” tutorials, exploits, and vulnerabilities. MadCap, another pro-Palestine group, previously promoted a “Hackers VIP Forum” for \$400/year.
- Other groups, such as the pro-Russia group UserSec, sell classes starting at \$100 that allegedly teach a range of skills, such as CCTV and server hacking, open-source investigations, and malware.
- Several Moroccan hacktivist groups have promoted Dragon RaaS, which SentinelOne has [described](#) as “a ransomware group that walks the line between hacktivism and cybercrime” that is linked to a pro-Russia cybercrime syndicate.

We’ve also increasingly observed hacktivist groups claiming that they are selling data they allegedly accessed on Telegram and various darknet forums. For example, the Khmer hacktivist group ANON-KH claimed in April 2025 that they would sell data they allegedly stole from the Vietnamese Vietcombank for \$8,000.



⚠ Товарищи, хочу объявить вам о том что допилил материалы по обучению. Теперь вы можете попасть на курс по

- Взлом RTSP (Камеры видеонаблюдения)
- Перехват доступа к FTP/SMTP-серверу.
- Взлом VNC серверов.
- Deface - материал обновлён.
- Выгрузка баз данных с целевых серверов.

!!! Работа с малварями/Трафф

!!! Осинт/Деанон

!!! Обучение работы с Unix системами

💰 Прайсы от 100\$. По подробной информации о каждом курсе - писать в личные сообщения [REDACTED]

==

Comrades, I want to announce to you that I have completed the training materials. Now you can get into the course on

- *Hacking of RTSP (CCTV Cameras)*
- *Interception of access to the FTP/SMTP server.*

Hacking VNC servers.

- *Deface - the material has been updated.*

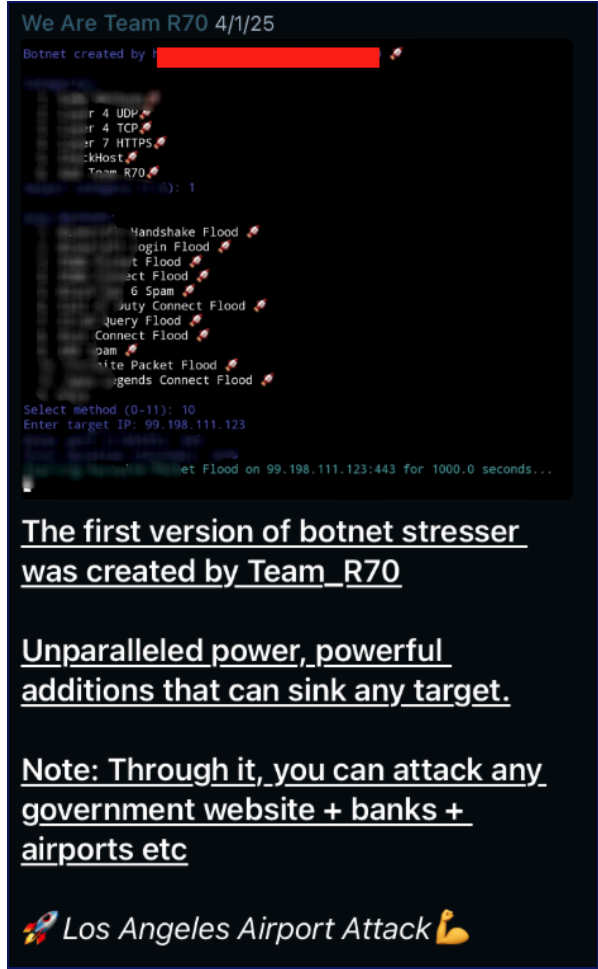
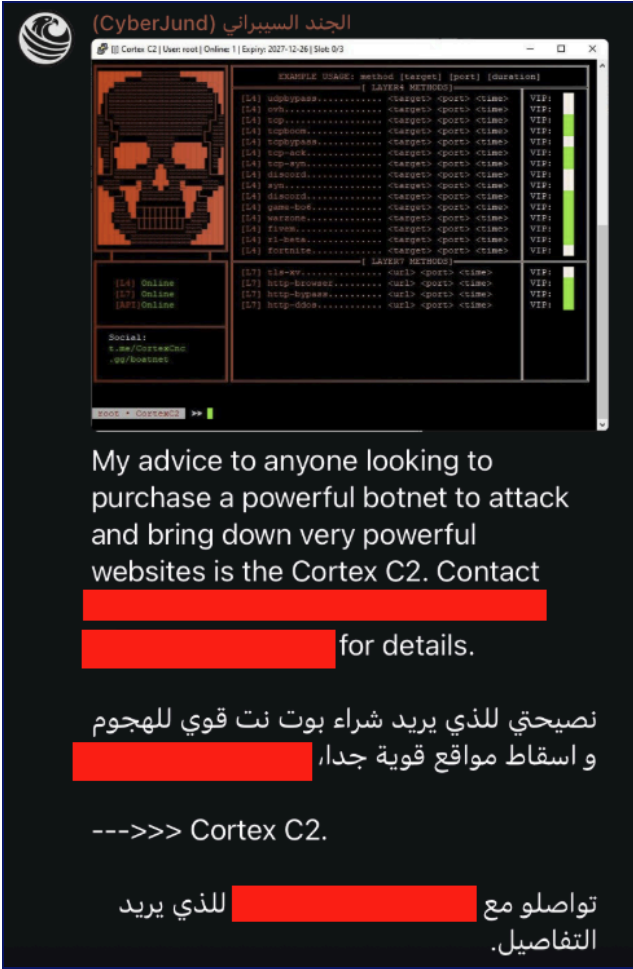
!!! *Malware/Traff*

- *Unloading databases from target servers.*

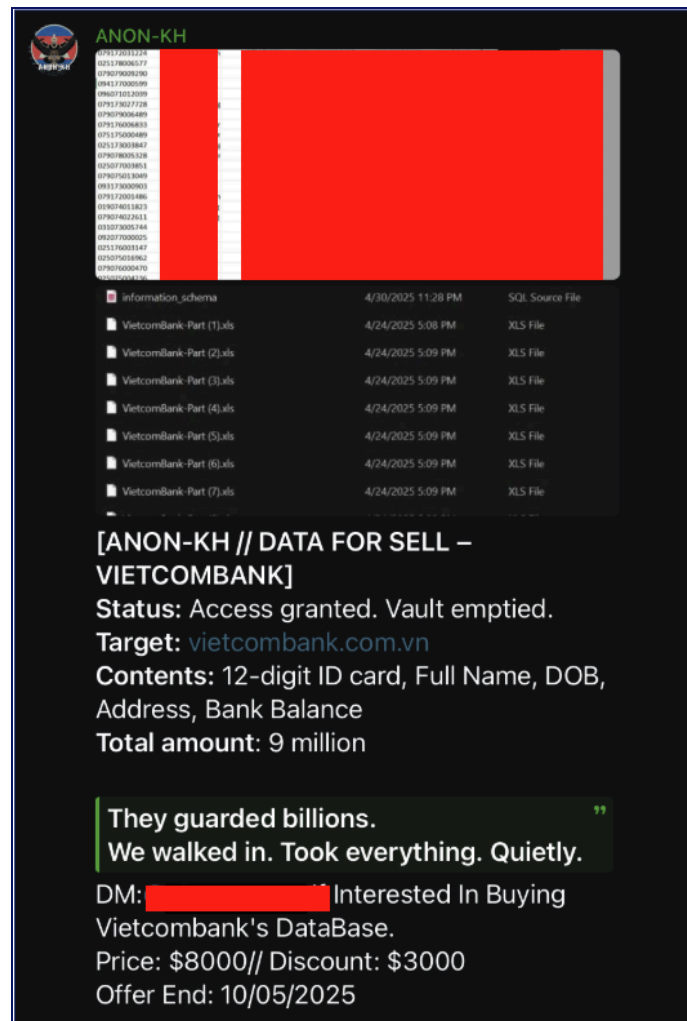
!!! *Osint/Deanon*

!!! *Work with Unix systems*

A Telegram post from the pro-Russia hacktivist group UserSec promoting its for-sale training materials. Redactions added by Graphika.



Telegram post from the pro-Palestine hacktivist group CyberJund promoting a botnet (left). Telegram post from the Yemeni hacktivist group Team R70 promoting its own DDoS-as-a-service stresser and claiming it was used against an airport in Los Angeles (right). Redactions added by Graphika.



Telegram post from the Cambodian hacktivist group ANON-KH claiming it was selling data from the Vietnamese bank Vietcombank for \$8,000. Redactions added by Graphika.

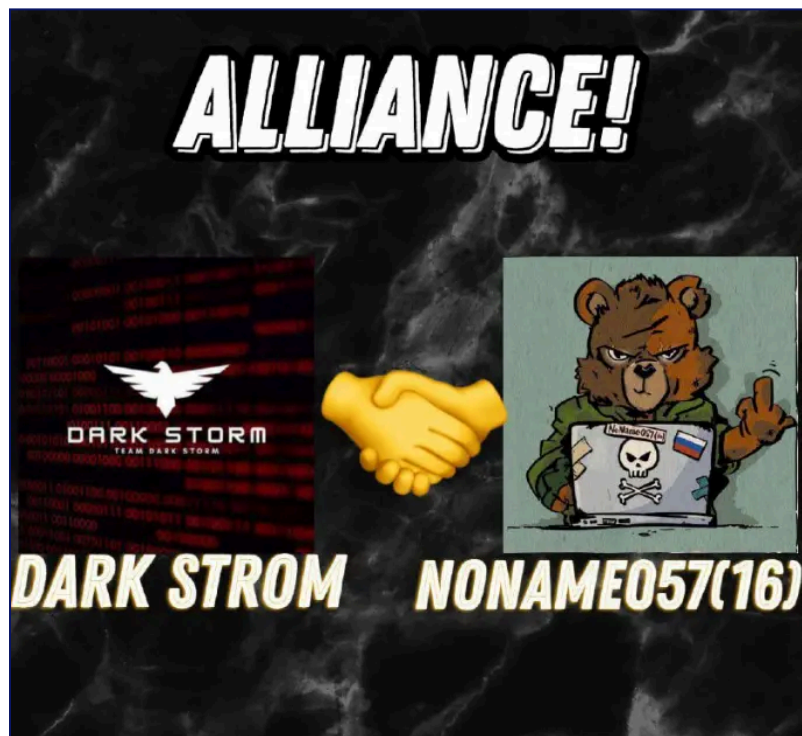
Community Dynamics: Alliances & Feuds

Like other online communities, the global hacktivist landscape is subject to its own social dynamics, including the presence of more active and public members who set the tempo for attacks and hacking campaigns, the emergence of new players, and the creation or breakups of alliances. Aligned hacktivists promote and amplify each other's activity while fighting or insulting groups with differing ideologies or with whom they have personal feuds.

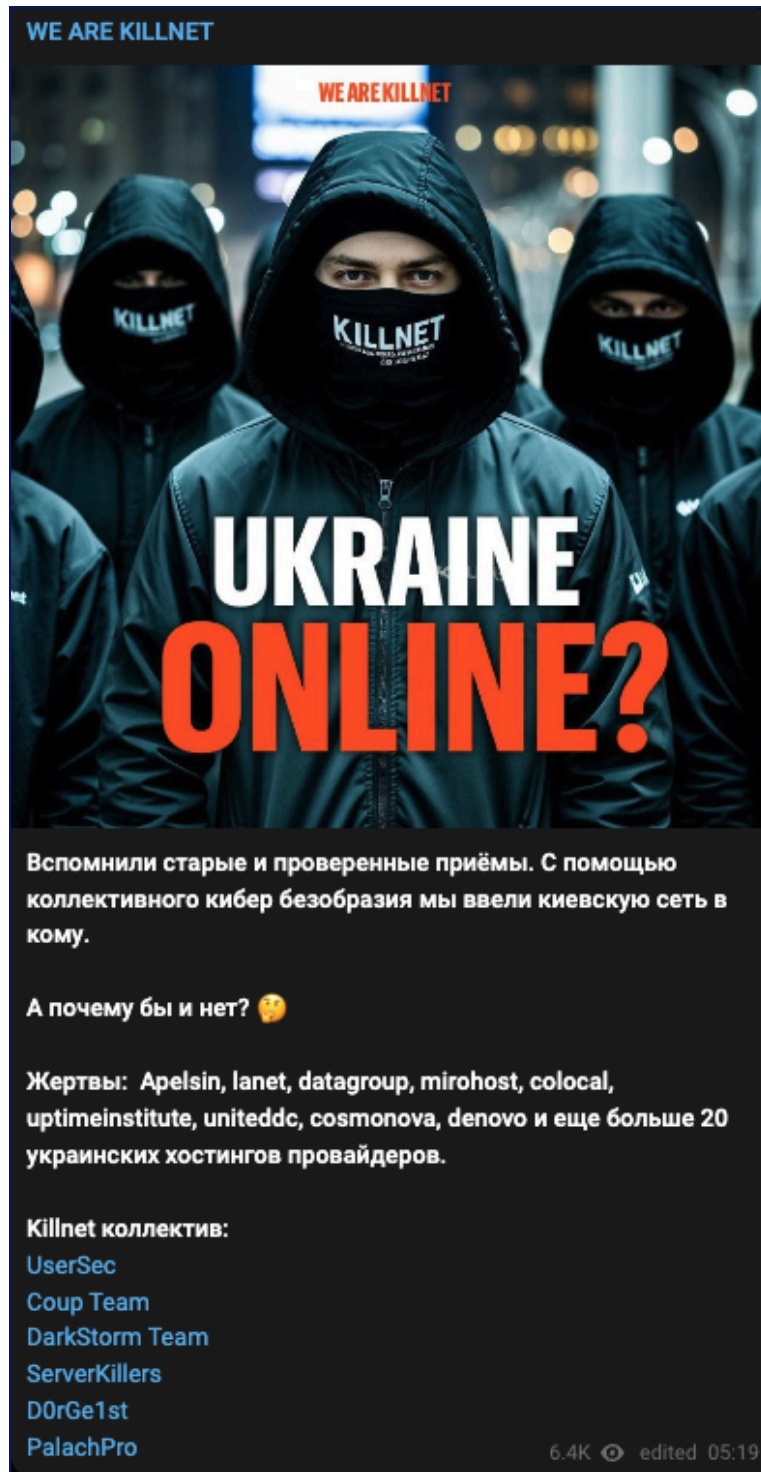
Alliances and Joint Campaigns

Alliances, hacktivist collectives, and joint campaigns are key structures of the hacktivist community that we monitor. Since 2022, we have tracked close to 20 alliances and collectives, some of which can contain dozens of hacktivist groups, and most of which are transregional. These alliances and collectives permit hacktivist groups to loosely coordinate their activities,

more easily and quickly line up behind attacks against a specific target country, and amplify the overall perception of their effectiveness. These alliances also enable smaller hacktivist groups with lower technical skills to gain visibility, engage in cross-promotion, and grow their followings.



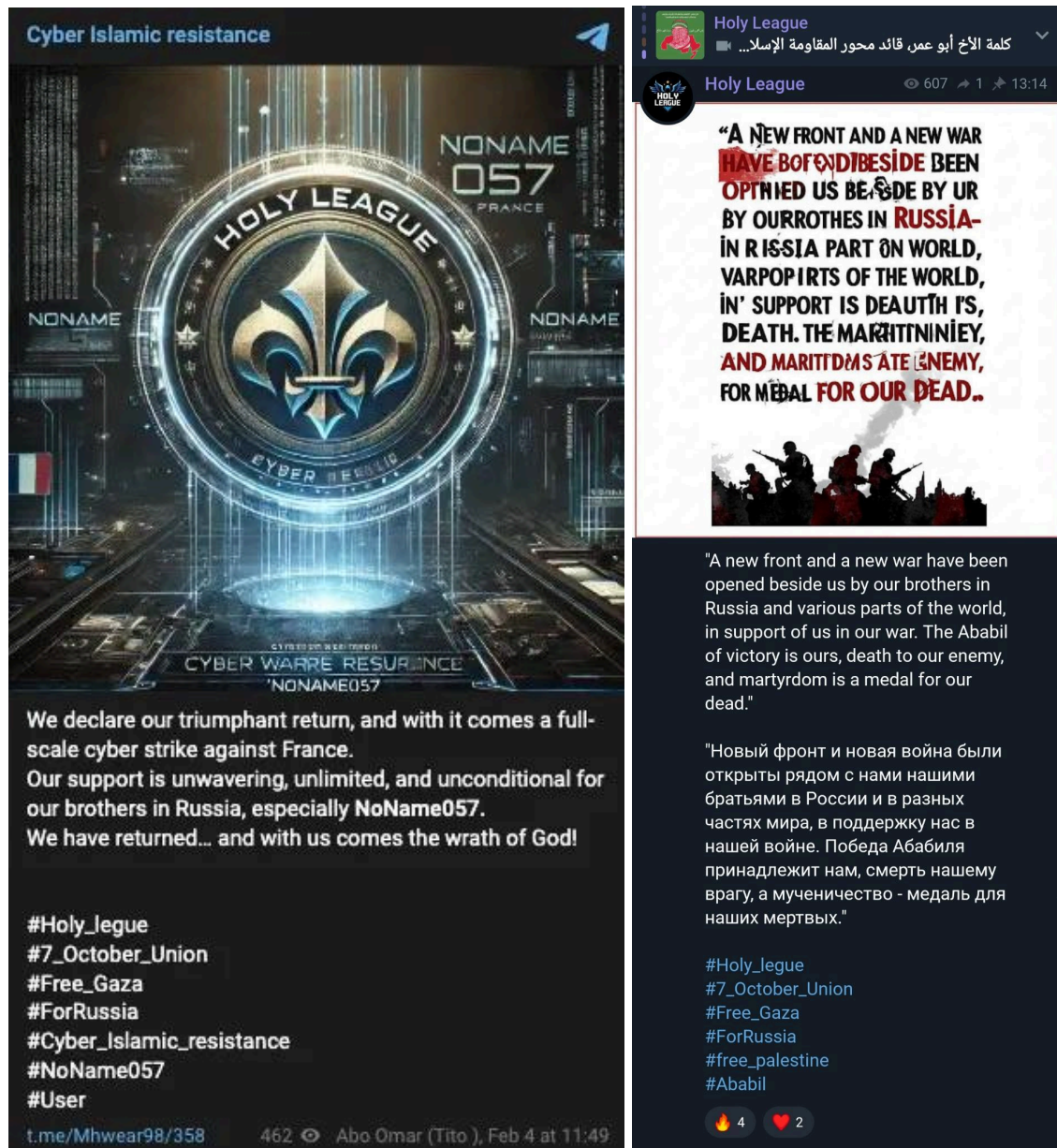
The pro-Palestine hacktivist group Dark Storm Team shared this image in an April 2025 Telegram post announcing an alliance with the pro-Russia hacktivist group NoName057(16) as NoName057(16) [conducted attacks](#) against Finnish websites. The misspelling is part of the original image.



In June 2025, the pro-Russia hacktivist group Killnet posted a Telegram message that suggested it was [attempting to form](#) a “collective” of groups that includes pro-Russia hacktivists like UserSec and pro-Palestine ones like Dark Storm Team.

In addition, these transregional collectives and joint campaigns have resulted in a breakdown of ideological and geopolitical barriers, resulting in groups attacking countries they otherwise likely would not have. Since the Holy League collective – an intergroup alliance [comprising](#) pro-Russia, pro-Palestine, and occasionally other groups – [emerged](#) in 2024, we have increasingly witnessed

pro-Palestine groups joining attacks against Ukraine or aligned countries and pro-Russia groups participating in attacks against Israel or supportive nations. While its activity is sporadic, Holy League remains one of the most persistent collectives we've monitored.



Telegram posts promoting the Holy League collective.

Similar to the branding efforts of individual groups, alliances and joint campaigns also utilize distinct images, typically a collage of the logos of participating groups, and hashtags to promote their efforts. Starting in [February 2025](#), various pro-Russia and pro-Palestine groups engaged in multiple rounds of a campaign they dubbed #Hack_For_Humanity, appending the hashtag to joint attacks against [NATO member countries](#), as well as Israel and countries perceived as supporting its actions in Gaza, including the [United Arab Emirates](#) and [Cyprus](#).



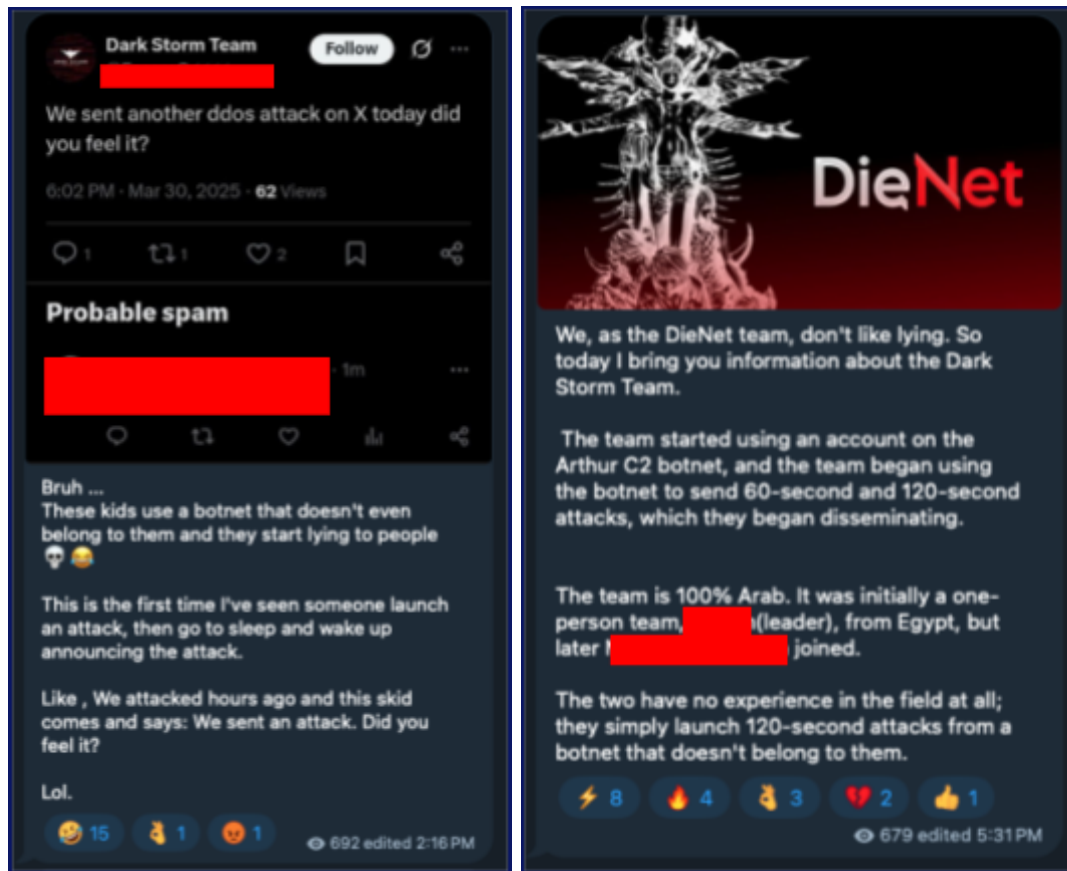
An image containing the logos of various hacktivist groups that participated in the Hack For Humanity campaign.

Feuds

In addition to helping them form alliances, hacktivist groups' ideological, geopolitical, and personal motivations also routinely put them at odds with adversarial groups, resulting in inter-community feuds that place public and private sector entities in the crosshairs.

For example, in April 2025, after the Algerian military [shot down](#) a Malian drone near their shared border and tensions [escalated](#), we [observed](#) pro-Algerian and Malian hacktivist groups engage in retaliatory attacks targeting government websites, banks, and other entities in both countries. In March 2025, after Dark Storm Team claimed it was responsible for disruptions of [X](#), DieNet accused it of "lying" and taking credit for an attack DieNet performed.

Even personal feuds present a risk to public and private sector entities, which become collateral damage in hacktivist campaigns. For example, in May 2025, we [observed](#) the Vietnamese hacktivist group [Special Forces Electronic Army](#) (SFEA) and its allies attack banks and government websites in Cambodia after the Cambodian group BL4CK CYB3R called SFEA a "[skidd](#)," an insulting term for an unskilled hacker. The Vietnamese-Cambodian group attacks had initially started after SFEA threatened Cambodia with a "large-scale war" in late April. The timing occurred a day before the 50th anniversary of Vietnam's reunification, although SFEA did not directly mention the anniversary.



In March 2025, the pro-Palestine hacktivist group DieNet accused another pro-Palestine group, Dark Storm Team, of "lying" about disrupting the social media platform X (left). DieNet then named two alleged members of Dark Storm Team (right). Redactions added by Graphika.

Platform Moderation & Hacktivist Persistence

Like other malign actors engaged in violative activity on social media platforms, hacktivist groups face difficulties maintaining an online presence and have had to contend with increases in platform moderation, particularly on Telegram. In addition, while several groups have maintained a presence for years, several others have gone defunct, changed their names, or only appear sporadically, making consistent tracking difficult without a robust monitoring methodology.

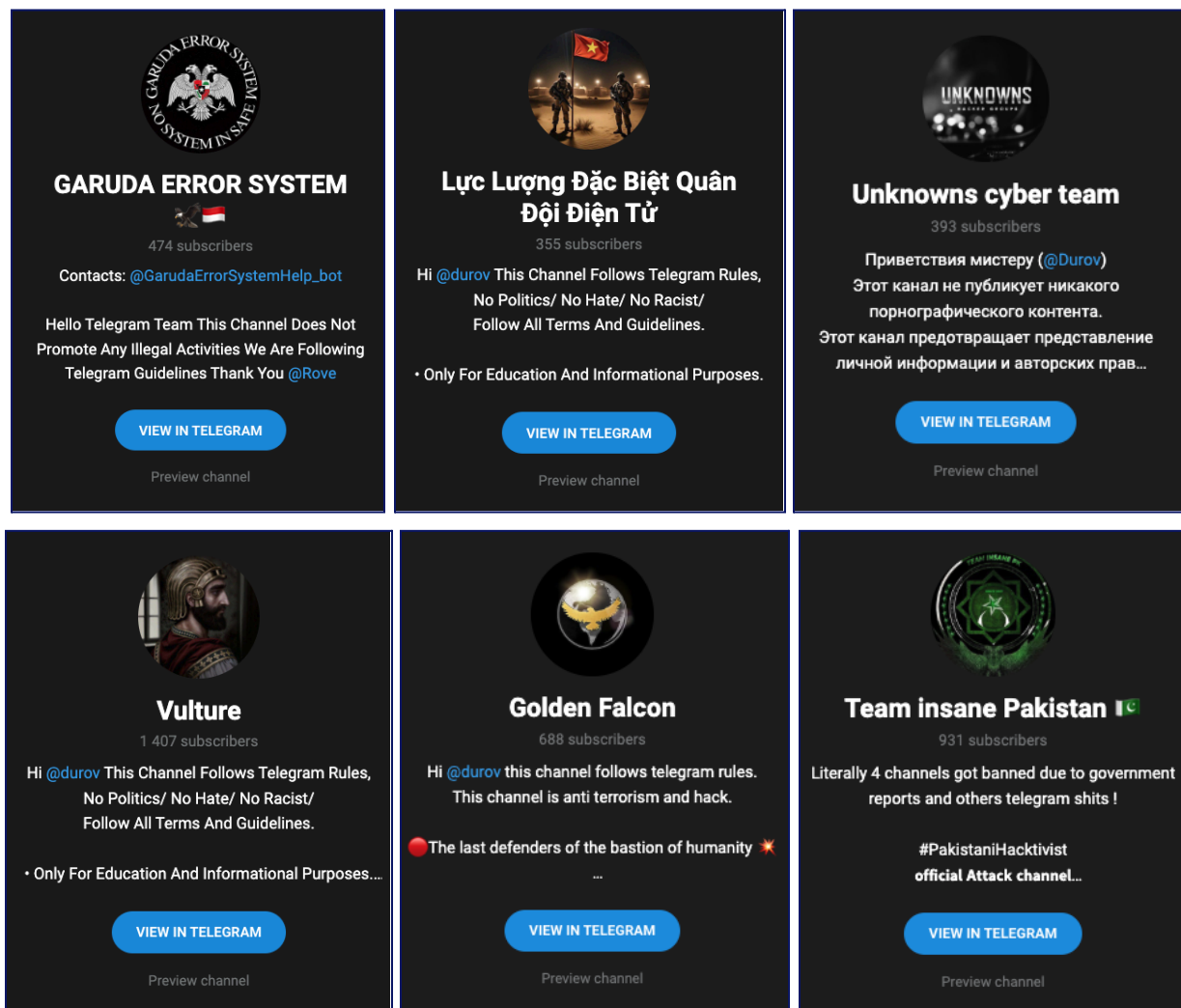
Dealing With Deplatforming

Hacktivist groups have primarily operated on Telegram, likely due to the platform's traditionally less stringent moderation than mainstream Western social media platforms. However, we have observed a stark increase in Telegram deplatforming these groups after French authorities [arrested](#) CEO Pavel Durov in August 2024, and the platform indicated it would [increase moderation](#). While the reasons for removal remain vague, several groups have stated that their channels were taken down or blocked for violating Telegram's terms of service on copyright, the release of personal data, or the promotion of illegal goods.

Groups that have received significant attention after attacking high-profile targets, like NoName057(16), or that take credit for significant disruptions, like Dark Storm Team, end up repeatedly deplatformed. Smaller groups have also been disrupted.

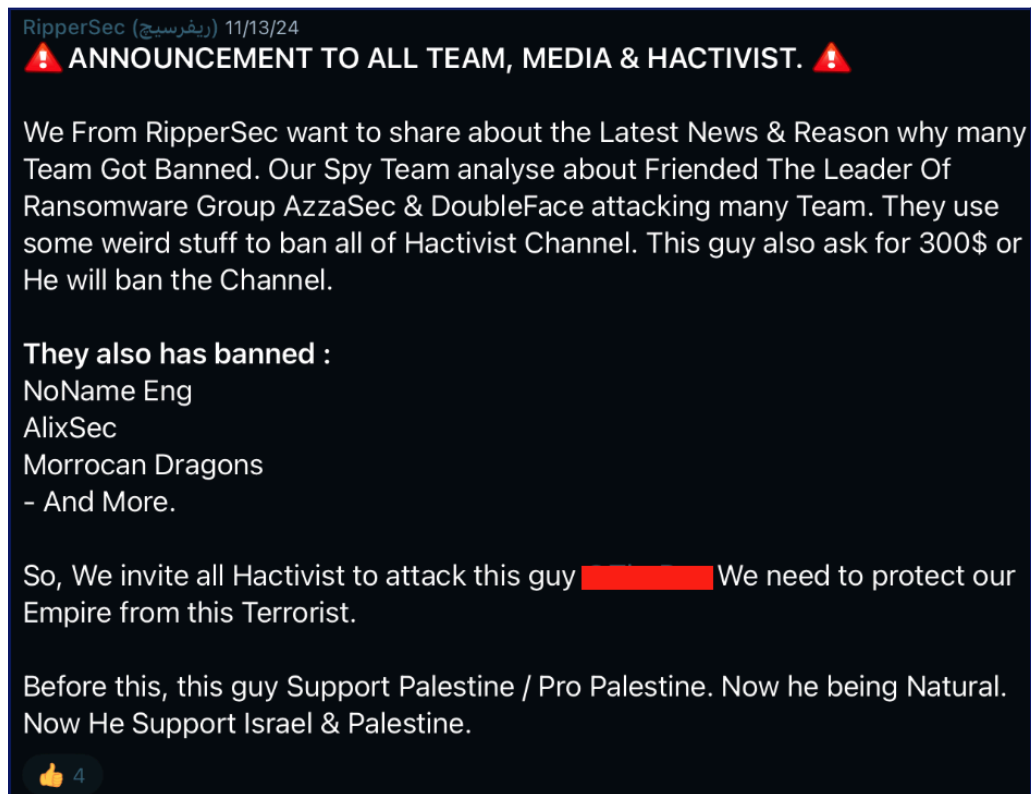
This deplatforming can notably impact a hacktivist group's on-platform audience as they are forced to establish new channels and followings. For example, NoName057(16)'s Telegram channel had about 85k subscribers before it was removed in late 2024. It has had to establish new channels several times. Its current Russian-language channel has about 4.4k subscribers.

When they re-emerge, deplatformed groups often use their removals to claim they are being silenced by their "enemies" and Western powers. We've also observed groups leave messages in their bios that appeal to Durov directly not to ban them.

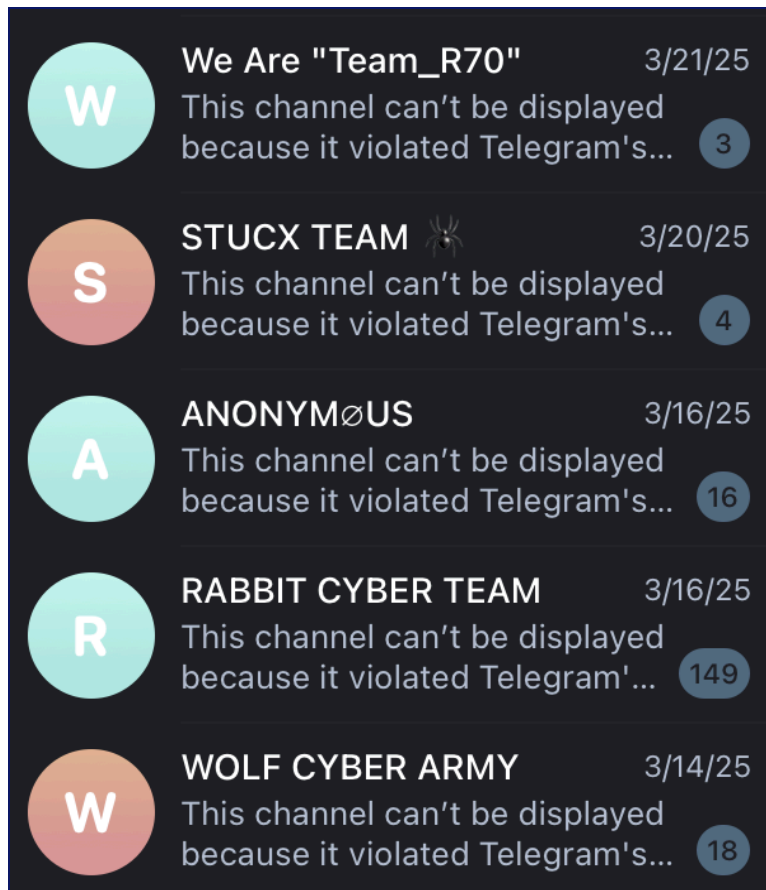


Several hacktivist groups have put messages in their Telegram channel descriptions asking Telegram founder Pavel Durov not to ban their accounts or complaining about bans.

Despite facing challenges with deplatforming and bans, many of the hacktivist groups we monitor are persistent in their attempts to maintain and expand their online presence. They routinely re-emerge on Telegram with new handles and channels, relying on allies to promote their new presence. Some have attempted to establish a presence on X, potentially viewing it as safer from moderation. Some Bengali and Pakistani hacktivist groups administer Facebook pages and related groups to share their content, engage with their communities, promote hacking courses, and recruit new members. A minority of groups have attempted to move their communications to platforms like Signal, Discord, TOX, or the Matrix-based decentralized chat app Element.



In November 2024, the Malaysian hacktivist group RipperSec accused the leader of the pro-Palestine group AzzaSec of attempting to extort other hacktivists by threatening to get their Telegram channels banned. Redactions added by Graphika.



Examples of the Telegram channels for several Southeast Asian and Middle Eastern hacktivist groups being unavailable due to platform suspensions for "violating Telegram's terms of service."

Appendix: 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.



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.

