

# Anonymous Sudan

Threat Intelligence Report

# Who Are Anonymous Sudan?

Since January 23, 2023, a threat actor identifying as “Anonymous Sudan” has been conducting denial of service (DDoS) attacks against multiple organizations in Sweden. This group claims they are “hacktivists,” politically motivated hackers from Sudan.

Truesec has been investigating this group to shed light on their activities and help identify their true motives. In our research we have also collaborated with our partner Baffin Bay Networks.

## What Is Anonymous?

To understand this group, it's also important to understand the hacktivist collective they claim to be a part of.

Anonymous is a loose collective for online activism and protests that emerged in the early 2000s. It is essentially a label that almost anyone can use to claim to be a politically motivated hacker. Anonymous uses hacking, distributed denial of service (DDoS) attacks, and other forms of digital activism to promote social and political change. Its members define Anonymous as a set of campaigns, where a campaign is a composition of individuals who, for a period of time, share a common set of values and goals and publicly claim to be Anonymous.

Over the years, Anonymous has been involved in a wide range of campaigns and operations, including protests against police brutality and racism, campaigns to promote internet freedom and online privacy, and efforts to support political dissidents and activists in countries such as Iran and Syria. An analysis of social media posts by persons that actively promote activities in the name of “Anonymous” shows a diverse group of individuals promoting a plethora of both counterculture and anti-Western agendas.

## Analysis of OpSweden

When a member of the Anonymous collective wishes to gain traction for online activism against a particular target, this is done in social media by announcing an “operation” in the form of a hashtag “#OpXXXX” where “XXXX” is the name of the target country or organization.

On January 21, 2023, the Danish-Swedish right-wing activist Rasmus Paludan burnt a Quran outside the Turkish embassy in Stockholm. Two days later, Islamic members announced to the Anonymous online collective what they called “#OpSweden,” an operation to punish Sweden for burning the Quran. Multiple other actors from Islamic countries in Asia and the Middle East then amplified this claim.

The image below shows the relationship between the various actors involved in amplifying OpSweden.

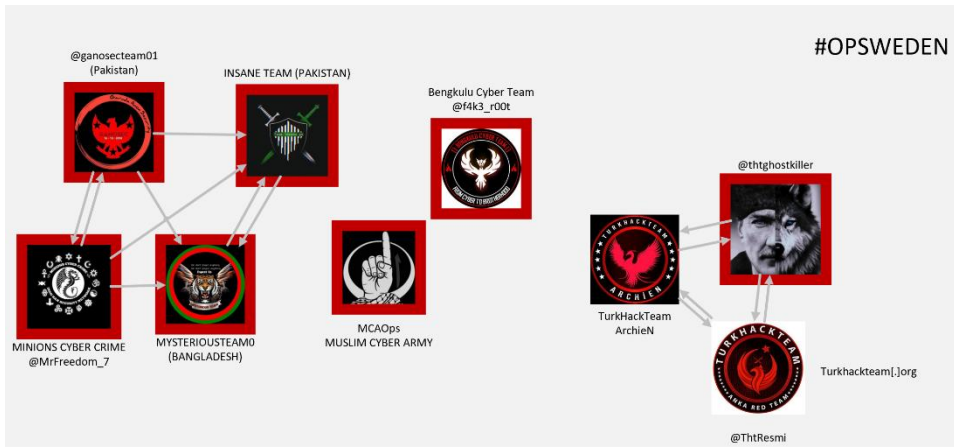


Image 1: Actors in OpSweden.

The attacks were a combination of DDoS and web defacement operations, typical for Anonymous operations. It is assessed that only some members were actually involved in the attacks. The attacks were, however, amplified on social media by other self-proclaimed Anonymous hackers, mainly from Islamic countries.

## Analysis of OpSudan

The original *Anonymous Sudan* emerged in Sudan in response to the country's ongoing political and economic challenges. In 2019 a popular uprising led to a military coup that ousted President Omar al-Bashir. Since then, Anonymous Sudan has continued to be a vocal and active presence in the country's political landscape. They also launched the #OpSudan during the protests.

The original Anonymous Sudan is also known for its use of digital activism, which includes hacking and distributed denial of service (DDoS) attacks on government and other high-profile websites. These tactics have been used to disrupt government websites and draw attention to issues such as internet censorship and restrictions on free speech.

In addition to their online activities, the original Anonymous Sudan has also been active in street protests and other forms of direct action. The campaign has been involved in demonstrations against the current transitional government, which they view as insufficiently democratic and representative of the people's interests.

One of the more prominent actors involved in OpSudan was an individual with the moniker @GhostSec. This actor has been in use for a long time and has a solid follower base. They have been involved in multiple anti-Russia and pro-Ukraine ops.

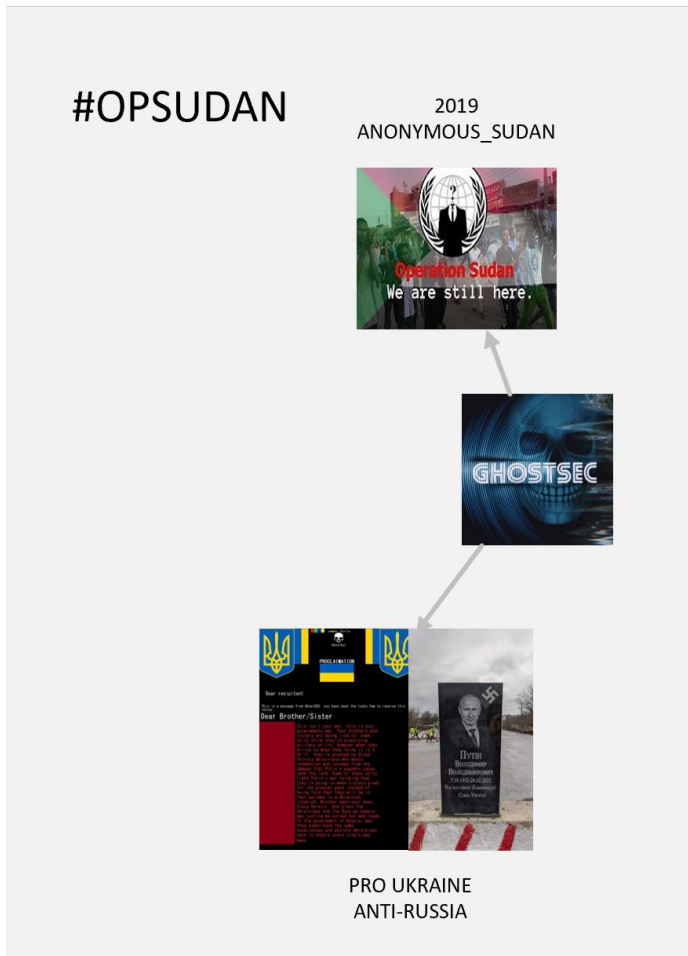


Image 2: GhostSec and OpSudan

## Analysis of Anonymous Russia

There is an online group that identifies itself as Anonymous Russia, but this group has virtually no interaction with the rest of the loose Anonymous collective. They are instead part of a Russian social media cluster of hackers that includes threat actors like KillNet, UserSec, and Passion Botnet. These are all Russian groups that promote Russian narratives and conduct DDoS attacks to support Russia's geopolitical agenda. Many of them are also suspected of having ties to the Russian government.

The separation between Russian hackers and the larger Anonymous Collective also includes the choice of social media platforms to promote their activities. The larger Anonymous collective usually promotes and amplifies their activities on Twitter, while the Russian hackers promote their activities on Telegram.

The DDoS attacks against Sweden in January 2022 were promoted and amplified on Twitter. There was virtually no traction for the #OpSweden operation in Telegram or elsewhere in the Russian hacker sphere.

## What Is the New Anonymous Sudan?

The threat actor behind the most recent DDoS attacks against Sweden claims to be Anonymous Sudan and that it is an actual Anonymous operation (individuals claiming to be Anonymous that have a common goal). However, there are several indications that this new “Anonymous Sudan” has nothing to do with the original Anonymous Sudan or the larger Anonymous collective.

- The campaign is not announced in the style of most Anonymous campaigns, using an operation name with the “#OpSweden” tag or similar.
- Those involved in the campaign don’t have any connection to Sudan or the “Anonymous Sudan 2019” campaign.
- The group is only active on Telegram, like Russian hacktivist groups, and only interacts with Russian actors. There is no traction among the Anonymous collective in Islamic countries, like during the TurkHackTeam “OpSweden.”
- Their operation is instead amplified in the Russian hacktivism sphere by #Infinity Hackers Group, #KILLNET, and #ANONYMOUS RUSSIA.
- Uses the site check-host[.]net to check the status of their channel, the same as KillNet, Passion Net, and other Russian hacktivist groups.
- The group claims that the “Sudanese help Russia because Russia helped Sudan.”
- Most posts are made in English and Russian, but not Arabic.<sup>1</sup>
- User location for the Telegram account is listed as Russia.



Image 3: Registration Data on the Anonymous Sudan Channel

When the Anonymous Sudan account was first created on Telegram, the group’s only activity was a short statement that the group would attack “enemies of Sudan” and then a few posts amplifying posts by Russian hacktivist groups KillNet and Anonymous Russia.

Below is an example of a post from Anonymous Sudan amplifying a pro-Russian message from KillNet.

<sup>1</sup> Since claims that Anonymous Sudan may be tied to Russia, the actor has apparently begun to update their posts, including adding some Arabic text, in an attempt to disguise the origin. Until recently however all posts have been in English and Russian only.

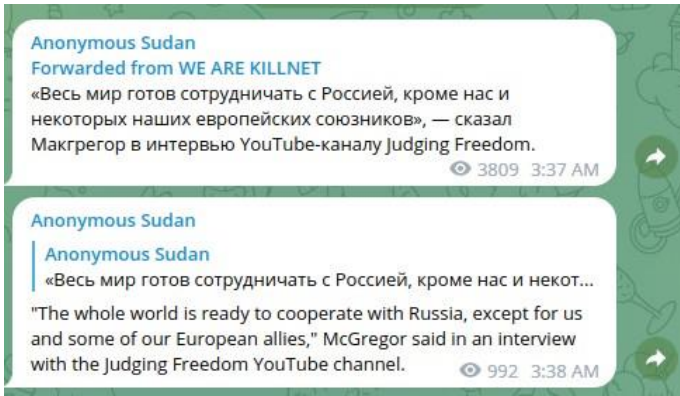


Image 4: Anonymous Sudan amplifies Russian propaganda by KillNet.

The Russian hacktivist group UserSec has been especially active in promoting Anonymous Sudan. On January 11, 2023, before Anonymous Sudan was registered on Telegram, a representative for UserSec referred to bringing a new group that was “multi-cultural” and “real pros.” The same group posted on January 15, 2023, that something “large” and “very cool” would happen soon.

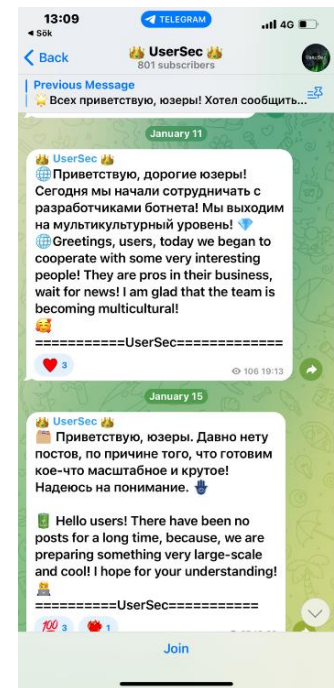


Image 5: Russian Hacktivists UserSec Posts

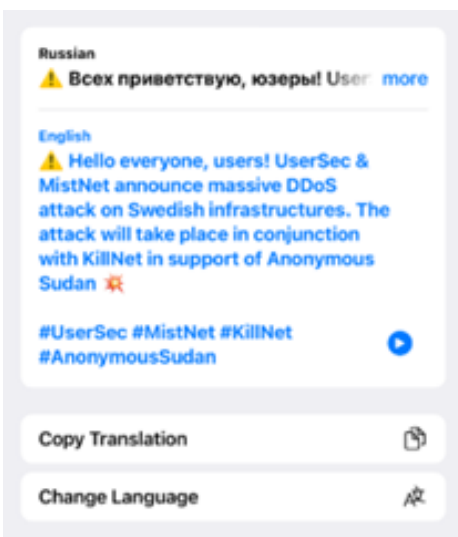


Image 6: Post on Russian hacktivist group UserSec’s Telegram channel.

Further proof of the connection between Anonymous Sudan and Russian hacktivist groups was revealed in the large DDoS attack against Swedish websites on February 19, 2023. This time the attacks were openly coordinated between the Russian hacktivist groups KillNet, UserSec, and MistNet.

Again there is no observable traction or amplification of Anonymous Sudan among actors from Islamic countries in the regular Anonymous collective, only among the Russian ecosystem.

On February 19, 2023, a representative for the Anonymous collective also denounced the new “Anonymous Sudan” as not being part of the Anonymous collective.



Image 7: Anonymous collective denounces Anonymous Sudan.

## Analysis of Adversary Infrastructure

In our research into Anonymous Sudan, we have also cooperated with our partners, Baffin Bay Networks. Thanks to this cooperation, we can now also illuminate some technical aspects of the infrastructure used by the group claiming to be Anonymous Sudan.

Unlike most hacktivist groups, Anonymous Sudan does not use an illegal botnet to generate the traffic volume necessary for DDoS attacks. Instead, they have had a cluster of 61 paid servers hosted at IBM/Softlayer in Germany. The attacks have then been routed through open proxies to disguise the real origin of the attacks.

This use of paid infrastructure strongly suggests that the operation is financed by someone with more money than a relatively new and previously unknown hacktivist group typically has available. This is not the first time a Russia-affiliated hacktivist group used paid infrastructure. The Russian hacktivist group NoName057(16) has also reportedly used paid infrastructure.

The fact that the threat actor uses paid infrastructure doesn't prove that the attacks are government-sponsored, but it is additional evidence that the operation has been carefully organized by someone willing to pay for it, not a spontaneous action by activists.

As of February 23, 2023, IBM/Softlayer has reportedly taken action against these servers, pending a full investigation. The same morning Anonymous Sudan also took down a post on Telegram shortly after publishing it that had included a list of new targets, this time in Denmark.

## Possible Coordination Between Threat Actors

The Microsoft Threat Intelligence team has announced, cited in Swedish media, that Russian and Turkish hackers may have been coordinating their activities to maximize the effects of the disinformation operation against Sweden. Microsoft also claims that Russian and Turkish hackers may have been aware that something was planned in advance<sup>2</sup>.

Truesec has no independent information to confirm this. The initial DDoS attack on organizations in Sweden, initiated on January 23, 2023, and amplified in the wider Anonymous collective, is primarily attributed to Turkish hackers, but the timing of their activities did not coincide.

The timing of attacks against Denmark in February, however, did correlate. On January 21, 2023, Turkish hackers announced they had DDoSed a Danish gaming company. The same day "Anonymous Sudan" announced they would begin attacking websites in Denmark the following day.

---

<sup>2</sup> [www.aftonbladet.se/nyheter/a/EQzrm2/ryska-och-turkiska-hackare-samverkade-efter-koranbranningen](https://www.aftonbladet.se/nyheter/a/EQzrm2/ryska-och-turkiska-hackare-samverkade-efter-koranbranningen)

## Timeline of Events

The Telegram channel “Anonymous Sudan” was first created on January 18, 2023. This was just three days before Rasmus Paludan publicly burned a Quran outside the Turkish Embassy in Stockholm.

There was also other activity in the Russian hacktivist community in January prior to Paludan’s protest, indicating that new actors are entering this ecosystem. A detailed chronology of the events is shown below:

Date	Event
2023-01-08	New Telegram channel, mistnet@telegram, is created <sup>3</sup> .
2023-01-11	Russian hacker group UserSec announces that they will become “multi-cultural” and that the new group are real pros.
2023-01-15	Russian hacker group UserSec announces they are preparing “something large and very cool.”
2023-01-16	Right-wing Journalist Chang Frick posts on Twitter that Rasmus Paludan will burn a Quran outside the Embassy of Turkey in Stockholm <sup>4</sup> .
2023-01-17	Rasmus Paludan announces on social media that he will burn a Quran <sup>5</sup> .
2023-01-18	New Telegram channel, Anonymous Sudan”, is created.
2023-01-19	Paludan again announces his intentions on social media.
2023-01-19	New post in Telegram channel mistnet@telegram: “Soon...”
2023-01-20	Police permit for Paludan’s action approved by Swedish Police.
2023-01-20	First mention of Paludan’s planned action in Swedish media.
2023-01-21	Rasmus Paludan burns a Quran outside the Embassy of Turkey.
2023-01-23	TurkHackTeam announces #OpSweden on social media.
2023-01-23	Anonymous Sudan declares attacks against Sweden on Telegram, but this gains no media traction as the actions by TurkHackTeam get the spotlight.
2023-02-01	Last post about #OpSweden from TurkHackTeam
2023-02-04	Anonymous Sudan launches DDoS attacks against U.S. organizations, including the web page of the CIA <sup>6</sup> .
2023-02-10	Anonymous Sudan begins DDoS attacks against organizations in Sweden.
2023-02-19	Anonymous Sudan begins DDoS attacks against organizations in Sweden in coordination with Russian groups KillNet, MistNet, and UserSec.

<sup>3</sup> Both user\_sec and mistnet present themselves as anti-NATO activists and are both heavily engaged in amplifying posts by Anonymous Sudan

<sup>4</sup> <https://twitter.com/ChangFrick/status/1615025562036076563>

<sup>5</sup> <https://www.secure.instagram.com/p/Cnghb2VDMQ2/>

<sup>6</sup> <https://theycyberexpress.com/anonymous-sudan-vs-us/>



2023-02-19	Anonymous Sudan announces they are now part of Russian KillNet.
2023-02-19	A representative of the Anonymous collective denounces Anonymous Sudan, saying they are not part of the Anonymous collective.
2023-02-21	Turkish hackers announce a DDoS attack against a Danish game-developing company, citing the burning of a Quran. Paludan has dual citizenship in both Denmark and Sweden.
2023-02-22	Anonymous Sudan begins DDoS attacks in Denmark, again citing Rasmus Paludan's burning of the Quran.

The timeline above shows that there is a lot of activity in Russian hacktivist circles around and before the action by Rasmus Paludan. It also indicates that the launch of "Anonymous Sudan" coincided with the preparations for Paludan's action, but days before his action became public knowledge outside a relatively small group of people, including Paludan and his followers. This group includes the right-wing journalist Chang Frick, who is known to have connections to the Russian propaganda channel Russia Today<sup>7</sup>.

## Conclusions

While the Anonymous collective is a diverse and sprawling group that includes many different agendas, observations suggest that the group claiming to be "Anonymous Sudan" has nothing to do with the greater Anonymous collective or the users behind the original Anonymous Sudan or the #OpSudan Anonymous actions.

They appear instead to belong to the ecosystem of Russian hacktivist collective that includes KillNet and other groups, some of which are reported to have ties to the Russian intelligence and security services, although this is not confirmed<sup>8</sup>. Anonymous Sudan amplifies actions by Russian hacktivists and are, in turn, amplified by some Russian hacktivist groups.

The Telegram channel used by Anonymous Sudan to promote their attacks was created on January 18, 2023, just three days before the actions by Rasmus Paludan. The timeline suggests that Anonymous Sudan was created as part of a plan for an information operation aiming to harm Sweden by amplifying Rasmus Paludan's action. Some of the Russian hacktivist channels on Telegram most active in amplifying the posts of Anonymous Sudan were also promoting them and hinting at "something large" happening before even Rasmus Paludan's protest burning of a Quran was made public.

The fact that the group calling themselves "Anonymous Sudan" has access to paid infrastructure in the form of 61 servers for their attacks suggests that someone is financing them and that they are not simple activists.

It is not clear if this plan was created on extremely short notice, based on the right-wing journalist Chang Frick's posts on January 16, 2023, or if Russian intelligence knew in advance because they were involved in planning Paludan's actions, but it stretches belief that hackers from Sudan would follow social media accounts of fringe characters in Swedish right-wing extremism.

<sup>7</sup> [www.telegraph.co.uk/world-news/2023/01/26/kremlin-linked-journalist-organised-quran-burning-turkish-embassy/](https://www.telegraph.co.uk/world-news/2023/01/26/kremlin-linked-journalist-organised-quran-burning-turkish-embassy/)

<sup>8</sup> <https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet>

The most likely explanation is instead that the new so-called “Anonymous Sudan” is part of a Russian information operation, and the true motive is to create fear and uncertainty in Sweden and amplify outrage in Turkey at Paludan’s actions to complicate Sweden’s NATO application.

It is also highly likely that the initial hacktivism in the name of Anonymous, under the tag “#OpSweden” amplified by hackers in the Islamic world, had no connection to Anonymous Sudan. It’s possible that the threat actors behind Anonymous Sudan decided to let the hacktivists behind #OpSweden do their work for them and not ramp up their own attacks until the “#OpSweden” attacks started to peter out.

A secondary motive for these attacks could be to internally strengthen the narrative that Russia is not isolated and create the illusion that there are online activists all over the world supporting Russia.

If “Anonymous Sudan” was created as a Russian information operation and they are now officially a part of the Russian hacktivist group KillNet, then it is likely that the suspected ties between KillNet and the Russian government are correct. Groups like KillNet often rely on online contributions from their fans to finance their operations, so conducting a false flag operation is not really in their self-interest.