



ThreatMon



**ANONYMOUS SUDAN:
IN-DEPTH
ANALYSIS
BEYOND
HACKTIVIST
ATTACKS**



@MonThreat



@threatmon



@TMRansomMonitor

Contents

Summary	3
Threat Actor Profiles: Anonymous Sudan	3
Who is Anonymous Sudan	3
Anonymous Sudan Activities	3
What Types of Attacks it Uses	4
Which Sectors are Targeted	4
Anonymous Sudan Attacks	5
Country Based Attacks	5
Sweden:.....	5
Denmark:	9
Australia:.....	11
France:	14
Israel:.....	17
Indian:.....	21
United States of America:	24
Germany:.....	27
Overview of Attacks in the Last Three Months	29
Countries Attacked in the Last Three Months.....	29
Sectors Attacked in the Last Three Months.....	29
Support Groups	30
IOC List	31

Summary

Anonymous Sudan is a newly formed hacking group that has launched DDoS attacks on various organisations in Sweden, Denmark, France, Australia and Germany. The group claims to be retaliating against countries that oppose Sudan and expresses support for groups that support them. Anonymous Sudan has a pro-Russian stance and has taken responsibility for disrupting government operations, hospitals and airport services, with potentially serious consequences. The group has issued threats against a wide range of targets and has displayed a religious motivation in its attacks.

This report covers the ideology of the Anonymous Sudan group and their attacks in the last 3 months, which were covered by the ThreatMon team.

Threat Actor Profiles: Anonymous Sudan

Who is Anonymous Sudan

Anonymous Sudan started on January 18, 2023, right after the Telegram Group was founded, with the announcement "We will launch a cyber attack on any country that is against Sudan". Just 5 days after its establishment, the group launched attacks against the burning of the Holy Quran in Stockholm, the capital of Sweden, and continued its attacks until March 2023. They launched denial of service (DDoS) attacks on numerous organizations in Sweden. The sectors they attacked include Government, Education, Bank, Airport, Healthcare. Anonymous Sudan has made announcements that they will support groups that support them for a while. The group has launched a series of DDoS attacks, particularly against Sweden, Denmark, France, Australia and Germany in retaliation for hostile behavior by Muslims, suggesting that the group may be religious hackers. Anonymous Sudan's attacks are thought to have disrupted government operations, healthcare facilities and airport services with potentially serious consequences. The group has claimed responsibility for a number of attacks and issued threats against a wide range of targets.

Anonymous Sudan Activities

The group's first activity was to target the Swedish government and companies from different sectors in response to the burning of the Holy Quran in Stockholm. France was also targeted by Anonymous Sudan for its anti-Islamic actions. Sudanese hackers had previously expressed support for Russian hackers because of their support for Sudan, demonstrating a pro-Russian stance. The fact that Anonymous Sudan claimed to have assisted KillNet in its attack on the German Federal Intelligence Service (Bundesnachrichtendienst), which KillNet claimed to have supported for the first time, suggests that KillNet has a connection with Anonymous Sudan.

What Types of Attacks it Uses

Anonymous Sudan is mostly involved in DDoS attacks and rarely in other types of attacks. Anonymous Sudan posts links to Check-host.net in its telegram group as evidence of attacks.

Which Sectors are Targeted

Anonymous Sudan has launched attacks against a wide range of sectors, including the Government, Education, Banks, Airports and Healthcare. The group has claimed responsibility for a number of attacks and issued threats against a wide range of targets.

Anonymous Sudan Attacks

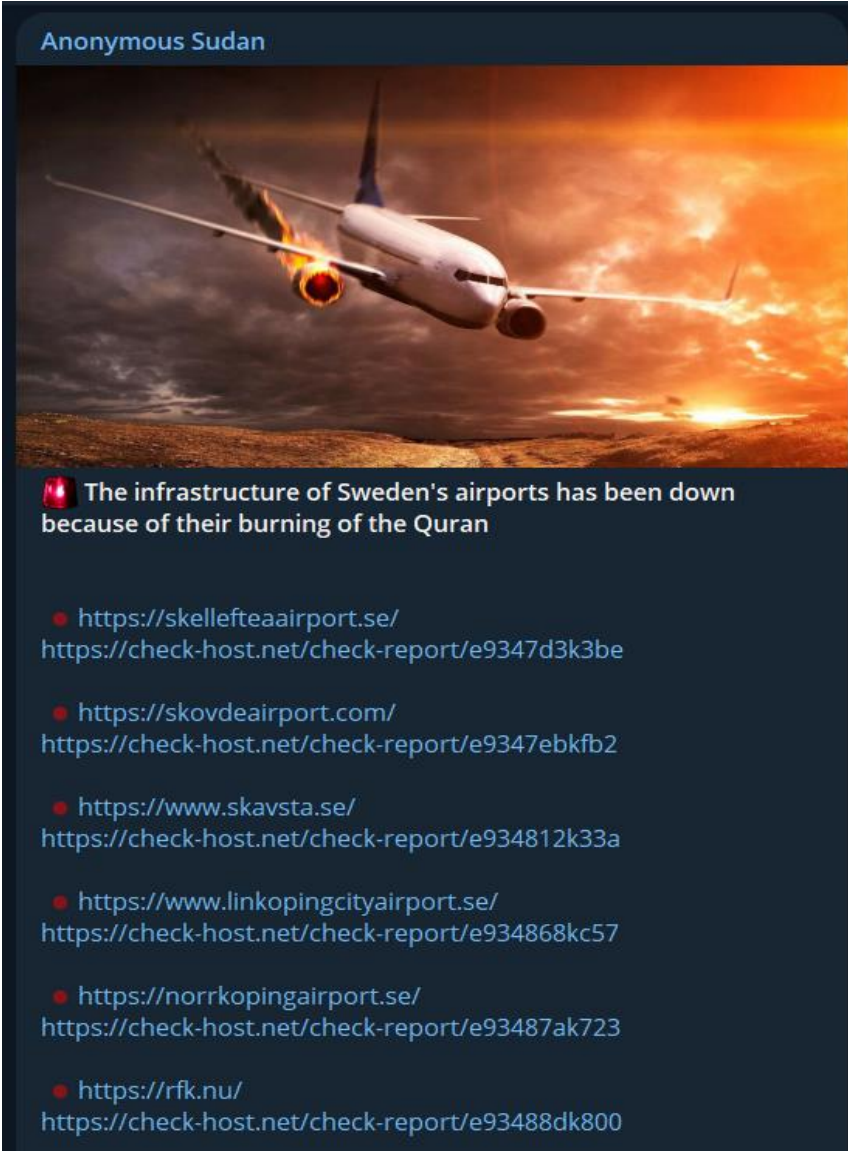
Country Based Attacks

Sweden:


Anonymous Sudan could not remain silent when a Danish-Swedish far right group burned the Quran in front of the Turkish Embassy in Stockholm on 21 January under the protection of Swedish police. Anonymous Sudan and its supporters targeted Sweden.

Sweden, targeted by Anonymous Sudan, was attacked a total of 186 times. In this attack, many airlines, hospitals, schools and more were targeted.

08 February 2023 Anonymous Sudan Sudan launched a DDoS attack on 21 airlines in Sweden. Airline websites became unavailable for a while.



Anonymous Sudan

 The infrastructure of Sweden's airports has been down because of their burning of the Quran

- <https://skellefteairport.se/>
<https://check-host.net/check-report/e9347d3k3be>
- <https://skovdeairport.com/>
<https://check-host.net/check-report/e9347ebkfb2>
- <https://www.skavsta.se/>
<https://check-host.net/check-report/e934812k33a>
- <https://www.linkopingcityairport.se/>
<https://check-host.net/check-report/e934868kc57>
- <https://norrkopingairport.se/>
<https://check-host.net/check-report/e93487ak723>
- <https://rfk.nu/>
<https://check-host.net/check-report/e93488dk800>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

10 February 2023, "Sweden's infrastructure health sector will be under attack due to the Quran burning, we hope Sweden will be prepared for this." After the announcement, 18 hospitals were victimised.

Anonymous Sudan



Infrastructure: Hospitals - The Swedish health sector has been dropped due to the burning of the Quran

- <https://www.nusjukvarden.se/>
<https://check-host.net/check-report/e99fbc3kcd5>
- <https://www.sahlgrenska.se/>
<https://check-host.net/check-report/e99f826k35>
- <https://www.sodersjukhuset.se/>
<https://check-host.net/check-report/e99f828k3eb>
- <https://sjukhus.sophiahemmet.se/>
<https://check-host.net/check-report/e99f829k636>
- <https://www.akademiska.se/>
<https://check-host.net/check-report/e99fa36k7eb>
- <https://www.vgregion.se/>
<https://check-host.net/check-report/e99f832k522>
- <https://www.erstadiakoni.se/>
<https://check-host.net/check-report/e99f837k85>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

11 February 2023 Anonymous Sudan attacks 26 universities in Sweden. As a result of DDoS attacks on universities, education was disrupted for a while.

Anonymous Sudan




Infrastructure: The Swedish educational sector has been dropped due to the burning of the Quran

- <https://www.his.se/>
<https://check-host.net/check-report/e9bfe0bked6>
- <https://www.su.se/>
<https://check-host.net/check-report/e9bfe13kf0b>
- <https://www.slu.se/>
<https://check-host.net/check-report/e9bfe15kf2e>
- <https://www.du.se/>
<https://check-host.net/check-report/e9bfe16k2bc>
- <https://www.uu.se/>
<https://check-host.net/check-report/e9c00a5ke11>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

12 February 2023, Anonymous Sudan Sudan Sudan crashed the infrastructure of 16 banks in Sweden with DDoS attacks. Customers were left dissatisfied as they could not make transactions in the banks, causing a crisis in the banks.

Anonymous Sudan



The infrastructure of Sweden's Banks has been down because of their burning of the Quran

- <https://www.abgsc.com/>
<https://check-host.net/check-report/ea070f8kfbf>
- <https://www.avanza.se/>
<https://check-host.net/check-report/ea071b0ke88>
- <https://www.carnegie.se/>
<https://check-host.net/check-report/ea07104k7f4>
- <https://www.swedbank.com/>
<https://check-host.net/check-report/ea071d6ke15>
- <https://www.jak.se/>
<https://check-host.net/check-report/ea07122k286>

Denmark:

On 28 March 2023, Anonymous Sudan shared in a Telegram post that they will target Denmark after Sweden due to the burning of the Holy Quran. He stated that these attacks will have a great impact and that they will not stop attacking.

! We declare and confirm.. We will return to attack Denmark this time severely because of the burning of the Quran again, and we will not stop attacking again..

! We will distribute the attacks to Australia and Denmark, but the biggest focus will be on Denmark



! The infrastructure of Denmark railway has been down because of their burning of the Quran

• <https://www.dsb.dk/> | Danish train operating company, and the largest in Scandinavia

<https://check-host.net/check-report/edb8067k85b>

• <https://www.bane.dk/> | Rail Net Denmark

<https://check-host.net/check-report/edb8404k1e5>

• <https://www.lokaltog.dk/> | Danish railway company responsible for operating trains and related passenger services

<https://check-host.net/check-report/edba769k528>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

On 2 April 2023, Anonymous Sudan caused disruption of ticket purchases, check-in, etc. as a result of DDoS attacks on 11 airlines in Denmark.

Anonymous Sudan



 The infrastructure of Denmark airports has been down because of their burning of the Quran

- <https://aal.dk/>
<https://check-host.net/check-report/f6ce5c6kf31>
- <https://ekvh.dk/>
<https://check-host.net/check-report/f6ce5c8k35e>
- <https://esbjergairport.dk/>

Australia:

24 March 2023, Australian fashion house Not A Man's Dream has become the new target of Anonymous Sudan for a provocative act against the feelings of Muslims by placing words containing the Arabic name "Allah" on designs of naked women during a fashion exhibition in Melbourne.

They targeted many hospitals in Australia.

Anonymous Sudan




Infrastructure: Hospitals - The Australia health sector has been down Because of the placement of words in the Arabic language that contain the name "God" Almighty, in the designs of naked women, during a fashion exhibition that was held in Melbourne.

- <https://www.rah.sa.gov.au/>
<https://check-host.net/check-report/f442e36kd75>
- <https://www.calvarycare.org.au/>
<https://check-host.net/check-report/f442e37k9cb>
- <https://www.wslhd.health.nsw.gov.au/>
<https://check-host.net/check-report/f442e39kd61>
- <https://www.burnsidehospital.asn.au/>
<https://check-host.net/check-report/f442e3ck4fc>

24 March 2023 Australian Airports DDoS attacks rendered their infrastructure unusable for a time. Traveller had to wait for a while and systems were down.

Anonymous Sudan

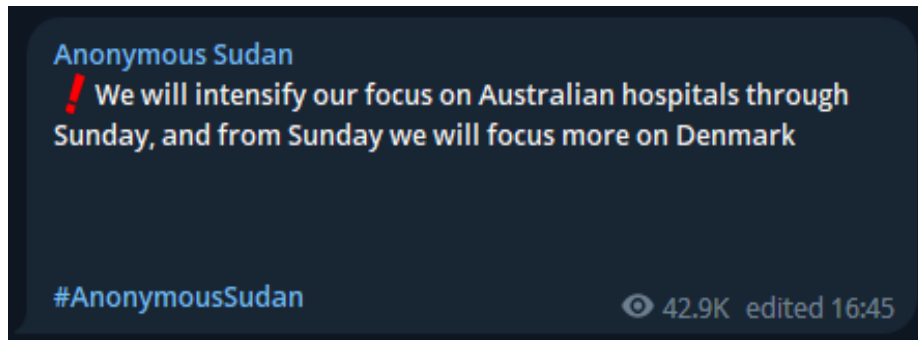


Infrastructure: Australia Airports has been down

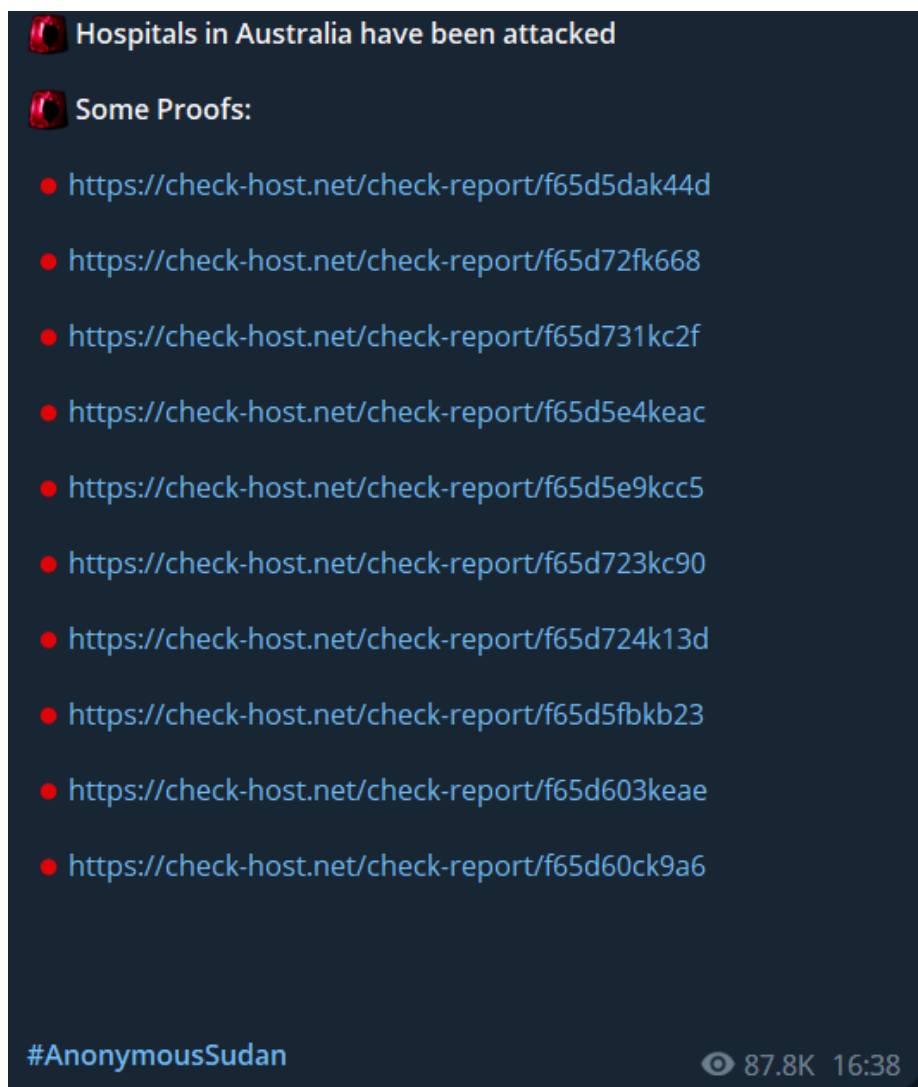
- <https://www.sydneyairport.com.au/>
<https://check-host.net/check-report/f45ff4ckb99>
- <https://www.darwinairport.com.au/>
<https://check-host.net/check-report/f45feek9b>
- <https://www.cairnsairport.com.au/>
<https://check-host.net/check-report/f45fef8k1de>
- <https://www.perthairport.com.au/>
<https://check-host.net/check-report/f45f6afkc54>
- <https://www.goldcoastairport.com.au/>
<https://check-host.net/check-report/f45ff53k673>
- <https://www.bne.com.au/>
<https://check-host.net/check-report/f45f6b0kfd4>
- <https://www.adelaideairport.com.au/>
<https://check-host.net/check-report/f45f6b4ke09>
- <https://www.canberraairport.com.au/>
<https://check-host.net/check-report/f45f6b6k721>
- <https://hobartairport.com.au/>
<https://check-host.net/check-report/f45f6b8k6ca>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

Starting on 24 March, the Australian attacks continued until Sunday 2 April 2023. During the process, they damaged critical infrastructures in attacks on different sectors.



Hospitals in Australia were crippled by DDoS attacks, patients could not be cared for for a certain period of time and systems became unusable.



France:

Anonymous Sudan could not remain silent about the publication in France of a magazine with cartoons depicting the Prophet Mohammed naked. To take revenge on France, the Muslim group launched numerous DDoS attacks, causing an infrastructure crisis in all areas.

15 March 2023, Anonymous Sudan, the first attack against France was against airline companies. They caused 5 airline companies to collapse their infrastructure due to DDoS attacks, so flight operations had to be disrupted for a while.



France airports

- <https://www.parisaeroport.fr/> | Aéroports de Paris
<https://check-host.net/check-report/f181040k968>
- <https://www.parisvatry.com/> | Paris-Vatry Airport
<https://check-host.net/check-report/f181a99kc69>
- <https://www.lyonaeroports.com/> | Lyon-Saint Exupéry Airport
<https://check-host.net/check-report/f196567ke73>
- <https://www.marseille.aeroport.fr/> | Marseille Provence Airport
<https://check-host.net/check-report/f19655dkfef>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

16 March 2023, Anonymous Sudan caused damage to the infrastructure of 9 companies as a result of DDoS attacks on the French health sector. Thus, hospitals could not accept patients and people could not benefit from the health sector.



 French Health Sector | Hospitals

- <https://www.aphp.fr/>
<https://check-host.net/check-report/f1cd7e2k3ae>
- <https://www.musee-armee.fr/>
<https://check-host.net/check-report/f1cd71fk76c>
- <https://www.chu-besancon.fr/>
<https://check-host.net/check-report/f1cd726k776>
- <https://hopital-necker.aphp.fr/>
<https://check-host.net/check-report/f1cd72bke63>

17 March 2023, Anonymous Sudan, which frequently makes DDoS attacks, targeted universities this time. Universities whose infrastructures collapsed were suspended for a while.



 Universities in France | Education

- <https://www.universite-paris-saclay.fr/>
<https://check-host.net/check-report/f216f8ckc3>
- <https://psl.eu/>
<https://check-host.net/check-report/f216c4ck9dd>
- <http://www.sorbonne-paris-cite.fr/>
<https://check-host.net/check-report/f216e63ke61>
- <https://www.univ-angers.fr/>
<https://check-host.net/check-report/f216cc2kb0a>

Israel:

After the sad event, which was reacted in the world due to the uncontrolled violence of Israeli security forces against Al-Aqsa Mosque, Anonymous Sudan, Mysterious Team Bangladesh under the Muslim Cyber Army stated that they will continue their attacks until 7 April and the main attack will be on 7 April. They said that they would carry out FreePalestine OPIsrael operations to defend Palestinian rights with DDoS attacks against many ministries, universities and security infrastructures affiliated to Israel.

The image shows a screenshot of a tweet and a video player. The tweet is from the account 'Muslim Cyber Army' (@MCAOps), which has been retweeted. The text of the tweet reads: 'This is a message to #Anonymous Family and cyber warriors from across the planet: #OpIsrael cyber raid on April 7th 2023, we call upon our brothers and sisters to hack, deface, hijack, database leak, and DNS terminate the Israeli Cyberspace by any means necessary. #FreePalestine'. Below the tweet is a video player. The video features a person wearing a Guy Fawkes mask and a black hoodie with a white globe logo. The text '#OpIsrael' is prominently displayed in the background. The video player shows a progress bar at 0:48 / 1:11, 5,641 views, and a timestamp of 7:32 AM · Apr 4, 2023 · 31.2K Views. The video content includes a scene of a group of people in an outdoor setting, possibly a protest or a public gathering.

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

Anonymous Sudan announced that it would attack Israel with great force on April 7th. It claimed to attack with 35 million requests per second on Layer7 and 4 TB UDP - 1.7 TB SYN on Layer4. After the announcement on 2 April 2023, the first victims were hospitals in Israel. As a result of DDoS attacks on hospitals, it became unusable for a while.

Anonymous Sudan





Infrastructure: Hospitals - Israel health sector has been dropped Because of what they did in Palestine

- <https://www.shamir.org/>
<https://check-host.net/check-report/f6d13b8k973>
- <https://www.schneider.org.il/>
<https://check-host.net/check-report/f6d1577kcf3>
- <http://www.kmc.org.il/>
<https://check-host.net/check-report/f6d13bdk586>
- <http://hy.health.gov.il/>
<https://check-host.net/check-report/f6d157ek8c4>
- <https://www.rambam.org.il/>
<https://check-host.net/check-report/f6d13c2ka6f>
- <https://www.elishahospital.com/>
<https://check-host.net/check-report/f6d13c3k430>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

On 4 April 2023, Anonymous Sudan, who wanted to avenge what was done in Palestine, targeted schools.

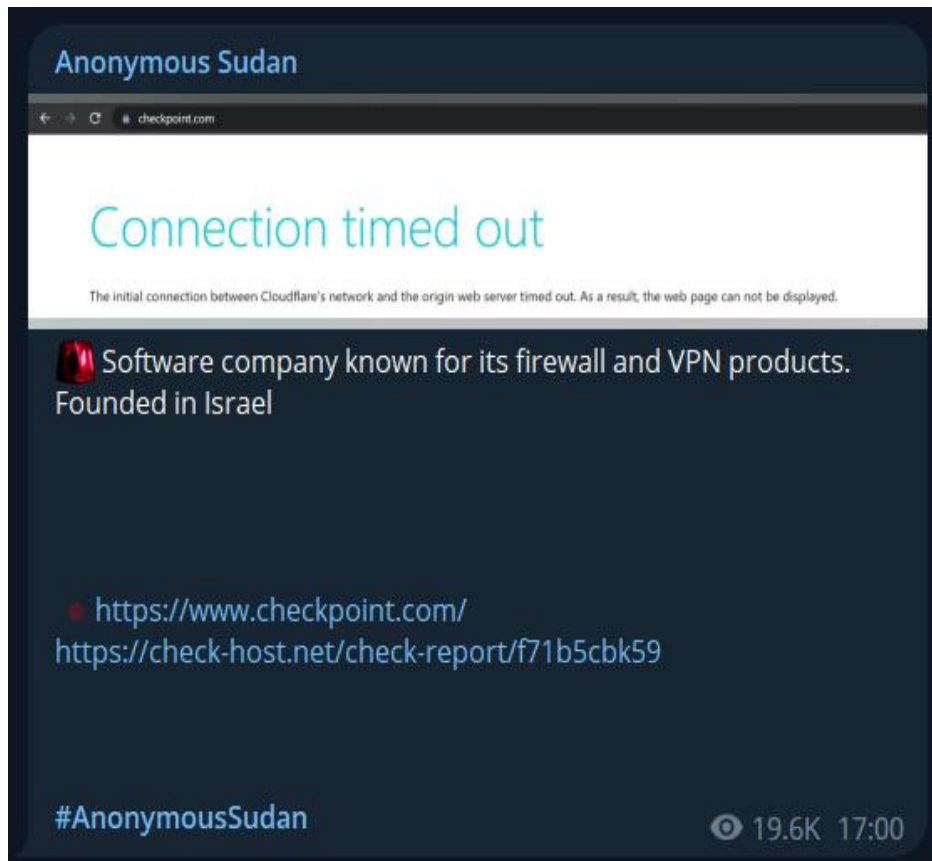


 Infrastructure: Universities - Israel education sector has been dropped Because of what they did in Palestine

- <https://huji.ac.il/>
<https://check-host.net/check-report/f71067ck3e>
- <https://www.weizmann.ac.il/>
<https://check-host.net/check-report/f7107dak91b>
- <https://www.biu.ac.il/>
<https://check-host.net/check-report/f71074dkd19>
- <https://www.haifa.ac.il/>
<https://check-host.net/check-report/f710774k49f>
- <https://in.bgu.ac.il/>
<https://check-host.net/check-report/f71068ckb17>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

CheckPoint, a software company established in Israel and known for its firewall and VPN products were targeted. Stating that the reason for this intense attack against Israel is because of what it has done to Palestine, Anonymous Sudan is not content with its own attacks, but warns people to "Attack", invites people to attack and attacks with great force. Among the sectors attacked; Airlines, Banks, Israeli National Intelligence Organization, Hospitals, Universities, Newspapers and many different institutions and organizations. It has been observed that other groups have not remained silent to these calls and that different groups and threat actors continue these attacks with different plans.



Indian:

On 7 April 2023, Anonymous Sudan, which stated in a telegram that they would target "The reason we attack India because of what they do to Muslims and we will start our attacks on India in the next hour", first targeted airports.




Infrastructure: India Airports has been down Because Of What They Are Doing To Muslims

- <https://www.aai.aero/> | Airports Authority Of India
<https://check-host.net/check-report/f7c2ac1k814>
- <https://www.newdelhairport.in/> | Indira Gandhi International Airport
<https://check-host.net/check-report/f7c2696ka6a>
- <http://csmia.adaniairports.com/> | Mumbai International Airport
<https://check-host.net/check-report/f7c3ac2k407>
- <https://www.hyderabad.aero/> | Hyderabad International Airport
<https://check-host.net/check-report/f7c26f8k153>
- <https://www.goanairport.com/> | Goa International Airport
<https://check-host.net/check-report/f7c287bkd17>
- <https://cial.aero/> | Cochin International Airport
<https://check-host.net/check-report/f7c2879kaa7>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

10 April 2023, Indian Hospitals were targeted. As a result of DDoS attacks, the infrastructure of 10 hospitals was damaged and became unusable for a certain period of time.

 Infrastructure: Hospitals - health sector in India has been down Because Of What They Are Doing To Muslims

● <https://www.apollohospitals.com/>
<https://check-host.net/check-report/f82a7fekbfe>

● <https://www.aimsindia.com/>
<https://check-host.net/check-report/f82a7f9k772>

● <https://www.billrothhospitals.com/>
<https://check-host.net/check-report/f82a7f6kbd8>

● <https://www.hindujagroup.com/>
<https://check-host.net/check-report/f82a7eak137>

● <https://www.kimshospitals.com/>
<https://check-host.net/check-report/f82a7e6k794>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

They hacked 3 Indian e-commerce companies and leaked sensitive data. These .txt files contain e-mail and passwords of customers.




Anonymous Sudan



3 Indian e-commerce companies have been hacked and some data will be leaked for proof

#AnonymousSudan 19.2K 14:31

Anonymous Sudan

-  **snapdeal.txt**
271 B
-  **tatacliq.txt**
406 B
-  **flipkart.txt**
419 B

18.8K 14:46

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

```
snapdeal - Notepad
File Edit Format View Help
bir [redacted] ayu [redacted]
97 [redacted] ;Fri [redacted]
kur [redacted] ;993 [redacted]
kunc [redacted] ;Kun [redacted]
alo [redacted] ;938 [redacted]
89 [redacted] ;saga [redacted]
sna [redacted] ;kat [redacted]
kat [redacted] ;kat [redacted]

tatacliq - Notepad
File Edit Format View Help
ya [redacted] ;Sat [redacted]
Pc [redacted] ;250 [redacted]
pan [redacted] .com;pank [redacted]
rah [redacted] ;raw [redacted]
div [redacted] ;abhi [redacted]
lal [redacted] ;1@L [redacted]
man [redacted] ;Mana [redacted]
emi [redacted] ;Mana [redacted]
atu [redacted] ;Kil [redacted]
shr [redacted] ;aG6 [redacted]
kun [redacted] ;993 [redacted]
han [redacted] ;ata [redacted]

flipkart - Notepad
File Edit Format View Help
ya [redacted] ;Mal [redacted]
ri [redacted] ;ame [redacted]
ta [redacted] ;900 [redacted]
70 [redacted] ;250 [redacted]
70 [redacted] ;250 [redacted]
70 [redacted] ;250 [redacted]
89 [redacted] ;897 [redacted]
90 [redacted] ;icf [redacted]
88 [redacted] ;sce [redacted]
94 [redacted] ;Ayu [redacted]
cha [redacted] ;dee [redacted]
mal [redacted] ;@mal [redacted]
abh [redacted] ;abh [redacted]
875 [redacted] ;aka [redacted]
pri [redacted] ;Ind [redacted]
```


United States of America:

The group shared a screenshot of Twitter's website on the Telegram channel with the message "This page is down" and stated that they sent a message to Elon Musk with this attack.

Anonymous Sudan had requested Starlink for Sudan, whose infrastructure collapsed as a result of the military coup.



User reports indicate problems at Twitter

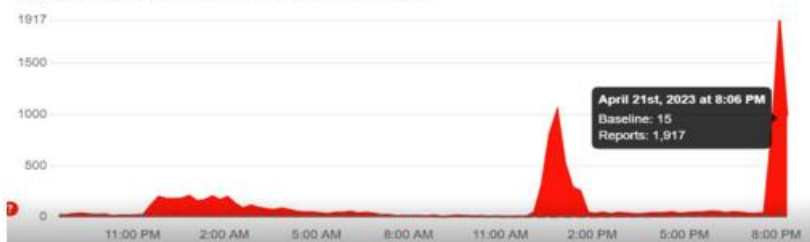
Twitter is a microblog which allows users to publish short messages of 280 characters or less. Twitter users are able to post their tweets from from numerous devices and platforms, including the iPhone, Android, Blackberry, or Windows Phone devices and traditional computers.

I have a problem with Twitter

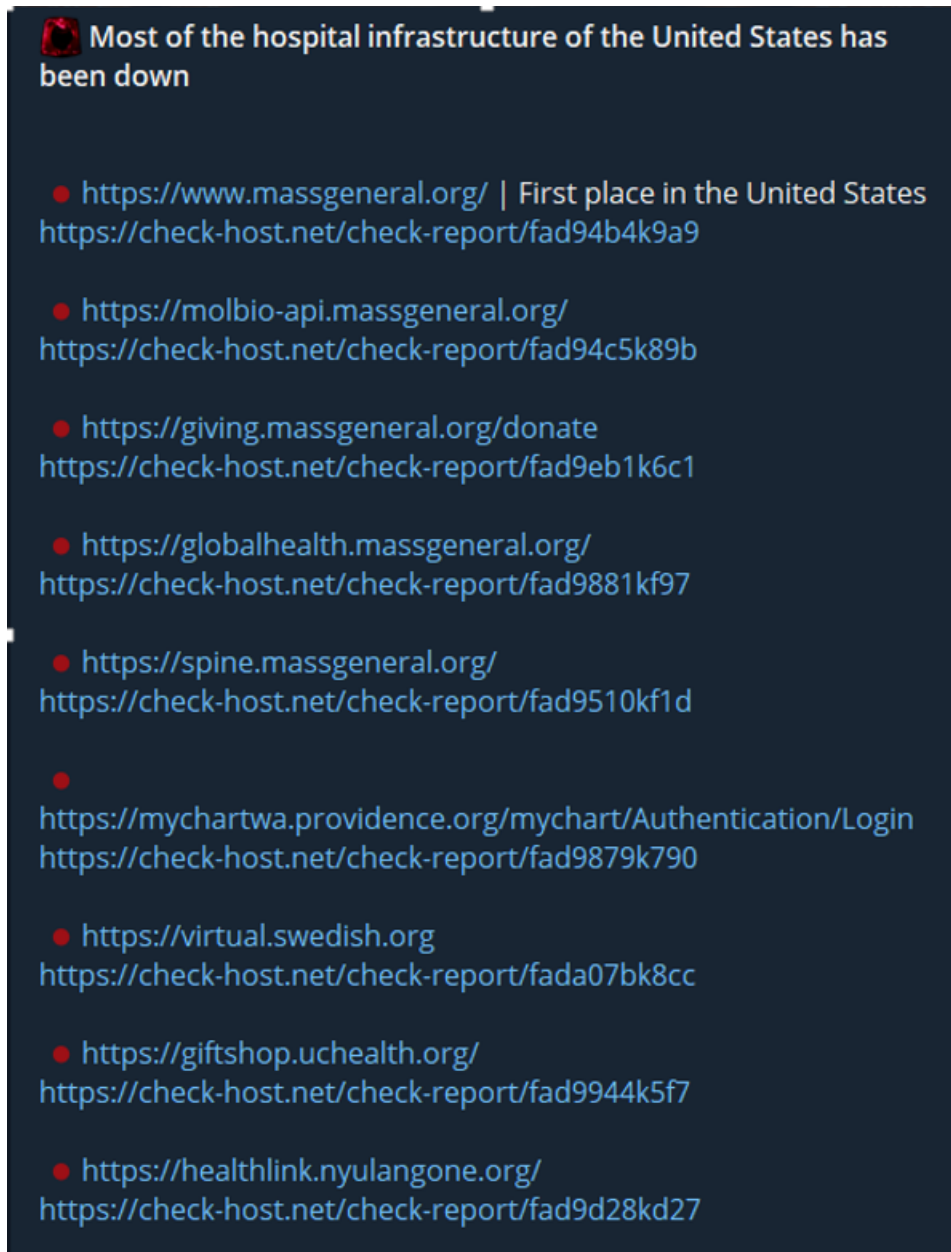
Select the option you are having issues with and help provide feedback to the service.


Website App Server Connection Something else...

Twitter outages reported in the last 24 hours



"The United States of America must be prepared, this will be a very big attack, as we did in Israel, we will soon do it in the United States," Anonymous Sudan said in a Telegram post. On 25 April 2023, as a result of DDoS attacks on hospitals, the procedures became unusable for a while.



 **Most of the hospital infrastructure of the United States has been down**

- <https://www.massgeneral.org/> | First place in the United States
<https://check-host.net/check-report/fad94b4k9a9>
- <https://molbio-api.massgeneral.org/>
<https://check-host.net/check-report/fad94c5k89b>
- <https://giving.massgeneral.org/donate>
<https://check-host.net/check-report/fad9eb1k6c1>
- <https://globalhealth.massgeneral.org/>
<https://check-host.net/check-report/fad9881kf97>
- <https://spine.massgeneral.org/>
<https://check-host.net/check-report/fad9510kf1d>
- <https://mychartwa.providence.org/mychart/Authentication/Login>
<https://check-host.net/check-report/fad9879k790>
- <https://virtual.swedish.org>
<https://check-host.net/check-report/fada07bk8cc>
- <https://giftshop.uchealth.org/>
<https://check-host.net/check-report/fad9944k5f7>
- <https://healthlink.nyulangone.org/>
<https://check-host.net/check-report/fad9d28kd27>

Germany:

Anonymous Sudan has claimed that it is attacking various countries and sectors to show its support for Muslims, who often face hostility and rejection. Its new target is Germany, where DDoS attacks have been launched in many areas, claiming racism against Muslims.



ANONYMOUS SUDAN

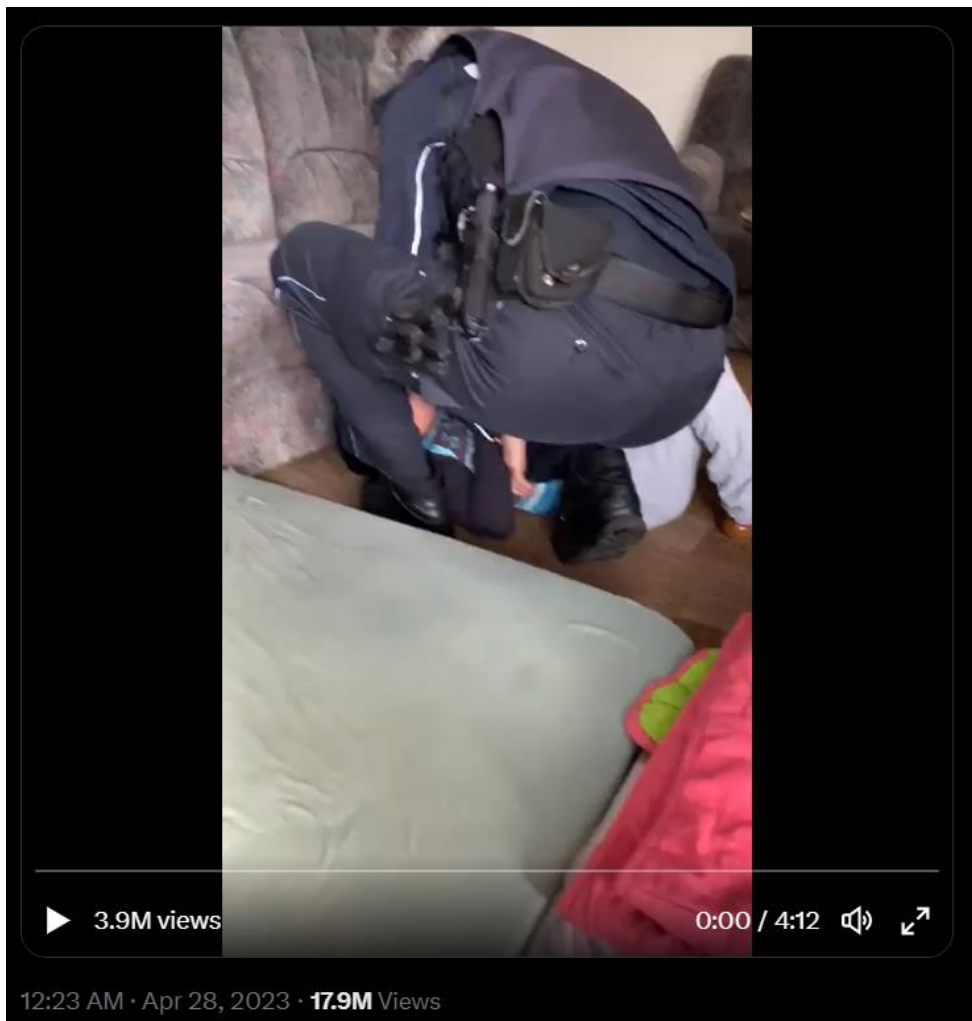


 The reason for our attack on Germany: Because of their racism against Muslims

- <https://www.bnd.bund.de/> | German Federal Intelligence
<https://check-host.net/check-report/fad74e7kb15>
- <https://www.hahn-airport.de/> | Frankfurt-Hahn Airport
<https://check-host.net/check-report/fad7b28kd2f>
- <https://www.stuttgart-airport.com/> | Stuttgart Airport
<https://check-host.net/check-report/fad74fek9cf>

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

On April 29, 2023, a post shared on Twitter led to a DDoS attack on the Federal Police website in response to the kidnapping of a Muslim family's children by German police. Shortly afterwards, the German bank Deutsche Bank AG was attacked for the same reason.



Reason: the abduction of children of a Muslim family by force

- <https://www.bundespolizei.de/> | Federal Police (Germany)
- ★ <https://check-host.net/check-report/fb913d0k6a3>

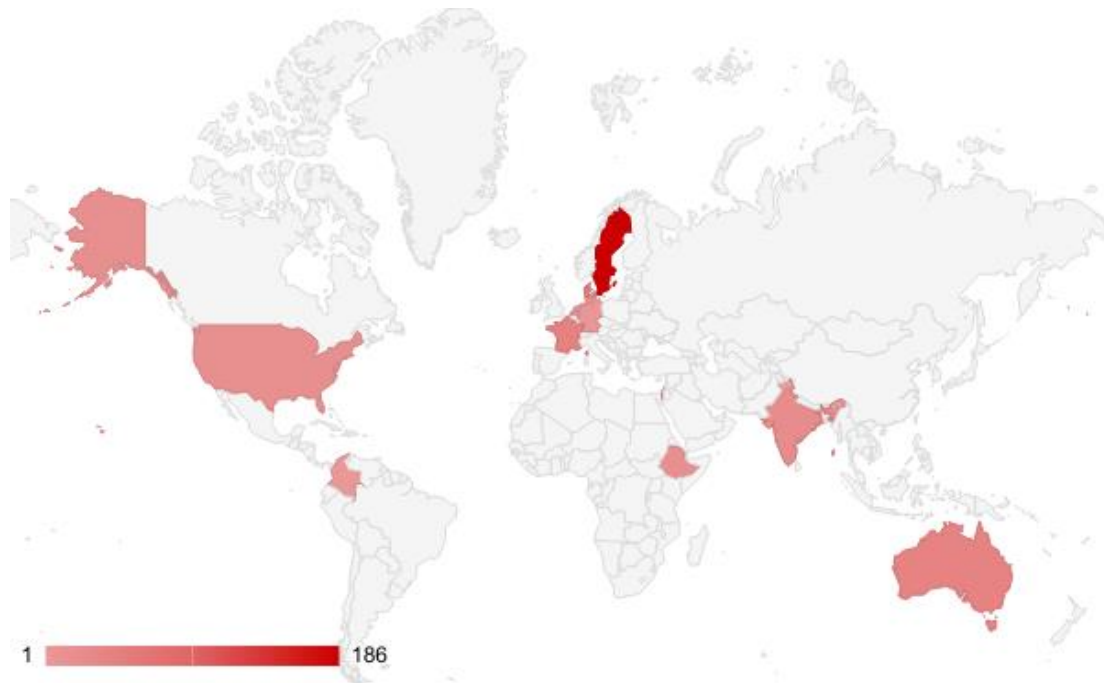
#AnonymousSudan

12.5K edited 16:50

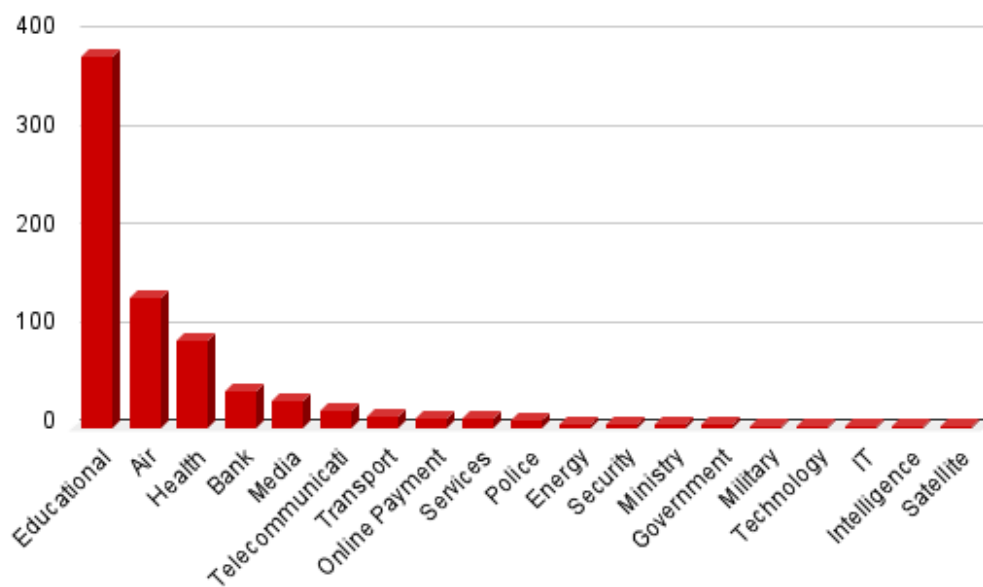
Overview of Attacks in the Last Three Months

Countries Attacked in the Last Three Months

The 11 countries targeted by Anonymous Sudan were subjected to a total of 445 DDoS attacks.



Sectors Attacked in the Last Three Months



Support Groups

List of supporters of the widespread group Anonymous Sudan:

- PHOENIX
- Infinity Hackers
- Headquarters Scribe
- Kill Delta
- Killnet Team
- Anonmyous Russia
- Killnet Reservs
- MistNet
- User Sec
- Turk Hack Team
- AnonGhost Team
- Anon Cyber VietNam
- Ghost Clan
- Your Anon Riots
- Saudi Exile
- Mysterious Team
- Cyber Of Garuda
- Gano Sec Team
- Dragon Force Malaysia Official
- Anon Ops United
- Anonymous Palestine Freedom
- Fighters
- Anon Ops Revolt 2
- Anon Ops Rise

IOC List

As a result of DDoS attacks carried out by Anonymous Sudan and its supporters, 9,205 IP addresses in IPv4 format were detected. According to the list below, 250 IP information has been shared.

TYPE	VALUE
IP	43[.]157[.]119[.]224
IP	5[.]189[.]195[.]117
IP	47[.]108[.]138[.]242
IP	1[.]10[.]226[.]106
IP	117[.]67[.]95[.]27
IP	115[.]153[.]131[.]118
IP	125[.]78[.]177[.]123
IP	119[.]42[.]107[.]124
IP	88[.]135[.]44[.]155
IP	60[.]166[.]129[.]62
IP	49[.]89[.]75[.]132
IP	180[.]243[.]113[.]30
IP	23[.]250[.]8[.]132
IP	141[.]0[.]11[.]253
IP	176[.]59[.]74[.]159

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

IP	181[.]3[.]142[.]135
IP	47[.]100[.]174[.]47
IP	117[.]60[.]45[.]83
IP	177[.]126[.]210[.]8
IP	181[.]3[.]219[.]27
IP	115[.]148[.]27[.]117
IP	138[.]36[.]157[.]187
IP	168[.]205[.]217[.]45
IP	119[.]148[.]34[.]238
IP	185[.]8[.]41[.]32
IP	13[.]232[.]254[.]85
IP	27[.]72[.]240[.]251
IP	203[.]77[.]209[.]25
IP	36[.]89[.]180[.]29
IP	177[.]101[.]191[.]49
IP	200[.]106[.]116[.]201
IP	182[.]34[.]102[.]103
IP	113[.]128[.]29[.]245
IP	168[.]205[.]217[.]214

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

IP	78[.]212[.]27[.]227
IP	218[.]149[.]25[.]193
IP	103[.]36[.]48[.]191
IP	185[.]200[.]37[.]86
IP	181[.]101[.]98[.]146
IP	179[.]97[.]243[.]10
IP	110[.]171[.]84[.]180
IP	125[.]164[.]105[.]204
IP	183[.]163[.]235[.]224
IP	177[.]82[.]233[.]255
IP	104[.]129[.]200[.]130
IP	46[.]101[.]20[.]227
IP	104[.]227[.]101[.]53
IP	181[.]101[.]47[.]82
IP	45[.]228[.]178[.]7
IP	47[.]108[.]166[.]78
IP	182[.]52[.]229[.]152
IP	47[.]114[.]57[.]232
IP	61[.]7[.]168[.]66

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

IP	144[.]126[.]133[.]250
IP	39[.]85[.]124[.]184
IP	222[.]190[.]198[.]91
IP	36[.]6[.]90[.]16
IP	139[.]224[.]199[.]43
IP	223[.]241[.]0[.]185
IP	118[.]175[.]174[.]96
IP	177[.]23[.]164[.]21
IP	112[.]65[.]53[.]11
IP	198[.]58[.]101[.]125
IP	178[.]253[.]58[.]242
IP	118[.]24[.]170[.]46
IP	94[.]240[.]60[.]190
IP	207[.]236[.]12[.]225
IP	58[.]244[.]197[.]164
IP	118[.]172[.]150[.]51
IP	110[.]137[.]149[.]45
IP	124[.]248[.]180[.]42
IP	114[.]104[.]140[.]134

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

IP	182[.]34[.]192[.]165
IP	115[.]219[.]132[.]19
IP	186[.]126[.]205[.]230
IP	60[.]168[.]37[.]75
IP	125[.]27[.]39[.]86
IP	117[.]91[.]130[.]87
IP	117[.]44[.]25[.]225
IP	181[.]101[.]105[.]150
IP	20[.]71[.]185[.]34
IP	111[.]225[.]152[.]26
IP	115[.]151[.]2[.]143
IP	181[.]102[.]50[.]199
IP	118[.]172[.]144[.]160
IP	181[.]102[.]196[.]37
IP	115[.]209[.]115[.]224
IP	1[.]2[.]129[.]15
IP	36[.]89[.]165[.]13
IP	172[.]58[.]3[.]103
IP	60[.]189[.]105[.]92

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

IP	117[.]28[.]60[.]143
IP	117[.]67[.]93[.]41
IP	125[.]126[.]223[.]188
IP	181[.]101[.]105[.]193
IP	72[.]36[.]155[.]130
IP	115[.]209[.]112[.]42
IP	59[.]63[.]112[.]58
IP	140[.]255[.]151[.]101
IP	94[.]137[.]9[.]246
IP	103[.]7[.]115[.]113
IP	131[.]196[.]141[.]234
IP	84[.]40[.]106[.]154
IP	191[.]97[.]44[.]109
IP	114[.]101[.]62[.]191
IP	181[.]4[.]2[.]238
IP	223[.]247[.]95[.]24
IP	223[.]215[.]170[.]115
IP	206[.]81[.]17[.]232
IP	60[.]189[.]108[.]136

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

IP	15[.]228[.]145[.]145
IP	162[.]247[.]46[.]223
IP	198[.]144[.]120[.]224
IP	182[.]46[.]110[.]135
IP	116[.]232[.]34[.]73
IP	79[.]137[.]96[.]188
IP	177[.]93[.]96[.]147
IP	119[.]165[.]117[.]190
IP	181[.]3[.]109[.]238
IP	163[.]204[.]220[.]76
IP	130[.]185[.]120[.]150
IP	103[.]215[.]157[.]125
IP	181[.]102[.]191[.]53
IP	209[.]53[.]17[.]185
IP	47[.]113[.]188[.]210
IP	123[.]182[.]59[.]10
IP	112[.]87[.]89[.]10
IP	116[.]22[.]31[.]114
IP	182[.]107[.]232[.]54

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

IP	77[.]50[.]60[.]6
IP	139[.]180[.]194[.]87
IP	188[.]166[.]30[.]24
IP	103[.]248[.]218[.]10
IP	39[.]225[.]234[.]241
IP	87[.]237[.]65[.]178
IP	181[.]209[.]72[.]234
IP	185[.]220[.]101[.]14
IP	101[.]108[.]197[.]5
IP	177[.]101[.]190[.]63
IP	183[.]166[.]162[.]125
IP	186[.]126[.]250[.]88
IP	117[.]93[.]118[.]193
IP	183[.]148[.]152[.]129
IP	49[.]88[.]112[.]17
IP	124[.]112[.]71[.]246
IP	14[.]20[.]183[.]191
IP	181[.]101[.]161[.]80
IP	101[.]51[.]105[.]134

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

IP	147[.]135[.]112[.]147
IP	115[.]223[.]159[.]153
IP	14[.]242[.]211[.]56
IP	192[.]246[.]205[.]199
IP	188[.]6[.]37[.]220
IP	174[.]75[.]238[.]76
IP	128[.]199[.]155[.]16
IP	163[.]204[.]222[.]172
IP	107[.]173[.]222[.]196
IP	107[.]183[.]64[.]109
IP	114[.]25[.]68[.]77
IP	125[.]87[.]82[.]208
IP	156[.]135[.]170[.]45
IP	117[.]26[.]228[.]114
IP	138[.]25[.]153[.]242
IP	91[.]92[.]78[.]201
IP	165[.]192[.]76[.]148
IP	182[.]253[.]235[.]152
IP	47[.]106[.]187[.]166

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

IP	64[.]118[.]87[.]36
IP	183[.]163[.]120[.]92
IP	64[.]90[.]48[.]164
IP	181[.]101[.]18[.]225
IP	119[.]165[.]112[.]109
IP	125[.]87[.]101[.]90
IP	51[.]159[.]21[.]239
IP	63[.]250[.]32[.]243
IP	88[.]135[.]44[.]232
IP	175[.]155[.]139[.]181
IP	36[.]57[.]87[.]189
IP	223[.]247[.]94[.]63
IP	5[.]202[.]241[.]44
IP	119[.]42[.]118[.]102
IP	112[.]78[.]165[.]194
IP	177[.]126[.]215[.]25
IP	181[.]101[.]215[.]69
IP	119[.]42[.]121[.]5
IP	47[.]101[.]200[.]100

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

IP	193[.]30[.]249[.]16
IP	220[.]89[.]201[.]47
IP	64[.]118[.]84[.]6
IP	49[.]89[.]32[.]5
IP	181[.]102[.]204[.]81
IP	47[.]110[.]56[.]196
IP	43[.]248[.]24[.]186
IP	47[.]94[.]33[.]119
IP	110[.]78[.]168[.]190
IP	95[.]179[.]143[.]244
IP	60[.]166[.]128[.]57
IP	117[.]65[.]98[.]139
IP	73[.]120[.]56[.]160
IP	181[.]5[.]240[.]83
IP	49[.]70[.]48[.]58
IP	78[.]157[.]21[.]159
IP	112[.]84[.]210[.]126
IP	59[.]66[.]173[.]42
IP	181[.]215[.]184[.]230

Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks

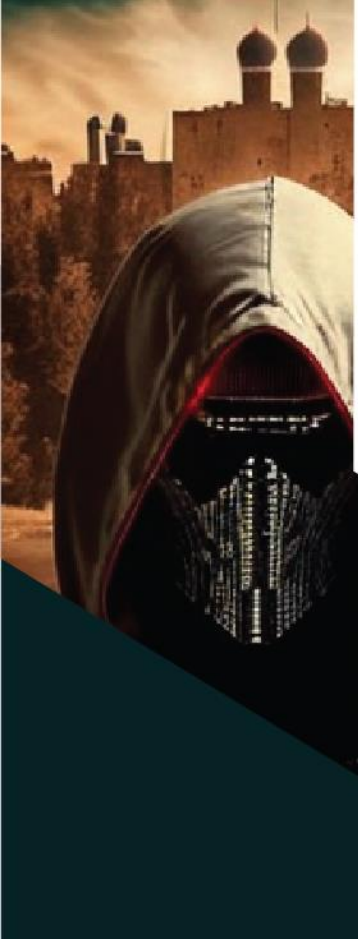
IP	181[.]106[.]208[.]54
IP	177[.]125[.]161[.]88
IP	168[.]195[.]196[.]14
IP	116[.]209[.]57[.]90
IP	104[.]248[.]117[.]133
IP	47[.]245[.]31[.]57
IP	113[.]221[.]47[.]195
IP	176[.]235[.]144[.]146
IP	186[.]126[.]133[.]177
IP	113[.]195[.]165[.]63
IP	27[.]22[.]76[.]216
IP	185[.]129[.]118[.]36
IP	176[.]56[.]107[.]157
IP	37[.]32[.]10[.]215
IP	106[.]6[.]202[.]207
IP	178[.]253[.]61[.]70
IP	181[.]3[.]57[.]70
IP	178[.]253[.]42[.]246
IP	165[.]3[.]69[.]210

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

IP	47[.]1111[.]114[.]106
IP	36[.]69[.]88[.]223
IP	81[.]16[.]8[.]177
IP	45[.]70[.]59[.]170
IP	181[.]101[.]33[.]209
IP	222[.]133[.]169[.]72
IP	165[.]22[.]162[.]120
IP	109[.]94[.]220[.]158
IP	181[.]7[.]220[.]136
IP	83[.]219[.]153[.]255
IP	36[.]57[.]40[.]52
IP	60[.]182[.]231[.]74
IP	221[.]199[.]195[.]19
IP	154[.]86[.]11[.]151
IP	124[.]113[.]217[.]157
IP	47[.]113[.]219[.]111
IP	179[.]83[.]160[.]172
IP	223[.]243[.]4[.]233
IP	134[.]73[.]173[.]142

Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks

IP	181[.]14[.]54[.]224
IP	41[.]33[.]229[.]210
IP	42[.]249[.]163[.]139
IP	181[.]102[.]212[.]91
IP	177[.]129[.]89[.]33
IP	193[.]202[.]11[.]214
IP	176[.]56[.]107[.]248



ThreatMon

010100011010000110100101100010000000101000101
1001000000111001101101101010101010010100100100
0110011000010110110011001000100101011010101010
1110100011001010111100001110100000100000000
1011010010110111001100111001000000001101
00001101000011001010111001000110010
0110111101110010001000000001100111
0001101001011011100110011001110010

45305 Catalina cs St 150, Sterling VA 20166