

LODGED
CLERK, U.S. DISTRICT COURT
3/20/2024
CENTRAL DISTRICT OF CALIFORNIA
BY: TV DEPUTY

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
3/20/2024
CENTRAL DISTRICT OF CALIFORNIA
BY: clec DEPUTY

United States of America

v.

AHMED SALAH YOUSIF OMER,

Defendant.

Case No. 2:24-mj-01591

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the dates of January 18, 2023, through present, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section
18 U.S.C. § 371

Offense Description
Conspiracy to violate 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I) and (VI) (Intentionally Damaging a Protected Computer)

This criminal complaint is based on these facts:

Please see attached affidavit.


Continued on the attached sheet.

/s/ Elliott Peterson
Complainant's signature

Elliott Peterson, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: March 20, 2024


Judge's signature

City and state: Los Angeles, California

Hon. Steve Kim
Printed name and title



AFFIDAVIT

I, Elliott Peterson, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed for approximately twelve years. I am currently assigned to the FBI's Anchorage Field Office, where I specialize in the investigation of computer and high-technology crimes, including computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous cyber-related investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against and arrest warrant for AHMED SALAH YOUSIF OMER ("AHMED"), for a violation of 18 U.S.C. § 371, Conspiracy to violate 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I) and (VI) (Intentionally Damaging a Protected Computer).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant, and it does not purport to set forth all of my

knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times listed are on or about those indicated.

III. SUMMARY OF PROBABLE CAUSE

4. Since early 2023, I have been investigating an online organization calling itself "Anonymous Sudan," which has conducted many significant Distributed-Denial-of-Service (DDoS) attacks¹ against numerous victims around the world and continues to claim credit almost daily for new attacks as of the time of this writing.

5. Many U.S. companies, including Cloudflare, Microsoft, PayPal, X (formerly Twitter), and Yahoo have suffered high-profile attacks by Anonymous Sudan in the last year. There are many more companies that have been threatened with attacks by Anonymous Sudan, or which Anonymous Sudan has claimed to have attacked, but for which I have not yet independently verified damages associated with the attacks. For most victims, attacks appear to have caused damage to their websites and other associated web-based functionalities, often rendering the websites inaccessible for periods of time, or otherwise causing the services to be degraded. Some of these victims sustained millions of dollars in losses from these attacks. In addition,

¹ DDoS attacks are a type of network attack in which multiple Internet-enabled devices are used to flood computers with data or requests, for the purpose of rendering them inaccessible to legitimate users or unable to communicate with the Internet.

Anonymous Sudan has claimed credit for attacks on sensitive government and critical infrastructure targets both within the United States and around the world, including the Department of Justice, the Federal Bureau of Investigation, the State Department, a major hospital in Los Angeles, transportation infrastructure, educational infrastructure, and government websites and infrastructure in Europe, Africa, and the Middle East.

6. All of the attacks and targets referenced above are merely those attributed to the administrators of Anonymous Sudan. The administrators also sell DDoS services to other criminal actors. My investigation to date has determined that the Anonymous Sudan administrators employ a powerful DDoS tool that has been called at various times the "Godzilla Botnet," the "Skynet Botnet," and "InfraShutdown" (hereafter, the "Skynet Botnet"). While I have gathered evidence demonstrating the administrators' own criminal usage of this tool, I have also found logs indicating that their paid customers are similarly using this tool to launch DDoS attacks against various victims worldwide. Indeed, I have found more than 100 users of this tool, including administrators and customers. As described below, I conducted an undercover test of the Skynet Botnet posing as such a customer, which confirmed it in fact functions to conduct denial-of-service attacks on victim computers for paying customers.

7. Based on my review of source code and administrator logs contained on the command-and-control (C2) server² of the Skynet Botnet, and further based on my review of online accounts, including email and other services, including detailed browsing histories and IP address records, I have determined that Anonymous Sudan and the associated DDoS tool appear to be primarily operated by AHMED and an additional co-conspirator.

IV. STATEMENT OF PROBABLE CAUSE

A. Background on Anonymous Sudan and Its DDoS Tool

8. As noted above, "Anonymous Sudan" is an organization that has claimed responsibility for or otherwise been identified as conducting numerous DDoS attacks against entities both in the United States and elsewhere. The first part of its name appears to be a reference to the former hacktivist collective known as "Anonymous," which was a decentralized international group and movement primarily known for its various cyberattacks against governments and corporations. The latter part of the name, "Sudan," appears to be a reference to the country where Ahmed formerly resided, as described below.³ Anonymous Sudan has

² A command-and-control server, or "C2" server, is a server used to control a botnet or other criminal tool by providing instructions to other computer devices that have been configured to listen for, and respond to, commands.

³ There has been some media and threat research company reporting suggesting that Anonymous Sudan may be state-sponsored Russian actors masquerading as Sudanese actors with Islamist motivations, and Anonymous Sudan has publicly claimed an affiliation with pro-Russian hacktivist collective "Killnet." However, my investigation to date has indicated that Anonymous Sudan is in fact led by Sudan-based individuals, including AHMED and a co-conspirator, although the group may share ideologies with, and sometimes appears to act in concert with, Killnet and similar hacktivist groups.

operated a series of Telegram⁴ channels, and public reporting indicates that they have been doing so since at least January 18, 2023. Anonymous Sudan's attacks and Telegram posts regarding those attacks suggest that the group acts at least in part out of ideological and geopolitical motives, although it is also clear that Anonymous Sudan's posts additionally serve to advertise the power and efficacy of the associated DDoS tool they offer to customers as a paid service. Below is an image associated with one of Anonymous Sudan's Telegram channels:



⁴ Telegram is a popular encrypted communication service that also allows users to create their own discussion channels and make both public and private posts.

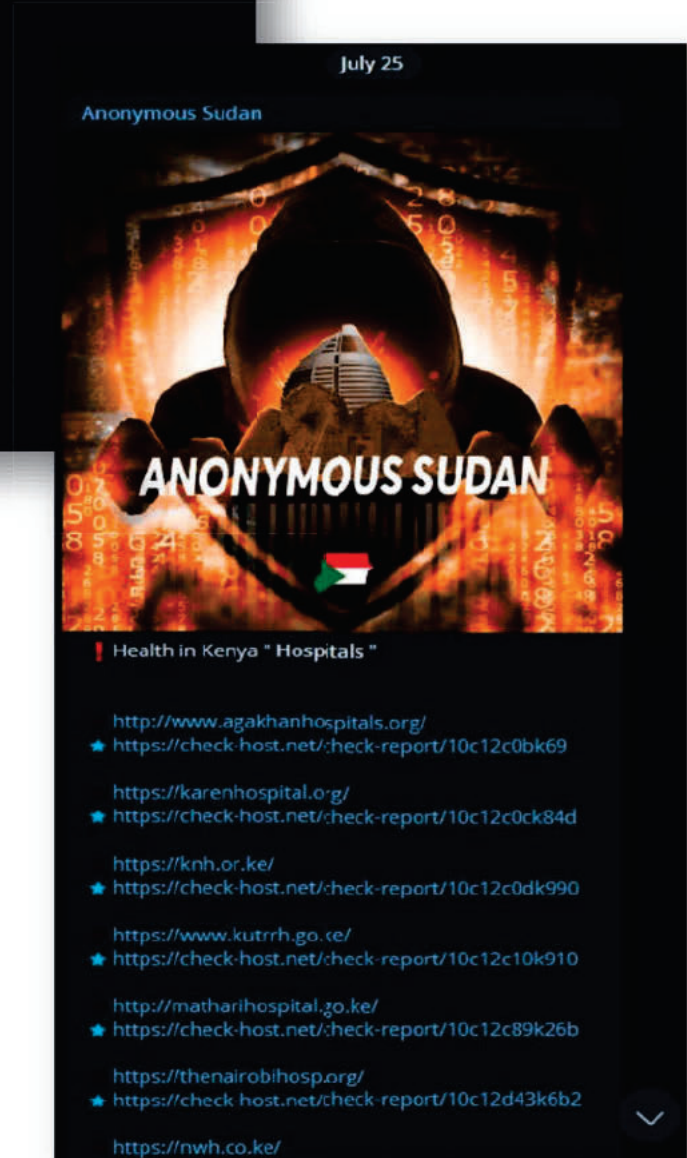
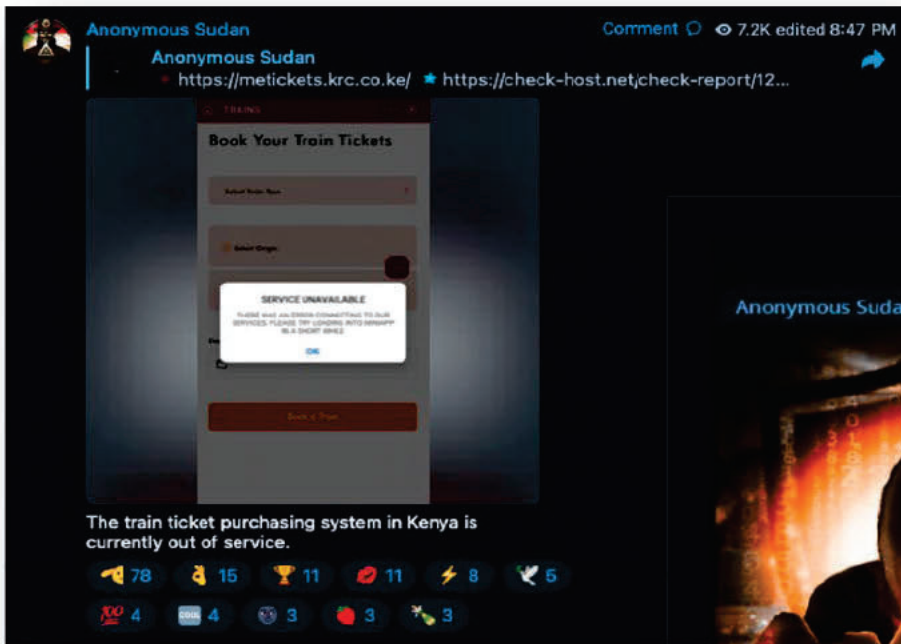
B. Notable Attacks Claimed by Anonymous Sudan

9. As noted above, some of the most damaging and highest profile attacks by Anonymous Sudan were on platforms belonging to Microsoft, which took place primarily in June 2023. From interviews with Microsoft employees, I learned that the widely reported Skynet Botnet DDoS attacks conducted against Microsoft impacted many portions of Microsoft's Internet-based services, such as Outlook 365 and other services hosted in Microsoft's Azure cloud platform. According to Microsoft employees, these outages, which required employees to spend time mitigating and responding to the attacks, resulted in millions of dollars of losses. Microsoft related that these attacks caused disruptions at a Microsoft data center in the Los Angeles region, among other locations.

10. PayPal Inc. was another high-profile victim of Anonymous Sudan, which conducted multiple attacks against the PayPal platform, including an attack it described as a "test" on PayPal in July of 2023. Anonymous Sudan warned in subsequent posts that it would be targeting other organizations in the United States, and that it "ha[d] an appointment with you [PayPal] soon. This was only a 30-second test attack." I interviewed employees of PayPal after the attacks. PayPal employees told me that the attacks resulted in severe disruptions to their platform causing millions of dollars of losses. PayPal performed its own independent investigation into the Anonymous Sudan group, concluding that the attacks against their platform were in fact launched by Anonymous Sudan, and

further, that customer accounts belonging to members of Anonymous Sudan likely existed on their platform, as discussed further below.

11. In July 2023, Anonymous Sudan claimed credit for numerous attacks on Kenyan infrastructure. The attacks lasted more than a week, and they reportedly resulted in massive disruption to government services. They included an attack on the Kenyan eCitizen portal, a government website that provides over 5,000 government services, as well as a large bank, Kenya's largest telecom company, several media websites, ten university websites, seven hospitals, and the website of Kenya's transport agency. The group posted that it had attacked Kenya because Kenya had "released statements doubting the sovereignty of [the Sudanese] government." Screenshots relating to these attacks are reproduced below. The first image depicts a screenshot and a claim that the train ticket purchasing system in Kenya was rendered unavailable. The second image, titled "Health in Kenya 'Hospitals,'" purports to show several hospitals' websites as unavailable.



12. In August of 2023, the social media platform X (formerly known as Twitter) was hit with attacks also claimed by Anonymous Sudan. The platform was offline in more than a dozen

countries for more than two hours, according to public reporting. The group posted the following message on Telegram: "Make our message reach to [sic] Elon Musk: 'Open Starlink in Sudan.'" "

13. In November 2023, Anonymous Sudan attacked OpenAI, the company that developed the large language model artificial intelligence tool ChatGPT, causing intermittent outages to the platform. Anonymous Sudan claimed responsibility for the attacks and warned of persistent DDoS attacks unless OpenAI modified its chatbot's behavior and dismissed its head of research.

14. On July 4 and 5, 2023, Anonymous Sudan claimed to have attacked a major video game developer and publisher headquartered in Los Angeles. The group posted, "[Company name], we have access to the back end of [game platform], and we can shut down your servers whenever we want... This is all part of our campaign against US companies of all kinds, and serves as a reminder that no company can escape our reach." Employees of the gaming company confirmed that the attacks took place and told me that the attacks caused major disruptions to their platform, specifically impacting a data center in Los Angeles.

15. On July 8 and 9, 2023, the social media sites Tumblr and Flickr were the targets of further attacks claimed by Anonymous Sudan, according to public reporting. Anonymous Sudan posted the following thereafter: "any US company can be a target, no matter who or what company, if it is American we will target it."

16. Anonymous Sudan has also conducted numerous attacks against government agencies in the United States. For example, around October 2023, Anonymous Sudan claimed credit for attacks against the websites for the FBI and the State Department: FBI.gov and State.gov. I have confirmed that these attacks in fact occurred. Screenshots relating to the State Department attacks are reproduced below:

They became afraid | شافوا البل كويس 🤪

<https://www.bleepingcomputer.com/news/security/cisa-issues-ddos-warning-after-attacks-hit-multiple-us-orgs/>


🔥 113 😊 103 👍 83 ❤️ 75 ⚡ 3 🤖 1

👤 1 🗣️ 1

👁️ 22.2K 1:34 PM

Leave a comment >

Anonymous Sudan

 **Anonymous Sudan**
<https://www.cisa.gov/news-events/alerts/202...>

دي الولايات المتحدة الناس البتشهد بيها ؟ مجموعة سودانية صغيرة بقدرات محدودة اجبرت اقوي حكومة في العالم تنزل تغريدات عن هجماتنا ، و حواصل في ضربها و خلي تصريحات وزير الخارجية حقهم تفيدهم و تحميهم

Is this the mighty United States that everyone attests to? A small sudanese group with limited capabilities forced "the most powerful government" in the world to publish articles and tweets about our attacks?


We will continue humiliating you in this campaign and we will see if Anthony Blinken's statements will help you defend from our attacks.

#AnonymousSudan
#FUCK_AnthonyBlinken
#FUCK_USA


June 2

Anonymous Sudan

← Tweet

 **Sprinter**
@sprinter4330

US Secretary of State Antony Blinken indicated that the United States could intervene in Sudan where rival factions are fighting for control of the capital Khartoum.



📄 **US indicates it could intervene in Sudan, imposes sanctions**
US Secretary of State Antony Blinken indicated that the United States could intervene in Sudan where rival factions are fighting for control of the capital.

8:11 PM · June 2, 2023 · 75.6K views

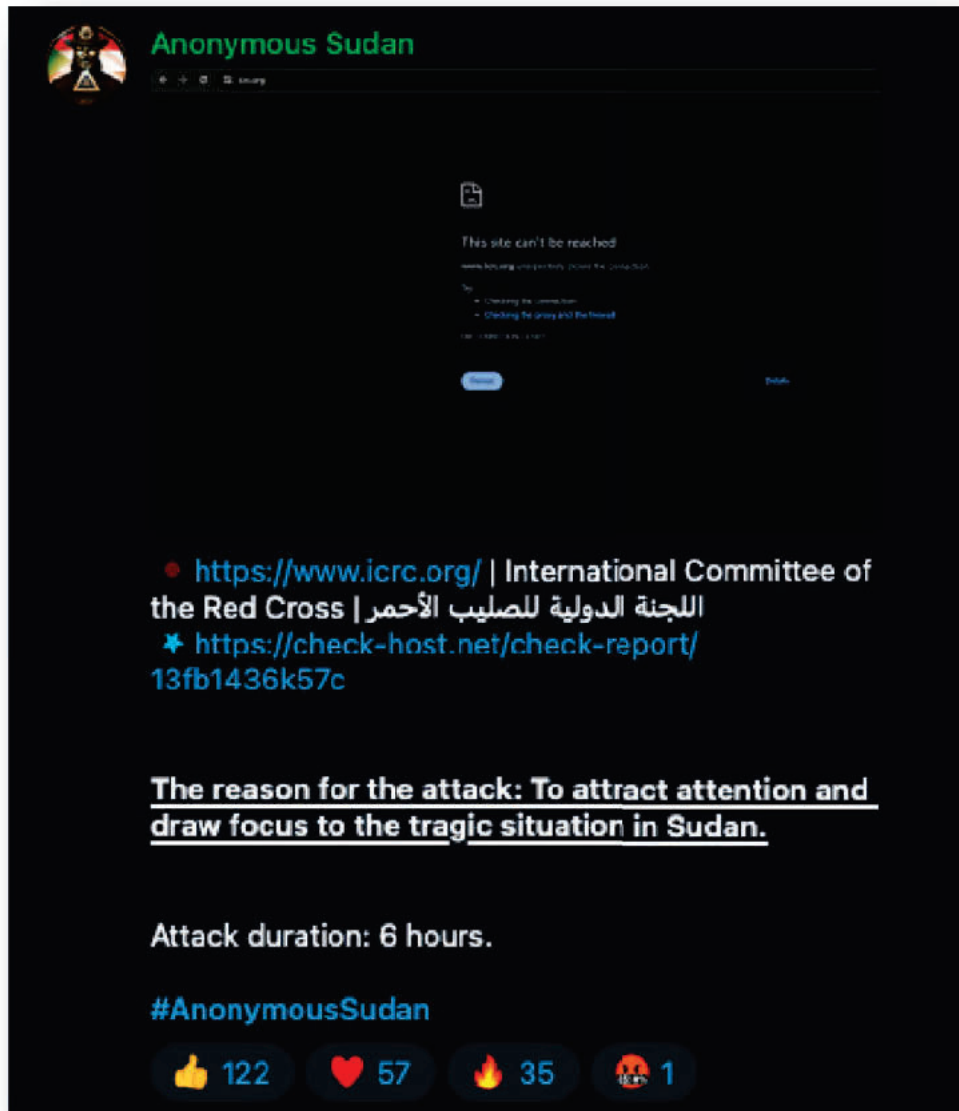
140 Retweets · 58 Quotes · 430 Likes · 11 Replies

وأشار وزير الخارجية الأمريكي أنتوني بلينكين إلى أن الولايات المتحدة قد تتدخل في السودان حيث تتقاتل الفصائل المتناحرة للسيطرة على العاصمة الخرطوم.

! Are you sure of your decision? There would be a warning, surprise attack on the infrastructure of the United States

17. Also in October 2023, Anonymous Sudan claimed credit for attacks against major U.S. and international news outlets, including the Washington Post, the New York Post, CNN, the Daily Mail, the Associated Press, and Fox News. In these attacks, Anonymous Sudan generally provided "proof" of damage in the form of third-party reports indicating that the websites had ceased responding to requests during the time period of the attack. The motivation for this series of attacks was attributed to "Crush," an Anonymous Sudan "spokesperson." Specifically, "Crush" had threatened "in the coming period, we will target any western media outlet that lies and posts false propaganda and news."

18. On December 18, 2023, Anonymous Sudan claimed credit for DDoS attacks against, among others, the International Committee of the Red Cross. A screenshot of this claim, noting the purported reason for the attack and showing the International Red Cross's website as nonresponsive, appears below:



19. On February 16, 2024, Anonymous Sudan announced a series of attacks against a major hospital based in the city of Los Angeles. This attack appeared to last several days. The FBI interviewed employees of the hospital during and after the attack and learned that the attack caused the hospital's website and most of their web services to cease functioning. As a

result of the attack, the hospital was forced to redirect emergency room patients to other hospitals for several hours.

20. Anonymous Sudan has continued their attack activity with no signs of abatement, until today, [REDACTED]

[REDACTED] I am currently monitoring three Telegram channels associated with Anonymous Sudan. The most active, currently titled "Anonymous Sudan - InfraShutdown," is often updated multiple times a day, including as recently as March 20, 2024, and it generally claims credit for attacks against high-profile targets. These frequently include large tech companies, internet service providers, and critical infrastructure associated with countries around the world -- for example, airport websites, telecommunications companies, financial institutions, and government agency webpages.

21. Below is a brief summary of Anonymous Sudan's Telegram postings during March 2024, which is illustrative of the group's wide-ranging and destructive ongoing activities, as well as the general frequency of its attacks and posts:

a. March 1, 2024 - Anonymous Sudan claimed to have launched DDoS attacks against Armenia Telecom Infrastructure, causing an outage. The post includes a screenshot indicating massive disruptions to internet availability within Armenia. In the post, Anonymous Sudan suggested that anyone desiring similar DDoS attack power could subscribe to their "InfraShutdown" service.

b. March 2, 2024 - Anonymous Sudan offered a "Limited Internet Shutdown Package," valid for the following 48

hours, which would enable customers to shut down internet service providers ("ISPs") in specified countries for \$500 (USD) an hour.

c. March 3, 2024 - Anonymous Sudan claimed credit for "Huge Bahrain Telecom Cyber Attack," targeting a prominent Bahrainian ISP called "Zain." Anonymous Sudan posted screenshots and other images to demonstrate the impact of the attacks and the resulting disruptions and damages to the victim. Anonymous Sudan then directly addressed the victim, stating, "Zain, if you want us to stop contact us at InfraShutdown_bot and we can make a deal."

i. I know from my training and experience that this behavior -- soliciting a payment from the DDoS victim in exchange for stopping the attacks -- is referred to as DDoS extortion, which is a common tactic found in the DDoS space, especially for services such as Anonymous Sudan whose attacks generate more traffic than smaller ISPs can withstand.

d. March 4, 2024 - Anonymous Sudan reposted messages from Zain, in which Zain was attempting to explain the disruption to its customers. Anonymous Sudan mocked Zain's response and encouraged Zain to reach out directly to Anonymous Sudan. Anonymous Sudan then posted screenshots seeming to indicate that internet service had been entirely disrupted throughout Zain's network. Later the same day, Anonymous Sudan threatened other ISPs in Bahrain, stating, "The turn is coming up for the rest of the telecom companies in Bahrain... Everyone go back to their offices."

i. I am aware that concurrent to these attacks, U.S. government-contracted internet services within Bahrain were impacted. I am still seeking information from Bahrainian authorities on the extent of the damage resulting from these attacks.

e. March 5, 2024 - Anonymous Sudan provided a screenshot indicating that services were down at Facebook.⁵ Anonymous Sudan then claimed credit for an attack against another major U.S. ISP and provided a link to a news article discussing the attack. Anonymous Sudan also provided an update on the attack against Zain, stating that "we have finally reached a deal with them." Several hours later, Anonymous Sudan claimed to have conducted a "Huge Egypt Telecom Cyber Attack," and began to provide evidence supporting their claims of causing a major disruption to this ISP. Anonymous Sudan also provided a justification for the attack: "to send a message to the Egyptian government that they should hold accountable anyone who insults Sudanese people on social media, just as we do in Sudan to those who insult Egyptians." Interspersed with posts offering proof of the impact and damages resulting from these attacks were solicitations to sign up for the Skynet Botnet service, priced at \$150 per day, with up to 100 attacks per day.

f. March 6, 2024 - Anonymous Sudan claimed credit for attacks against additional ISPs in Egypt.

⁵ I am aware of public reports regarding outages at Facebook around this same time. I was told via a third party that these disruptions were due to internal problems, and not a DDoS attack.

g. March 12, 2024 - Anonymous Sudan posted that they had conducted "a massive cyber-attack on the Infrastructure of the State of Alabama." Media reporting noted that the websites of multiple Alabama State government agencies had been affected, causing intermittent disruptions of those sites and diverting state resources to deal with the attacks.

h. March 15, 2024 - Anonymous Sudan posted, "We have conducted a massive cyber-attack on the infrastructure of a critical US federal executive department: United States Department of Justice," adding, "We therefore claim any damage to the overall health of the infrastructure of the United States Department of Justice." I am aware from speaking with many users within the Department of Justice that its systems were in fact degraded on that date, resulting in inaccessibility to web-based services.

C. Functioning of the "botnet"

22. Among the victims of the Skynet Botnet were several customers using Amazon Web Services. I have interviewed employees at Amazon who examined data associated with Skynet Botnet attacks against Amazon customers. They determined that the attacks were being transmitted not from compromised victim devices, as would ordinarily be the case with a botnet, but from devices that were configured to automatically forward certain categories of Internet traffic. Also called "Open Proxy Resolvers," these "auto-forwarding" devices comprise the public part of the Skynet Botnet, and they were often the only information a Skynet Botnet attack victim would see in their

network data. Amazon employees determined that these devices were actually receiving commands from an array of cloud-based servers, many of which were hosted at a U.S. server-hosting provider.

23. Based upon my interviews and examination of records provided by the U.S. server-hosting provider and Google, I believe the Skynet Botnet is not actually a botnet, but rather a "Distributed Cloud Attack Tool," or DCAT, consisting of three principal components: (1) a C2, (2) a fleet of cloud-based servers that receive commands from the C2 server and forward them to (3) an array of open proxy resolvers run by unaffiliated third parties, which transmit the DDoS attack data to the victims.

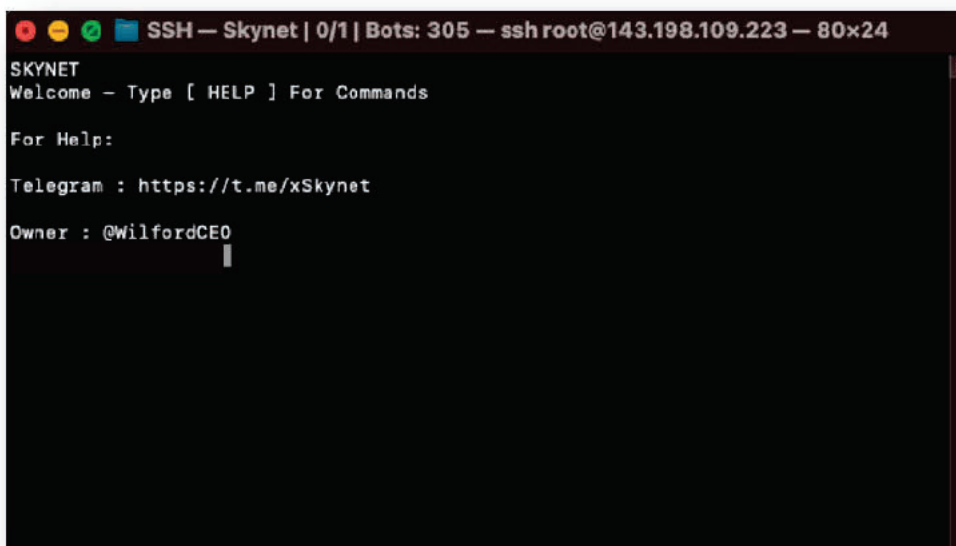
D. Undercover Use of DDoS Tool

24. To evaluate the use of the Skynet Botnet/DCAT to paying customers, in addition to its use by the Anonymous Sudan group for its hacktivist aims, I conducted an undercover purchase of the tool. The "Skynet" Telegram channel, which advertises the Skynet DDoS tool, references contacting an individual using the handle "WilfordCEO." Accordingly, I directed a cooperating witness⁶ to communicate with WilfordCEO regarding obtaining access to the Skynet DDoS tool. WilfordCEO initially quoted a price of \$700 for one week of access, but

⁶ [REDACTED]

after negotiation, he agreed to accept payment of \$600 via bitcoin. In the exchange, the cooperating witness asked WilfordCEO if the cooperating witness was buying access to Skynet or the Godzilla botnet. WilfordCEO replied, "all same," confirming my understanding that these names are used interchangeably to refer to the same DDoS tool. WilfordCEO assured the cooperating witness that the attack methods were "strong." When told that we intended to attack major platforms like Google and Amazon, WilfordCEO replied that the best attack method would be "overload."

25. After the cooperating witness provided WilfordCEO with a proposed username and password, WilfordCEO replied with the message "193.149.180.43 221 ssh." Based on my training and experience, I understood that WilfordCEO was indicating that the cooperating witness should log in to the referenced IP address, using Secure Shell Protocol (SSH), via port 221. Accordingly, I did so, entering the login and password credentials that were previously provided to WilfordCEO. Upon logging in, I was greeted with a text-based landing page that I recognized from previous Anonymous Sudan and Skynet Telegram posts. A screenshot of this landing page appears below:



```
SSH — Skynet | 0/1 | Bots: 305 — ssh root@143.198.109.223 — 80x24
SKYNET
Welcome - Type [ HELP ] For Commands

For Help:

Telegram : https://t.me/xSkynet

Owner : @WilfordCEO
```

26. I then proceeded to use this service to launch DDoS attacks against servers I had specially configured to record the results of the attacks. After conducting the test attacks, I worked with others to examine the attack traffic. From a packet-per-second perspective, which is a measurement of the relative speed of data traffic flowing to a web server, the attacks were incredibly powerful relative to other attacks I have seen in my experience investigating DDoS. Additionally, we were able to determine that servers located in the Central District of California were participating in the attacks.

27. I subsequently obtained a copy of the server to which WilfordCEO had directed me to log in, the Skynet server used in the testing above, pursuant to a search warrant. From review of that information, I uncovered logs related to the operation of Anonymous Sudan and the Skynet service, particularly, login and other records of administration, as well as a database containing data on attacks launched with the Skynet service. In

many cases, I was able to correlate attacks launched by the Administrator, or "root" account, to actual attacks claimed by Anonymous Sudan in their Telegram account, including many of the attacks described above. This also confirmed my understanding that WilfordCEO is one of the actors behind Anonymous Sudan. I was additionally able to locate my covert account, and a listing of the attacks that I had launched during my covert testing of the service, confirming that the database contained accurate data. In total, this data indicated that in approximately one year of operation, Anonymous Sudan's Skynet DDoS tool had been used to launch over 35,000 DDoS attacks. At least 70 unique IP addresses within Los Angeles County alone were attacked during this same one-year period.

E. Identification of AHMED

28. During my investigation, I have consulted with various private sector companies, including companies such as PayPal that were attacked by Anonymous Sudan. In an interview with PayPal employees, I learned that after PayPal performed its own independent investigation of Anonymous Sudan in the wake of the DDoS attacks it suffered, PayPal identified certain accounts on its platform that it believed were likely used by Anonymous Sudan actors. I obtained records related to the email accounts linked to these PayPal accounts. Those records led me to identify several email accounts used by AHMED.

29. I have reviewed administrative login information from the various Anonymous Sudan servers I have searched, and I found many instances when administrator logins to Anonymous Sudan

servers were made by someone using the same IP addresses, at roughly the same times, as were used to log in to the email accounts associated with AHMED. Based on my training and experience and knowledge of this investigation, I understand that this kind of extensive IP address overlap indicates that AHMED is an Anonymous Sudan administrator.

30. For example, log fragments I exported from a memory capture of the Skynet server I obtained pursuant to a search warrant depict that on December 31, 2023, the "root" user (*i.e.*, the administrator of Anonymous Sudan) logged in from IP address 41.95.11.113. Approximately six seconds after logging in, this user issued a DDoS attack command. Approximately 20 minutes prior, this same IP was used to access Google services from an email account which AHMED had access to, as explained further below. The IP address is associated with a mobile telecom provider located in Sudan, which is where my records indicate AHMED was located at that same time.

31. Similarly, on January 3, 2024, IP address 41.95.87.244 was used to log in to the "root" account on the Skynet server, at approximately 13:44 UTC. A screenshot of this log appears below:

```
succubus -> 2024/01/03 13:44:48 [root:Login] 41.95.87.244:9717
succubus -> 2024/01/03 13:44:48 [root:Login] 41.95.87.244:9717
succubus -> 2024/01/03 13:45:01 [root:Command] !http-majesty_skynet
https://beta.goldendragon888.net/app/transactions/ 80 300
```

32. This IP address is assigned to the same Sudanese mobile telecom provider referenced above. Google records depict the same pattern as previously described; that is, accounts associated with AHMED access Google services immediately before and after the Skynet logins, using the same IP addresses. An example is depicted in the screenshot below, which shows access to Google services from this same IP address on the same date and almost contemporaneously with the root Skynet logins:

2024-01-03 13:53:41 UTC	41.95.87.244
2024-01-03 13:53:40 UTC	41.95.87.244
2024-01-03 13:52:48 UTC	41.95.87.244
2024-01-03 13:52:43 UTC	41.95.87.244
2024-01-03 13:26:46 UTC	41.95.87.244
2024-01-03 13:26:46 UTC	41.95.87.244
2024-01-03 13:26:45 UTC	41.95.87.244
2024-01-03 13:26:45 UTC	41.95.87.244

This pattern is reflected across the various Anonymous Sudan servers I have examined; where I can find an example of an administrator login to an Anonymous Sudan server, that same IP address is often associated with access to Google services, at roughly the same time, by AHMED.

33. Based on this and other information, I obtained search warrants for numerous email accounts used by AHMED. I found evidence in these accounts confirming his identity, including identification documents such as passports, school transcripts,

agreed to waive those rights and speak with me. During the interview, among other things, the sibling stated that he was familiar with the "Godzilla" DDoS tool (one of the alternative names for the Skynet Botnet, as previously described), which employs back-end code that he wrote, and he claimed that AHMED is primarily responsible for that tool, which AHMED operates using a laptop computer from, among other places, their shared home in Sudan.

36. Prior to my interview with the sibling, I had observed a post by Anonymous Sudan on Telegram threatening to conduct a DDoS attack against the United Arab Emirates. Approximately an hour into the interview, I observed a new message posted in the Anonymous Sudan Telegram channel stating that the attack had started. I do not believe that the sibling could have initiated this attack, as I was interviewing the sibling during the time the attack began. Shortly after, I asked the sibling to communicate telephonically with AHMED. The sibling communicated with AHMED in Arabic (a language that I do not speak). The sibling then informed me that he had asked AHMED to stop the attack, and that the attack in fact had been stopped, and the corresponding Anonymous Sudan Telegram post had been deleted. I have not yet independently verified the attack against the United Arab Emirates; however, based on my training and experience, AHMED's apparent ability to end the attack, and his apparent deletion of the Telegram post, provides further evidence of his use and control of the Skynet Botnet, and his control over Anonymous Sudan's Telegram channel.

G. Interview of AHMED

37. On March 20, 2024, after interviewing AHMED's sibling, I then interviewed AHMED [REDACTED]

[REDACTED] AHMED was advised of his Miranda rights and agreed to waive those rights and speak to me. During the interview, among other things, AHMED admitted that he was the individual behind the moniker WilfordCEO (with whom I communicated to purchase access to the Skynet Botnet, as previously described), and that he was involved with the administration of the Skynet Botnet and Anonymous Sudan.

V. CONCLUSION

38. For the reasons described above, there is probable cause to believe that AHMED has violated 18 U.S.C. § 371, Conspiracy to violate 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I) and (VI) (Intentionally Damaging a Protected Computer).

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 20th day of March, 2024.



HONORABLE STEVE KIM
UNITED STATES MAGISTRATE JUDGE