



UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2024 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

AHMED SALAH YOUSIF OMER,
aka "WilfordCEO,"
aka "Zac,"
aka "Soldi01,"
ALAA SALAH YUSUUF OMER,

Defendants.

CR No. 2:24-cr-00614-MEMF

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(B)(ii) (c)(4)(A)(i)(I), (II), (III), (IV), (V), (VI), (c)(4)(E), (c)(4)(F): Unauthorized Impairment of a Protected Computer; 18 U.S.C. §§ 981(a)(1)(C), 982, 1030, and 28 U.S.C. § 2461(c): Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this Indictment:

A. The Conspiracy and Defendants

1. Anonymous Sudan was a group that conducted distributed denial of service, or "DDoS," attacks against governments, companies, and infrastructure to impair the functioning of the victims' computers and/or networks. Members of Anonymous Sudan also sold the tools used to conduct these attacks to other individuals for a fee.

1 2. Defendant AHMED SALAH YOUSIF OMER ("AHMED OMER"), also
2 known as ("aka") "WilfordCEO," aka "Zac," aka "Soldi01," was a
3 Sudanese national.

4 3. Defendant ALAA SALAH YUSUUF OMER ("ALAA OMER") was a
5 Sudanese national.

6 4. Unindicted co-conspirators 1, 2, and 3 ("UICC 1," "UICC 2,"
7 and "UICC 3") were members of Anonymous Sudan. The identities of
8 UICC 1 and UICC 2 are known to the Grand Jury.

9 5. Members of Anonymous Sudan conducted DDoS attacks using
10 tools called, at various times, "Godzilla Botnet," "SkyNet," and
11 "InfraShutdown." These tools relied upon large numbers of proxy
12 devices, which relayed attack commands and associated network traffic
13 from Anonymous Sudan's command-and-control server to the victim
14 computers.

15 6. Members of Anonymous Sudan also claimed to conduct computer
16 compromise and data theft attacks and would extort victims for the
17 return of the data or offer to sell the data to third parties.
18 Members of Anonymous Sudan also claimed to similarly extort some of
19 their DDoS victims in exchange for cessation of the DDoS attacks.

20 7. Anonymous Sudan had several Telegram channels in which they
21 posted information about their attacks, their DDoS tools and pricing,
22 and their victims. One of these channels was called "Anonymous
23 Sudan" and later "Anonymous Sudan - @InfraShutdown"; another was
24 called "SkyNet/Godzilla-BotNet." These channels had, at various
25 times, as many as 80,000 subscribers.

26 8. Defendant AHMED OMER, UICC 1, or other Anonymous Sudan
27 members with administrative privileges on the Telegram channels used
28 those channels to claim credit for hundreds of DDoS and other cyber-

1 attacks on government entities, hospitals, health care organizations,
2 law enforcement, financial institutions, and critical infrastructure
3 in numerous countries, including but not limited to the United
4 States, Sweden, the Netherlands, Germany, Denmark, France, Poland,
5 Australia, Israel, Sudan, Saudi Arabia, India, Egypt, Ethiopia,
6 Ukraine, the United Arab Emirates, Kenya, Nigeria, Chad, the United
7 Kingdom, Bahrain, South Africa, and Armenia.

8 B. Definitions

9 9. A DDoS attack is a type of computer-based attack in which
10 an Internet-connected victim computer is flooded with data and/or
11 queries in such a manner to render it unable to communicate with
12 other devices on the Internet or to perform the services which it is
13 intended to perform.

14 10. Anonymous Sudan's command-and-control (or C2) server was
15 connected to the Internet and used to initiate DDoS attacks.

16 11. Telegram is a cloud-based encrypted messaging service that
17 allows users to post messages in public channels and message other
18 users directly.

19 12. Check Host (check-host.net) is a service that allowed users
20 to create a report indicating whether an Internet-based service was
21 functional at a particular time.

COUNT ONE

[18 U.S.C. § 371]

[ALL DEFENDANTS]

The Grand Jury hereby realleges and incorporates paragraphs 1 through 12 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECTS OF THE CONSPIRACY

Beginning no later than January 2023, and continuing to on or about March 20, 2024, in Los Angeles County, within the Central District of California, and elsewhere, defendants AHMED OMER, ALAA OMER, UICC 1, UICC 2, UICC 3, and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and specifically:

a. to cause loss to one or more persons during a one-year period aggregating at least \$5,000 in value, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I);

b. to cause the modification, impairment, and potential modification or impairment of the medical examination, diagnosis, treatment, and care of one or more individuals, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(II);

c. to cause physical injury to any person, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(III);

1 d. to cause a threat to public health or safety, in
2 violation of Title 18, United States Code, Section 1030(a)(5)(A),
3 (c)(4)(B)(i), (c)(4)(A)(i)(IV);

4 e. to cause damage affecting a computer used by or for an
5 entity of the United States Government in furtherance of the
6 administration of justice, national defense, or national security, in
7 violation of Title 18, United States Code, Section 1030(a)(5)(A),
8 (c)(4)(B)(i), (c)(4)(A)(i)(V);

9 f. to cause damage affecting ten or more protected
10 computers during a one-year period, in violation of Title 18, United
11 States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI);

12 g. to attempt to cause and knowingly and recklessly cause
13 serious bodily injury, in violation of Title 18, United States Code,
14 Section 1030(a)(5)(A), (c)(4)(E);

15 h. to attempt to cause and knowingly and recklessly cause
16 death, in violation of Title 18, United States Code, Section
17 1030(a)(5)(A), (c)(4)(F); and

18 i. to transmit in interstate and foreign commerce, with
19 the intent to extort money and other things of value, a communication
20 containing (i) a threat to cause damage to a protected computer, and
21 (ii) a demand and request for money and other things of value in
22 relation to damage to a protected computer, where such damage was
23 caused to facilitate the extortion, in violation of Title 18, United
24 States Code, Section 1030(a)(7)(A), (C), (c)(3)(A).

25 B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE
26 ACCOMPLISHED

27 The objects of the conspiracy were to be accomplished, in
28 substance, as follows:

1 1. Defendant AHMED OMER, UICC 1, and UICC 2 would set up and
2 operate the DDoS attack infrastructure for Anonymous Sudan.

3 2. Defendant AHMED OMER and UICC 1 would use this attack
4 infrastructure to direct DDoS attacks to websites and Internet-
5 connected services around the world to degrade or disrupt their
6 functionality.

7 3. Defendant AHMED OMER and UICC 1 would post messages on
8 Telegram in channels they controlled claiming credit for these
9 attacks, often providing proof of their efficacy in the form of Check
10 Host reports showing that the victim computers were offline.

11 4. Defendant ALAA OMER would provide computer code and
12 programming support to assist with the operation of Anonymous Sudan's
13 attack infrastructure, including code used to enable communication
14 among servers employed to conduct DDoS attacks.

15 5. UICC 2 would develop and provide one of the DDoS attack
16 tool sets used by Anonymous Sudan, referred to as "SkyNet."

17 6. UICC 3 would act as a public affairs spokesperson for
18 Anonymous Sudan who would amplify Anonymous Sudan's cyberattacks in
19 close coordination with the group's other members.

20 7. Defendant AHMED OMER, UICC 1, and UICC 3 would also
21 advertise the use of their attack infrastructure to paying customers
22 via their Telegram channels, including by adding their contact
23 information to the end of their posts claiming successful attacks.
24 These advertisements included information about features,
25 subscription lengths, and pricing for various subscriptions.

26 8. If a customer indicated interest in paying for use of the
27 attack infrastructure, defendant AHMED OMER would negotiate a price
28 with the customer, and upon receipt of payment, would provide server

1 credentials allowing the buyer to launch DDoS attacks.

2 C. OVERT ACTS

3 In furtherance of the conspiracy and to accomplish its objects,
4 on or about the following dates, defendants AHMED OMER, ALAA OMER,
5 UICC 1, UICC 2, UICC 3, and others, committed various overt acts
6 within the Central District of California, and elsewhere, including
7 but not limited to the following:

8 **Creation of Attack Infrastructure & Communications Channels**

9 Overt Act No. 1: On January 9, 2023, defendant AHMED OMER or
10 another co-conspirator created the Telegram channel "Skynet/Godzilla-
11 botnet."

12 Overt Act No. 2: On January 18, 2023, defendant AHMED OMER or
13 another co-conspirator posted a message on Telegram stating, "We will
14 attack any country with Cyber attacks against those who oppose
15 Sudan."

16 Overt Act No. 3: Beginning on an unknown date no later than
17 February 2, 2023, and continuing until March 2024, defendant ALAA
18 OMER developed and maintained a websocket architecture, called WS-
19 API, with an attached comment reading "Websocket API for Ahmed's
20 server. Coded with love by: "Alaa Sala" [@alaaelrefaie]," which he
21 transmitted to defendant AHMED OMER. This software was maintained
22 via a GitHub repository and operated on various Anonymous Sudan
23 servers, performing essential functions in coordinating communication
24 among the servers as part of Anonymous Sudan's attack infrastructure.

25 **Attacks on the United States**

26 Attacks on the U.S. Government

27 Overt Act No. 4: On February 3, 2023, defendant AHMED OMER
28 sent a series of private messages on Telegram with a link to a

1 particular U.S. Central Intelligence Agency website and stated, in
2 part, "hit here, my servers got ban[ned]."

3 Overt Act No. 5: On February 3, 2023, defendant AHMED OMER
4 sent a private message on Telegram stating "cia.gov, go hit, I can
5 check if down."

6 Overt Act No. 6: On April 25, 2023, defendant AHMED OMER or
7 another co-conspirator posted a message on Telegram stating, "We
8 declare cyber war on the United States, The United States will be our
9 primary target."

10 Overt Act No. 7: On April 27, 2023, defendant AHMED OMER or
11 another co-conspirator posted a message on Telegram stating, "The
12 United States must be prepared, it will be a very big attack, like
13 what we did in Israel, we will do in United States 'soon'."

14 Overt Act No. 8: On April 28 and 29, 2023, defendant AHMED
15 OMER sent private messages on Telegram to coordinate DDoS attacks
16 targeting U.S. airports. Defendant AHMED OMER stated, "I am carrying
17 out an organized attack on the United States. We can target the
18 airport." Defendant AHMED OMER then provided a list of airport
19 websites including jfkairport.com, flysfo.com, and others.

20 Overt Act No. 9: On April 28, 2023, defendant AHMED OMER or
21 another co-conspirator posted a message on Telegram indicating that
22 they had attacked the Hartsfield-Jackson Atlanta International
23 Airport, together with Check Host report links indicating that the
24 airport's website was offline.

25 Overt Act No. 10: On June 5, 2023, defendant AHMED OMER or
26 another co-conspirator posted a message on Telegram stating, "This is
27 a continuous campaign against US/American companies & infrastructure
28 because of the statement of the US Secretary of State saying there is

1 a possibility of American invasion of Sudan."

2 Overt Act No. 11: On October 7, 2023, defendant AHMED OMER
3 sent a Telegram private message to another user stating "im going to
4 hold <https://defense.gov>."

5 Overt Act No. 12: From October to November 2023, defendant
6 AHMED OMER or another co-conspirator, using the Anonymous Sudan C2
7 server, initiated multiple attacks on the website defense.gov.

8 Overt Act No. 13: From October to November 2023, defendant
9 AHMED OMER or another co-conspirator, using the Anonymous Sudan C2
10 server, initiated attacks against State Department websites.

11 Overt Act No. 14: On October 19 and 20, 2023, defendant AHMED
12 OMER or another co-conspirator, using the Anonymous Sudan C2 server,
13 initiated an attack against the Federal Bureau of Investigation
14 website at fbi.gov/how-can-we-help-you.


15 Overt Act No. 15: On October 19, 2023, AHMED OMER sent private
16 messages on Telegram containing screenshots of logs depicting the
17 Anonymous Sudan C2 server conducting the attack against the Federal
18 Bureau of Investigation.

19 Overt Act No. 16: On October 20, 2023, defendant AHMED OMER or
20 another co-conspirator posted a message on Telegram indicating that
21 they had attacked the website for the Federal Bureau of
22 Investigation, together with a Check Host report link indicating that
23 the website was offline.

24 Overt Act No. 17: On March 12, 2024, defendant AHMED OMER or
25 another co-conspirator, using the Anonymous Sudan C2 server,
26 initiated attacks on various government networks for the State of
27 Alabama, including alabama.gov and alea.gov. These attacks caused
28 widespread outages to information systems throughout Alabama.

1 Overt Act No. 18: On March 12, 2024, defendant AHMED OMER or
2 another co-conspirator posted a message on Telegram stating, "We have
3 conducted a massive cyber attack on the infrastructure of the State
4 of Alabama, United States." The post went on to name specific
5 affected agencies, including the Alabama Law Enforcement Agency, the
6 State of Alabama, Alabama's Office of Information Technology, and the
7 Alabama Supercomputer Authority.

8 Overt Act No. 19: On March 15, 2024, defendant AHMED OMER or
9 another co-conspirator conducted a DDoS attack using Anonymous
10 Sudan's infrastructure against the web-based systems of the U.S.
11 Department of Justice, causing connectivity outages and resulting in
12 serious disruptions to various services, across Department of Justice
13 networks spanning the United States.

14 Overt Act No. 20: On March 15, 2024, defendant AHMED OMER or
15 another co-conspirator posted a message on Telegram stating, "We've
16 launched a massive cyber attack on the infrastructure of an important
17 U.S. federal executive  United States Department of Justice ...This
18 attack was fully carried out by @InfraShutdown DDoS infrastructure//
19 ...Therefore, we demand any damage to the infrastructure of the U.S.
20 Department of Justice."

21 Attacks on U.S. Healthcare Providers

22 Overt Act No. 21: On February 1, 2023, defendant AHMED OMER
23 sent private messages on Telegram asking how to "find" all health
24 sites in a given country, explaining that he wanted all "health sites
25 in one country."

26 Overt Act No. 22: On February 16, 2024, defendant AHMED OMER
27 or another co-conspirator, using the Anonymous Sudan C2 server,
28 initiated an attack on Cedars-Sinai Hospital in the Los Angeles area,

1 affecting multiple systems and causing emergency services and
2 patients to be temporarily re-routed to different hospitals.
3 Targeted domains included www.cedars-sinai.org/find-a-doctor.html and
4 www.cedars-sinai.org/mycslink.html, which was the hospital's patient
5 portal service.

6 Overt Act No. 23: On February 16, 2024, defendant AHMED OMER
7 or another co-conspirator posted a message on Telegram stating, "BIG
8 US HEALTH CYBER ATTACK !! We have executed a major cyber attack on
9 the infrastructure of one the biggest hospitals in the US: 🇺🇸 Cedars-
10 Sinai Health Systems... We therefore claim any damage to the hospital
11 Cedars-Sinai and their health systems + any collateral damage."

12 Overt Act No. 24: On February 16, 2024, defendant AHMED OMER
13 sent a private Telegram message to a Telegram user containing a
14 screenshot of connections to various Cedars-Sinai subdomains and
15 third-party resources, indicating that many of these hospital-related
16 services were now closed.

17 Overt Act No. 25: On February 17, 2024, defendant AHMED OMER
18 or another co-conspirator posted a message on Telegram stating, "3
19 hours+ and still holding, they're trying desperately to fix it but to
20 no avail Bomb our hospitals in Gaza, we shut down yours too, eye for
21 eye..."

22 Attacks on U.S. Companies

23 Overt Act No. 26: On March 18, 2023, defendant AHMED OMER,
24 using the Anonymous Sudan C2 server, initiated an attack against
25 numerous IP addresses, including IP addresses owned by Google.

26 Overt Act No. 27: On April 15, 2023, defendant AHMED OMER sent
27 a private message on Telegram stating, "I need down Google llc, l4,
28 but I can't. Can you help me?"

1 Overt Act No. 28: On June 30, 2023, defendant AHMED OMER or
2 another co-conspirator used the Anonymous Sudan attack infrastructure
3 to attack financial services company Stripe. The attack impaired
4 Stripe's network for at least two hours.

5 Overt Act No. 29: On June 30, 2023, defendant AHMED OMER or
6 another co-conspirator posted a message on Telegram indicating that
7 Anonymous Sudan had attacked Stripe, stating, "It is an Irish-
8 American financial services and software company as a service
9 company," together with a Check Host report link indicating that the
10 service was offline.

11 Overt Act No. 30: From July 2, 2023, through July 5, 2023,
12 defendant AHMED OMER or another co-conspirator used the Anonymous
13 Sudan attack infrastructure to attack servers controlled by Riot
14 Games, causing significant disruptions to their services.

15 Overt Act No. 31: On July 2, 2023, defendant AHMED OMER or
16 another co-conspirator posted a message on Telegram indicating that
17 Anonymous Sudan had attacked Riot Games, noting, "Login is down."

18 Overt Act No. 32: On July 5, 2023, defendant AHMED OMER or
19 another co-conspirator posted a message on Telegram stating, "Riot
20 games, we reached the backend of league of legends and anytime we
21 want we can shut down your servers...All of this is part of our
22 campaign targeting American companies of all sorts, this is to remind
23 everyone that no company is out of our radar and we can target
24 anything."

25 Overt Act No. 33: On July 5, 2023, defendant AHMED OMER or
26 another co-conspirator posted a message on Telegram stating, "Riot
27 Games, Inc. It is an American video game developer, publisher, and
28 eSports tournament organizer | You cannot join any game, the game has

1 been down[ed]."

2 Overt Act No. 34: On July 5, 2023, defendant AHMED OMER sent
3 Telegram private messages to Telegram user "Ghost Killer" asking for
4 assistance with a DDoS attack targeting a Riot Games website.

5 Overt Act No. 35: On July 16, 2023, and November 3, 2023,
6 defendant AHMED OMER or another co-conspirator, using Anonymous
7 Sudan's attack infrastructure, initiated attacks against PayPal.

8 Overt Act No. 36: On July 16, 2023, defendant AHMED OMER or
9 another co-conspirator posted a message on Telegram stating, "PayPal,
10 We have an appointment with you soon, This was only a 30-second test
11 attack," together with a Check Host report link indicating that the
12 service was offline.

13 Overt Act No. 37: On September 21, 2023, defendant AHMED OMER
14 or another co-conspirator, using Anonymous Sudan's C2 server,
15 initiated an attack against threat-intelligence company
16 Falconfeedsio.

17 Overt Act No. 38: On September 21, 2023, defendant AHMED OMER
18 or another co-conspirator posted a message on Telegram that stated,
19 "Falconfeedsio, would you like more? All of this is just testing. We
20 are preparing to handle over 100 million requests per second. We'll
21 see if [DDoS protection company name] can mitigate[] it :)."

22 Overt Act No. 39: On September 22, 2023, defendant AHMED OMER
23 or another co-conspirator posted a message on Telegram saying,
24 "Godzilla-Botnet is back on top...Coming soon, Google :)!"

25 Overt Act No. 40: On September 22, 2023, defendant AHMED OMER
26 or another co-conspirator, using Anonymous Sudan's C2 server,
27 initiated attacks against Google.com and the Google Play Store.

28 Overt Act No. 41: On September 24, 2023, defendant AHMED OMER

1 or another co-conspirator, using Anonymous Sudan's C2 server,
2 initiated an attack against online gaming platform Steam.

3 Overt Act No. 42: On September 24, 2023, defendant AHMED OMER
4 or another co-conspirator posted a message on Telegram stating that
5 Steam was "strongly down by skynet / Godzilla-Botnet /
6 AnonymousSudan," together with Check Host report links indicating
7 that the service was offline.

8 Overt Act No. 43: On September 29, 2023, defendant AHMED OMER
9 or another co-conspirator, using Anonymous Sudan's C2 server,
10 initiated an attack against the video streaming service Hulu.

11 Overt Act No. 44: On September 29, 2023, defendant AHMED OMER
12 or another co-conspirator posted a message on Telegram saying, "Hulu
13 is strongly down by skynet / Godzilla-Botnet / AnonymousSudan,"
14 together with a Check Host report link indicating that the service
15 was offline.

16 Overt Act No. 45: On September 29, 2023, defendant AHMED OMER
17 or another co-conspirator, using Anonymous Sudan's C2 server,
18 initiated an attack against Netflix.

19 Overt Act No. 46: On September 29, 2023, defendant AHMED OMER
20 or another co-conspirator posted a message on Telegram stating,
21 "Netflix is strongly down by Skynet / Godzilla-Botnet /
22 AnonymousSudan" and noting that the reason for the attack was "[d]ue
23 to the content of their movies. "LGBTQIA+" together with a Check
24 Host report link indicating that the service was offline.

25 Overt Act No. 47: On October 21, 2023, defendant AHMED OMER
26 sent a private message on Telegram containing screenshots of logs
27 depicting Anonymous Sudan's C2 server conducting attacks against the
28 ride-sharing platform Lyft.

1 Overt Act No. 48: On October 27 and 28, 2023, defendant AHMED
2 OMER or another co-conspirator, using Anonymous Sudan's C2 server,
3 initiated an attack against CNN at the site edition.cnn.com.

4 Overt Act No. 49: On October 27 and 28, 2023, defendant AHMED
5 OMER sent private messages on Telegram containing screenshots of logs
6 depicting Anonymous Sudan's C2 server conducting the attack on
7 edition.cnn.com.

8 Overt Act No. 50: On October 28, 2023, defendant AHMED OMER or
9 another co-conspirator posted messages on Telegram indicating that
10 Anonymous Sudan had attacked CNN.com, together with a Check Host
11 report link indicating that the website was offline, and then
12 stating, "The attack has been restarted again. 'CNN DOWN'."

13 Overt Act No. 51: On October 28, 2023, defendant AHMED OMER or
14 another co-conspirator, using the Anonymous Sudan C2 server,
15 initiated an attack against The Washington Post.

16 Overt Act No. 52: On October 28, 2023, defendant AHMED OMER
17 sent private messages on Telegram containing screenshots of logs
18 depicting Anonymous Sudan's C2 server conducting the attack on The
19 Washington Post.

20 Overt Act No. 53: On October 31, 2023, defendant AHMED OMER or
21 another co-conspirator, using the Anonymous Sudan C2 server,
22 initiated an attack against the Associated Press.

23 Overt Act No. 54: On October 31, 2023, defendant AHMED OMER
24 sent private messages on Telegram containing screenshots of logs
25 depicting Anonymous Sudan's C2 server conducting the attack on the
26 Associated Press.

27 Overt Act No. 55: On November 1, 2023, defendant AHMED OMER or
28 another co-conspirator posted on Telegram that Anonymous Sudan had

1 attacked the Associated Press for six hours, together with a Check
2 Host report link indicating that the news outlet's website was
3 offline.

4 Overt Act No. 56: On November 2, 2023, defendant AHMED OMER or
5 another co-conspirator, using Anonymous Sudan's C2 server, initiated
6 an attack against Yahoo News.

7 Overt Act No. 57: On November 2, 2023, defendant AHMED OMER
8 sent private messages on Telegram containing screenshots of logs
9 depicting Anonymous Sudan's C2 server conducting the attack on Yahoo
10 News.

11 Overt Act No. 58: On November 3, 2023, defendant AHMED OMER or
12 another co-conspirator posted messages on Telegram indicating that
13 Anonymous Sudan had attacked Yahoo, together with two Check Host
14 report links indicating that the service was offline.

15 Overt Act No. 59: On November 4, 2023, defendant AHMED OMER or
16 another co-conspirator, using the Anonymous Sudan C2 server,
17 initiated an attack against the commercial retailer Target.

18 Overt Act No. 60: On November 4, 2023, defendant AHMED OMER
19 sent private messages on Telegram containing screenshots of logs
20 depicting Anonymous Sudan's C2 server conducting the attack on
21 Target.

22 Overt Act No. 61: On November 5, 2023, defendant AHMED OMER or
23 another co-conspirator posted a message on Telegram indicating that
24 Anonymous Sudan had attacked Target, together with two Check Host
25 report links indicating that the company's website was offline.

26 Overt Act No. 62: From November 7, 2023, through November 8,
27 2023, defendant AHMED OMER or another co-conspirator conducted DDos
28 attacks via Anonymous Sudan's server against servers controlled by

OpenAI, causing significant disruption to OpenAI's ChatGPT service.

Overt Act No. 63: On November 8, 2023, defendant AHMED OMER or another co-conspirator posted a message on Telegram indicating that Anonymous Sudan had attacked OpenAI's ChatGPT service, and that some functions in ChatGPT had stopped working after the attack.

Overt Act No. 64: On November 8, 2023, defendant AHMED OMER or another co-conspirator posted on Telegram that the link for ChatGPT was now "completely dead now worldwide."

Overt Act No. 65: On November 8, 2023, defendant AHMED OMER or another co-conspirator posted a message on Telegram stating, "OpenAI / ChatGPT, learn from Microsoft, we fucked them up and down continuously until they admit it's our attack by force, in the same way we will force you to admit it's a DDoS attack like dogs."

Overt Act No. 66: On November 9, 2023, defendant AHMED OMER or another co-conspirator, using the Anonymous Sudan C2 server, initiated attacks against the DDoS-protection service Cloudflare.

Overt Act No. 67: On November 9, 2023, defendant AHMED OMER or another co-conspirator posted a message on Telegram stating, "Cloudflare is strongly down by Skynet / Godzilla-Botnet / Anonymous Sudan," together with a Check Host report link indicating that the CloudFlare service was offline.

Overt Act No. 68: On January 1, 2024, defendant AHMED OMER or a co-conspirator, using Anonymous Sudan's C2, launched DDoS attacks against several corporate victims, including Reddit, Steam, GitHub, VirusTotal, and OVH.

Overt Act No. 69: On January 6, 2024, defendant AHMED OMER or a co-conspirator, using Anonymous Sudan's C2, launched a DDoS attack against api.x.ai, the website corresponding to X's "Grok" Artificial

1 Intelligence tool.

2 Attacks on Microsoft

3 Overt Act No. 70: From June 5, 2023, to June 9, 2023,
4 defendant AHMED OMER or another co-conspirator, using the Anonymous
5 Sudan C2 server, initiated a series of attacks against servers
6 controlled by Microsoft Corporation, including Microsoft's Outlook
7 webmail service, causing substantial disruption to Microsoft's
8 services.

9 Overt Act No. 71: On June 5, 2023, defendant AHMED OMER or
10 another co-conspirator posted messages on Telegram indicating that
11 they were attacking the Microsoft Outlook webmail service, together
12 with Check Host report links indicating that the service was offline.

13 Overt Act No. 72: On June 5, 2023, defendant AHMED OMER or
14 another co-conspirator posted a message on Telegram stating, in part,
15 "Microsoft, the fate of your services is under our hands, we decide
16 when to shut it down and when to leave it open. Today, almost all of
17 your major services were down for over 1.5 hours...We can target any
18 US Company we want. Americans, do not blame us, blame your
19 government for thinking about intervening in Sudanese internal
20 affairs. We will continue to target large US companies, government
21 and infrastructure."

22 Overt Act No. 73: On June 5, 2023, defendant AHMED OMER or
23 another co-conspirator posted a message on Telegram stating,
24 "Microsoft, since you lied and said you fixed the issue by yourselves
25 and said it's a technical issue, you brought disaster upon yourself.
26 We will teach you the lesson of honesty today. Don't dare to lie
27 again, we can choose to shut down your services whenever we want, so
28 silent and humble yourselves. Outlook and related Microsoft Services

1 have been downed once again," followed by a Check Host report link
2 indicating that the service was offline.

3 Overt Act No. 74: On June 5, 2023, defendant AHMED OMER or
4 another co-conspirator posted a message on Telegram stating,
5 "Microsoft, today we played football with your services. Let's play a
6 fun game. The fate of your services, which is used by hundreds of
7 millions of people everyday, is under our dominion and choice. You
8 have failed to repel the attack which has continued for hours, so how
9 about you pay us 1,000,000 USD and we teach your cyber-security
10 experts how to repel the attack and we stop the attack from our end?
11 1 million USD is peanuts for a company like you! Otherwise, enjoy
12 long hours of downtime, millions of angry customers worldwide and
13 loss of billions of dollars. If you want us to teach you the method
14 to prevent the attack, talk in the bot and we will negotiate :
15 @AnonymousSudan_Bot."

16 Overt Act No. 75: On July 14, 2023, defendant AHMED OMER or
17 another co-conspirator, using Anonymous Sudan's attack
18 infrastructure, attacked Microsoft.

19 Overt Act No. 76: On July 14, 2023, defendant AHMED OMER or
20 another co-conspirator posted a message on Telegram stating,
21 "Microsoft, Do you think we will forget you?" followed by three Check
22 Host report links indicating that the Microsoft cloud storage service
23 OneDrive was offline.

24 Overt Act No. 77: On July 19, 2023, defendant AHMED OMER or
25 another co-conspirator, using Anonymous Sudan's attack
26 infrastructure, attacked Microsoft.

27 Overt Act No. 78: On July 19, 2023, defendant AHMED OMER or
28 another co-conspirator posted a message on Telegram stating,

1 "Microsoft, Do you think we will forget you?" followed by Check Host
2 report links indicating that the Microsoft Azure portal was down.

3 Attacks on Archive of Our Own (AO3)

4 Overt Act No. 79: On July 10, 2023, defendant AHMED OMER or
5 another co-conspirator, using the Anonymous Sudan C2 server,
6 initiated an attack against U.S. not-for-profit fan art organization,
7 Archive of Our Own (AO3).

8 Overt Act No. 80: On July 10, 2023, AHMED OMER sent private
9 messages on Telegram with screenshots of logs depicting the Anonymous
10 Sudan C2 server conducting the attack on AO3.

11 Overt Act No. 81: On July 10, 2023, defendant AHMED OMER or
12 another co-conspirator posted a message on Telegram indicating that
13 Anonymous Sudan had attacked AO3, together with two Check Host report
14 links indicating that the service was offline.

15 Overt Act No. 82: On July 10, 2023, defendant AHMED OMER or
16 another co-conspirator posted a message on Telegram stating, "Message
17 to AO3 admins and fans : We bear the good news that we will continue
18 attacking AO3 and will not stop anytime soon. ... We can bypass any
19 protection you put, we will make sure the site goes off for the
20 longest time possible as your 'experts' scratch their heads
21 cluelessly to find a solution. ... Finally, 'experts' of AO3, we hope
22 you enjoy your extra work hours. Fans of AO3, you only motivate us to
23 continue attacking with your insults and shallow threats, it doesn't
24 harm us and won't make us stop."

25 Overt Act No. 83: On July 11, 2023, defendant AHMED OMER or
26 another co-conspirator posted a message on Telegram stating, "AO3, no
27 matter what you do, it is impossible to mitigate our attacks. You
28 need to be realistic and check our DDOS history. We will give you 24

1 hours to think about this offer : We can negotiate a price with you
2 to halt all DDoS attacks immediately, and help you apply DDoS
3 mitigation. To negotiate, contact us at our bot :
4 @AnonymousSudan_Bot."

5 **Attacks on the Netherlands**

6 Overt Act No. 84: On January 27, 2023, defendant AHMED OMER
7 used the Anonymous Sudan attack infrastructure to attack at least
8 seven Dutch airports.

9 Overt Act No. 85: On January 27, 2023, defendant AHMED OMER or
10 another co-conspirator posted a message on Telegram in English and in
11 Russian, stating, "The infrastructure of all airports in the
12 Netherlands has been brought down," together with Check Host report
13 links indicating that the websites for several Dutch airports were
14 offline during the time period of the attack.

15 Overt Act No. 86: On January 27, 2023, defendant AHMED OMER
16 sent a private message to another Telegram user asking if he was
17 responsible for the Anonymous Russia channel. Defendant AHMED OMER
18 then sent a copy of the January 27, 2023, Anonymous Sudan post about
19 attacking Dutch airport infrastructure and asked if the user could
20 share the post.

21 **Attacks on France**

22 Overt Act No. 87: On July 1, 2023, defendant AHMED OMER
23 exchanged private messages on Telegram discussing DDoS attack methods
24 to employ against French telecommunications company Orange SA, with
25 AHMED OMER eventually stating, "I can down <https://www.orange.tn>."

26 **Attacks on Europol and the European Union**

27 Overt Act No. 88: On October 1, 2023, defendant AHMED OMER or
28 another co-conspirator, using the Anonymous Sudan C2 server,

1 initiated an attack against a Europol website.

2 Overt Act No. 89: On November 10, 2023, defendant AHMED OMER
3 or another co-conspirator, using the Anonymous Sudan C2 server,
4 initiated an attack against a Europol website.

5 Overt Act No. 90: On December 9, 2023, defendant AHMED OMER or
6 another co-conspirator, using the Anonymous Sudan C2 server,
7 initiated an attack against a Europol website.

8 Overt Act No. 91: On December 9, 2023, defendant AHMED OMER or
9 another co-conspirator, using the Anonymous Sudan C2 server,
10 initiated attacks against six European Union government websites.

11 Overt Act No. 92: On December 9, 2023, defendant AHMED OMER or
12 another co-conspirator posted a message on Telegram indicating
13 Anonymous Sudan had attacked European Union government websites,
14 together with Check Host report links indicating that the websites
15 were offline.

16 **Attacks on International Committee for the Red Cross**

17 Overt Act No. 93: On December 19, 2023, defendant AHMED OMER
18 or another co-conspirator, using the Anonymous Sudan C2 server,
19 initiated an attack against the International Committee for the Red
20 Cross.

21 Overt Act No. 94: On December 19, 2023, defendant AHMED OMER
22 sent private messages on Telegram containing screenshots of logs
23 depicting Anonymous Sudan's C2 server conducting the attack on the
24 International Committee for the Red Cross.

25 Overt Act No. 95: On December 19, 2023, defendant AHMED OMER
26 or another co-conspirator posted a message on Telegram indicating
27 that they were attacking the International Committee for the Red
28 Cross, together with a Check Host report link indicating that the

1 organization's website was offline.

2 Attacks on Israel

3 Overt Act No. 96: On April 13, 2023, defendant AHMED OMER or
4 another co-conspirator sent a series of private messages on Telegram
5 asking for assistance in attacking <https://www.iec.co.il>, the website
6 for Israel Electric.

7 Overt Act No. 97: On April 14, 2023, defendant AHMED OMER or
8 another co-conspirator posted messages on Telegram indicating that
9 they had attacked websites in Israel for a rocket alert system, an
10 electric company, and a water company, which the messages explained
11 as follows: "Red Alert is an Israeli website and mobile app that
12 provides real-time alerts for incoming missile attacks and other
13 security threats in Israel"; "The IEC is the sole provider of
14 electricity in Israel, and its website allows customers to manage
15 their accounts, pay bills, and report outages"; and "Mekorot -
16 Israel's national water company, responsible for supplying water to
17 homes and businesses throughout the country."

18 Overt Act No. 98: On May 3, 2023, defendant AHMED OMER sent a
19 series of private messages on Telegram coordinating DDoS attacks
20 against targets including Israel's military and supreme court.

21 Overt Act No. 99: On May 5, 2023, defendant AHMED OMER or
22 another co-conspirator posted a message on Telegram stating, "We are
23 now playing with Israel again. The strong strikes will be when there
24 is a missile attack from Gaza. At this moment, we will attack with
25 all our might to bring down Iron Dome and electricity together."

26 Overt Act No. 100: On May 22, 2023, defendant AHMED OMER sent a
27 private message on Telegram providing the Red Alert website and
28 asking, "how to down."

1 Overt Act No. 101: On May 22, 2023, defendant AHMED OMER sent
2 private messages on Telegram stating, "check <https://oref.org.il>, if
3 you find backend im ready to pay u good money." The other party then
4 sent AHMED OMER an IP address, to which AHMED OMER replied, "I fuck
5 this ip but [www.oref](http://www.oref.org.il) won't down."

6 Overt Act No. 102: On October 7, 2023, at approximately 4:11
7 UTC, defendant AHMED OMER used an Internet-connected device to view
8 the Red Alert website.

9 Overt Act No. 103: On October 7, 2023, beginning at
10 approximately 4:14 UTC, defendant AHMED OMER or another co-
11 conspirator launched a series of DDoS attacks via the Anonymous Sudan
12 C2 server against the domains email.redalert.me, redalert.me,
13 redalert.me/api/app, and api.tzavaadom.co.il.

14 Overt Act No. 104: On October 7, 2023, at approximately 4:33
15 UTC, defendant AHMED OMER or another co-conspirator posted a message
16 on Telegram stating, "'Tzevaadom' application and the 'Redalert'
17 application are currently unavailable. These are the alert
18 applications in Israel. #AnonymousSudan #SKYNET #GodzillaBotnet."

19 Overt Act No. 105: On October 7, 2023, defendant AHMED OMER or
20 another co-conspirator posted a message on Telegram stating, "All
21 alert applications in Israel are down."

22 Overt Act No. 106: On October 7, 2023, defendant AHMED OMER or
23 another co-conspirator posted a message on Telegram stating, "We are
24 currently targeting some critical endpoints in the alert systems of
25 Israel, which may affect the Iron Dome. Glory to the Palestinian
26 Resistance, we are with you."

27 Overt Act No. 107: Beginning on October 7, 2023, and continuing
28 until at least October 9, 2023, defendant AHMED OMER or a co-

1 conspirator used the Anonymous Sudan DDoS service to launch DDoS
2 attacks at the Jerusalem Post website, including the web address for
3 the Jerusalem Post's home page, and web addresses for specific
4 stories about the ongoing attacks against Israel by Hamas, including
5 <https://www.jpost.com?FuckISrael-AnonymousSudan>.

6 Overt Act No. 108: On October 8, 2023, defendant AHMED OMER or
7 a co-conspirator posted a message on Telegram containing a screenshot
8 of a post by the Jerusalem Post describing the ongoing DDoS activity
9 against the Jerusalem Post. Beneath the screenshot, defendant AHMED
10 OMER or a co-conspirator posted the text "Cry, cry for we are
11 enjoying your tears."

12 Overt Act No. 109: On October 8, 2023, defendant AHMED OMER or
13 a co-conspirator posted a message on the Anonymous Sudan Telegram
14 channel stating "+24 hours and the website is still down," including
15 a link to the Jerusalem Post website and a Check Host report link
16 indicating the website was offline.

17 Overt Act No. 110: On October 9, 2023, defendant AHMED OMER or
18 a co-conspirator posted a message on Telegram stating, "+50 hours and
19 the website is still down."

20 Overt Act No. 111: On October 9, 2023, defendant AHMED OMER or
21 a co-conspirator posted a message on Telegram stating, "All articles
22 in The Jerusalem Post have been deleted."

23 Overt Act No. 112: On October 15, 2023, UICC 1 or another co-
24 conspirator sent an email with the subject line "HOW MANY ISRAELI
25 PROXIES WITH UNLIMITED BANDWIDTH YOU HAVE." The email stated "I
26 would like to have access to as many unique Israeli IPs as possible.
27 The nature of my project may require significant data transfer so I
28 would like to ensure that there are no bandwidth limitations during

1 the access period. I anticipate needing this service for a few hours
2 to days."

3 Attacks on Sudan

4 Overt Act No. 113: On April 14, 2023, defendant AHMED OMER and
5 an unindicted co-conspirator sent a series of private messages on
6 Telegram with AHMED OMER stating, "if internet down, please hit all
7 sudan gov sites," to which the unindicted co-conspirator replied, "Do
8 you have their websites, can you share?" Defendant AHMED OMER then
9 responded, "just gov.sd," and the unindicted co-conspirator provided
10 a Check Host report link indicating that the website was offline.
11 Defendant AHMED OMER then replied, "Don't attack now, when I tell
12 you," to which the unindicted co-conspirator responded, "Okay, can I
13 get some crypto for today's attack?"

14 Attacks on the United Arab Emirates

15 Overt Act No. 114: On December 2, 2023, defendant AHMED OMER,
16 or another co-conspirator, using Anonymous Sudan's C2 server,
17 initiated an attack against Dubai International Airport, at
18 dubaiairports.ae.

19 Overt Act No. 115: On December 2, 2023, defendant AHMED OMER or
20 another co-conspirator posted a message on Telegram indicating that
21 they had attacked Dubai International Airport, together with a Check
22 Host report link indicating that the airport's website was offline.

23 Overt Act No. 116: On December 14, 2023, defendant AHMED OMER
24 or another co-conspirator, using Anonymous Sudan's C2 server,
25 initiated an attack against Dubai airport websites and login portals.

26 Overt Act No. 117: On December 14, 2023, defendant AHMED OMER
27 or another co-conspirator posted a message on Telegram stating,
28 "Major problems with long delays and several canceled flights

1 reported at Dubai International Airport."

2 Overt Act No. 118: On February 1, 2024, defendant AHMED OMER or
3 another co-conspirator, using the Anonymous Sudan C2 server,
4 initiated an attack against login.flydubai.com, a website operated by
5 Dubai government owned airline Fly Dubai.

6 Overt Act No. 119: On February 1, 2024, defendant AHMED OMER
7 sent private messages on Telegram containing screenshots of logs
8 depicting Anonymous Sudan's C2 server conducting the attack on Fly
9 Dubai.

10 Attacks on Kenya

11 Overt Act No. 120: On September 28, 2023, defendant AHMED OMER
12 or another co-conspirator defaced the government website of Nyeri in
13 Kenya, posting a message across the website that read "Hacked by
14 Anonymous Sudan."

15 Overt Act No. 121: On October 13, 2023, defendant AHMED OMER or
16 another co-conspirator, using the Anonymous Sudan C2 server,
17 initiated an attack against various transportation services in Kenya,
18 including taxi and train services.

19 Overt Act No. 122: On October 13, 2023, defendant AHMED OMER
20 sent private messages on Telegram containing screenshots of logs
21 depicting Anonymous Sudan's C2 server conducting the attack on
22 transportation services in Kenya.

23 Overt Act No. 123: On February 17, 2024, defendant AHMED OMER
24 or another co-conspirator, using the Anonymous Sudan C2 server,
25 initiated an attack against a Kenyan government records and services
26 website.

27 Overt Act No. 124: On February 17, 2024, defendant AHMED OMER
28 sent private messages on Telegram containing screenshots of logs

1 depicting Anonymous Sudan's C2 server conducting the attack on the
2 Kentan government records and services website.

3 Attacks on Chad

4 Overt Act No. 125: On December 24, 2023, defendant AHMED OMER
5 or another co-conspirator, using Anonymous Sudan's C2 server,
6 initiated attacks against Google's Chadian translation website,
7 translate.google.td and the Chadian Ministry of Interior website,
8 interieur.gouv.td.

9 Overt Act No. 126: On December 24, 2023, defendant AHMED OMER
10 or another co-conspirator posted a message on Telegram indicating
11 that they had attacked the official website for the Chadian
12 government, the Chadian Ministry of Interior and Security, and a
13 Chadian bank, together with Check Host report links indicating that
14 the websites were offline.

15 Overt Act No. 127: On January 10, 2024, defendant AHMED OMER or
16 another co-conspirator posted a message on Telegram stating, "We have
17 conducted a massive cyber-attack on the infrastructure of the the
18 biggest telecommunications provider in Chad SUDATCHAD (AS328594) We
19 hit all their infrastructure, including critical routers, network
20 administration and other network devices. We claim any damages to
21 the health of the ISP SUDATCHAD."

22 Overt Act No. 128: On January 10, 2024, UICC 1 or another co-
23 conspirator sent an email to Netblocks, a company that reports on
24 Internet connectivity, stating "There's some reports of disruptions
25 in sudachad connectivity. Can you please check this and report any
26 loss in connectivity?" The company replied to this email referencing
27 their own Twitter posting,
28 <https://twitter.com/netblocks/status/1745120545669021955>, which

1 contained a graphic indicating that Internet connectivity to
2 SUDATCHAD had been completely severed.

3 Overt Act No. 129: On January 10, 2024, UICC 1 or another co-
4 conspirator sent another email to Netblocks stating "Apparently a
5 hacker group called anonymous sudan caused the outage. There is
6 indeed some sort of connectivity problems. Please report this. I'm a
7 journalist." The email included a link to the Anonymous Sudan
8 Telegram account.

9 Attacks on The United Kingdom

10 Overt Act No. 130: On February 19, 2024, defendant AHMED OMER
11 or another co-conspirator used the Anonymous Sudan attack
12 infrastructure to attack the University of Cambridge and the
13 University of Manchester.

14 Overt Act No. 131: On February 19, 2024, defendant AHMED OMER
15 or another co-conspirator posted a message on Telegram stating,
16 "MAJOR UK UNIVERSITY CYBER ATTACK ! We have executed a major cyber
17 attack on the digital infrastructure of 2 of the biggest UK
18 universities: 🇬🇧 University of Cambridge 🇬🇧 University of
19 Manchester...⚠️ We therefore claim any harm to the aforementioned
20 universities &: any collateral damage."

21 Overt Act No. 132: On February 20, 2024, defendant AHMED OMER
22 or another co-conspirator posted a message on Telegram stating, "our
23 successful attack really causing issues for UK universities," and
24 quoting public comments about the attacks, including, "The impact is
25 profound, hampering not only the delivery of education but also the
26 very essence of academic accessibility and progress. As institutions
27 scramble to mitigate the damage, the question of safeguarding against
28 future attacks becomes paramount. This cyber onslaught has disrupted

internet and IT services critical for academic operations."

Attacks on Bahrain

Overt Act No. 133: On March 3, 2024, defendant AHMED OMER or another co-conspirator, using the Anonymous Sudan C2 server, initiated an attack against telecommunications provider Zain Bahrain, causing disruptions to a United States Department of Defense network operating in Bahrain.

Overt Act No. 134: On March 2, 2024, defendant AHMED OMER sent private messages on Telegram containing screenshots of logs depicting Anonymous Sudan's C2 server conducting the attack on Zain Bahrain.

Overt Act No. 135: On March 3, 2024, defendant AHMED OMER or another co-conspirator posted a message on Telegram stating, "HUGE BAHRAIN TELECOM CYBER ATTACK PART 2 In addition to 🎯 ZAINBAHRAIN , we have also targeted the biggest telecommunications in Bahrain: 🎯 Batelco 🚫🚫 By this, we have effectively cut off the internet in bahrain for the reasons above. Attack was carried out by @InfraShutdown."

Overt Act No. 136: On March 5, 2024, defendant AHMED OMER or another co-conspirator posted a message on Telegram stating, "After more than 48 hours of holding the Zain Bahrain network offline, we have finally reached a deal with them. Therefore, we'll stop all attacks on their networks immediately. This entire experience proves the revolutionary power of @InfraShutdown team in holding huge networks for days and getting multi-billion companies to their knees. You can request an attack of any scale and unlock this never seen before power by contacting @InfraShutdown_bot."

Promotion of DDoS Services for Sale

Overt Act No. 137: On February 27, 2023, defendant AHMED OMER

1 or another co-conspirator posted a message on Telegram stating,
2 "After tests, we found the best reliable ddos service for you at
3 reasonable prices. We tested the power and it was very strong.
4 @xSkynet@xGodzillAxNewSxPowerxProofs Layer 7 #AnonymousSudan," then
5 the same message again but with the following additional contact
6 information:

7 <https://t.me/xSkyneth><https://t.me/xGodzillAxNewSxPowerxProofs>
8 #AnonymousSudan Owner : @WilfordCEO Admin : @xTsSunami SkyNet

9 Overt Act No. 138: On June 2, 2023, defendant AHMED OMER or
10 another co-conspirator posted a message on Telegram stating, "In case
11 you want to buy a very strong botnet Layer 7, you can buy from here,
12 they have great power, we tried it .. it's very cool," followed by
13 the contact information @xSkynet and @xGodzillAxNewSxPowerxProofs.

14 Overt Act No. 139: On November 11, 2023, defendant AHMED OMER
15 or another co-conspirator posted a message on Telegram stating,
16 "offer valid until 15/11 // for vip power : 100\$ →→ Access 1 Day //
17 600\$ →→ Access 7 Days // 1700\$ →→ Access 30 Days // To Purchase,
18 Contact: @WilfordCEO."

19 Overt Act No. 140: On November 12, 2023, defendant AHMED OMER
20 or another co-conspirator posted a message on Telegram stating, "We
21 have an vulnerability to bypass CloudFlare protection. Through it,
22 you can take down any website using CloudFlare with very little
23 power, as low as 10k requests per second can completely bring down
24 the website. For purchase: 5,000 USD."

25 Overt Act No. 141: On November 19, 2023, defendant AHMED OMER
26 or another co-conspirator posted a message on Telegram stating, "Are
27 you looking for the best place to purchase DDoS services? This is the
28 service we use in many of our attacks. We've combined our Power with

1 theirs, and it has become a tremendous Power. When you make the
2 purchase, you will receive the full power, 100%. The prices are
3 relatively good for the power you will get. There is an offer that
4 will expire on the 28th, which is in 9 days. 100\$ →→ Access For One
5 Day. 600\$ →→ Access For One Week. 1700\$ →→ Access For One Month.
6 Purchase, Contact: @WilfordCEO They also have a reasonably priced
7 stresser, but with limited power. To know the prices, visit their
8 channel. #SKYNET #SKYNET-STRESSER."

9 Overt Act No. 142: On February 21, 2024, defendant AHMED OMER
10 or another co-conspirator posted a message on Telegram stating, "We
11 have botnet with a power of up to 2 TB, priced at \$300 per day. 100
12 attacks per day. To Purchase, Contact: @WilfordCEO."

13 Overt Act No. 143: On February 21, 2024, defendant AHMED OMER
14 or another co-conspirator posted a message on Telegram offering for
15 sale a three-week subscription for \$3,000 to a specific DDoS tool
16 with a programmable interface having up to 2.4 terabytes per second
17 of attack power.

18 Overt Act No. 144: On February 29, 2024, defendant AHMED OMER
19 or another co-conspirator posted a message on Telegram stating, "Who
20 wants our power that can down internet in entire countries today? We
21 are giving exclusive access to our power (all layers) at
22 @InfraShutdown To contact @InfraShutdown_bot."

23 Overt Act No. 145: On March 6, 2024, defendant AHMED OMER or
24 another co-conspirator posted a message on Telegram stating, "We have
25 botnet with a power of up to 1 TB, priced at \$150 per day. 100
26 attacks per day. To Purchase, Contact: @WilfordCEO TEST = \$30."

COUNT TWO

[18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)(i), (ii), (c)(4)(A)(i)(I)]

[DEFENDANT AHMED SALAH YOUSIF OMER]

In or around June 2023, in Los Angeles County, within the Central District of California, and elsewhere, defendant AHMED SALAH YOUSIF OMER, also known as ("aka") "WilfordCEO," aka "Zac," aka "Soldi01," knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage and attempted to cause damage by impairing the integrity and availability of data, programs, systems, and information on protected computers belonging to Microsoft Corporation, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), thereby causing and attempting to cause loss to one or more persons during a one-year period aggregating at least \$5,000 in value.

COUNT THREE

[18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)(i), (ii), (c)(4)(A)(i)(I)]

[DEFENDANT AHMED SALAH YOUSIF OMER]

Beginning no later than July 2, 2023, and continuing to on or about July 5, 2023, in Los Angeles County, within the Central District of California, and elsewhere, defendant AHMED SALAH YOUSIF OMER, also known as ("aka") "WilfordCEO," aka "Zac," aka "Soldi01," knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage and attempted to cause damage by impairing the integrity and availability of data, programs, systems, and information on protected computers belonging to Riot Games, Inc., as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), thereby causing and attempting to cause loss to one or more persons during a one-year period aggregating at least \$5,000 in value.

COUNT FOUR

[18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)(i), (ii), (c)(4)(A)(i)(I),
(c)(4)(A)(i)(II), (c)(4)(A)(i)(III), (c)(4)(A)(i)(IV), (c)(4)(E),
(c)(4)(F)]

[DEFENDANT AHMED SALAH YOUSIF OMER]

On or about February 16, 2024, in Los Angeles County, within the Central District of California, and elsewhere, defendant AHMED SALAH YOUSIF OMER, also known as ("aka") "WilfordCEO," aka "Zac," aka "Soldi01," ("AHMED OMER") knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage and attempted to cause damage by impairing the integrity and availability of data, programs, systems, and information on protected computers belonging to Cedars-Sinai Hospital, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), thereby causing and attempting to cause loss to one or more persons during a one-year period aggregating at least \$5,000 in value; causing and attempting to cause the modification, impairment, and potential modification or impairment of the medical examination, diagnosis, treatment, and care of one or more individuals; causing and attempting to cause physical injury to any person; causing and attempting to cause a threat to public health or safety; and attempting to cause and knowingly and recklessly causing serious bodily injury or death.

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offenses set forth in Count One of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) all right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), any defendant so convicted shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. §§ 982 and 1030]

3. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1030, in the event of any defendant's conviction of the offenses set forth in Counts Two through Four of this Indictment.

4. Any defendant so convicted shall forfeit to the United States of America the following:

a. All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

b. Any property used or intended to be used to commit the offense; and

c. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

5. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence;

1 (b) has been transferred, sold to or deposited with a third party;
2 (c) has been placed beyond the jurisdiction of the court; (d) has
3 been substantially diminished in value; or (e) has been commingled
4 with other property that cannot be divided without difficulty.

5
6 A TRUE BILL

7
8 /s/
9 Foreperson

10 E. MARTIN ESTRADA
11 United States Attorney

12 

13 DAVID T. RYAN
14 Assistant United States Attorney
15 Chief, National Security Division

16 KHALDOUN SHOBAKI
17 Assistant United States Attorney
18 Chief, Cyber & Intellectual
19 Property Crimes Section

20 CAMERON L. SCHROEDER
21 Assistant United States Attorney
22 Cyber & Intellectual Property
23 Crimes Section

24 AARON FRUMKIN
25 Assistant United States Attorney
26 Cyber & Intellectual Property
27 Crimes Section
28