ANDY GREENBERG SECURITY OCT 16, 2024 1:44 PM

Hacker Charged With Seeking to Kill Using Cyberattacks on Hospitals

The US has accused two brothers of being part of the hacker group Anonymous Sudan, which allegedly went on a wild cyberattack spree that hit hundreds of targets—and, for one of the two men, even put lives at risk.

Federal Bureau of Investigation headquarters building in Washington D.C., United States on July 3, 2023. PHOTOGRAPH: GETTY IMAGES

FOR HACKERS SEEKING to maximize chaos, so-called denial-of-service attacks that knock targets offline with waves off junk traffic are typically more of a blunt cudgel than a weapon of mass destruction. But according to the US Department of Justice, a pair of Sudanese brothers allegedly behind the hacktivist group Anonymous Sudan launched a spree of those crude cyberattacks that was both powerful and cruel enough in its choice of victims—extending to dozens of hospitals in multiple countries, Israel's missile alert system, and hundreds of other digital services—that one of them is now being charged not only with criminal hacking but also with the rare added allegation of seeking to cause physical injury and death.

On Wednesday the DOJ unsealed charges against brothers Ahmed and Alaa Omer, who allegedly launched a punishing bombardment of more than 35,000 distributed denial-of-service, or DDoS, attacks against hundreds of organizations, taking down websites and other networked systems as part of both their own ideologically motivated hacktivism, as a means of extortion, or on behalf of clients of a cyberattack-for-hire service they ran for profit. According to US prosecutors and the FBI, their victims included Microsoft's Azure cloud services, OpenAI's ChatGPT, video game and media companies, airports, and even the Pentagon, the FBI, and the Department of Justice itself.

In image of Ahmed Omer's passport released by the FBI.

“We declare cyber war on the United States,” Ahmed Omer posted in a message to Anonymous Sudan's Telegram channel in April of last year, according to the indictment. "The United States will be our primary target.”

Anonymous Sudan also targeted hospitals in the US, Denmark, Sweden, and India. In at least one case in February, prosecutors say, the attacks on Cedars-Sinai Health Systems in Los Angeles caused hours of downtime for health care services that diverted patients to other hospitals. In that Los Angeles incident, the Justice Department claims that one of the two hackers explicitly sought to cause potentially deadly harm.

“Bomb our hospitals in Gaza, we shut down yours too, eye for eye,” Ahmed Omer allegedly wrote on Telegram in the midst of the attack. As a result of those hospital attacks, prosecutors are bringing charges against Ahmed Ohmer that carry a potential life sentence, which prosecutors describe as the most severe criminal charges ever brought against a hacker accused of denial-of-service attacks.

In earlier cases, US authorities claim, the hackers used cyberattacks to disrupt Israel's Tzeva Adom or "Code Red" missile alert app, tearing the system offline in the midst of deadly rocket attacks by Hamas, including during Hamas's attacks on October 7th of last year.

An Anonymous Sudan image included in the FBI's complaint against the Omer brothers.

"The actions taken by this group were callous and brazen," Martin Estrada, a US attorney for the Central District of California and lead prosecutor in the case, told reporters in a conference call. "This group was motivated by their extremist ideology, essentially a Sudanese nationalist ideology."

Despite publicizing its charges against the two men, Estrada declined to make clear the whereabouts of the two alleged hackers—though he noted that they are in custody. An FBI affidavit accompanying the indictment states that an FBI agent, Elliott Peterson, interviewed both of the Omer brothers and that Ahmed Omer admitted to being an Anonymous Sudan administrator.

Law enforcement agencies also appear to have carried out an operation to take down Anonymous Sudan's infrastructure in March of this year, which prevented the group from carrying out further attacks. The Telegram channel where the group boasted of its targeting and advertised its for-profit attack service went entirely silent around that time and has since ceased to exist. "Anonymous Sudan in name and in operation is effectively dead," says Chad Seaman, a principal security researcher for tech firm Akamai and a member of Big Pipes, a working group focused on DDoS that closely tracked the group and collaborated with law enforcement in its investigation.

From mid-2023 until that takedown, Anonymous Sudan distinguished itself among self-proclaimed hacktivists with a series of shockingly large and high-profile DDoS attacks. In June of last year, for instance, it pummeled Microsoft's Azure cloud services for days, knocking it intermittently offline and demanding a million-dollar ransom to stop. It also repeatedly took down OpenAI's ChatGPT in December and wrote on Telegram that it was targeting the company due to the pro-Israeli posts of one of its employees.

Anonymous Sudan has at times, in fact, appeared to have formal or informal ties to anti-Israel forces: According to prosecutors, it launched disruptive cyberattacks that

targeted Israel's Tzeva Adom missile alert system on October 7, 2023, in the midst of attacks by the militant wing of Hamas that killed nearly 1,200 Israelis. As Israel's ensuing bombardment and invasion of the Gaza strip killed tens of thousands of Palestinian civilians over the months that followed, Anonymous Sudan frequently described the motivation for its attacks in its Telegram posts as the defense of Palestinians.
In December of 2023, for instance, Anonymous Sudan took OpenAI's ChatGPT offline with a sustained series of DDoS attacks in response to the company's executive Tal Broda vocally supporting the Israel Defense Forces' missile attacks in Gaza. “More! No mercy! IDF don't stop!” Broda had written on X over a photo of a devastated urban landscape in Gaza, and in another post denied the existence of Palestine.

“We will continue targeting ChatGPT until the genocide supporter, Tal Broda, is fired and ChatGPT stops having dehumanizing views of Palestinians," Anonymous Sudan responded in a Telegram post explaining its attacks on OpenAI.

Still, Anonymous Sudan's true goals haven't always seemed entirely ideological, Akamai's Seaman says. The group has also offered to sell access to its DDoS infrastructure to other hackers: Telegram posts from the group as recently as March offered the use of its DDoS service, known as Godzilla or Skynet, for $2,500 a month. That suggests that even its attacks that appeared to be politically motivated may have been intended, at least in part, as marketing for its moneymaking side, Seaman argues.

“They seem to have thought, ‘We can get involved, really put a hurting on people, and market this service at the same time,’” Seaman says. He notes that, in the group's anti-Israel, pro-Palestine focus following the October 7 attacks, “there’s definitely an ideological thread in there. But the way it weaved through the different victims is something that maybe only the perpetrators of the attack fully understand.”

At times, Anonymous Sudan also hit Ukrainian targets, seemingly partnering with pro-Russian hacker groups like Killnet. That led some in the cybersecurity community to suspect that Anonymous Sudan was, in fact, a Russia-linked operation using its Sudanese identity as a front, given Russia's history of using hacktivism as false flag. The charges against Ahmed and Alaa Omer suggest that the group was, instead, authentically Sudanese in origin. But aside from its name, the group doesn't appear to have any clear ties to the original Anonymous hacker collective, which has been largely inactive for the last decade.

Aside from its targeting and politics, the group has distinguished itself through a relatively novel and effective technical approach, Akamai's Seaman says: Its DDoS service was built by gaining access to hundreds or possibly even thousands of virtual private servers—often-powerful machines offered by cloud services companies—by renting them with fraudulent credentials. It then used those machines to launch so-called layer 7 attacks, overwhelming web servers with requests for websites, rather than the lower-level floods of raw internet data requests that DDoS hackers have tended to use in the past. Anonymous Sudan and the customers of its DDoS services would then target victims with vast numbers of those layer 7 requests in parallel, sometimes using techniques called "multiplexing" or "pipelining" to simultaneously create multiple bandwidth demands on servers until they dropped offline.

For at least nine months, the group's technical power and brazen, unpredictable targeting made it a top concern for the anti-DDoS community, Seaman says—and for its many victims. "There was a lot of uncertainty about this group, what they were capable of, what their motivations were, why they targeted people," says Seaman. "When Anonymous Sudan went away, there was a spike in curiosity and definitely a sigh of relief."

The Justice Department's decision to level a criminal charge against Ahmed Omer that could lead to a life sentence for a denial-of-service attack may seem haphazard, given that state-sponsored cyberattacks and ransomware have often caused far more serious damage to health care networks, says Josh Corman, a researcher at the Institute for Security and Technology who has long focused on health care-targeted hacking. Corman says he's nonetheless encouraged to see prosecutors recognize that even crude cyberattacks can have serious—and even lethal—effects on victims.

"Yes, denial-of-service attacks can degrade and deny patent care to cause loss of life," says Corman. "While this is the first, and it may seem arbitrary until we get more details, it could be heartening to see that we understand the outsize consequences of these attacks."

Updated 5 pm ET, October 16, 2024: While Anonymous Sudan is accused of launching thousands of attacks, the number of targets was in the hundreds. We've updated the story to clarify that distinction.

You Might Also Like ...

Andy Greenberg is a senior writer for WIRED covering hacking, cybersecurity, and surveillance. He's the author of the new book *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. His last book was *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most… Read more

SENIOR WRITER

TOPICS CYBERSECURITY HACKING RUSSIA ISRAEL ISRAEL-HAMAS WAR ANONYMOUS SECURITY DDOS

READ MORE

Man Arrested for Snowflake Hacking Spree Faces US Extradition

Alexander “Connor” Moucka was arrested this week by Canadian authorities for allegedly carrying out a series of hacks that targeted Snowflake’s cloud customers. His next stop may be a US jail.

MATT BURGESS

Inside a Firewall Vendor's 5-Year War With the Chinese Hackers Hijacking Its Devices

Sophos went so far as to plant surveillance “implants” on its own devices to catch the hackers at work—and in doing so, revealed a glimpse into China's R&D pipeline of intrusion techniques.

ANDY GREENBERG

Cybercriminals Pose a Greater Threat of Disruptive US Election Hacks Than Russia or China

A report distributed by the US Department of Homeland Security warned that financially motivated cybercriminals are more likely to attack US election infrastructure than state-backed hackers.

LILY HAY NEWMAN

ICE's $2 Million Contract With a Spyware Vendor Is Under White House Review

Immigration and Customs Enforcement's contract with Paragon Solutions faces scrutiny over whether it complies with the Biden administration's executive order on spyware, WIRED has learned.

VAS PANAGIOTOPOULOS

Zero-Click Flaw Exposes Potentially Millions of Popular Storage Devices to Attack

A vulnerability categorized as “critical” in a photo app installed by default on Synology network-attached storage devices could give attackers the ability to steal data and worse.

KIM ZETTER

Meet ZachXBT, the Masked Vigilante Tracking Down Billions in Crypto Scams and Thefts

He just untangled a $243 million bitcoin theft, what may be the biggest-ever crypto heist to target a single victim. And he has never shown his face.

ANDY GREENBERG

Nigeria Drops Charges Against Tigran Gambaryan, Jailed Binance Exec and Former IRS Agent

After eight months, one of the US’s most prominent crypto-crime investigators is finally coming home.

ANDY GREENBERG

Florida Man Accused of Hacking Disney World Menus, Changing Font to Wingdings

Plus: Cops take down a notorious infostealer, Strava leaks world leaders' locations, and a hacking scandal is causing chaos in Italy.

MATT BURGESS

'We're a Fortress Now': The Militarization of US Elections Is Here

From bulletproof glass, drones, and snipers to boulders blocking election offices, the US democratic system is bracing for violent attacks in 2024.

DAVID GILBERT

The WIRED Guide to Protecting Yourself From Government Surveillance

Donald Trump has vowed to deport millions and jail his enemies. To carry out that agenda, his administration will exploit America's digital surveillance machine. Here are some steps you can take to evade it.

ANDY GREENBERG

US Intel Says Insider Threats Are 'Likely' During the Election

A government memo viewed by WIRED states that insider threats "could derail or jeopardize a fair and transparent election process."

TESS OWEN

DHS Warns Law Enforcement Election Deniers May Attempt to Bomb Drop Boxes

In a series of reports reviewed by WIRED, analysts at the Department of Homeland Security warn of a “heightened risk” of right-wing extremists carrying out attacks around the election.

DELL CAMERON