Democracy Dies in Darkness

U.S. charges Sudanese men with running powerful cyberattack-for-hire gang

Government says two brothers targeted big U.S. corporations, a hospital and an Israeli defense system in a mostly ideologically driven operation.

5 min 14

By Joseph Menn

October 16, 2024 at 1:18 p.m. EDT

Federal prosecutors charged two Sudanese brothers Wednesday with running one of the most prolific cyberattack-for-hire gangs of all time, a small group they blamed for a stunning 35,000 denial-of-service attacks in a single year.

A grand jury indictment charged Ahmed Salah Yousif Omer and Alaa Salah Yusuuf Omer with conspiracy and impairing computers, including in at least one hospital in the United States. Convictions could lead to potential life sentences.

The pair are alleged to have operated Anonymous Sudan, a prodigious outfit with 80,000 subscribers on Telegram that managed to knock offline key pages at the likes of Microsoft, OpenAI and PayPal since January 2023. The indictment says they did all that with just three unindicted accomplices from their war-torn home country.

The group charged $600 or less for major denial-of-service attacks, and the majority of their actions were driven by a Sudanese nationalist ideology, said Martin Estrada, U.S. attorney for the Los Angeles region.

“What’s unusual is the predominance of the ideological motive, with financial sprinkled in,” Estrada told The Washington Post. “They were both prolific and expansive in the targets they attacked.”

The brothers were arrested abroad in March and have been in custody since then, Estrada said. He declined to name the country holding them and declined to comment on whether the United States would seek their extradition. The programs and computers they used have been seized, and there have been no more attacks from that network.

Younger brother Ahmed was the primary administrator of Anonymous Sudan and is either 21 or 22, according to an FBI agent’s affidavit filed with a criminal complaint against him. Both brothers are highly educated and were interviewed in custody, the prosecutor said. Estrada declined to say where they had spent time outside Sudan.

The legal documents and interviews with people involved in the case provided multiple surprises, not the least of which was that Anonymous Sudan was actually run from a country that has been riven by a civil war and famine in recent years.

Besides many major U.S. companies, the group took down government sites in the United States, Dubai, Chad, Bahrain and other nations, according to the indictment. It also allegedly handicapped Israel's Red Alert system for warning citizens about incoming rocket fire on Oct. 7, 2023, the day of the Hamas invasion and attack. In posts to Telegram channels with more than 80,000 members, Anonymous Sudan declared it was acting in solidarity with Palestinians.

For a time, the group described itself as working with Killnet, a Russian hacktivist group that attacked targets in Ukraine and elsewhere. Some security researchers had earlier expressed a belief that it was a front for Russian intelligence or government-protected criminal gangs.

But multiple investigators said they had turned up no evidence of involvement by officials in Russia, Sudan or anywhere else. Estrada said there was also no sign of outside financial support. No information about attorneys for the brothers was immediately available.

In one way, that lack of broader help makes the alleged effort more terrifying: A handful of people with few resources in a country torn by civil war managed to take down infrastructure for OpenAI's ChatGPT and for Microsoft's Outlook webmail and Azure, and to attack public sites belonging to the FBI, CIA and other agencies. Estrada said the brothers were highly skilled and worked for years in the trade.

They pulled off the Anonymous Sudan attacks by defrauding cloud services and host providers, including some in the United States, and by rotating through accounts rapidly, often before the end of a single billing cycle, according to private-sector investigators. Those sites sent internet traffic through relay points that amplified them. To the victims, those relay points looked like the starting point of the attacks.

Leveraging those cloud networks, which they marketed in the criminal underground as Godzilla and Skynet, Anonymous Sudan used other sophisticated techniques and ended with a so-called Layer 7 denial-of-service, in which it tied up the applications on sites until they were so overwhelmed they rendered the sites unusable, the legal filings said.

Microsoft, PayPal and many other victims lost millions of dollars in the attacks, the filings said, while the attack on the large Cedars-Sinai Medical Center in Los Angeles crashed the patient portal and forced ambulances to go elsewhere. Because Anonymous Sudan bragged of its impact on hospitals, the brothers were indicted on charges of impairing computers "and attempting to cause and knowingly and recklessly causing serious bodily injury or death."

Some of the attacks on big companies served as effective marketing to potential outside clients, Estrada said. There are scores of criminal groups selling distributed-denial-of-service (or DDoS) attacks. In most cases, those attacks lack technical expertise and merely inconvenience the victims.

"It's not often you see a DDoS action that could legitimately get people killed," said one private-sector investigator who is part of a multi-company volunteer group called Big Pipes that has been fighting such attacks for years.

In this case, the group and allies tracked the Anonymous Sudan activity and found a program on a key server that included the hacker handle of one of the brothers. That handle led them to a GitHub account with more code and email accounts that the FBI got a warrant to search. The group's members asked not to be named for security reasons.

"This group was presented to us by our private-sector partners as the biggest threat out there," Estrada said. "To take out the biggest threats out there, we need partnerships."