

Two accused of DDoSing some of the world's biggest tech companies

Federal authorities have charged two Sudanese nationals with running an operation that performed tens of thousands of distributed denial of service (DDoS) attacks against some of the world's biggest technology companies, as well as critical infrastructure and government agencies.

The service, branded as Anonymous Sudan, directed powerful and sustained DDoSes against Big Tech companies, including Microsoft, OpenAI, Riot Games, PayPal, Steam, Hulu, Netflix, Reddit, GitHub, and Cloudflare. Other targets included CNN.com, Cedars-Sinai Medical Center in Los Angeles, the US departments of Justice, Defense and State, the FBI, and government websites for the state of Alabama. Other attacks targeted sites or servers located in Europe.

Two brothers, Ahmed Salah Yousif Omer, 22, and Alaa Salah Yusuuf Omer, 27, were both charged with one count of conspiracy to damage protected computers. Ahmed Salah was also charged with three counts of damaging protected computers. Among the allegations is that one of the brothers attempted to "knowingly and recklessly cause death." If convicted on all charges, Ahmed Salah would face a maximum of life in federal prison, and Alaa Salah would face a maximum of five years in federal prison.

Havoc and destruction

"Anonymous Sudan sought to maximize havoc and destruction

against governments and businesses around the world by perpetrating tens of thousands of cyberattacks,” said US Attorney Martin Estrada. “This group’s attacks were callous and brazen—the defendants went so far as to attack hospitals providing emergency and urgent care to patients.”

The prosecutors said Anonymous Sudan operated a cloud-based DDoS tool to take down or seriously degrade the performance of online targets and often took to a Telegram channel afterward to boast of the exploits. The tool allegedly performed more than 35,000 attacks, 70 of which targeted computers in Los Angeles, where the indictment was filed. The operation allegedly ran from no later than January 2023 to March 2024.

<https://arstechnica.com/information-technology/2024/10/us-prosecutors-take-down-operation-accused-of-35000-ddoses-over-14-months/>