PRESS RELEASE

Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World

Wednesday, October 16, 2024

For Immediate Release

U.S. Attorney's Office, Central District of California

LOS ANGELES – A federal grand jury indictment unsealed today charges two Sudanese nationals with operating and controlling Anonymous Sudan, an online cybercriminal group responsible for tens of thousands of Distributed Denial of Service (DDoS) attacks against critical infrastructure, corporate networks, and government agencies in the United States and around the world.

In March 2024, pursuant to court-authorized seizure warrants, the U.S. Attorney's Office and FBI seized and disabled Anonymous Sudan's powerful DDoS tool, which the group allegedly used to perform DDoS attacks, and sold as a service to other criminal actors.

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.

"Anonymous Sudan sought to maximize havoc and destruction against governments and businesses around the world by perpetrating tens of thousands of cyberattacks," said United States 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. My office is committed to safeguarding our nation's infrastructure and the people who use it, and we will hold cyber criminals accountable for the grave harm they cause."

"The FBI's seizure of this powerful DDoS tool successfully disabled the attack platform that caused widespread damage and disruptions to critical infrastructure and networks around the world," said Special Agent in Charge Rebecca Day of the FBI Anchorage Field Office. "With the FBI's mix of unique authorities, capabilities, and partnerships, there is no limit to our reach when it comes to combating all forms of cybercrime and defending global cybersecurity."

"These charges and the results of this investigation, made possible through law enforcement and private sector partnerships, have an immeasurable impact on the security of networks in the U.S. and of its allies, and demonstrates the resolve of the Defense Criminal Investigative Service (DCIS) to safeguard the Department of Defense from evolving cyber threats," said Kenneth A. DeChellis, DCIS Cyber Field Office, Special Agent in Charge. "Cybercriminals need to understand that if they target America's warfighters, they will face consequences."

According to the indictment and a criminal complaint also unsealed today, since early 2023, the Anonymous Sudan actors and their customers have used the group's Distributed Cloud Attack Tool (DCAT) to conduct destructive DDoS attacks and publicly claim credit for them. In approximately one year of operation, Anonymous Sudan's DDoS tool was used to launch over 35,000 DDoS attacks, including at least 70 targeting computers in the greater Los Angeles area.

Victims of the attacks include sensitive government and critical infrastructure targets within the United States and around the world, including the Department of Justice, the Department of Defense, the FBI, the State Department, Cedars-Sinai Medical Center in Los Angeles, and government websites for the state of Alabama. Victims also included major U.S. technology platforms, including Microsoft Corp. and Riot Games Inc., and network service providers. The attacks resulted in reported network outages affecting thousands of customers.

Anonymous Sudan's DDoS attacks, which at times lasted several days, caused damage to the victims' websites and networks, often rendering them inaccessible or inoperable, resulting in significant damages. For example, Anonymous Sudan's DDoS attacks shuttered the emergency department at Cedars-Sinai Medical Center, causing incoming patients to be redirected to other medical facilities for approximately eight hours. Anonymous Sudan's attacks have caused more than $10 million in damages to U.S. victims.

The March 2024 disruption of Anonymous Sudan's DCAT tool, called variously "Godzilla," "Skynet," and "InfraShutdown," was accomplished through the court-authorized seizure of its key components. Specifically, the warrants authorized the seizures of computer servers that

launched and controlled the DDoS attacks, computer servers that relayed attack commands to a broader network of attack computers, and accounts containing the source code for the DDoS tools used by Anonymous Sudan.

An indictment is merely an allegation, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

If convicted of all charges, Ahmed Salah would face a statutory maximum sentence of life in federal prison, and Alaa Salah would face a statutory maximum sentence of five years in federal prison.

The investigation of Anonymous Sudan was conducted by the FBI's Anchorage Field Office, the Defense Criminal Investigative Service, and the State Department's Diplomatic Security Service Computer Investigations and Forensics Division.

Assistant United States Attorneys Cameron L. Schroeder and Aaron Frumkin of the Cyber and Intellectual Property Crimes Section are prosecuting this case, with substantial assistance from Trial Attorney Greg Nicosia of the National Security Division's National Security Cyber Section. Assistant United States Attorneys Schroeder and Frumkin, along with Assistant United States Attorney James Dochterman of the Asset Forfeiture Section, also obtained the seizure warrants for computer servers constituting Anonymous Sudan's DCAT tool.

The DOJ Criminal Division's Office of International Affairs, the FBI's International Operations Division and Behavioral Analysis Unit, and the U.S. Attorney's Office for the District of Alaska aided in this investigation.

These law enforcement actions were taken as part of Operation PowerOFF, an ongoing, coordinated effort among international law enforcement agencies aimed at dismantling criminal DDoS-for-hire infrastructure worldwide, and holding accountable the administrators and users of these illegal services. Akamai SIRT, Amazon Web Services, Cloudflare, Crowdstrike, DigitalOcean, Flashpoint, Google, Microsoft, PayPal, SpyCloud and other private sector entities provided assistance in this matter.

redacted_ahmed_complaint_v.2.pdf indictment_embargo.pdf

Contact
Cameron Esner
Public Information Officer
cameron.esner@usdoj.gov
(213) 894-6683

Updated October 16, 2024

Topics

CYBERCRIME | NATIONAL SECURITY

Component

USAO - California, Central

Press Release Number: 24-256

Related Content

PRESS RELEASE

Two Foreign Nationals Arrested for Allegedly Laundering At Least $73 Million Through Shell Companies Tied to Cryptocurrency Investment Scams

A grand jury indictment was unsealed today in U.S. District Court charging two Chinese nationals, one of them a San Gabriel Valley resident, alleging they played leading roles in a...

May 16, 2024

PRESS RELEASE

West Covina Man Arrested for Allegedly Attempting to Pick Up Money from Elderly Victims Who Were Defrauded in Phishing Scheme

A San Gabriel Valley man has been arrested on federal charges stemming from his alleged attempt to obtain additional funds from two elderly victims who had already paid thousands as...

April 29, 2024

PRESS RELEASE

SoCal Man Arrested on Federal Charges Alleging He Schemed to Advertise and Sell 'Hive' Computer Intrusion Malware

Federal authorities have arrested a San Fernando Valley man on federal charges alleging a scheme to market and sell malware that gave the malware purchasers control over victim computers and...

April 11, 2024

Central District of California
312 N. Spring St. Suite 1200
Los Angeles, CA 90012

Phone: (213) 894-2400
Fax: (213) 894-0141