United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

U.S. Attorneys » Southern District of New York » News » Press Releases

Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE Tuesday, May 27, 2014

Leading Member Of The International Cybercriminal Group "Lulzsec" Sentenced In Manhattan Federal Court

Monsegur Cooperated With Law Enforcement To Reveal Structure And Methods Of Numerous Criminal Cyber Groups, And Enabled Authorities To Identify Key Cyber Criminals, Make Arrests, And Prevent And Remediate Numerous Cyber Attacks

Preet Bharara, the United States Attorney for the Southern District of New York, announced that HECTOR MONSEGUR, a/k/a "Sabu," formerly a leading member of a group of sophisticated computer hackers known as "LulzSec," was sentenced today in Manhattan federal court to time served and one year of supervised release for his participation in computer hacking activity that victimized media outlets, government agencies and contractors, and private corporations around the world by hacking into, disabling, and at times exfiltrating data from the victims' computer systems. MONSEGUR pled guilty in August 2011 to computer hacking conspiracy, computer hacking, computer hacking in furtherance of fraud, conspiracy to commit access device fraud, conspiracy to commit bank fraud, and aggravated identity theft pursuant to a cooperation agreement with the Government. U.S. District Judge Loretta A. Preska imposed today's sentence.

According to the criminal Information and related filings in Manhattan federal court, and statements made at MONSEGUR's guilty plea:

Hacks by Anonymous, Internet Feds, and LulzSec

Since at least 2008, Anonymous has been a loose confederation of computer hackers and others. MONSEGUR and other members of Anonymous, including Jeremy Hammond, took responsibility for a number of cyber attacks between December 2010 and June 2011, including distributed denial of service ("DDoS") attacks against the websites of Visa, MasterCard, and PayPal, as retaliation for the refusal of these companies to process donations to Wikileaks, as well as hacks or DDoS attacks on foreign government computer systems.

Between December 2010 and May 2011, members of the Internet Feds computer hacking collective similarly waged a deliberate campaign of online destruction, intimidation, and criminality. Members of Internet Feds engaged in a series of cyber attacks that included breaking into computer systems, stealing confidential

information, publicly disclosing stolen confidential information, hijacking victims’ email and Twitter accounts, and defacing victims’ Internet websites. Specifically, MONSEGUR and other members of Internet Feds, including Ryan Ackroyd, a/k/a “kayla,” a/k/a “lol,” a/k/a “lolspoon,” Jake Davis, a/k/a “topiary,” a/k/a “atopiary,” Darren Martyn, a/k/a “pwnsauce,” a/k/a “raepsauce,” a/k/a “networkkitten,” and Donncha O’Cearrbhail, a/k/a “palladium,” conspired to commit computer hacks including the hack of the website of Fine Gael, a political party in Ireland; the hack of computer systems used by security firms HBGary, Inc., and its affiliate HBGary Federal, LLC, from which Internet Feds stole confidential data pertaining to 80,000 user accounts; and the hack of computer systems used by Fox Broadcasting Company, from which Internet Feds stole confidential data relating to more than 70,000 potential contestants on “X-Factor,” a Fox television show.

In May 2011, following the publicity that they had generated as a result of their hacks, including those of Fine Gael and HBGary, MONSEGUR, along with Ackroyd, Davis, and Martyn, formed and became the principal members of a new hacking group called “Lulz Security” or “LulzSec.” Like Internet Feds, LulzSec undertook a campaign of malicious cyber assaults on the websites and computer systems of business and governmental entities in the United States and throughout the world. Specifically, MONSEGUR and his co-conspirators, as members of LulzSec, conspired to commit computer hacks including the hacks of computer systems used by the Public Broadcasting System, in retaliation for what LulzSec perceived to be unfavorable news coverage in an episode of the news program “Frontline”; Sony Pictures Entertainment (“Sony”), in which LulzSec stole confidential data concerning approximately 100,000 users of Sony’s website; and Bethesda Softworks (“Bethesda”), a video game company based in Maryland, in which LulzSec stole confidential information for approximately 200,000 users of Bethesda’s website.

Among other things, at law enforcement direction, Monsegur engaged in proactive cooperation that enabled the Government to identify, locate, and arrest eight of his co-conspirators, including Hammond. In addition, as a direct result of Monsegur's cooperation, the Government was able to prevent or mitigate over 300 cyberattacks that were being planned or carried out by others, including on the computer servers of U.S. and foreign governments, international intergovernmental organizations, and private corporations. Monsegur also provided information on vulnerabilities in certain critical infrastructure, including at a U.S. water utility, that enabled law enforcement to secure that infrastructure.

In pronouncing the sentence, Judge Preska said Monsegur’s cooperation was “truly extraordinary.” She also said, “The fact that Monsegur immediately chose to cooperate and went back online . . . allowed the extraordinary cooperation.”

In addition, at today’s proceeding, Judge Preska ordered MONSEGUR, 30, of New York, New York, to pay a $1,200 special assessment fee. MONSEGUR previously served seven months in prison in connection with the crimes to which he pled guilty.

Mr. Bharara praised the investigative work of the Federal Bureau of Investigation.

The investigation was initiated and led by the FBI, and its New York Cyber Crime Task Force, which is a federal, state, and local law enforcement task force combating cybercrime; with assistance from the PCeU, a unit of New Scotland Yard's Specialist Crime Directorate, SCD6; the Garda; and the U.S. Attorneys’ Offices for the Eastern District of California, the Central District of California, the Northern District of Georgia, and the Eastern District of Virginia; as well as the Department of Justice Criminal Division’s Office of International Affairs and its Computer Crime and Intellectual Property Section.

The case is being handled by the Office’s Complex Frauds and Cybercrime Unit. Assistant U.S. Attorney James Pastore is in charge of the prosecution.

Component(s):

USAO - New York, Southern

Press Release Number:
14- 156

Updated May 13, 2015