List of targets of arrested computer hackers

March 6 2012

The five computer hackers charged in New York on Tuesday and a sixth who pleaded guilty are accused of involvement in some of the most notorious hacking incidents of the past 18 months.

The following are some of the cyberattacks in which the two Britons, two Irishmen and two Americans allegedly played a role as members of Anonymous, Lulz Security or associated groups:

-- December 2010: Operation Payback. Distributed denial of service (DDoS) attacks by members of Anonymous on the websites of MasterCard, PayPal and Visa in retaliation for their refusal to accept donations for WikiLeaks. In a DDoS attack, a website is bombarded with traffic, slowing it down or knocking it offline completely.

-- January 2011: Defacing a website of the Irish political party Fine Gael after accessing computer servers in Arizona used to maintain the website, www.finegael2011.com.

-- January 2011: Operation Tunisia. DDoS attacks by members of Anonymous on Tunisian government computer systems, including defacing the prime minister's website.

-- Early 2011: Operation Algeria. DDoS attacks by members of Anonymous on Algerian government websites and cyber attacks on government computer systems.

-- Early 2011: Operation Yemen. Cyberattacks by members of

Anonymous on Yemeni government computer systems and unauthorized downloads of "certain information."

-- Early 2011: Operation Zimbabwe. Cyberattacks by members of Anonymous on Zimbabwean government computer systems and an attempt to steal information from a Zimbabwean government email server.

-- Early 2011: A cyberattack on computer systems of the Tribune Company, which owns the Chicago Tribune and Los Angeles Times, using misappropriated login credentials.

-- February 2011: A cyberattack on private computer security firm HBGary that involved the theft of 60,000 emails from HBGary employees and the HBGary chief executive, as well as defacing his Twitter account.

-- April-May 2011: A cyberattack on a Fox Broadcasting Company website that involved the theft of names, dates of birth, telephone numbers, email and residential addresses for more than 70,000 potential contestants on the Fox television show the "X-Factor."

-- May 2011: A cyberattack on Sony Pictures Entertainment that revealed the passwords, email addresses, home addresses and dates of birth of 100,000 users of the www.sonypictures.com website and a subsequent online attack against Sony Music Entertainment.

-- May 2011: A cyberattack on the Public Broadcasting System website in retaliation for coverage of WikiLeaks on the PBS program "Frontline." The website of the PBS news program "NewsHour" was defaced and confidential information was stolen.

-- June 2011: A cyberattack on Infragard-Atlanta, an informationsharing partnership between the FBI and private industry, involving the theft of passwords and other information, and another against Unveillance, which involved downloading emails of the Unveillance chief executive.

-- June 2011: A cyberattack on the US Senate's website. Internal directory data was stolen from Senate.gov but no sensitive information was compromised.

-- June 2011: A cyberattack on videogame maker Bethesda Softworks and the theft of usernames, passwords and email accounts for 200,000 users of Bethesda Softwork's www.brinkthegame.com.

-- December 2011: An attack on the computer systems of private intelligence firm Stratfor that involved the theft of credit card information for 60,000 users, account information about 860,000 Stratfor subscribers or clients and emails from the Texas-based firm. Only one of the defendants, Jeremy Hammond, 27, of Chicago, was charged in connection with the Stratfor hack.

(c) 2012 AFP

Citation: List of targets of arrested computer hackers (2012, March 6) retrieved 20 April 2024 from https://phys.org/news/2012-03-hackers.html