FBI CYBER DIVISION

Private Sector Advisory

May 2, 2013

(U) Foreign-based hacktivists targeting US Commercial and Government websites

(U) According to multiple news sources, Anonymous-affiliated groups will partake in OP USA on 7 May 2013. OP USA is described as a cyber attack on US-based web sites and servers, with a focus on the financial industry. Organizers claim OP USA is in response to alleged war crimes the US has committed against Iraq, Afghanistan, and Pakistan.

(U) Anonymous-affiliated groups threaten doxes, DNS attacks, defacements, redirects, data leaks, and DDoS

(U) According to open source information, one of the groups called the N4m3le55 Cr3w threatens that OP USA aims at "wiping the US government off the cyber map with the aid of doxes, DNS attacks, defacements, redirects, data leaks, and distributed denial-of services (DDoS) attacks". Organizers also claim to have provided their supporters with the necessary tools to achieve their goals. They have listed various DDoS tools, hacking applications, and resource forums.

(U) OP USA participants declared by Mauritania Attacker of OP ISRAEL

(U) According to open source information, OP USA was officially announced and organized by "Mauritania Attacker", who launched OP ISRAEL and is the founder of Mauritania Hacker Team and AnonGhost Team. Open-source reporting declared the OP ISRAEL to be a failure with minimal impact for online operations.

(U) Mauritania Attacker is organizing world-wide support for OP USA through a Twitter account. OP USA appears to have a strong North African participation; in addition to being organized by Mauritania Attacker, the Moroccan Hackers and Anonymous Tunisia are also listed as participant. Below is a list of groups provided by Mauritania Attacker of confirmed hackers that have been organized to participate in OP USA:

- AnonGhost Team
- TheHackersArmy
- Mauritania HaCker Team
- Moroccan Hackers
- Riad
- Anonymous Tunisia
- Ajaxtem
- MLA (Muslim Liberation Army)
- ZHC (Zcompany Hacking Crew)
- Khorasan Hackers Army
- The Ixx as-Din al-Qassam cyber fighters Team

(U) Beware of possible cyber threat to United States-based and foreign financial institutions on or about May 7, 2013

(U) The FBI reminds the public there exists the potential for cyber-related threats to public institutions that can cause a disruption of service to the institutions' websites.

(U) The FBI is aware of a possible cyber-related threat to United States-based and foreign financial institutions on or about May 7, 2013. The complete list of the targeted financial institutions is provided below. It is believed that the cyber threat will target web sites and servers, which will affect public access to the financial institutions' websites. The duration of the threat is not known. Individuals are urged to exercise reasonable caution and vigilance when accessing these institutions websites during this time period.

(U) Reporting Notice

(U) The FBI encourages recipients to report information concerning suspicious activity to the local FBI field office Cyber Task Force, http://www.fbi.gov/contact/fo/fo.htm, or contact the FBI's 24/7 Cyber Watch Center at 855-292-3937. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Note: Law Enforcement Response

(U) Information contained in this product is for official use only. No further dissemination is authorized.