FBI FLASH

FBI LIAISON ALERT SYSTEM
#C-000007-DD

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

(U) The FBI is providing the following information with high confidence:

SUMMARY

(U) Recent announcements indicate hacktivists are planning to launch a cyber campaign titled "OpUSA" on or about May 7, 2013. Hacktivists intend to use DNS attacks, defacements, redirects, data leaks, Distributed Denial-of-Service (DDoS) attacks, and doxing. The campaign is targeting United States (US) Web sites and servers, with a focus on: financial institutions, including foreign financial institutions; e-commerce; and government Web sites. Based on open source reporting, many of the same groups planning to participate in OpUSA are believed to have participated in a similar recent campaign. The technical details outlined in this alert are based on activities conducted by those groups during that prior campaign.

(U) Significant attack activity may start on May 6 and continue until May 9, 2013. Due to the time difference between the US and the countries in which the participating groups may reside, it is anticipated that most attack activity should occur during late afternoon or early evening Eastern Daylight Time (EDT); however, these groups may operate during late evening or early morning EDT, with the perception that US-based organizations may not have technical personnel available to address attacks during those times.

TECHNICAL DETAILS

(U) The main attack vectors anticipated for OpUSA are DDoS, Structured Query Language injection (SQLi), and cross-site scripting (XSS). DDoS attacks will likely be the main attack vector with an expected peak rate of approximately 30 gigabits per second (Gbps). The attack traffic may be globally attributed, with anticipated network spikes of up to 9 Gbps originating from Indonesian Class C Internet Protocol Address (IPA) space. The observed DDoS attacks are expected to be mainly SYN flood and spoofed UDP attacks. Attackers are expected to rely primarily on simple DDoS tools, such as the Low Orbit Ion Cannon (LOIC), the High Orbit Ion Cannon (HOIC), and ByteDos and may use minor botnets for the attacks. Some actors may utilize vulnerability scanning tools such as Acunetix to scan and identify Web site vulnerabilities.

(U) Traditional DDoS mitigation techniques should be implemented to include, but not limited to, temporarily suspending or rate limiting IPAs or IP blocks with anomalous request activity, limiting the number of sessions from each IPA, and reducing connection timeout wait time. It is also recommended to analyze infrastructure with publically available vulnerability scanning tools and patching with the latest application and security updates.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or
FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937