FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section

2 August 2011

(U) Law Enforcement at Risk for Harassment and Identity Theft through "Doxing"

(U//FOUO) The FBI assesses with high confidence [a] that law enforcement personnel and hacking victims are at risk for identity theft and harassment through a cyber technique called "doxing." "Doxing" is a common practice among hackers in which a hacker will publicly release identifying information including full name, date of birth, address, and pictures typically retrieved from the social networking site profiles of a targeted individual.

(U//FOUO) In response to law enforcement activities that have occurred against Anonymous[b] and LulzSec[c] since January 2011, members of these groups have increased their interest in targeting law enforcement in retaliation for the arrests and searches conducted. Hackers and hacktivists—hackers who commit a computer crime for communicating a socially or politically motivated message—have been openly discussing these activities on Twitter and posting information pertaining to law enforcement on their Twitter accounts and Internet Relay Chat (IRC) channels.

- (U//FOUO) In June 2011 members of Anonymous and LulzSec discussed an identified FBI agent in the IRC channel #lulzsec. The detailed information included when he or she started working for the FBI, training, assignments, and previous employment.[1] FBI analysis suggests that this information was derived from a 2009 affidavit that was available on the Wired.com Web site.[2]

- (U//FOUO) On 26 July 2011 the Twitter account OpMonsanto, an account used by members of Anonymous, warned of the intention to "dox" FBI agents following the 19 July 2011 arrests of 16 individuals for their presumed role in Anonymous' activities: "OpMonsanto: To any FBI agent involved in the continued unjust raiding of peaceful Anons: Expect us. You are no longer entitled to your privacy."[3]

[a] (U) **High confidence** generally indicates that the FBI's judgments are based on high-quality information or that the nature of the issue makes it possible to render a solid judgment. **Medium confidence** generally means that the information is credibly sourced and plausible, but can be interpreted in various ways, or is not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. **Low confidence** generally means that the information's credibility or plausibility is questionable, the information is too fragmented or poorly corroborated to make solid analytic inferences, or that the FBI has significant concerns or problems with the sources.
[b] (U) **Anonymous** is an international hacktivist group responsible for denial-of-service attacks, Web site defacements, and computer intrusions.
[c] (U) **LulzSec** is a hacker group consisting of overlapping members of Anonymous and responsible for various computer intrusions.

- (U) On 31 July 2011 more than 70 law enforcement Web sites were hacked and large amounts of confidential data was exfiltrated. These Web sites included state and local police departments that were not associated with the takedowns. The data consisted of e-mail addresses, usernames, Social Security numbers, home addresses, phone numbers, password dumps, internal training files, informant lists, jail inmate databases, and active warrant information. Operation AntiSec[d] claimed that the intrusion was in response to "bogus, trumped-up charges" against the individuals associated with Anonymous' attacks on PayPal.[4]

(U//FOUO) Recently, Anonymous members have also "doxed" the employees of companies that were victims of their previous attacks, who are perceived as working with law enforcement.

- (U) In July 2011 a sealed search warrant affidavit pertaining to the 19 July takedown was available on the Internet. The affidavit contained the personal information of employees of two US companies, as well as FBI personnel. The personal information consisted of names, units, and job titles.[5]

(U) Outlook and Implications

(U//FOUO) The 19 July takedown of Anonymous and LulzSec members has increased members' interest in targeting law enforcement in retaliation for the arrests and searches conducted. As more arrests are made against suspected members of Anonymous and LulzSec, the FBI expects hacking activities and "doxing" that targets law enforcement and government interests will continue. This could compromise investigations and result in harassment and identity theft of the individuals named in the "dox."

(U//FOUO) Precautionary measures to mitigate potential harassment and identity theft risk to being "doxed" include:

- Safeguarding material containing personal information pertaining to officers and named victims;
- Changing passwords and do not reuse passwords for multiple accounts;
- Using strong passwords;
- Monitoring credit reports;
- Monitoring online personal information, including what others post about you on services such as social networking sites;
- Being careful when giving out contact information; and
- Being aware of social engineering tactics aimed at revealing sensitive information.

[d] (U) **AntiSec** is an operation conducted by members of Anonymous and LulzSec targeting government and law enforcement interests.

(U) Intelligence Collection Requirements

(U//FOUO) This intelligence bulletin addresses the FBI Standing Collection Requirements for Identity Theft contained in USA-IDTA-CYD-SR-0108-10, and for Cyber Intrusions: Hacktivists contained in WW-CYBR-CYD-SR-0057-11.

(U) This intelligence bulletin was prepared by the Domestic Threats Cyber Intelligence Unit of the FBI. Comments and queries may be addressed to the Unit Chief at 202-651-3051.

(U) Endnotes

[1] (U//FOUO) Internet Relay Chat; #lulzsec; 10 June 2011; Information obtained through the National Cyber Forensics-Training Alliance.
[2] (U) Online Article; February 2009; www.wired.com/images_blogs/threatlevel/files/love_guru_affidavit.pdf; accessed on 29 July 2011.
[3] (U//FOUO) Twitter; 26 July 2011; Information obtained through the National Cyber Forensics-Training Alliance.
[4] (U) Online Article; 31 July 2011; Trent Nouveau; "AntiSec in Massive Law Enforcement Smack"; www.tgdaily.com/security-features/57594-antisec-in-massive-law-enforcement-smackdown; accessed on 1 August 2011.
[5] (U) Online Article; July 2011; http://media.nbcbayarea.com/documents/search-warrant-072511.pdf; accessed on 27 July 2011.

Distribution

FBI Intranet
DI/OCA
JWICS
LEO
LNI
SIPRNet

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Please return to:
Federal Bureau of Investigation
Editorial Review Unit
935 Pennsylvania Ave., NW, Room 11079C
Washington, DC 20535

Customer and Intelligence Product Information

Title: (U) Law Enforcement at Risk for Harassment and Identity Theft through "Doxing"
Dated: 2 August 2011
Customer Agency: _____

Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Actionable Value

2. The product helped me decide on a course of action. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Timeliness Value

3. The product was timely to my intelligence needs. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

ERU INTERNAL USE ONLY
Product tracking #: IB-1353
Return to: _____

Comments (please use reverse or attach separate page, if needed):