NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0007-NCCIC-120020110630

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND/OR KEY RESOURCES COMMUNITY AT LARGE. PLEASE DISTRIBUTE IT AS NECESSARY TO COMMUNICATIONS STAKEHOLDERS IN THE PUBLIC AND PRIVATE SECTORS.

(U) HACKTIVIST GROUPS TARGET U.S. AND FOREIGN NETWORKS

EXECUTIVE SUMMARY

(U//FOUO) This Bulletin is being provided for your Executive Leadership, Operational Management, and Security Administrators situational awareness. The National Cybersecurity and Communications Integration Center (NCCIC), through coordination with its partners and monitoring of multiple sources, is tracking reports that members of the hacktivist collectives 'LulzSec' and 'Anonymous' have combined their efforts and continue to perpetrate cyber attacks targeting U.S. and foreign networks.[i,ii] LulzSec Members have posted statements on the internet claiming the attacks, referred to as 'Operation AntiSecurity' (AntiSec), are '*designed to demonstrate the weakness of general internet securit*y' and have allowed them to collect massive amounts of data.

(U) LulzSec is purported to be a group of former Anonymous members who typically use widely available and crude tools to hijack or deface web pages as a political statement.[iii] They also routinely post information regarding planned and ongoing activities on publicly available Internet Relay Chat (IRC) sessions and social networking sites like Twitter. Recent attacks by LulzSec and Anonymous have proven simple Tactics, Techniques and Procedures (TTPs) are often successful, even against entities who have invested a significant amount of time and capital into designing and securing their information networks.

(U//FOUO) While LulzSec has generated a significant amount of media coverage and at least a moderate degree of financial impact to several commercial firms, it has primarily resulted in negative publicity for the entities whose networks were affected.

DETAILS

(U//FOUO) The National Cybersecurity and Communications Integration Center (NCCIC), continues to track reports that members of the hacktivist collectives 'LulzSec' and 'Anonymous' have combined their efforts to continue to perpetrate cyber attacks targeting foreign and U.S. networks. LulzSec Members have posted statements on the internet claiming the attacks, referred to as 'Operation AntiSecurity' (AntiSec), are designed to demonstrate the weakness of general internet security and have allowed them collect massive amounts of data. Commonly exfiltrated data include personal information such as usernames, password, real names, and

email addresses, phone numbers, and anything else that resides in the targeted sites' databases. LulzSec posts these lists and encourages others to "ravage the following list of emails and passwords" in order to compromise the users' accounts on other web based applications.[iv,v]

(U) Hacktivists associated with Anonymous have typically been considered more of a nuisance than a real threat. They typically use crude tools such as the Low Orbit Ion Cannon (LOIC), Pyloris, or Botnets to perform simple DDoS attacks and SQL injection to hijack or deface web pages as a political statement. Communication between group members is usually through IRC chat channels, social networking sites, or other unsophisticated methods. For example, on one occasion, LulzSec set up a "hack request" phone line for people to call in targets to be attacked.

(U) However, in some cases, Anonymous members (or possibly sympathizers) used a combination of methods to hack email networks, Twitter accounts, and web pages. On several occasions, LulzSec and Anonymous members have tweeted statements such as "DDoS is of course our least powerful and most abundant ammunition. Government hacking is taking place right now behind the scenes. #AntiSec", indicating at least some members are engaged in activities that go further than just being a nuisance. Regardless, recent attacks by LulzSec and Anonymous have proven simple TTPs are often enough to successfully target and compromise large entities that have invested a significant amount of time and capital into building secure networks and training their personnel. For example, the June 2011 LulzSec/Anonymous initiated AntiSec campaign resulted in the successful compromise of sensitive but unclassified law enforcement and intelligence data, including FBI IIRs, DHS alerts, and intelligence products that contained information about sensitive and high-profile Federal Government operations.

(U//FOUO) Information about possible identities for LulzSec members has been posted on publicly available internet sites by disgruntled members and rival hackers. Additionally, several members of LulzSec and Anonymous were arrested in the U.S. and abroad. LulzSec also claimed they have ended their hacking campaign and rejoined with Anonymous, while vowing to continue their attacks. Based on their previous behavior and recent statements on publicly available social media sites, the intensity of their attacks could continue or actually increase in the short term as a result of continued publicity and to show support for members who have been arrested.

(U//FOUO) It is often difficult to characterize whether threats of a cyber attack by members of or sympathizers to hacktivist groups like LulzSec and Anonymous are credible until they have occurred. Normally, the measure of success is based on whether the threat actually comes to fruition and if information is stolen or a network made un-available. However, recent media publicity highlighting ongoing cyber activity and the perception that obtaining access to sensitive information on government and private sector networks is easily accomplished seems to have encouraged LulzSec and Anonymous to continue their malicious activity.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0007-NCCIC-120020110630

(U//FOUO) The NCCIC, along with its components and partners will continue to monitor the full spectrum of information and sources available to it for indications of a cyber attack by LulzSec, Anonymous, or sympathetic groups and provide further information to Federal, State, local, Tribal, and Territorial (F/S/L/T/T) Departments and Agencies and CIKR partners as it becomes available. To date, the NCCIC has not received any reports of widespread or significant increases in scanning, probing, or attacks against F/S/L/T/T computer or telecommunications networks. Additionally, there have been no reports of widespread or significant increases in scanning, probing, or attacking of CIKR partner computer or telecommunications networks that can be associated with AntiSec. The NCCIC suggests F/S/L/T/T and CIKR partners develop a comprehensive mitigation plan that includes an External Affairs strategy, in case an attack occurs. Additionally, the US-CERT has unclassified indicators that can be shared with F/S/L/T/T and CIKR partners to identify malicious activity associated with previous attacks by Anonymous and the NCC Watch can assist with telecommunications issues.

RECOMMENDATIONS / WAY AHEAD

(U//FOUO) Some members of LulzSec have demonstrated moderately higher levels of skill and creativity that include using combinations of methods and techniques to target multiple networks. This does not take into account the possibility of a higher-level actor providing LulzSec or Anonymous more advanced capabilities. Therefore, it may be advisable to adjust monitoring of both internal and external resources for indications of a pending or ongoing attack on cyber or telecommunications networks.

(U) The NCCIC recommends that U.S., Federal/State/local/Tribal/Territorial Departments and Agencies, and private sector partners ensure they have processes in place to notify their leadership and network operators if their organization becomes a possible target by hacktivists or other malicious actors, and what notifications they are required or plan to make in the event of an attack.

(U) Should a cyber attack occur, ensure backup and recovery procedures are in place and enabled. Be prepared to execute a full spectrum defensive plan that includes contact information for external sources to draw on for assistance. Collect and centrally manage detailed aspects of the attack so you can provide accurate information to Operations, Security, and Law Enforcement personnel as necessary. Such a plan may also include materials identifying who to contact at your Internet service provider, possibly via alternate means, and at any time of day or night to minimize the duration and effect of a cyber attack. Similarly, have contact information readily available for public and private entities to draw on for assistance: the NCCIC, US-CERT, FBI Joint Terrorism Task Force, local FBI Field Office, applicable Information Sharing Analysis Center (ISAC), and Sector Specific Agency.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0007-NCCIC-120020110630

(U) For the situational awareness of F/S/L/T/T and CIKR partners, below are URLs to the National and Cyber Threat Levels the NCCIC monitors.

- National Terrorism Advisory System: http://www.dhs.gov/alerts
- NCRAL: Contact NCCIC Watch & Warning (NCCIC@HQ.dhs.gov)
- MS-ISAC: http://www.msisac.org/index.cfm
- IT-ISAC: https://www.it-isac.org/
- ES-ISAC: http://www.esisac.com/
- FS-ISAC: http://www.fsisac.com/

POINTS OF CONTACT

(U) While the U.S. Government doesn't endorse a particular solution, identifying vendors with experience combating such an attack may reduce the time it takes to get assistance mitigating such an attack and restoring service or operations. Additionally, the US-CERT web page offers a wide variety of technical and non-technical information to make use of both before and after an incident:

http://www.us-cert.gov/nav/t01/

(U) A variety of documents with information regarding defensive measures to combat a computer network attack are available at:

http://www.cert.org/tech_tips/

(U) Many organizations can suffer financial loss as a result of a cyber attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement.

(U) Data breaches which involve a monetary loss or include a financial nexus such as a compromise to your financial, credit or debit accounts, or personal information can be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.

http://www.secretservice.gov/field_offices.shtml

(U) U.S. persons and companies interested in pursuing an investigation of a cyber attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact information web page:

http://www.fbi.gov/contactus.htm

(U) Non-U.S. entities may need to discuss malicious cyber activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

(U) U.S. Federal Government Departments and Agencies should report cyber attacks and incidents to US-CERT. Non-U.S. F/S/L/T/T Government Departments and Agencies interested in determining the source of certain types of cyber attacks may require the cooperation of your internet service provider and the administrator of the attacked networks. Tracking an intruder this way may not always be possible. If you are interested in trying do to so, contact your service provider directly, as the US-CERT is not able to provide this type of assistance. We do encourage you to report your experiences, however. This helps the NCCIC and US-CERT understand the nature and scope of security incidents on the Internet, and we may be able to relate your report to other activity that has been reported to us.

TERMS OF REFERENCE

(U) Anonymous - (used as a mass noun) is an Internet meme originating 2003 on the imageboard 4chan, representing the concept of many online community users simultaneously existing as an anarchic, digitized global brain. It is also generally considered to be a blanket term for members of certain Internet subcultures, a way to refer to the actions of people in an environment where their actual identities are not known.

(U) Lulz - often used to denote laughter at someone who is the victim of a prank, or a reason for performing an action. This variation is often used on the 'Oh Internet' wiki and '4chan' image boards.

(U) Distributed Denial of Service (DDoS) - an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

(U) Hacktivist - a portmanteau of *hack* and *activism*.

(U) Internet Relay Chat (IRC) - a form of real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called channels, but also allows one-to-one communication via private message as well as chat and data transfer, including file sharing.

(U) Low Orbit Ion Cannon (LOIC) - an open source network attack application, written in C#. LOIC was initially developed by Praetox Technologies, but later it was released into the public domain.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0007-NCCIC-120020110630

POINTS OF CONTACT

(U) This product was produced as a collaborative effort between the NCCIC Functional Groups and the DHS/NCICC Component Organizations (United States Computer Emergency Readiness Team [US-CERT], Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], the National Communications System/National Coordinating Center for Telecommunications [NCS/NCC], and the Office of Intelligence and Analysis/Cyber, Infrastructure, and Science Division/Cyber Threat Analysis Branch [I&A/CISD/CTAB]).

(U) Please direct questions to the NCCIC Duty Officer (NDO). The NCCIC will continue to coordinate with the appropriate component organizations listed below:

NCCIC Duty Officer	**US-CERT**	**NCS/NCC**	**ICS-CERT**
NCCIC@hq.dhs.gov	SWO@us-cert.gov	NCS@hq.dhs.gov	ICS-CERT-SOC@dhs.gov
703-235-8831	703-235-8832/8833	703-235-5080	877-776-7585

[i] Cnet, http://news.cnet.com/8301-27080_3-20072675-245/lulzsec-anonymous-announce-hacking-campaign/ , 20 June 2011, accessed 29 June 2011

[ii] Gizmodo, http://gizmodo.com/5813560/lulzsec-and-anonymous-declare-open-war-against-all-governments-and-fat-cats, 20 June 2011, accessed 29 June 2011

[iii] Backtrace Security, http://backtracesecurity.com/page2, accessed 29 June 2011

[iv] Sophos, http://nakedsecurity.sophos.com/2011/05/13/hackers-steal-fox-tv-passwords-deface-twitter-and-linkedin-pages/, 13 May 2011, accessed 6 June 2011

[v] Sophos, http://nakedsecurity.sophos.com/2011/06/04/infragard-atlanta-an-fbi-affiliate-hacked-by-lulzsec/, 4 June 2011, accessed 6 June 2011