

UNCLASSIFIED



NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER BULLETIN

A-0010-NCCIC -160020110719

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

“ANONYMOUS” AND ASSOCIATED HACKER GROUPS CONTINUE TO BE SUCCESSFUL USING RUDIMENTARY EXPLOITS TO ATTACK PUBLIC AND PRIVATE ORGANIZATIONS

EXECUTIVE SUMMARY

(U) This Bulletin is being provided for your Executive Leadership, Operational Management, and Security Administrators situational awareness. The actors who make up the hacker group “Anonymous” and several likely related offshoots like “LulzSec”, continue to harass public and private sector entities with rudimentary exploits and tactics, techniques, and procedures (TTPs) commonly associated with less skilled hackers referred to as “Script Kiddies”¹. Members of Anonymous routinely claim to have an overt political agenda and have justified at least a portion of their exploits as retaliation for perceived ‘social injustices’ and ‘freedom of speech’ issues. Attacks by associated groups such as LulzSec have essentially been executed entirely for their and their associates’ personal amusement, or in their own hacker jargon “for the lulz”.

(U) Anonymous insist they have no centralized operational leadership, which has been a significant hurdle for government and law enforcement entities attempting to curb their actions. With that being said, we assess with high confidence that Anonymous and associated groups will continue to exploit vulnerable publicly available web servers, web sites, computer networks, and other digital information mediums for the foreseeable future.

(U) So far, Anonymous has not demonstrated any capability to inflict damage to critical infrastructure, instead choosing to harass and embarrass its targets. However, some members of LulzSec have demonstrated moderately higher levels of skill and creativity, evidenced in attacks using combinations of methods and techniques to target multiple networks. To date, their attacks have largely resulted in the release of sensitive documents and personally identifiable information. These attacks have the potential to result in serious harm, particularly to Law Enforcement and other Federal, State and Local Government personnel who may be targeted as a result. Also, this assessment does not take into account the



¹ Script Kiddie: Unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites.

UNCLASSIFIED

UNCLASSIFIED

possibility of a higher-level actor providing Anonymous, LulzSec or a similar group with more advanced capabilities.

BACKGROUND

(U) Anonymous emerged in 2003 on the internet message board / web forum 4chan as a collective group of individuals whose primary purpose was to operate in complete anonymity (as the group name implies), and carry out random acts across the web for their collective amusement. Since then, Anonymous has conducted a number of malicious cyber acts and employed a variety of TTPs (discussed later). In their earlier years, Anonymous' acts seemed to be somewhat random; it wasn't until 2008 that Anonymous became associated with hacktivist² activities.



(U) Anonymous' lack of a centralized leadership structure and distributed (often international) personnel poses a significant hurdle for law enforcement organizations hoping to curb the flow of cyber attacks against organizations. Additionally, international law governing cyber crime varies between countries, and often times, attributing malicious activities to cyber operators is difficult.

(U) Though Anonymous' hacktivist activities are commonly reported to have started in 2008, the group has claimed responsibility for several other cyber attacks motivated by "social injustices" as early as 2006. It wasn't until their

distributed denial of service (DDOS) attacks on the Church of Scientology's public facing website (which Anonymous justified as being in retaliation to perceived violations of American's right to freedom of speech) that the group began to garner significant media attention and internet notoriety. Several attacks against other organizations in 2008 followed the attack targeting the Church of Scientology's website, though it is difficult to judge Anonymous's intent behind the attacks³. Anonymous also organized several physical protests in response to the alleged Church of Scientology censorship campaign (pictured above).



(U) 2009 brought new opportunities for Anonymous to flex their newfound hacktivism muscle, with at least two attacks targeting organizations that Anonymous viewed as pro-censorship, and involvement in protests in response to the 2009 Iranian elections, where Mahmoud Ahmadinejad was named the winner despite discrepancies in the number of votes. Anonymous, in collaboration

² Hacktivist: The nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, and virtual sabotage.⁴

³ Later 2008 attacks included random acts of malice such as an invasion of a public web forum for the Epilepsy Foundation, and attacks against Support Online Hip Hop/All Hip Hop.

UNCLASSIFIED

with the Bit Torrent⁴ site The Pirate Bay, set up a pro-Iranian Green Party website where internet users could voice support for Iranians who were protesting the election results. In 2009 and early 2010 (respectively), Anonymous also conducted DDOS attacks targeting the Governments of Germany and Australia.

(U) Anonymous increased its notoriety in 2010 with high-profile attacks motivated by the arrest of U.S. Army Private Bradley Manning in connection to Wikileaks, releasing several thousand classified U.S. government documents on the internet. Though Anonymous's past actions indicate these cyber attacks should have been motivated by Anonymous's views on freedom of speech, their public statements indicated that the intent was to retaliate against mistreatment of Pvt. Manning while he was in U.S. custody.

(U) Anonymous' activities increased throughout 2011 with a number of high-profile attacks targeting both public and private sector entities. Several of these attacks utilized DDoS as their primary tool, while others relied on cross-site scripting exploits to conduct website defacements. Interestingly, Anonymous justified nearly all of their attacks conducted between 2010 and 2011 by citing social or political injustices by each victim organization.

(U) In 2011, a group of relatively more talented individuals spun off from Anonymous to form the hacker group "LulzSec," to which has been attributed several high profile exploitation/attack incidents involving public and private sector organizations. Though LulzSec initially claimed to operate independently of Anonymous, it became clear that the level of coordination between the two groups was greater than initially thought. Upon completing what they termed a "voyage" of hacking for a period of time, it is confirmed that a small cohort of LulzSec returned to Anonymous.



TACTICS, TECHNIQUES, AND PROCEDURES

(U) Anonymous utilizes the internet to recruit and train new personnel, conduct reconnaissance on potential targets, exploit vulnerabilities found in information systems, deny access to resources, alter information presented by organizations, and steal sensitive information. Though the TTPs and tools employed by Anonymous are commonly thought to be rudimentary and unsophisticated, their success to date executing operations and gaining media attention is on par with high profile incidents allegedly involving sophisticated "Advanced Persistent Threat" (APT) actors. They have relied on taking advantage of weaknesses in applications, thus allowing them to bypass, at least initially, conventional network defenses such as firewalls and anti-virus applications to access sensitive data. Additionally, Anonymous and closely associated groups appear to be building upon recent successes by conducting highly visible messaging campaigns over publicly available social media forums such as Twitter^(USPER), YouTube^(USPER), and Facebook^(USPER).

(U) Anonymous and associated groups pride themselves on being 'social media' savvy, and routinely use forums such as Twitter, Facebook, and public web pages to announce intended targets, ongoing attack results, and post files stolen from victim computer networks. These announcements can provide

⁴ Bit Torrent: A Peer-to-Peer File Sharing Protocol.

UNCLASSIFIED

computer network defenders the opportunity to pro-actively supplement their computer network defenses and provide awareness to management, employees, and partners. For example, cybersecurity experts who have analyzed previous Anonymous attacks have noted there was a significant amount of reconnaissance prior to the attack. Other cybersecurity experts have recommended that public and private sector entities go through the same steps hackers would to determine the extent of attack surface available to a malicious actor. An example of this might entail using internet search engines like Google ^(USPER) to identify sensitive information and computer network vulnerabilities that have been cached as they catalogue the content of the WWW.

ANTICIPATED FUTURE TARGETS

(U) Members of the group LulzSec were possibly associated with the 15 June 2011 DDOS attack on the Central Intelligence Agency's (CIA) public-facing website. Although no information was stolen or released to the public, and the website was not defaced, the site was targeted in a manner consistent with other LulzSec and Anonymous attacks. Anonymous also declared that the group was at "war" with the Intelligence Community (IC) and has identified it as a future target. Anonymous is likely targeting the IC because it views it as violating its core belief in total freedom of information. Additionally, following the release of government e-mail account data from the July 2011 Booz Allen compromise, an Anonymous operator stated on Twitter that, "We are working on two of the biggest releases for Anonymous in the last 4 years. Put your helmets on. It is war."

(U) Anonymous has also stated its intent to target companies related to certain Critical Infrastructure / Key Resources sectors. On 12 July 2011, Anonymous released personally identifiable information of approximately 2500 employees of U.S. Agricultural Company Monsanto, and claimed to have taken down corporate web assets and mail servers. Additionally, in a separate statement on 12 July 2011, Anonymous declared their intention to attack several U.S., Canadian, and British companies, including Exxon Mobil and ConocoPhillips, who were associated with development of oil sands in Alberta, Canada.

(U) Future attacks are likely to continue but will likely remain limited in scope due to a lack of advanced capabilities. These attacks are also likely to target the Federal government and critical infrastructure sectors, particularly in response to publicized events relating to civil liberties, cyber security, or allegations of censorship (online or otherwise).

THE WAY AHEAD

(U) 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.

UNCLASSIFIED

UNCLASSIFIED

(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.

(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/>

ADDITIONAL INFORMATION

(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>

UNCLASSIFIED

UNCLASSIFIED

(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*.

POINTS OF CONTACT

(U) This was produced as a collaborative effort between the NCCIC Components and Functional Groups (US-CERT, ICS-CERT, NCS/NCC, I&A/CISD/CTAB).

(U) Please direct questions to the NCCIC Duty Officer (NDO). 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