NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0016-NCCIC –120020110901

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

(U//FOUO) "ANONYMOUS" UPCOMING US OPERATIONS, IMPACT, AND LIKELIHOOD

EXECUTIVE SUMMARY

(U) The loosely organized hacking collective known as "Anonymous" has announced through several mediums that they plan on conducting cyber attacks, peaceful protests, and other unspecified activity targeting a variety of organizations. The purpose of this product is to judge the likelihood of occurrence for these events, as well as the potential impact.

- (U//FOUO) Occupy Wall Street (OWS): DHS/NCCIC assesses that it is likely peaceful protests will occur on Wall Street on 17 September 2011. These protests may be accompanied by malicious cyber activity conducted by Anonymous.
- (U//FOUO) Operation FaceBook (OPFB): DHS/NCCIC assesses that it is unlikely that a coordinated or sophisticated cyber attack will be conducted by Anonymous (at large) targeting FaceBook.com (FB) on 5 November 2011. However, there remains the possibility that low-level or lone-wolf attempts may occur.
- (U//FOUO) Project Mayhem (PM): DHS/NCCIC assesses that a combination of inconsequential physical mischief and potentially disruptive malicious cyber activity will be conducted leading up to the culmination date of 21 December 2012. At this point, specific tactics, techniques and procedures (TTP) are unknown.
- (U//FOUO) Operation Halliburton: Little is known about this potential upcoming operation. DHS/NCCIC assesses that targeting US corporations is consistent with past Anonymous targets.

(U) Anonymous has devoted resources to creating new cyber attack and exploitation tools:

- (U) Anonymous claimed publicly it will be deploying a new DDoS tool called #RefRef in September. There have been several publicly disclosed tools claiming to be versions of #RefRef however there has been nothing to validate these claims.
- (U//FOUO) The recent release of a distributed denial of service (DDOS)[1] tool known as "Apache Killer," that could be leveraged by Anonymous poses a significant risk to organizations that are operating vulnerable internet facing Apache web servers.

[1] Distributed Denial of Service - An attempt to make an information system unavailable (deny service) by flooding its resources with multiple requests originating from several (distributed) attacking systems.

17 September 2011: Occupy Wall Street (OWS); "US Day of Rage"

(U) Anonymous has come out publicly supporting a 17 September 2011 protest on Wall Street, originally announced by the group "Adbusters"[2] on 13 July 2011. According to the Adbusters website, they are hoping to motivate 20,000 Americans to congregate on Wall Street. Similar acts are emerging targeting financial districts in Madrid, Milan, London, Paris and San Francisco during the same time frame. The Adbusters are coordinating logistical activities and news distribution for OWS via their public facing website, OccupyWallSt[dot]org.

(U) The Anonymous YT video uses information from Adbusters' "Tactical Briefing," calling for protestors to adopt a nonviolent Tahrir-acampadas model. The call is to members to "flood into lower Manhattan, set up tents, kitchens, peaceful barricades and occupy Wall Street for a few months… Once there, we shall incessantly repeat one simple demand in a plurality of voices."

(U) According to their public website, Adbusters has publicly stated their intent to conduct nonviolent protests in order to, "demand that America's resources be invested in human needs and environmental protection instead of war and exploitation." They have also posted a Pledge of Nonviolence, stating that they:

- Will use anger at injustice as a positive nonviolent force for change;
- Will use no violence, verbal or physical, toward any person;
- Will not carry weapons of any kind;
- When participating in a nonviolent direct action, such as civil resistance, will not run or resist arrest; will remain accountable for our actions as a means of furthering witness to injustice;
- As participants in a nonviolent action, will respect the directions of the designated coordinators.

(U) Adbusters is also currently scheduling an upcoming peaceful protest targeting the Washington, DC National Mall in October 2011, motivated by the 10TH anniversary of the invasion of Afghanistan and the beginning of the 2012 federal austerity budget.

(U//FOUO) **DHS/NCCIC'S OWS ASSESSMENT:** The ideologies set forth by Adbusters seem to align at a basic level with the stated intent of Anonymous' newly adopted Hacktivist agenda. These protests are highly likely to occur due to the high level of media attention garnered by the partnership between Adbusters and Anonymous, and due to the heightened media response to the San Francisco BART protests. Though the protests will likely to be peaceful in nature, like any protest, malicious individuals may use the large crowds as cover to conduct illegal activity such as vandalism. Judging based on past behaviors by the group, Anonymous' participation in these protests may include malicious cyber activity, likely in the form of DDOS attacks targeting financial institutions and government agencies.

[2] Adbusters is a non-profit, anti-consumerist organization formed in 1989 in Vancouver, Canada.

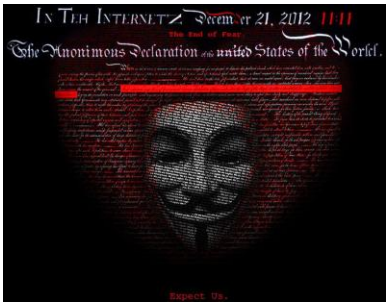
5 November 2011: Operation FaceBook (OPFB)

(U) In July 2011, a YouTube.com video emerged with an individual claiming to be associated with Anonymous stating that they were planning an attack targeting FB on 5 November 2011 – a day of significance for Anonymous because of their use of the Guy Fawkes mask to conceal member identities. The vague video stated that Anonymous would "kill" FB because of privacy abuses. Though the message appeared in a similar format to other YouTube.com videos posted by Anonymous, it is unclear if the same individuals who created past videos for Anonymous are responsible for the OPFB video and some security firms have gone so far as to state the video is most likely an individual masquerading as the "official" Anonymous spokesperson. After making their initial announcement on YT, the individuals created a Twitter feed (#OP_FaceBook), and an Internet Relay Chat (IRC)[3] channel (#OpFaceBook) to distribute information to followers.

(U) Weeks later, #AnonOps, the "official" Twitter account associated with Anonymous group leadership, stated that the broader Anonymous collective does not agree with the statements made by the individuals planning OPFB. A later Twitter message posted by AnonOps stated that, "(Anonymous) absolutely disowns OPFB… (Anonymous is) supposed to fight for the users, not against them. Don't violate private citizen privacy please."

(U//FOUO) **DHS/NCCIC'S OPFB ASSESSMENT:** Due to discontent with OPFB expressed by Anonymous, it is unlikely that they will conduct a high-profile attack against FB as a group on 5 November 2011; however, lone wolf hackers and disgruntled FB users may attempt to conduct attacks or exploitation targeting FB - these efforts will likely be unsuccessful and limited in scope. Furthermore, it is unlikely Anonymous' new tool, #RefRef will be used against FB in November 2011, though we may see it used against other targets beginning in the September 2011 timeframe.

21 December 2012: Project Mayhem (PM)



(U) "Project Mayhem," (PM) was announced by Anonymous in August 2011, and according to their public website projectmayhem2012[dot]org, is set to culminate on 21 December 2012[4]. The PM website has several links to YT videos, which appear to have been randomly selected and have no direct tie to PM or past/current/future Anonymous malicious activity. Furthermore, there is no dialogue or hints as to specific tactics, techniques and procedures (TTP) that Anonymous plans on employing on or prior to 21 December 2012. There are also several seemingly related[5] internet wiki-style portals and web forums, operating under the PM name, devoted to discussing random malicious acts - some involving physical disruption and some involving targeting information systems - but no direct discussion of attack scenarios.

[3] Internet Relay Chat (IRC) is a form of real-time Internet text messaging, or synchronous conferencing.
[4] 21 December 2012 phenomenon comprises of a range of beliefs that cataclysmic or transformative events will occur on the day which is regarded as the end-date for the 5,125 year long Mesoamerican Long Count calendar.
[5] Several of these wikis and portals discuss coordination on 4chan[dot]org and other known Anonymous collaboration sites.

(U) The name "Project Mayhem" is derived from the popular 1999 film Fight Club. The project refers to a secret operation carried out by the Fight Club to topple the corporate American system. In the movie, the Club carries out numerous malicious acts such as defacement of buildings with graffiti, sabotage, and arson. In the finale, the main character is ultimately responsible for destroying buildings belonging to major financial institutions with explosives.

(U//FOUO) **DHS/NCCIC'S PM ASSESSMENT:** While Anonymous' PM will not likely be as spectacular as the activities it was named after in the movie Fight Club, little is known about their plans for this event. We anticipate several more YT videos and public statements via Twitter leading up to the culmination date of 21 December 2012. Based on previous incidents involving Anonymous, we can expect DDOS, web defacement, SQL injection[6], and potentially in-person protests targeting worldwide government institutions and private corporations. Though the characters in the movie Fight Club who carried out their version of PM utilized deadly force and terrorist tactics, Anonymous is not likely to use violent force in their operations.

Unspecified Date: Operation Halliburton

(U//FOUO) Additionally, in August 2011 the NCCIC learned of a possible cyber attack operation planned against Halliburton, a US Oil and Natural Gas sector company. While details of any planned attack are sparse at present, DHS/NCCIC assesses that such an attack would be consistent with Anonymous' targeting preferences.

TACTICS, TECHNIQUES, AND PROCEDURES

(U) Several racist, homophobic, hateful, and otherwise maliciously intolerant cyber and physical incidents throughout the past decade have been attributed to Anonymous, though recently, their targets and apparent motivations have evolved to what appears to be a hacktivist[7] agenda.

(U) Anonymous utilizes a crude target nomination procedure, outlined below, that is coordinated on one of several communications mediums – IRC, websites (#chan[8], etc), insurgency wiki, or anonymous meme[9] themed website:

[6] SQL Injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application (like queries).

[7] Hacktivist – A cyber exploitation or attack actor whose intent is driven by a social, religious, political or cultural ideology.

1. An individual on the communications medium posts an appeal to Anonymous leadership requesting members to target a victim;
2. Those individuals who agree, follow suit with vague details given as to intentions and/or tactics;
3. "Lulz ensue,"[10] or they don't;
4. If "lulz ensue," go back to step 2 and see if more people join the action, or;
5. Lose interest.

(U) Anonymous utilizes several tactics to humiliate victim individuals and organizations. The most common involve:

- "Dropping someone's docs," or exfiltrating information from a compromised system and posting it publicly;
- Pranks targeting victims in real life (IRL) leveraging stolen personally identifiable information (PII), such as unwanted pizza delivery, telephone or fax machine harassment, and other tactics;
- Defacing websites or social network profile pages to embarrass and/or annoy organizations;
- DOS / DDOS attacks.

(U) Anonymous has recently used Twitter to attempt to solicit ideologically dissatisfied, sympathetic employees from within institutions in the financial sector in an attempt to gain information and access. To date these attempts appear unsuccessful, however, given their other tactics, unwilling coercion through embarrassment or blackmail may be a risk to personnel.

(U//FOUO) Though the TTPs and tools employed by Anonymous are commonly thought to be rudimentary and unsophisticated, their success in executing operations and gaining media attention is on par with high profile incidents allegedly involving sophisticated "Advanced Persistent Threat" (APT) actors. Anonymous' DDOS attacks targeting organizations' public facing websites, are often limited in scope and are unable to cause widespread, protracted disruption.

(U) Anonymous has shown through recently reported incidents that it has members who have relatively more advanced technical capabilities who can also marshal large numbers of willing, but less technical, participants for DDOS activities. These more skilled members of Anonymous may use SQL injection targeting vulnerable web servers to steal user credentials, though this type of exploitation is observed less frequently.

(U) According to Anonymous, they are working on a new attack tool called #RefRef that is able to use a server's resources and/or processing power to conduct a DOS against itself. It is unclear at this time what the true capabilities of #RefRef are; Anonymous has stated publicly that the tool will be ready for wider use by the group in September 2011. There have been several publicly disclosed tools claiming to be versions of #RefRef however there has been nothing to validate these claims.

(U) Recently a system resource exhaustion tool known as "Apache Killer," targeting Apache web servers was released on the Internet. This tool exploits a byte range request vulnerability in Apache technology that is patched in Version 2.2.20 released on 31 August 2011.

---

[8] #Chan (4chan, etc) websites – Online web forums created in the mid-2000s. The Anonymous collective got its name from the default user alias on these sites: "Anonymous".

[9] Meme – An idea, behavior or style that spreads from person to person within a culture.

[10] Lulz – Often used to denote laughter at someone who is a victim of a prank /malicious activity, or a reason for performing an action.

(U//FOUO) Apache web technology is widely deployed throughout the US financial services sector; therefore, consequent use by Anonymous of Apache Killer poses a significant risk to those firms in the sector that have vulnerable internet facing Apache web servers. Organizations across all critical sectors should assess the **urgent** need to patch vulnerable systems as soon as possible.

DHS/NCCIC'S ACTIONS

(U) This product was produced as a collaborative effort between the public and private sectors.

(U//FOUO) The NCCIC continues to monitor open source reporting regarding Anonymous and their plans targeting organizations and will report to the broader cybersecurity community if new information becomes available. The NCCIC is coordinating with individuals and organizations in the cybersecurity, intelligence and law enforcement communities to monitor (and report on) the development of new tools and TTP by Anonymous and other organizations. The NCCIC is coordinating with the financial sector and other critical sectors to monitor threat activity and will provide further updates in the form of alerts, advisories and bulletins, as appropriate.