NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0011-NCCIC -120020110914

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

"ANONYMOUS" AND ASSOCIATED HACKER GROUPS DEVELOPING AND DEPLOYING NEW CYBER ATTACK TOOLS

EXECUTIVE SUMMARY

(U//FOUO) This Bulletin is being provided for your Executive Leadership, Operational Management, and Security Administrators situational awareness. The hacker collective known as 'Anonymous' has successfully attacked a wide range of public and private sector entities since 2003 with relatively crude tools. Historically, they rely on tools such as the Low Orbit Ion Cannon (LOIC) or Botnets to deny access to websites, or hijack or deface web pages and post quasi-political statements, or perform other malicious activity. Since many of these older tools made it relatively easy for law enforcement and other government forces to identify the source of an attack and then arrest the perpetrator, Anonymous members may have recognized a need to have more advanced tools that offered a lesser degree of exposure. They recently claimed to have developed and possibly employed several new cyber attack tools for use in their self-proclaimed 'internet civil disobedience' campaigns. The NCCIC, coordinating with several of its partners, believes there are at least four new tools being shared among and employed by Anonymous members: #RefRef, Apache Killer, Anonware, and Universal Rapid Gamma Emitter (URGE).

(U//FOUO) Anonymous has stated that they are possibly going to use one of their new tools for 'OpBritain' on October 15, 2011, targeting Barclays, Vodafone, Lockheed Martin, and Atos. Other future targets announced by Anonymous may include FaceBook (OpFB) on November 5th, and the Fullerton, CA Police Department on a date to be determined. The tools would also be candidates for use during the upcoming 17 September, 2011 'Day of Rage' and 'OccupyWallStreet' protests that Anonymous has been widely advertising their planned participation in. Due to Anonymous' vague leadership structure and use of denial and deception, an actual attack may come with little warning or the threat could be a feint. Additionally, it may be difficult for government, law enforcement, and private sector entities to curb Anonymous actions, regardless of whether a warning is received. That being said, the NCCIC assesses with high confidence that Anonymous and associated groups will continue to use existing and newly created tools to exploit vulnerable web servers, web sites, computer networks and other digital information mediums, in spite of the fact that there are often indications of reconnaissance and penetration testing prior to an attack.

BACKGROUND

(U//FOUO) LOIC has been popular with Anonymous because of its ease of use. It enables hackers with limited skill to engage in attacks by voluntarily joining a botnet and flooding a target server with network traffic; however, LOIC has a few drawbacks, the most important being the traceability of IP addresses involved. Network traffic records logged by the recipient of an attack can be identified if the attack was not routed through an anonymization network. Anyone with access to the logs, specifically law enforcement, could then trace the attack back to the individual computer used for conducting the attack. Thus, use of LOIC has been attributed by some members as the reason for the arrests of many alleged Anonymous members and associates over the last year. Those arrests led Anonymous members to clamor for a new tool that would provide better anonymity, and the purveyors of the '#RefRef' tool claim it offers that obfuscation. While '#RefRef' may have gotten the bulk of the attention lately, some security researchers believe another tool, 'Apache Killer' is a far greater source of concern. Below are descriptions and information for at least three probable new tools associated with or available for use by Anonymous and associated/sympathetic groups:

(U) **#RefRef:** originally claimed to be a platform neutral tool that leverages JavaScript to exploit a SQL vulnerability and allow unskilled users to launch DoS attacks against web sites.

(U//FOUO) A trusted Computer Network Defense partner has analyzed two separate, recently released scripts that can be used to carry out distributed denial-of-service (DDoS) attacks through slow-POST HTTP requests, slow-GET HTTP requests and SQL injection that are purported to be source code for #RefRef. They have assessed that neither script would likely perform DDoS attack attempts in the manner initially claimed by the tool's supposed creator. Though tools based on both scripts would likely be operable, it is unclear whether either has been used in Anonymous/AntiSec DDoS attacks, or whether either represents the #RefRef tool originally claimed to have been created by actor 'anonymousworldunited' and employed in attacks against pastebin.com.

(U//FOUO) The first variant was written in Perl and uses the target's own processing power against itself by uploading a JavaScript file to the target server and exploiting a SQL vulnerability, if present on the server. To exploit the vulnerability, the tool attempts to run a process that purportedly directs MySQL to execute the "benchmark" function to evaluate the expression "0x70726f62616e646f70726f62616e646f70726f62616e646f" 99,999,999,999 times, thus taxing the processor's resources and rendering it un-responsive. Also of note, "0x70726f62616e646f70726f62616e646f70726f62616e646f" is the ASCII string for "probandoprobandoprobando", the Latin word for "proving" strung together three times. Anonymous claimed the new tool would be made public in late August or early September.

(U//FOUO) The second variation, scripted in PHP, attempts to employ several DDoS attack methods commonly used by Anonymous activist groups, including slow-POST and slow-GET requests. The script's unnamed writers use multithreading and Keep-Alive mechanisms, attempting to maintain connections executing the various attack methods concurrently.

(U//FOUO) Other open source reports claiming to be based on interviews with the creators of #RefRef say it exploits a widespread SQL service by sending malformed SQL queries carrying a payload that forces the server to exhaust its resources. That reporting stream also mentions a user interface that has a field to input a refresh interval, thus combining http hammering with the SQL attack. If the scripts described above actually are versions of the #RefRef tool, they would not present any ‘new’ attack vectors, though they do employ methods uncommon among Anonymous hacktivists and may pose threats to un-patched SQL servers and poorly configured web-server applications.

(U//FOUO) On September 9, 2011 a Twitter user, @AnonCMD, claimed to be associated with Anonymous and responsible for the almost universally derided August 31, 2011 denial of service attacks against WikiLeaks, Pastebin and 4Chan, sites commonly used by Anonymous members to post files and communicate with fellow hacktivists. AnonCMD repeatedly asserted that the attacks were ‘field trials’ for #RefRef and part of a personal vendetta with WikiLeaks founder Julian Assange over money. A post by @AnonCMD follows:

"As we returned from our days of hibernation, we have noticed that some may have took claim of developing #RefRef. We have seem the blatantly fake www.RefRef.org, and some more accounts that have taken claim to #RefRef – They are simply not true.

RefRef will be released to the public on September 17th. 2011, and any code you may have stumbled upon is strictly false. It is JavaScript, not Perl.

And to prove the fact that #RefRef is still in the works, we tested it again, not on(@Pastebin) – sorry we still owe you for that one, but on (@WikiLeaks)www.WikiLeaks.org . This was a #RefRef test, and again, it worked flawlessly."

(U) **Apache Killer:** on 25 August 2011, developers at the Apache open source project warned users of the popular web server software (more than two thirds of all web sites) about a new denial-of-service (DoS) tool called ‘Apache Killer’ that exploits a bug in the program and was confirmed to be circulating in the wild. According to Apache, all versions in the 1.3 and 2.0 lines are vulnerable to attack. Researchers who have examined copies of the malware say the vulnerability is trivial to exploit and causes an Apache web server to use up its memory and crash. The Apache Foundation update, Apache 2.2.20, fixes the issue and it’s recommended that companies immediately patch their servers. Unfortunately, the group no longer supports the older Apache 1.3. and just over 5 percent of all Web servers are running revision 2.2.19. Apache has offered mitigation steps administrators with older versions can take to defend their web servers until a patch is available.

(U//FOUO) **Anonware:** a very basic tool. The source code itself is not very sophisticated and appears to be a framework from which a relatively inexperienced virus or malware writer can learn about and adapt malicious code. Researchers who have examined the source code stated that it essentially searches all available drives for .exe files, runs an .exe file supplied by the attacker, and then repackages the new .exe file so that it looks like nothing has happened. The "infected" file is created by using .net's run time CompileAssemblyFromSource method which allows a .net program to compile a new executable at run time. This is how the file "infection" is performed and is not considered a file infection in the true sense.

(U) **URGE:** tool claiming to be harmless while allowing an attacker to hijack Twitter trending topics and tweet messages within them. Anonymous claims it was created to ‘better raise awareness of the real problems of the world’ and used to get Twitter to ‘trend topics that matter’. Reports state it may need Microsoft’s .net Framework 4.0 to function.

(U) TACTICS, TECHNIQUES, AND PROCEDURES

(U//FOUO) 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 Tactics, Techniques, and Procedurs (TTPs) and tools employed by Anonymous are commonly referred to as being unsophisticated, their successes to date have gained them significant media attention. Though some media and blog attention has taken a negative sentiment towards the group and its activities, explicit condemnation of the group's activities has been mostly limited to the computer network defense community. Anonymous will likely continue to exploit weaknesses in system applications and network administration, thus allowing them to bypass network defenses and access sensitive data. Additionally, Anonymous and associated groups appear to be building upon recent successes to conduct their own and/or join in other highly visible messaging campaigns such as the September 17, 2011 'Worldwide Day of Rage'.

(U//FOUO) Anonymous and associated group's announcements on social media and other forums can provide computer network defenders an opportunity to pro-actively supplement their computer network defenses and provide awareness to management, employees, and partners. Anonymous members pride themselves on being 'social media' savvy, and routinely use forums such as Twitter$^{(USPER)}$, YouTube$^{(USPER)}$, FaceBook$^{(USPER)}$, and public web pages to announce intended targets, ongoing attack results, and post files stolen from victim computer networks. Additionally, 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 commercially available network security evaluation tools and 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. Network defenders and managers should also bear in mind that claims made by Anonymous could be purposeful misdirection and possibly a distraction from the real (and undisclosed) attack Anonymous is planning or already engaged in.

(U//FOUO) To date, Anonymous has not demonstrated a capability to inflict damage to critical infrastructure, instead choosing to harass and embarrass its targets. However, some members of LulzSec, a group closely associated with Anonymous, 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. This assessment does not take into account the possibility of a higher-level actor providing Anonymous or an associated group with more advanced capabilities.

(U//FOUO) The introduction of new tools such as Apache Killer, #RefRef, Anonware and Universal Rapid Gamma Emitter (URGE) clearly shows Anonymous' intention to not only continue their malicious activities, but improve their capabilities and provide a level of protection to anyone who participates. It is also likely to lead to changes in their tactics and techniques as they distribute new tools to members, those members become familiar with them, and new ways to employ them are then developed. Additionally, Anonymous has also increased the amount of physical 'protest' activity they either initiate or participate in, in conjunction with their cyber attacks, including the August 2011 attacks on the Bay Area Rapid Transit (BART) system and the upcoming 'Day of Rage'.

ANTICIPATED FUTURE TARGETS

(U) Future attacks targeting both public and private sector entities, particularly in response to publicized events relating to civil liberties, cyber security, or allegations of censorship (online or otherwise) are likely to continue.

THE WAY AHEAD

(U//FOUO) Anonymous members have stated on several occasions that they engage in denial and deception activities. Therefore, network administrators, defenders, and security personnel should factor that in as they develop courses of action to counter the threat of an attack by Anonymous, an associated group, or person. Rigorous monitoring and analysis of logs and behaviors for indications of reconnaissance, probing, or ongoing attack targeting both internally and externally hosted resources may provide the key to successfully defending against an attack by Anonymous or any other malicious actor.

(U) The NCCIC recommends that U.S., Federal/State/local/Tribal/Territorial Departments and Agencies, and private sector partners ensure they have their internally hosted network resources, but also externally hosted ones updated and patched to the highest level possible. We also recommend, where applicable, personnel awareness and training programs be put in place to ensure employees are fully aware of potential threats and threat vectors. Processes should also be put in place to notify leadership, network operators, and security officials if an organization becomes a 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.

(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 managing cyber incidents may reduce the time it takes to mitigate damage and restore 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.gov/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. We do encourage you to report your experiences to US-CERT and the NCCIC, 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.