
From: "Ted Vera" <ted@hbgary.com>
To: <mark@hbgary.com>; "Barr Aaron" <aaron@hbgary.com>
Sent: Thursday, January 20, 2011 2:04 PM
Attach: 20110114-Anonymous.pdf; VE-20101227-Cable.pdf; smime.p7s
Subject: Fwd: Question

---------- Forwarded message ----------
From: S. Alan Carroll <alan@endgames.us>
Date: Thu, Jan 20, 2011 at 12:00 PM
Subject: RE: Question
To: "ted@hbgary.com" <ted@hbgary.com>
Cc: Thomas Zebley <tzebley@iptrust.com>, Kevin Skapinetz <kskap@endgames.us>

Ted,

We have done some preliminary analysis on the Anonymous group (see attached). It is a cursory view of Anonymous and their activities. I have also included a Venezuela report we did concerning the possible US-reachable missile housings from Iran.

Not sure what we will be able to dig up, but I will definitely take a look into possible data collection surrounding your target example. Any other details you might have would help in the lookup routines.

Let me know if any of this information helps or if you have any other questions.

S. Alan Carroll

Engineering Manager

Endgame Systems, Inc.

Office: 404-941-3830

Mobile: 404-409-7403

Begin forwarded message:

From: Ted Vera <ted@hbgary.com>

Date: January 20, 2011 12:37:23 PM EST

To: Thomas Zebley <tzebley@iptrust.com>

Subject: Question

Hi Thomas,

We are doing a talk at an upcoming security expo related to analysis we are conducting on the Anonymous group. I wonder if this group is using any botnets to help attack their targets. Can EndGames search their database for specific targets (like the one below) during an operational window (date/time span) to see if any botnet(s) are participating in attacks? Below is an attack which is currently ongoing. I can also send you previous attacks to see if you have any historical data. If EndGames can provide any relevant data that we can cite in our report we'll give you credit for your contributions.

Operation Payback ITA ---NOW--- #OpVenezuela:http://bit.ly/dI8Oyt | Target: www.presidencia.gob.ve method http |Hive: net.operationfreedom.ru default.| Reason: http://bbc.in/g6ux7z | Sad/Shocking info: http://pastebin.com/LC7aAiYZ | Help with ideas here: http://bit.ly/fpUaCZ

Ted

--
Ted Vera | President | HBGary Federal
Office 916-459-4727x118 | Mobile 719-237-8623
www.hbgaryfederal.com | ted@hbgary.com

--
Ted Vera | President | HBGary Federal
Office 916-459-4727x118 | Mobile 719-237-8623
www.hbgaryfederal.com | ted@hbgary.com

Endgame Systems, Inc.
January 2011

Anonymous and WikiLeaks

Methods and Motivations of Cyber Attacks

Scope: UNCLASSIFIED
Anonymous and WikiLeaks

Endgame Systems, Inc.

Engineering & Analysis Department

Contents

Executive Summary

This paper explores the connection of the group Anonymous to WikiLeaks. It provides a brief background on the shared natural constituencies of each group, the propensity of Anonymous to defend the interests of WikiLeaks on the Internet, and the methods and tactics employed by the group. More importantly, it provides information on the specific innovations of Anonymous in executing Distributed Denial of Service (DDoS) attacks against specific targets.

Anonymous has co-opted a previously abandoned software platform to develop the capability to essentially form opt-in Botnets. This expands the potential pool of participants in a DDoS attack by removing skill and coordination limitations; all a participant must do is download the software, await targeting instructions, and execute a script with the simple push of a button. The only remaining obstacle for Anonymous is the cultivation and maintenance of interest in participation, which directly related to public interest in its particular causes. This is difficult, as public interest is ephemeral; however, a new development with respect to WikiLeaks might "awkaken" Anonymous and

generate new interest in participation in DDoS attacks.

WikiLeaks and Anonymous

Anonymous is a loose and nebulous confederation of Internet users who tend to congregate in a number of "stronghold" websites of a certain character. These websites include 4chan (particularly the "anything goes" /b/ imageboard), Encyclopaedia Dramatica, reddit, and other forum or imageboard websites that do not require registration to contribute. Anonymous features no distinct or recognized organization or leadership, operating instead by the momentum of Internet populism.

Perhaps the only commonality among people affiliated with Anonymous is a militant, fundamentalist view on the freedom of information, censorship, and corruption, especially with respect to governments or organizations leveraging governments. This manifests typically as strong objection to copyright restrictions and their perceived abuse. The genesis of Anonymous as a recognizable entity can be explicitly traced to the Church of Scientology's aggressive action against the publication of a CoS video featuring actor Tom Cruise [http://www.youtube.com/watch?v=UFBZ_uAbxS0]; Anonymous assembled itself as a vehicle to conduct an Internet campaign against the organization.

Anonymous can be found "conducting" operations in selected areas with perceived or actual Internet censorship. Most recently, there have been WikiLeaks- and censorship-related attacks on government websites in Tunisia in the wake of popular unrest in the country. More broadly, Anonymous takes a strongly anti-corporate stance, which means that if any corporate entity is seen as restricting access to or dissemination of media out of profit motives, it is seen as objectionable. In practice, however, this is restricted to particular causes popular with Anonymous. Accordingly, there is emphasis on music piracy, the Church of Scientology, WikiLeaks, etc.

The Modus Operandi of Anonymous with respect to Internet Attacks mainly include simple website defacement and Distributed Denial of Service (DDoS) attacks. A DDoS attack involves flooding the bandwidth or resources of a targeted system with constant connection requests. This will typically interrupt service to the targeted system for the duration of the attack, but should cause no lasting technical damage. As such, this is a

nuisance attack, but it can be asserted with a high degree of confidence that it is either a symbolic protest tactic, or that the attacker lacks the skill necessary to inflict lasting damage.

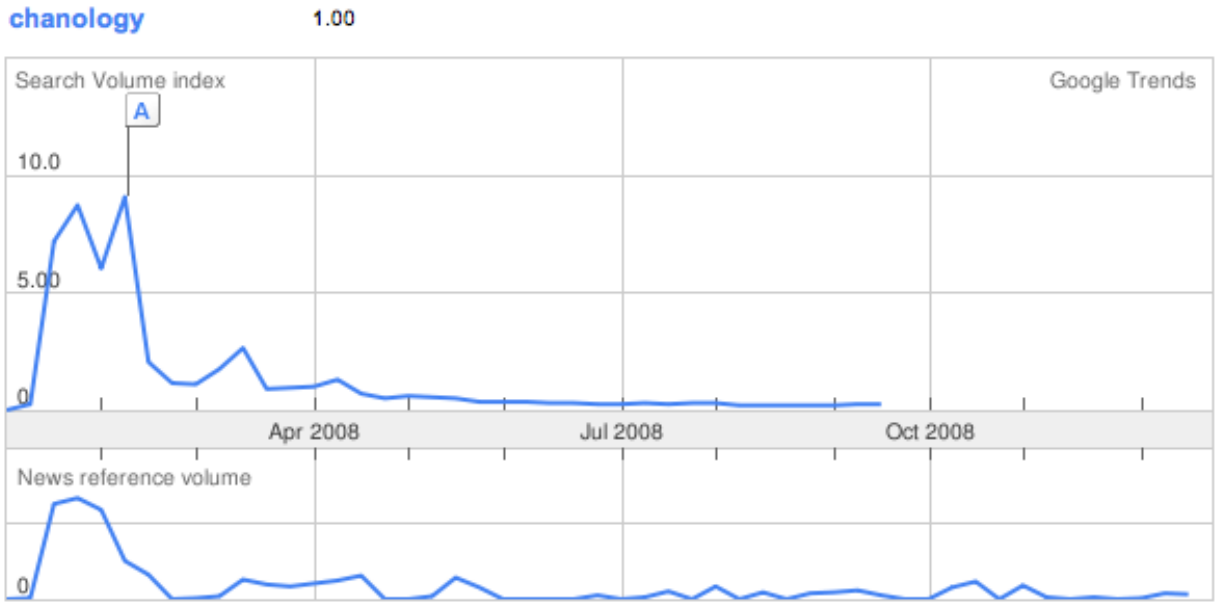
WikiLeaks is a more tightly-knit group that sees itself as a sort of journalistic clearinghouse for whistleblowers against powerful entities, with the aim of forcing transparency. The project is a sort of general philosophy of Open Source that has been extended to government. Before it became controversial in the United States it specialized in smaller-scale disclosures in other countries, such as Kenya, Peru, and Australia. The United States Government was aware of it, and noted with concern when it released such sensitive material as manuals on Guantanamo detention procedures. WikiLeaks is a definable, discrete organization with a discernible and highly public leadership.

Anonymous relates to WikiLeaks insomuch as it has an affinity for the freedom-of-information goals espoused by WikiLeaks. Few, if any, WikiLeaks figures have made direct mention to Anonymous, but Anonymous views itself as WikiLeaks' natural constituency, a sort of pro-bono backer of its efforts. Both organizations favor a distributed approach (i.e. multiple hosts, mirrors, a "legion" mentality), and both feature a self-selecting group of supporters with a high capacity for innovation. The obvious difference between the two entities is that WikiLeaks is a hierarchal organization. WikiLeaks sees itself as a formal, "serious" journalistic entity, and seeks financial, legal, and political support from formal sources such as left/libertarian politicians. Anonymous is informal and often ephemeral.

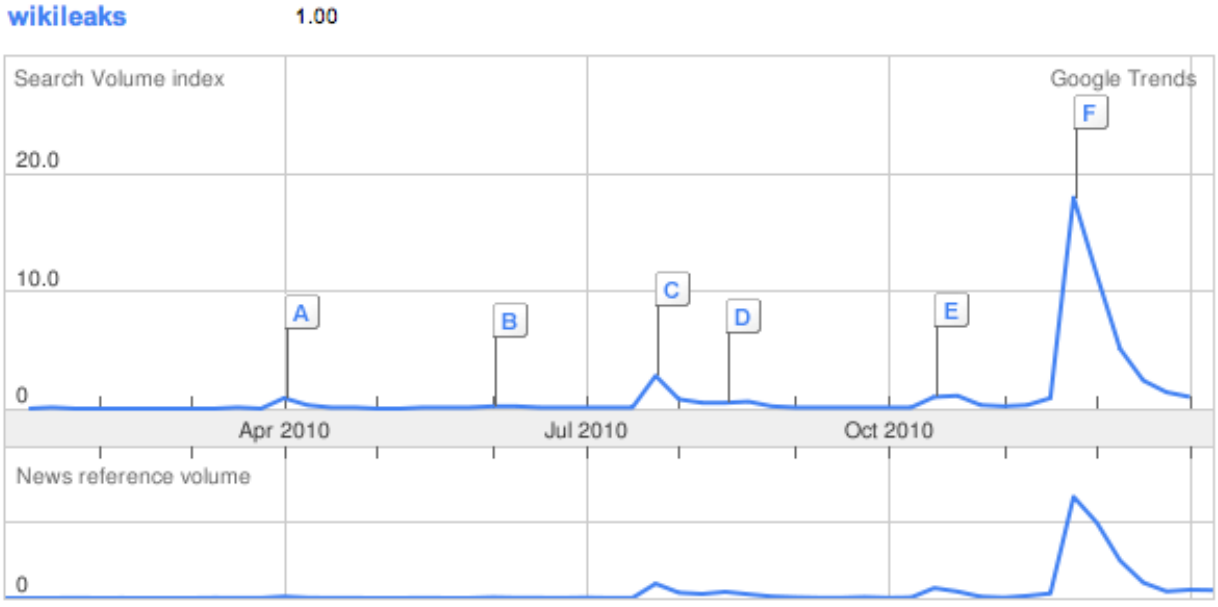
It is important not to conflate the two entities. WikiLeaks and Anonymous may share the same base of support, but they exist in different, if intersecting, orbits.

WikiLeaks and Anonymous seem to face issues of development and maintenance of public interest beyond the latent core support each enjoys. From the standpoint of Anonymous, this directly relates to the number of participants it may enlist in its operations; from the standpoint of WikiLeaks, this relates to the interest it may generate as it seeks to sustain itself. This is evident in the following graphs of trends in Google searches:

Scale is based on the average worldwide traffic of **chanology** in 2008. Learn more



Scale is based on the average worldwide traffic of **wikileaks** in the last 12 months. Learn more



As the figures above indicate, public interest, as evidenced by Google search records, is

rather ephemeral. Therefore it may be surmised that spikes in Anonymous activity will be related to further events related to either WikiLeaks or Julian Assange. For example, Anonymous may "wake up" should Assange be successfully extradited to either Sweden or the United States, indicted, or killed. There is a secondary concern related to the release of the key to a putative "insurance" file widely disseminated when WikiLeaks and Assange first encountered legal controversy.

Methods

The following section documents and details the software used in executing large and distributed Denial of Service (DoS) attacks. Normally, the instigators of the attack will enlist a number of participants, who will all need the knowledge necessary to execute sustained, repeated connections with a particular asset. Shortcomings associated with this technique involve the public spread of information before the attack, the need to enlist and coordinate many people, and the potential unevenness in technical knowledge. The LOIC (Low Orbit Ion Cannon) seeks to overcome those shortcomings by essentially creating an opt-in Botnet, which simply requires the participants to connect to a particular IRC channel and push a button to execute a script.

LOIC was originally developed by a private cyber security firm as a tool for stress testing websites. This firm uploaded the source code to SourceForge and abandoned it there for a number of years. Written in C#, it was later updated by a third party to include a "hivemind mode," which essentially takes advantage of an IRC channel controlled by the organizers to execute a mass DDoS attack. It is this IRC channel that represents the most potential for exploitation. The joined LOIC clients only receive commands from operators, administrators, or owners of the joined IRC channel.

Exploitation of the IRC channel to allow privileged access would enable the user to stop, redirect, or otherwise manipulate the attack. However, it is unlikely that attacks on individual LOIC participants would be effective: while their IP addresses could conceivably be collected upon their joining the IRC channel, it would be difficult to gather this information from passively existing in the channel. This is because the constructor for the client hard-sets relevant information that other clients display to null values (Appendix B:

Code Sample). As a result, other methods, such as control over the server or DNS request analysis must be used to monitor connections. Connections can be detected post-attack via logs of the victim. Additionally, particularly savvy users could selectively use various proxy systems to obfuscate their connections to the command and control server, while still performing actual attacks from unmodified Internet connections.

Because the LOIC client is open source, there is the potential that "attack-specific" clients could be created trivially, although there is no evidence that this has happened. Additionally, the open-source nature of the client works to prevent tampering of the source code by outside parties. Attempts to backdoor the client have been quickly uncovered[*]. However, work could be done to monitor less anonymous IRC channels during non-attack times. Larger networks exist, and the participants may not necessarily try to hide. Additionally, these backdoor fears may lead to abandonment of the LOIC software; however, as of January 2011, many potential participants are still referred to the SourceForge links to download.

There are actively maintained Java and Python ports of LOIC, used on platforms that do not support C# or Mono libraries. This effectively means that LOIC can be run on any recent system.

There is another DDoS client inspired by LOIC, the HOIC (High Orbit Ion Cannon), which is substantially less intricate. This program is also used by Anonymous, but it is not as sophisticated or popular. This client does not have IRC capabilities, and takes instructions from configuration scripts. HOIC seems to particularly target law enforcement for revenge, as evidenced by the readme file distributed with the program. The lack of IRC functionality makes monitoring difficult, but because of the similar constituencies of HOIC and LOIC, attacks may still be anticipated via LOIC-related intelligence.

[*] http://www.anonnewswire.org/entry/2009/07/31/efc-has-a-backdoor

Appendix A: Timeline of Anonymous DDoS Operations in December 2010

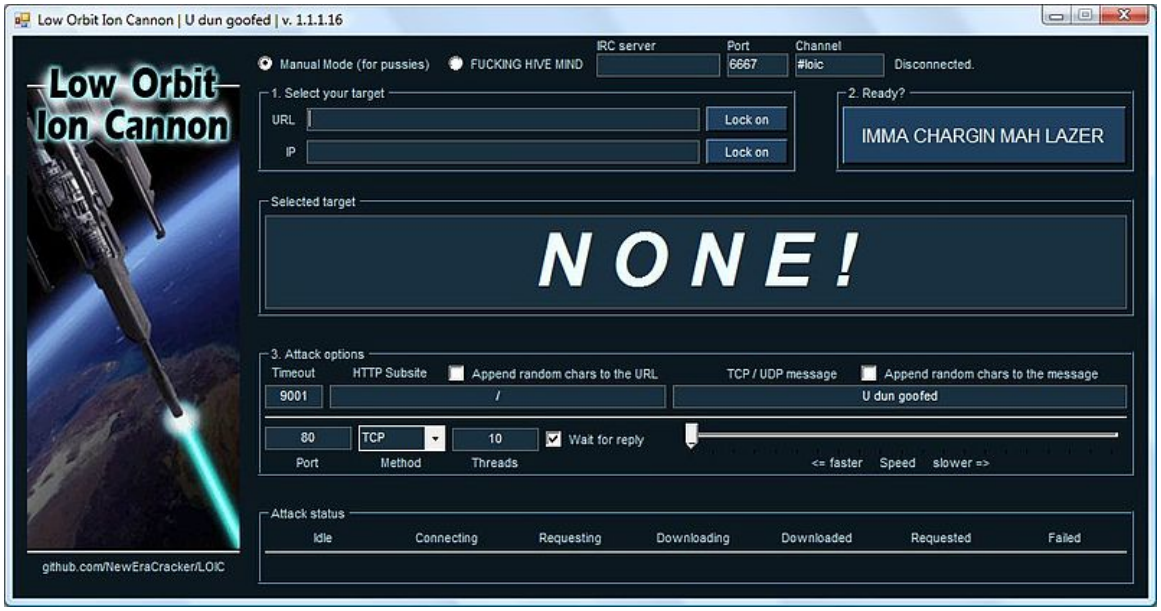
Date	Event
3 DEC 2010	PayPal announces the suspension of WikiLeaks' account, as well as the cessation of processing of donations to WikiLeaks. **Anonymous Response:** DDoS of Paypal's blog, along with encouragement of PayPal accountholders to close their accounts in favor of other services that have not denied payment processing to WikiLeaks. It is unknown how many cancelled their PayPal accounts, though the DDoS attack would last for days on an intermittent basis.
6 DEC 2010	Anonymous broadens the PayPal operation to one focusing on "avenging" Julian Assange in the wake of the issuance of a European Arrest Warrant connected to allegations of sex crimes in Sweden.
	US Rep. Ron Paul of Texas, popular among Anonymous, lends his support to WikiLeaks in the form of a Twitter post: "Re: Wikileaks- In a free society, we are supposed to know the truth. In a society where truth becomes treason, we are in big trouble." **Anonymous Plans:** Mirror WikiLeaks. Offer DDoS targets. Declaration of "infowar."
	DDoS on the website of PostFinance, the fifth largest retail bank in Switzerland and a subsidiary of the Swiss Post, which had announced the closure an account belonging to Julian Assange because of residency discrepancies.
7 DEC 2010	Continued PostFinance downtime.
	Over 500 users in the LOIC Hivemind.
	Attack on the website of Swedish prosecutors over the allegations against Assange.
	Attack on the US Senate website of Senator Joseph Lieberman of Connecticut by 600 LOIC-connected systems.
	Attack on the website of the Swedish law firm representing two women allegedly raped and assaulted by Assange.
	Small subgroup of Anonymous attacks the website of SarahPAC, the Political Action Committee of former Governor Sarah Palin

	of Alaska, for her suggestion that Assange "be hunted down like a terrorist."
8 DEC 2010	Anonymous begins attacking the website of MasterCard.
	The host of the Swedish law firm attacked on the previous day removes the firm's website from its servers, asks Anonymous to cease attacks.
	After twelve hours of attack against the website of MasterCard, LOIC redirects attacks to VISA.
	Twitter suspends the account of AnonOps, which was previously directing operations.
	Anonymous returns to attacking PayPal.
9 DEC 2010	LOIC at 500 computers, all targeting PayPal.
10 DEC 2010	A planned attack on Amazon is postponed in the wake of attacks on Anonymous' server infrastructure.
	Anonymous announces Operation:Leakspin, which involves dissemination into wide circulation of leaked US diplomatic cable material from WikiLeaks. This entails physical distribution of printed material, posting of videos to YouTube under misleading tags, etc.
11 DEC 2010	LOIC at 1200 computers, many of which targeted MasterCard.
13 DEC 2010	The first arrests related to participation in Anonymous DDoS attacks occur in the Netherlands. This causes an influx of Netherlands-based supporters and participants.
	Twitter and Facebook move to erase Anonymous-affiliated accounts.
14 DEC 2010	Anonymous attempts the first DDoS via fax against financial targets. Its success or failure is unknown.

Appendix B: Code Samples

```
IRC LIBARY USED: SmartIrc4net - the IRC library for .NET/C#
<http://smartirc4net.sf.net>
------
Code example 1:
public class IrcUser
    {
        private IrcClient _IrcClient;
        private string _Nick = null;
        private string _Ident = null;
        private string _Host = null;
        private string _Realname = null;
        private bool _IsIrcOp = false;
        private bool _IsAway = false;
        private string _Server = null;
        private int _HopCount = -1;

        internal IrcUser(string nickname, IrcClient ircclient)
        {
            _IrcClient = ircclient;
            _Nick = nickname;
        }
------
==============================
|| CONTROLING LOIC FROM IRC ||
==============================

As an OP, Admin or Owner set a channel topic or type message with (as an
example):
!lazor targetip=127.0.0.1 message=test_test port=80 method=tcp
wait=false random=true

To start attack type
!lazor start

Or just append "start" in the END of the topic
!lazor targetip=127.0.0.1 message=test_test port=80 method=tcp
wait=false random=true start

To reset options back to default:
!lazor default

To stop attack:
!lazor stop

And remove "start" from topic (if exists)
You can also replace "start" by "stop" in the END of the topic.
```

Screenshot of LOIC



Endgame Systems

817 West Peachtree Street

Suite 770

Atlanta, GA 30308

U.S.A.

Produced in the United States of America.

Jan-11