Attacks by "Anonymous" WikiLeaks Proponents not Anonymous

Aiko Pras, Anna Sperotto, Giovane C. M. Moura,
Idilio Drago, Rafael Barbosa, Ramin Sadre,
Ricardo Schmidt and Rick Hofstede

Design and Analysis of Communication Systems Group (DACS)
University of Twente, Enschede, The Netherlands
Email: a.pras@utwente.nl

http://www.utwente.nl/ewi/dacs/
CTIT Technical Report 10.41

December 10, 2010

1 Introduction

On November 28, 2010, the world started watching the whistle blower website WikiLeaks [1] to begin publishing part of the 250,000 US Embassy Diplomatic cables. These confidential cables provide an insight on U.S. international affairs from 274 different embassies, covering topics such as analysis of host countries and leaders and even requests for spying out United Nations leaders [2].

The release of these cables has caused reactions not only in the real world, but also on the Internet. In fact, a cyberwar started just before the initial release. Wikileaks has reported that their servers were experiencing distributed denial-of-service attacks (DDoS) [3]. A DDoS attack consists of many computers trying to overload a server by firing a high number of requests, leading ultimately to service disruption. In this case, the goal was to avoid the release of the embassy cables.

After the initial cable release, several companies started severed ties with WikiLeaks. One of the first was Amazon.com, that removed the WikiLeaks website from their servers [4]. Next, EveryDNS, a company in which the domain wikileaks.org was registered, dropped the domain entries from its servers. On December 4th, PayPal cancelled the account that WikiLeaks was using to receive

on-line donations. On the 6th, Swiss bank PostFinance froze the WikiLeaks assets and Mastercard stopped receiving payments to the WikiLeaks account. Visa followed Mastercard on December 7th.

These reactions caused a group of Internet activists (or "hacktivists") named Anonymous to start a retaliation against PostFinance, PayPay, MasterCard, Visa, Moneybrookers.com and Amazon.com, named "Operation Payback". The retaliation was performed as DDoS attacks to the websites of those companies, disrupting their activities (except for the case of Amazon.com) for different periods of time.

The Anonymous group consists of volunteers that use a stress testing tool to perform the attacks. This tool, named LOIC (Low Orbit Ion Cannon) [5], can be found both as a desktop application and as a Web page [6].

Even though the group behind the attacks claims to be anonymous, the tools they provide do not offer any security services, such as anonymization. As a consequence, a hacktivist that volunteers to take part in such attacks, can be traced back easily. This is the case for both current versions of the LOIC tool. Therefore, the goal of this report is to present an analysis of privacy issues in the context of these attacks, and raise awareness on the risks of taking part in them.

This reported is organised as follows: In the first section, we present an overview about the LOIC tool, its operation model, the type of attacks it can be used for, and the ways in which the tool can be remotely controlled in the context of "Operation Payback". Next, we describe a new variation of the LOIC tool, on-line available as a simple Web page. We then analyse how volunteering hacktivists, making part of "Operation Payback", can be easily traced back, given the simplicity of the tool. We conclude our report relating these attacks to the current international data retention laws.

2 Original LOIC Tool

The original LOIC Tool was built by Praetox Technologies as a stress testing application. The tool performs a simple DoS attack, by sending a sequence of TCP (Transmission Control Protocol), UDP (User Datagram Protocol) or HTTP (HyperText Transfer Protocol) requests to a target host. In Figure 1, we show the initial screen of LOIC.

The original tool allows the user to select a target host, a method of attack (TCP, UDP or HTTP), and some other parameters to customise the requests that will be sent. For example, the user can control the destination port number, the content of the messages (package payload), the number of concurrent threads, request timeout, etc.

The version that is currently in use in "Operation Payback" adds an option

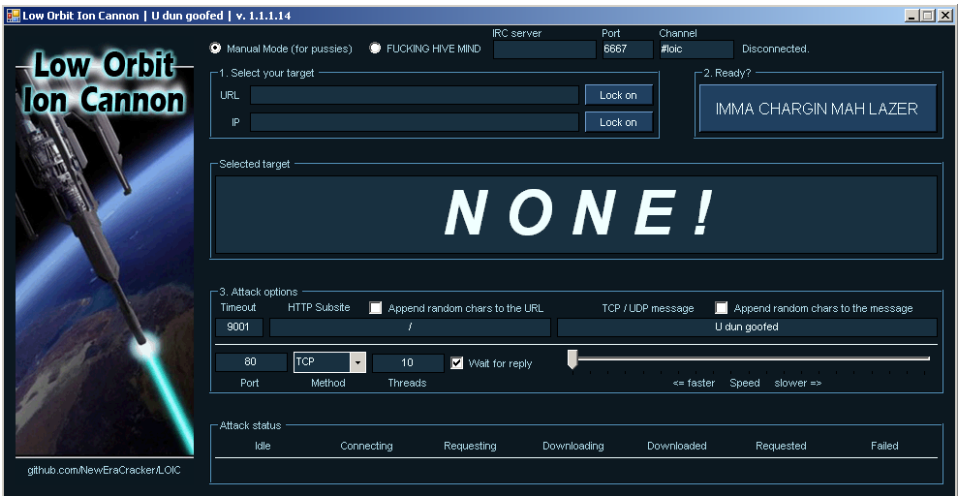

Figure 1: Current LOIC version, used in the "Operation Payback".

that allows the tool to be remotely controlled, using the IRC (Internet Relay Chat) protocol. In this case, the user machine becomes part of a botnet. We discuss this operation mode in details in the next sections. In Figure 2, we show how LOIC can be used to send requests to the same machine as the tool is installed.

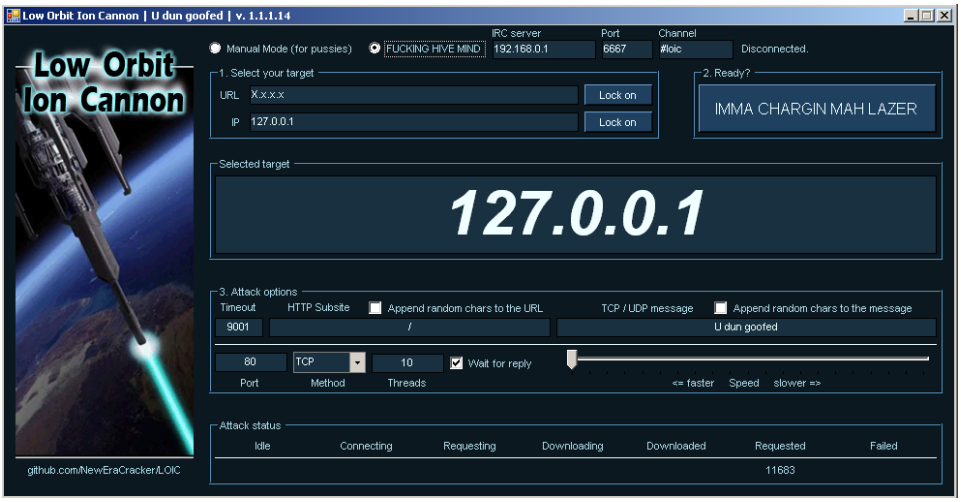

Figure 2: LOIC in action: local machine (127.0.0.1) is under attack.

2.1 Tool Description

LOIC has two modes of operation: the manual mode, where the target address and all other parameters have to be filled in by the user; and the automatic mode, where the attacks are remotely controlled. The automatic mode or *Hive Mind*, as it is called in the tool, can be seen as an option to voluntarily join a botnet. When using this mode, all parameters of an attack (including the target) are set up remotely via IRC. IRC is a network protocol designed to provide real-time group chat. However, it is often (mis)used to control botnets.

To use this mode, the user has to fill in the address of the IRC server and the name of the channel ("#loic" by default), through which the attack commands will be sent. In the "Operation Payback", this information was initially distributed via the *Anon_Operation* Twitter account. An example can be seen in Figure 3. As soon as this account has been suspended, the new targets started to be distributed through other Twitter accounts and IRC channels.

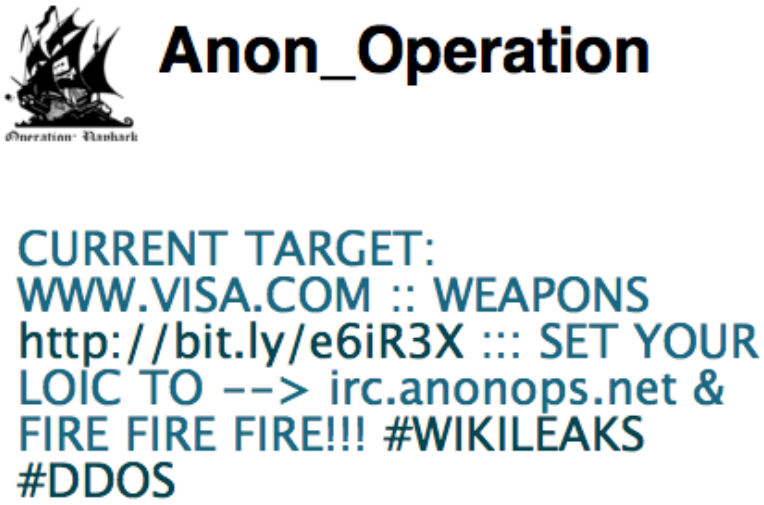

Figure 3: Message on Twitter informing a target and the IRC server for a new attack.

Once the tool is started in the automatic mode, the commands are set via the topic of the IRC channel. They have a straight-forward plain-text format:

```
!lazor args start
!lazor stop
```

As it could be expected, the first command starts an attack while the second

stops it again. The variable "args" contains a list of parameters, which includes the target host, the target port (when applicable), the attack method and a message to be included in the attack packets, among others. At the time of writing, the following was the topic in one of the channels associated with "Operation Payback":

```
!lazor default targethost=www.moneybookers.com subsite=/ speed=3
threads=15 method=tcp wait=false random=true checked=false
message=Sweet_dreams_from_AnonOPs port=80 start
```

2.2 Types of Attack

There are three types of attacks, each using a different packet type: UDP, TCP and HTTP. All attack types are similar; they open several connections to the same target host and continuously send a pre-defined string, set using the *message* parameter. In the UDP and TCP attacks, this string is simply sent in plain-text, while in the HTTP attack the message is included in the contents of a *HTTP GET* message. When a huge amount of messages is sent, the target host becomes overloaded and can no longer reply to requests from legitimate users.

The tool, however, does not attempt to protect the identity of the user, as the IP address of the attacker can be seen in all packets sent during the attacks. Internet Service Providers can resolve the IP addresses to their client names, and therefore easily identify the attackers. Moreover, Web servers normally keep logs of all served requests, so that target hosts also have information about the attackers.

3 Web-based LOIC (JS LOIC)

On December 9th, 2010, a new version of the LOIC tool was released, named "JS LOIC" [6]. This Web-based tool runs in any Javascript-supporting browser and, differently from the desktop version, does not required package installation. Next we present an analysis of the tool and how it exposes the users's real IP address.

3.1 Tool usage

Although JS LOIC looks very similar to its desktop variant, some differences can be identified. While the original LOIC tool supported two main modes of operation (*i.e.*, automatic and manual), the Web-based tool supports only one, namely the manual mode. As a consequence, the destination address/URL of the target host needs to be entered manually. At the moment of writing, an HTTPS server of Paypal was entered as the default destination host. A link to a list of current targets is provided as well, but the corresponding Web site was not reachable anymore.

Another difference compared to the desktop variant, is that JS LOIC does only support HTTP and no TCP and UDP attacks.

Figure 4 shows JS LOIC's interface with default settings. Besides the picture, the interface is divided in several 'steps'. The first step consists of the target URL/address, while the second step represents the button to start an attack.

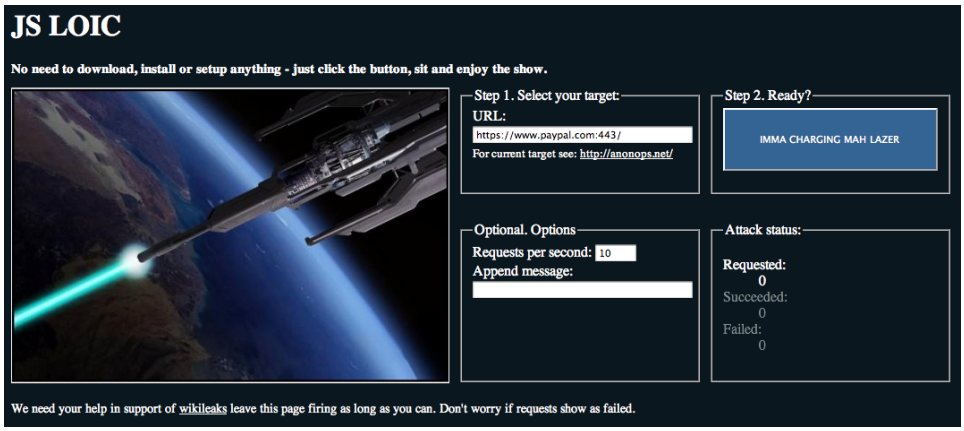

Figure 4: JS LOIC interface with default settings

3.2 How it works

After entering a target address/URL, an attack can be started. This is done by clicking the "IMMA CHARGING MAH LAZER" button. Before starting, some more advanced options can be entered in the Web interface, namely the amount of requests per second and a string that should be included in the attack messages.

Once the attack has been started, it will generate *HTTP GET* requests, based on random URLs. By trying to access these URLs, the source machine opens as many connections as possible to the target host. More concretely, LOIC will act as if it would download an image from the target host. The URLs consist of the following three parts:

1. *The target host's address/URL.* This is the URL which is provided in the Web interface, identifying the target host.

2. *A random*[1] *number in order to avoid caching.* By using this random number, the URL will differ from request to request. As a consequence, caching

[1] The current UNIX timestamp is used.

mechanisms will not work, since hosts will identify the requests as new ones every time.

3. *An optional message.* This is the message which could optionally be provided in the Web interface.

The rate at which the target host is tried to be connected is determined by the "Requests per second" field in the user interface. The default value is 10, resulting in 10 requests per second.

Figure 5 shows a trace of JS LOIC in operation. The following parameters were entered in the tool's Web interface:

- *URL*: 127.0.0.1, the local loopback address of the test host.
- *Appended message (optional)*: WikiLeaks JS LOIC.

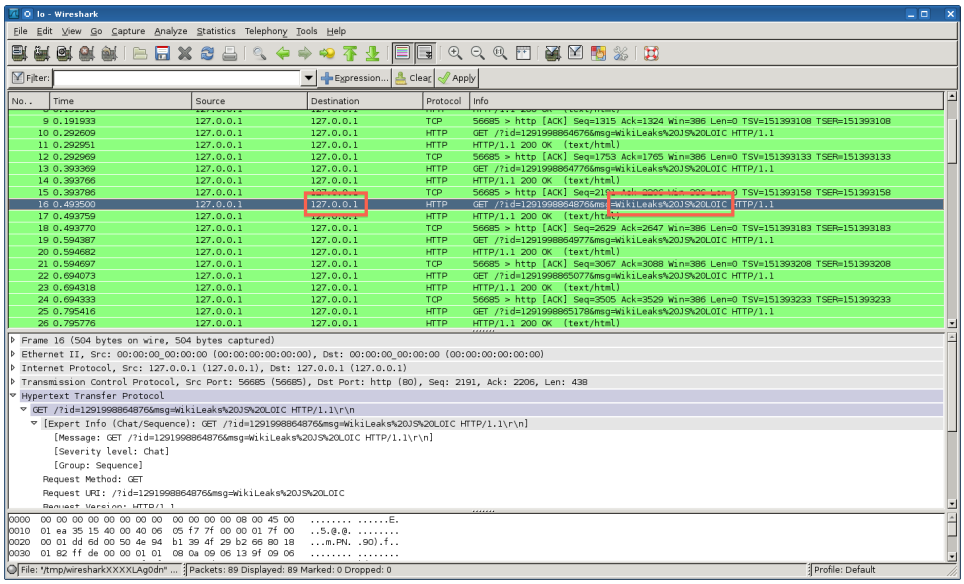

Figure 5: Wireshark trace of JS LOIC operation

As the trace shows, the (external) IP address of the test machine is used as the source IP address of the attack (leftmost red box in the figure). The rightmost red box shows the appended message and the destination URL. It can be concluded from the trace that the attacker's IP address is visible for the target host and other capturing hosts on the path towards the target host, and that no IP spoofing is used by the tool, for instance.

4 Is the Anonymous group really anonymous?

The time when hacking was an activity for a small elite is by now far away. The LOIC tool has shown that potentially anyone, more or less expert, can take part in a cyber operation from its own computer. It is out of the scope of this report to investigate where to draw the line between cyber-activism and cyber-crime, but it is clear that playing this game can put you in a legally uncertain position [7]. In the LOIC FAQ we read:

> Q: "Will I get caught/arrested for using it?"
> A: Chances are next to zero. Just blame you have a virus, or simply deny any knowledge of it.

We would like to rephrase the question as: is it technically feasible to identify a participant in the Anonymous operation? The answer depends on two factors: the tool and the generated data.

4.1 Does LOIC provide anonyminity?

In a lab-test conducted at the University of Twente, LOIC has been used to flood a fictitious target machine. The target has been equipped to analyze the traffic it was receiving by the LOIC tool. It became clear, already with the first analysis, that the tool does not take any precautions to obfuscate the origin of the attack. This means that the IP address of the attacker is included in the packets sent to the victim. The simplicity of the attack came to a surprise, since techniques are already known to obfuscate attack traffic. An example is *IP spoofing*, that substitute the original IP of the attacker with a fake one.

Basically, for the average user of the LOIC tool, it is like he was asked to send a menace letter with a return address.

4.2 Can data be retrieved?

The European directive on"the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks" (Directive 2006/24/EC) [8, 9] reports that, taking into account privacy legislation, telecommunication data must be "retained for periods of not less than six months and not more than two years from the date of the communication". Such data should be made available "for the purpose of the investigation, detection and prosecution of serious crime". This means that data are technically available, but only to public forces in case that they need to undertake an investigation.

Our analysis showed that users taking part in the Anonymous operations can be relatively easily traced. First, the LOIC tool does not provide anonyminity to its users. Second, operators must abide to the EU data retention policy and store communication data.

5 Conclusions

For a number of days the websites of MasterCard, Visa, PayPal and others are attacked by a group of WikiLeaks supporters (hacktivist). Although the group calls itself "Anonymous", researchers at the DACS group of the University of Twente (UT), the Netherlands, discovered that these hacktivists are easy traceable, and therefore anything but anonymous.

In this report we present an analysis of the two versions of the tool named LOIC (Low Orbit Ion Cannon, which is used by the hacktivists to perform their attacks. The main conclusion is that the attacks generated by the tool are relatively simple and unveil the identity of the attacker. Therefore, the name of this hacktivists group, "Anonymous Operation", is misleading: the hacktivists' original IP address is shown in clear.

If hacktivists use this tool directly from their own computers, instead of via anonymization networks such as Tor, the real Internet address of the attacker is included in every Internet message being transmitted, therefore making it easy to be traced back. We also found that these tools do not employ sophisticated techniques, such as IP-spoofing, in which the source address of others is used, or reflected attacks, in which attacks go via third party systems. The current attack technique can therefore be compared to overwhelming someone with letters, but putting your real home address at the back of the envelop.

In addition, hacktivists may not be aware that international data retention laws require that commercial Internet providers store data regarding Internet usage for at least 6 months. This means that hacktivists can still be traced easily after the attacks are over.

References

[1] WikiLeaks. http://wikileaks.nl, 2010.

[2] Guardian. US diplomats spied on UN leadership http://www.guardian.co.uk/world/2010/nov/28/us-embassy-cables-spying-un, 2010.

[3] WikiLeaks Twitter. http://twitter.com/wikileaks, 2010.

[4] CNN.com. WikiLeaks cut off from Amazon servers http://edition.cnn.com/2010/US/12/01/wikileaks.amazon, 2010.

[5] NewEraCracker. NewEraCracker/LOIC https://github.com/NewEraCracker/LOIC/, 2010.

[6] JS LOIC. http://files.hl2forums.com/uploads/1e55b2e_JS_LOIC_v0_1.htm, 2010.

[7] NOS.nl. 16-jarige bekent wikileaks-aanval. http://nos.nl/artikel/204089-arrestatie-in-den-haag-voor-wikileaksaanval.html, Dec. 2010.

[8] European Union. Directive 2006/24/ec. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, Dec. 2010.

[9] W. van Wanrooij and A. Pras. Data on retention. In J. Schoenwaelder and J. Serrat, editors, *Proceedings of the16th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2005), Barcelona, Spain*, pages 60–71, heidelberg, October 2005. Springer Verlag.