Detecting the Use of Anonymous Proxies

Jonathan McKeague, Ulster University, Londonderry, United Kingdom
Kevin Curran, Faculty of Computing and Engineering, Ulster University, Londonderry, United Kingdom

ABSTRACT
The Internet is built atop the Internet Protocol (IP) which has at its heart a unique identifier known as an IP address. Knowing the location of an IP address can be very useful in many situations such as for banks to know if a connection is in progress from online fraud hotspots. IP addresses can be spoofed allowing hackers to bypass geographical IP restrictions and thus render some category of fraud prevention useless. Anonymous proxies (AP) which act as intermediate relays which disguise the source IP addresses can play a large role in cybercrime. There is a need to ascertain whether an incoming IP connection is an original source matched IP address, or one being routed through an anonymising proxy. This article concentrates on various methods used by anonymising proxies, the characteristics of the anonymous proxies and the potential mechanisms available to detect if a proxy is in use.

KEYWORDS
Anonymous Proxies, Network Security, Security, Traffic Classification

1. INTRODUCTION
Almost 3 billion people access the Internet daily (ITU, 2013). Whether Internet users are checking and sending emails, reading an online newspaper, researching, doing online shopping or online banking, the need for a secure system is a major challenge for those who develop internet security systems (Mallia, 2013). This is especially true for users that use the internet to do business, or send private information, as more people are finding different ways to ‘hack’ into secure servers and exploit vulnerable data. In 2011 alone, the total amount that was stolen from businesses online amounted to $3.4 billion, which was up by $700 million from 2010 (Neustar, 2012). This figure is likely to increase, with businesses using the Internet more. It is therefore a priority for businesses to invest in methods to protect themselves against such attacks.

Internet misuse is also a major headache for employers due to the increase in popularity of websites such as Facebook, YouTube, Twitter and Google+. This has led to a decrease in the productivity

DOI: 10.4018/IJDCF.2018040105

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
of their employees, which in turn leads to less profit. Network administrators have therefore had to block many of these websites from being used in the workplace in an attempt to mitigate the problem. Initially they attempted to simply block the IP of the websites. IP addresses are registered to specific geographical locations, although they don’t give the exact area of where the user is located. However, it does pinpoint the country that is accessing the network (Goralski, 2008). IP blocking worked quite well, as anytime a user tried to access a website that had its IP blocked they would be denied access. This prompted users to try to find a way around the blocked IP’s.

One simple method was the use of a proxy. A proxy website masks the IP of the website that you are trying to view, which bypasses the IP blocking method used to detect the blocked website. Due to an increase in online banking, banks themselves have had to increase security in their systems and networks; examining IP’s is one method they utilize. If a user is making a transfer online and the IP looks fraudulent, then the account holder will be contacted before the transfer is verified. There are thousands of free PHP/CGI proxies to use online, making it a simple way to bypass this basic security feature. Even if the proxy server that was used was blocked there are thousands more to choose from, making the task of blocking them difficult (Lyon, 2009). The code for all of these proxies is open source, it can be downloaded and setup with ease, which means that anyone with a computer could theoretically create a proxy server. Another method that can be used to bypass security measures is Onion Routing (e.g. Tor Browser) which is used to anonymize a user’s traffic on the internet. This method uses a different port than what is typically used to access blocked websites. Onion Routing works by routing internet traffic through many different hosts, encrypting data at each different host (Dingledine et al, 2004).

This paper outlines a system called DetectProxy which can detect if any proxies are being used in the network by comparing the characteristics of the different proxies. This will be accomplished by analysing the packets entering the network using scripts to determine the type of proxy being used. Once the proxies have been identified, information will be sent to the network administrator. They will then be able to examine the time the proxy was in use and will give them the option to block the proxy if the proxy has been determined to be harmful or not needed on the network. Blocking the proxy will provide a more secure network for the business or institution.

2. ANONYMOUS PROXIES

This literature review will be split up into two different sections. The first section will discuss the different ways people can access networks and systems using anonymous proxies. The second section will discuss the different ways of stopping or blocking the anonymous proxies and the different tools used to aid this. Some of the main proxies or ways to access the Internet anonymously are PHProxy, CGIProxy, Glype, Onion Routing/Tor and SSL Proxy.

PHProxy is one of the most commonly used Anonymous Proxy Servers. The code is written in PHP and can be obtained from SourceForge1. It can run on Windows, BSD (Berkeley Software Distribution), Solaris and Linux platforms, therefore making it possible to run on the majority of platforms. When taking a closer look at the statistics of the amount of times the code has been downloaded, we will see that over the past year there has been a gradual decrease, with the most downloads being 573 in one month and the lowest being 243, these statistics can be found on the SourceForge website2. A sample of a proxy website that uses PHProxy can be found at http://wb-proxy.com/. This website simply allows the user to enter the URL destination that they would like, once entered it will re-direct the user to their website; this can be seen in Figure 1.

The resulting URL when the user clicks ‘Browse’ is as follows:

http://wb-proxy.com/index.php?q=aHR0cHM6Ly90d2l0dGVyLmNvbS8%3D
Pirates of the Copyright and Cyberspace: Issues Involved
www.igi-global.com/chapter/pirates-copyright-cyberspace/50714?camid=4v1a