Open Web Proxies
on the
Cornell University Network

Daniel Adinolfi, CISSP
dra1@cornell.edu
Senior Security Engineer
Cornell Information Security Office

Abstract
An ongoing, and perhaps increasing, problem facing many universities is the protection of copyrighted material made available through online services such as Books 24X7 or JSTOR. Several factors that make providing the protection of these services difficult to accomplish will be discussed.

To aid with the ongoing effort to minimize the abuse of these electronic resources at Cornell University, the Information Technology Security Office of Cornell University offers the following discussion of open web proxies. This white paper is intended for system and network administrators responsible for electronic resources at Cornell University to aid in the identification and removal of open web proxies.
Introduction

In the first half of the calendar year 2003, the Cornell Information Technology Security Office has responded to over a dozen reports concerning the abuse of open web proxies on the Cornell network. Open web proxies are servers that allow the caching or relaying of World Wide Web traffic without the use of authentication or authorization.

The abuse of open proxies is particularly troublesome when copyright material is involved. This abuse leads to violations of vendor licensing, which may result in the loss of this particular resource or financial fines, both of which could be detrimental to Cornell's mission.

This paper will provide a full description and problem statement concerning the existence of open proxies within an otherwise well protected infrastructure or service, will identify some techniques for finding open proxies within a given infrastructure, and outline some steps to mitigate this risk.

The Problem with Open Web Proxies

Open web proxies have become a growing problem within the Cornell network infrastructure. Two major issues have arisen around the existence of open web proxies. The first issue involves unauthorized use of Cornell assets. The second issue is the associated network usage charges that will result in this unauthorized use.

The first issue of unauthorized use arises when people not affiliated with Cornell University use open web proxies to access data that is restricted to Cornell University affiliates only. Authorized users are Cornell students, faculty, and staff, or anyone using the Cornell University Library. Mandated by the State of New York, everyone should and can make use of Cornell University Library facilities provided they are at the physical location of the library. The most significant abuse of this access is when unauthorized users exploit an open web proxy to access copyrighted publications that are available to Cornell through special licensing agreements. The abuse is a result of publications being downloaded in bulk, which violates the licensing agreement Cornell has with the vendors offering the publications in electronic form. In addition to violating vendor licensing agreements, within the Cornell network, this activity violates Cornell's Responsible Use of Electronic Communications policy as listed here: <http://www.univco.cornell.edu/policy/RU.html>.

Currently, access to vendor resources is regulated by the IP address used to access that information. Cornell University has given the vendors the range of IP addresses that make up the Cornell network. Any user accessing vendor resources from this address space has unlimited access to those resources. Authorized Cornell affiliates who require access from outside of Cornell's network space use an authenticated web proxy for this access. This authenticated web proxy requires users to log into the proxy before being given unlimited access to the vendor resources. Unauthorized users, on the other hand, search out open web proxies and exploit these proxies for access.
The second issue involves the use of Cornell's network in general. As of this summer, each IP address on Cornell's network will be billed based on usage. People using open web proxies are bouncing their web traffic off the servers running the proxies. That is a significant increase to the traffic going to and from those servers, and that increase will be reflected in the bills network and system administrators will receive for their systems. For example, a system that typically uses less than 2GB of bandwidth a day (this is typical of a normal PC user) would be charged $4 a month for network usage. If, on the other hand, this same system were to inadvertently be set up with an open proxy, it would not be unusual for network usage to increase to over 2GB of bandwidth per day resulting in a network usage charge of the $4 monthly fee plus three-tenths of a cent per megabyte over the 2GB each day under the current network billing rules for Cornell.

Experience has shown us that in the vast majority of cases the typical open web proxy is not an intentional service. Instead, it is either the misconfiguration of a web server or the result of actions performed by an uninformed system administrator allowing the web proxy to exist. The most common server associated with this problem is a WebStar web server running with its default configuration. Alternately, we have seen open web proxies based on IIS Servers that are misconfigured or are not taking advantage of built-in access controls. We have also found that many new web proxies are coming online every day because of a misunderstanding of how and why they work.

In response to the increase of these violations, the IT Security Office performed an initial port scan in early May 2003 as a method to assess the size of the existing problem. This scan searched for common ports used by web proxy software, specifically TCP port 1080, 8000, and 8080. Over 750 systems were found to have some software running a service at one of these ports. From these scans, there was no way to know if the server running at the open ports was needed for a legitimate service or if it was running without the knowledge of the system and network administrators. The Security Office has attempted to educate information technologies staff across campus with regard to the problems such rogue servers may cause. (Also, additional surveying tools have been tested and utilized to help locate open web proxies before they become a problem. The development of these tools is an on-going process with varying degrees of success.)

Finding Open Web Proxies

There are a set of standard ports at which web proxy software usually runs. These include the TCP ports 1080 (SOCKS), 3128 (Microsoft Proxy), 8000, and 8080. Also, there are a large number of viruses, trojan horse programs, and other software that open web proxy servers on systems without the knowledge of users or administrators. Scanning your subnet for systems listening on these ports is one way to find web proxies. Also, on each individual system, you can look to see what ports are listening with commands such as “netstat”. For more information on the large number of system administration tools, refer to each operating system's documentation or visit some of the online resources listed at <http://www.google.com/search?q=System+Administration+tools&ie=UTF-8&oe=UTF-8>.

Additionally, you can deduce the presence of web proxy software based on the existence of other, related software. WebStar web server software comes with web proxy plug-ins
out of the box. If a system is running the Microsoft Internet Information Server (IIS),
Microsoft Proxy Server or Microsoft ISA Server could be installed. On Unix systems,
squid is a common proxy server that is usually part of the full distribution of many Unix
variants.

<table>
<thead>
<tr>
<th>Product</th>
<th>Vendor</th>
<th>Web Site</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebStar</td>
<td>4D, Inc.</td>
<td><a href="http://www.4d.com/">http://www.4d.com/</a></td>
<td>MacOS 7.x, 8.x, 9.x</td>
</tr>
<tr>
<td>squid</td>
<td>open source</td>
<td><a href="http://www.squid-cache.org/">http://www.squid-cache.org/</a></td>
<td>Unix variants, including MacOS X, Linux, BSD variants, Solaris, HP-UX, AIX</td>
</tr>
</tbody>
</table>

**Removing or Reconfiguring Open Web Proxies**

It is rare that a web proxy requires anonymous access. It is even more rare that the web
proxy is necessary at all. Assuming the proxy is not a requirement for your environment,
removing or disabling the proxy is the best way to ensure no one takes advantage of its
presence to abuse Cornell resources.

- If you believe your system is running a trojan horse program that has a web proxy
  component:
  - Update and run antivirus software to find and disable the software.
  - If the antivirus software is not able to find or disable the proxy, you will
    need to remove the trojan horse software manually.
  - If this proves to be too difficult or time-consuming, you must backup,
    wipe, and reinstall the infected system. The Cornell University CIT
    Helpdesk <http://www.cit.cornell.edu/helpdesk/> can offer assistance with
    this entire process.

If you find that a web proxy is configured to run as part of another software package, you
will need to disable or reconfigure that software.

- If you are running WebStar <http://www.4d.com/products/webstar.html>, the
  method for disabling the open web proxy depends on the version of software you
  are running.
  - For version 3.x and lower, you will need to remove the WebStar Proxy
    extension and related plug-ins from the WebStar directory.
For version 4.x and higher, you can disable the proxy server via the WebStar Admin Tool: set the number of connections allowed through the proxy to zero. Alternately, you can remove the WebStar Proxy extension and related plug-ins. Either method will work for version 4.x and higher.

- If you are running IIS with either the Microsoft Proxy Server or Internet Security and Acceleration (ISA) Server, you can either disable the service within the IIS Administration tool or use the built-in access controls to limit who can use the proxy.
- If you are running a squid or SOCKS
  - Either disable the server, or
  - Use any built-in access controls to limit who can use the proxy.

Conclusion
Open web proxies are an ongoing nuisance on the Cornell University network. Network and system administrators must be vigilant in their efforts to remove these proxies or configure them such that they cannot be used without authorization. This paper has explained the nature of the abuse of open web proxies, how to identify them, and how to take corrective action to disable or properly configure open web proxies.

Appendix

For more information on the WebStar Proxy Server, contact the makers of WebStar, 4D, Inc. <http://www.4d.com/>.


For information on Squid proxies, visit <http://www.squid-cache.org/Doc/FAQ/FAQ-10.html#ss10.1>. For information on the SOCKS protocol and configuration, visit <http://www.socks.permeo.com/>.