

Anonymous Proxy: A Growing Trend in Internet Abuse, and How to Defeat It

ABSTRACT

Anonymous proxies are an unseen threat—a student’s or employee’s backdoor to malicious or productivity-sapping sites on the Internet. If your URL filtering solution relies on the old-school URL database/keyword approach, your ship is leaking and you may not see the holes.

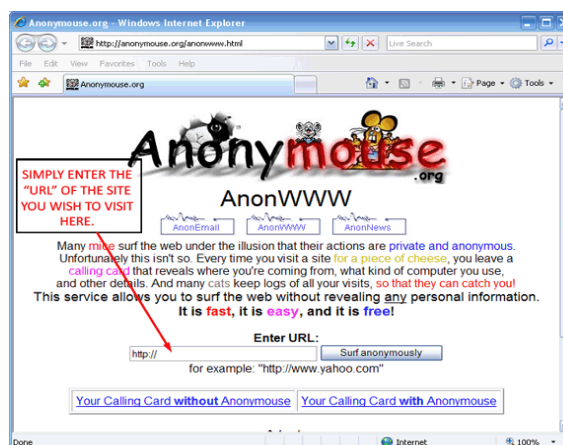
With hundreds of new proxy sites created each day, traditional URL filtering just can’t keep up, even when supplemented by standard keyword analysis. What follows is a primer on the problems, the sizable costs and time drain for IT professionals, and a discussion of an effective third-generation solution that goes far beyond the traditional strategy.

INTRODUCTION

Anonymous proxies are an unseen threat—a student’s or employee’s backdoor to malicious or productivity-sapping sites on the Internet. If your URL filtering solution relies on the old-school URL database/keyword approach, your ship is leaking and you may not see the holes. With hundreds of new proxy sites created each day, traditional URL filtering just can’t keep up, even when supplemented by standard keyword analysis. What follows is a primer on the problems, the sizable costs and time drain for IT professionals, and a discussion of an effective third-generation solution that goes far beyond the traditional strategy.

WHAT ARE ANONYMOUS PROXIES, AND WHY ARE THEY A BIGGER PROBLEM THAN WE THINK?

Anonymous proxies are the most popular and easiest way for users to bypass Internet filtering. Once connected to an anonymous proxy, users can view any site, even if the web filter should have blocked it. Proxy sites have proliferated considerably in the past few years due to availability of open source tools, which allow a proxy site to be created quickly and easily. This phenomenon emerged around 2002, when there were only a few sites offering anonymizing services. Now there are over 100,000 registered anonymous proxy sites, an estimated 300,000 home based anonymous proxies, and given the open source nature of the software, there are hundreds of new ones created every week¹. These proxies represent a frustrating and fairly recent variation of a general problem that administrators have battled over the last several years: the dangers and costs of uncontrolled internet abuse by students and employees. Although the Web can be a remarkable educational and business tool, it can also allow users to waste incredible amounts of time on unproductive and possibly hazardous activities.



Most schools and colleges are blocking or limiting web sites, but unfortunately the widespread use and proliferation of anonymous proxies has rendered URL-based web filters useless. This is worrying as schools and colleges have a duty of care to ensure that children are protected from the pernicious aspects of the Internet – pornography, violence, racism, etc. Schools and colleges suffer from limited budgets or are forced to use less than satisfactory solutions supplied through their local authority, and some are investing large sums in internet filtering solutions that students can simply and easily bypass.

The problem is enormous in the adult world as well, particularly with “Millennials,” an exceptionally tech-savvy new generation of employees who use every gadget imaginable; IM, social networking, YouTube, etc. are part of their everyday lives. But it is not just millennials who depend on the Internet for personal and social needs. Ninety percent of employees acknowledge that the Internet can be addictive², and their obsessions often include pornography, social networking (e.g. MySpace), or shopping sites. Seventy percent of porn traffic occurs during the nine-to-five work day, and 60 percent of online purchases are made during these hours³. Frustrating an addiction causes anger and withdrawal anxiety, and many users welcome opportunities to outwit filters, which is what anonymous proxies offer. Anonymous proxies are very attractive because they almost restore the ease, pleasure, and privacy that was originally associated with unfettered internet surfing. Why is this such a problem? According to a Symantec survey of corporate IT managers, 89 percent reported an increase in their risk exposure in the past five years, largely because of a new wave of technologies and the millennial workforce’s freewheeling attitude. The survey found that 36 percent of managers believed the increased risk warranted writing and enforcing new policies, and 67 percent considered at least restricting the use of the latest Web 2.0 applications and smart devices⁴.

¹ [http: “The Quandary of Web Anonymizers,” p.3, http://www.aladdin.com/esafe/whitepapers.aspx](http://www.aladdin.com/esafe/whitepapers.aspx)

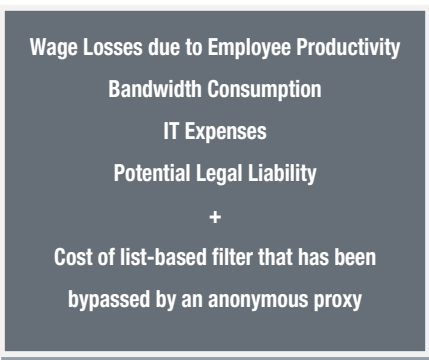
² Snapshot Spy, <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>

³ Ibid

⁴ <https://forums.symantec.com/syment/blog/article?message.uid=310250>

WHAT IS THIS PROBLEM COSTING YOUR COMPANY?

An International Data Corporation survey indicates that 30 to 40 percent of on-the-job internet use is non-work-related⁵. Other studies report that 64 percent of employees use the Internet at work for personal interests, and 37 percent of workers say they “surf the Web constantly” while on the job⁶. The productivity implications are staggering; they include wasted wages, lost business, and expensive efforts by IT departments to block unacceptable websites and clean up productivity-destroying malware acquired from web downloads. In addition, an organization’s legal vulnerability increases when employees illegally download copyrighted or proprietary material or offensive text and images that can be disseminated throughout the enterprise. Surfing also can have a negative effect on network performance, since users often visit sites to view bandwidth-consuming videos.



Organizations have generally responded to internet abuse by installing list-based filters that block access to offensive sites, limit hours of access to other sites (e.g. shopping), or allow access to some sites for some employees but not for all. Anonymous proxies have changed the game entirely. Essentially, an anonymous proxy is a tool for subterfuge; it attempts to fool and circumvent first line defenses against internet abuse. Anonymizers are so malicious because they are designed to evade standard filtering solutions; they are easy to build, access, and use; and they work, leaving organizations exposed to all of the problems mentioned above.

HOW DO ANONYMOUS PROXIES WORK?

An anonymous proxy is a special form of the normally innocent “proxy server.” In computer networks, a proxy server mediates the requests of clients by forwarding them to other servers. So a client might request a file, web page, etc. from the proxy, which then connects to another server, retrieves that file or web page, and delivers it to the client. Roughly, an anonymous proxy is a website user’s access to reach URLs that would otherwise be blocked by an effective list-based filter. The anonymizing website is not itself on the filter’s blacklist—or at least, not yet—and the user can go to that site, type in the blacklisted URL, and the proxy then connects to the forbidden web page. A standard web filter identifies only the proxy’s URL, which it accepts, but does not detect the destination URL, and therefore does not block the request.

There are at least three kinds of anonymous proxies: commercial, non-commercial, and private proxies located on home computers and accessed from school or work by the computers’ owners. Commercial sites make their money by either charging users or selling ads⁷. Non-commercial anonymous proxies are sometimes set up by libertarian-minded individuals who resent attempts to limit unregulated internet access. However, both kinds of sites can exist for more malicious reasons: to harvest usernames and passwords and disseminate malware and spyware. Some sites don’t function as proxies themselves, but are sources of software that individuals can download to create their own proxies. Since the software is normally open source, it is usually free, and requires little technical knowledge to download, install, and operate. Anonymizers can mask the IP addresses of the proxy computers, so it is hard to associate private proxies with specific individuals.

⁷ Snapshot Spy, <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>

⁸ Ibid.

⁹ http://proxy.org/cgi_proxies.shtml

A LOSING BATTLE

Anonymous proxies are particularly hard to block with traditional technology. Of course, IT professionals can try, but the task is overwhelming. Anonymous proxies are generally designed to go undetected. Their names—for example, “guardster.com”—are rarely indicative of their function, and IT staff generally must run a report to spot an inexplicable spike in visits before they will inspect a site. Also, anonymizing features are often hidden several layers down in what looks like an ordinary site, so the site’s function can be difficult to determine. Keyword analysis can sometimes work, especially on commercial proxies, which posts ads with words like “bypass,” “proxy,” and “filtering.” But non-commercial sites avoid much of this language, and private sites need not use any anonymizing terminology. Keyword filtering also sometimes over-blocks, preventing users from reaching legitimate sites.

But the biggest problem by far for IT is the rapid proliferation. Given the software is open source and given the ease in creating an anonymous proxy, when IT kills a site for an organization, ten more can rise in its place. New anonymous proxies are created all the time, and people can quickly become aware of them through word-of-mouth, email, instant messaging, listservs, blogs etc—or they can just create private sites. IT staff can spend hours a week tracking anonymous proxies, but they can’t keep pace, and by the time the filtering supplier gets it into the database and sends the information to the field, days, weeks, or even months can pass.

WHAT CAN AN ORGANIZATION DO?

A successful strategy against anonymous proxies must include at least three elements: 1) third-generation filtering technology that combines the best in traditional approaches with more sophisticated, point-of-request page analysis that spots anonymous proxies in real time; 2) clear and well publicized AUPs that not only forbid access to anonymous proxies but emphasize the organization’s ability to detect them; and 3) an organizational willingness to consistently enforce AUPs. Elements 2 and 3 are non-technical managerial issues, but both, of course, presuppose an organization can acquire the third-generation technology. Fortunately, a cutting-edge solution is available from Bloxx.

Bloxx’s patented Tru-View-Technology combines URL databases and keyword scoring with far more intelligent identification and live contextual analyses to rapidly classify web traffic in real time. It doesn’t matter which of the over fifty default Bloxx categories a URL belongs to—shopping, violence, travel, anonymous proxy—Tru-View Technology controls the URL with minimal effort from the IT staff. Tru-View automatically categorizes and filters up to six million web pages a day—including all pages not listed in the URL database—to provide zero-day protection. With respect to anonymous proxies, the technology not only looks for common words and phrases, but for code structures characteristic of such sites, and analyzes the relationships between these elements to build levels of classification confidence. If the level rises above a specified threshold, Tru-View will block the web page, even if no one in the organization had previously visited it. The technology also examines all layers of a site to find hidden proxy functionality, and it is extremely accurate. It will not, for example, mistake a Wikipedia page about anonymous proxies for an anonymous proxy itself. Yet if the Wikipedia page were to link to a real anonymous proxy, Tru-View Technology would block that site as soon as a user tries to visit. Moreover, the extensive reporting capabilities allow IT to identify users who try to access anonymous proxies.

CONCLUSION

In short, while the Internet can be a marvelous productivity tool, it can also be a tremendous drain, as well as a threat to our children. Tru-View Technology maximizes the positives and eliminates the negatives so that organizations can meet the challenges of an 8+ billion-page Internet that is growing by almost 50 percent every year. The Web’s expansion requires the kind of real-time, comprehensive, and discriminating Internet filtering that is only provided by Bloxx.

ABOUT BLOXX

Bloxx is a privately held company with offices in the U.S., U.K., The Netherlands, and Australia and offers web filtering appliance-based solutions for medium and large organizations in both the business and public sectors. In 2007, it was recognized by Deloitte as one of the U.K.'s Top 50 Fastest Growing Technology Companies in its prestigious "Fast 50." For more information please visit: www.bloxx.com.

ABOUT BLOXX TRU-VIEW TECHNOLOGY

Bloxx Tru-View Technology uses internationally patent pending technology to analyze and block web sites quicker and more accurately than other web filters, which use manual classification and keyword scoring. Tru-View Technology uses intelligent identification and analysis providing instant classification of web content as soon as it is accessed even if the content has not been seen by anyone before.

Bloxx Tru-View Technology helps organizations proactively manage users' access to web content which might lower productivity, expose the organization to risk and liability or pose a network security threat.

An estimated 1 million + users already benefit from enhanced security and performance with low administration and no cost per user charges. Additional protection is provided via anti-virus, anti-spyware and anti-phishing functionality, alongside onboard cache.

To learn more about Bloxx web filtering technology, book in for an online demonstration at bloxx.com/demo, call +44 (0)8700 4 25699 or email info@bloxx.com.



Deloitte. Deloitte.
Technology Fast50 Technology Fast50
EMEA 2008