

## The enemy within: Stop students from bypassing your defenses

Computer literate K-12 students regularly use anonymizing proxies to bypass their school's web filters to access pornography, social networking, and other blocked websites. This is a major security flaw because most infected networks are first exposed via the web. Moreover, it has serious legal ramifications for schools that are not in compliance with state and federal laws. However, reputation and real-time detection can automatically identify and block anonymizing proxies. This white paper discusses the risks of students bypassing web filters and the technologies that schools can use to combat them.

by Chris McCormack  
Sophos Product Marketing Manager

# The enemy within: Stop students from bypassing your defenses

## The threat of the web

The web has replaced email as the primary entry point for malware into a network, with a brand new infected webpage discovered approximately every 4.5 seconds<sup>1</sup>. The majority of these are legitimate sites – government agencies, Google, MySpace, Facebook, the Cambridge Dictionary, BusinessWeek, and many more have all fallen victim to hackers. Clicking on such pages poses a multitude of risks to networks, including the loss of confidential information, virus and spyware infection and botnet recruitment.

## Schools in the front line

K-12 schools are particularly at risk from web-delivered malware – and it is often introduced by the very people they need to protect: students. Not only are many children extremely technically skilled, but they have ample opportunity to work unobserved in internet-connected computer labs and libraries, which are used by hundreds of different students every day.

Unlike corporate environments, where adult users have jobs, salaries and reputations to worry about, K-12 students often don't know or don't care about

the consequences of their actions to the school network. Bypassing network controls to access restricted websites is usually just considered an entertaining challenge, or a way to burnish an anti-establishment image. However, in addition to ensuring their own network security, schools are held responsible by parents and state and federal laws – such as the Children's Internet Protection Act (CIPA) – with protecting young, impressionable minds from web predators and harmful content. One example of a student bypassing a school's web filters involved an eighth grader in Texas who downloaded pornography during a study group<sup>2</sup>.

## Bypassing web filters

Students across North America are increasingly turning to anonymizing proxies to bypass their school's web filters to view pornography or access banned social networking sites. Anonymizing proxies are widespread, with several hundred new proxies published daily. Easy to access and difficult for traditional security software to detect, anonymizing proxies are web sites that trick an organization's web filter into thinking the user is browsing legitimate content. The user visits the anonymizing site first and enters their intended URL, and the proxy then opens a portal to the student's desired destination. Traditional web filters only identify the anonymizing proxy URL, not the destination URL, and as such often allow the request. In some cases, the student simply configures his or her web browser to point automatically to the anonymizing proxy, ensuring that all web activity is hidden.



**K-12 schools are particularly at risk from web-delivered malware – and it is often introduced by the very people they need to protect: students.**



Aside from disguising banned content, anonymizing proxies change constantly, with scores of new ones appearing daily. K-12 school IT administrators spend hours each week tracking down and blocking anonymizing proxies, significantly affecting resources and overheads.

Many web sites also offer daily updated lists of anonymizing proxies. A quick Google search will produce hundreds of anonymizing proxy sites. There are even video instructions on YouTube that show students how to construct one. It is also not difficult for computer savvy students to set up their own anonymizing proxies at home, using one of the many free utilities available online.

## Defeating anonymizing proxies

There are a number of ways that schools can complement their existing web filtering technology to identify and block anonymizing proxies:

- Reputation detection services
- Real-time proxy detection
- User education

### Reputation detection services

Reputation detection services constantly track publicly known anonymizing proxy sites and the forums<sup>3</sup> that exchange their details. They are then able to update a school's web filters – ideally every 15 minutes or faster – to ensure that the web gateway security solution stays ahead of the student grapevine. Reducing the amount of time an anonymizing proxy is available to a student provides a major inconvenience to their ability to track and use such services.

“

Anonymizing proxies are widespread, with several hundred new proxies published daily.

”

The screenshot shows a Google search for "bypass school web filters". The search results include:

- Web** Video
- How do you bypass school/corporate internate filters - Network ...** 23 Apr 2006 ... How do you **bypass school/corporate internate filters** - Network Security Community and Forum - Our Network Security forum is the place for ... [www.danivweb.com/forums/thread43937.html](http://www.danivweb.com/forums/thread43937.html) - 62k - Cached - Similar pages
- Digg - Kids Outsmart Web Filters** Kids Outsmart **Web Filters**. news.com.com — Title says it all. As students are discovering innovative ways to **bypass school filters**, the administrators are ... [digg.com/security/Kids\\_Outsmart\\_Web\\_Filters\\_2](http://digg.com/security/Kids_Outsmart_Web_Filters_2) - 82k - Cached - Similar pages
- Bypass website filters at school? [Archive] - techPowerUp! Forums** 30 Mar 2008 ... [Archive] **Bypass website filters at school?** General Nonsense. [forums.techpowerup.com/archive/index.php/t-10361.html](http://forums.techpowerup.com/archive/index.php/t-10361.html) - 54k - Cached - Similar pages
- How to Bypass a School Filter - wikiHow** wikiHow article about How to **Bypass a School Filter**. ... If the **web filter** blocked even the IP address of the site, you can take each number in the IP and ... [www.wikihow.com/Bypass-a-School-Filter](http://www.wikihow.com/Bypass-a-School-Filter) - 39k - Cached - Similar pages
- Guide: 10 Ways To Bypass School Web Filters Vol. 1 - Critical ...** 29 Dec 2005 ... Guide: 10 Ways To **Bypass School Web Filters** Vol.1, Nothing stupid, serious questions and answers only - real guide not s. Options V ... [www.criticalsecurity.net/index.php?showtopic=3372](http://www.criticalsecurity.net/index.php?showtopic=3372) - 123k - Cached - Similar pages
- YouTube - Bypass school or home web filters** This video will show you how to **bypass** those pesky home and ... 1 min 10 sec - [www.youtube.com/watch?v=Fxfjxq1Koyo&feature=related](http://www.youtube.com/watch?v=Fxfjxq1Koyo&feature=related)
- Bypass your School and Work Filters with an Anonymous Proxy Server** **Bypass your School** and Work **Filters** with an Anonymous Proxy Server. ... **Web** Applications Penetration Testing - Security Measures - Security Assessment ... [ezinearticles.com/?Bypass-your-School-and-Work-Filters-with-an-Anonymous-Proxy-Server&id=112347](http://ezinearticles.com/?Bypass-your-School-and-Work-Filters-with-an-Anonymous-Proxy-Server&id=112347) - 45k - Cached - Similar pages
- Mattbob | How To: Bypass Your Schools Web Filtering System** How To: **Bypass Your Schools Web** Filtering System. These tips may not work depending on what software your **school** uses to **filter** certain websites but after a ... [mattbobjones.com/thoughtsidesas/how-to-bypass-your-schools-web-filtering-system/](http://mattbobjones.com/thoughtsidesas/how-to-bypass-your-schools-web-filtering-system/) - 115k - Cached - Similar pages
- Bypass school web filter, become a felon - Boing Boing** **Bypass school web filter**, become a felon. Posted by Xenii Jardin, June 28, 2005 3:44 PM | permalink. Thirteen high **school** students in Pennsylvania are up ... [www.boingboing.net/2005/06/28/bypass-school-web-fi.html](http://www.boingboing.net/2005/06/28/bypass-school-web-fi.html) - 25k - Cached - Similar pages

### Real-time proxy detection

Some anonymizing proxies are kept a closely guarded secret, or built at home for the exclusive use of one person. Because their details are not shared they are immune to reputation detection services and must be tracked in real time.

Real-time detection monitors and analyzes all web requests and responses for signs that traffic is being routed through an anonymizing proxy. If one is detected, the request can be blocked. Signs that a student is using an anonymizing proxy include URL strings hidden within other URLs, and partially encrypted URLs. Real-time detection relies on strong decryption capabilities, as many proxies use encryption to hide their actions.

## User education

User education is always a central pillar of enforcing a web acceptable use policy (AUP), and many schools require students and their parents to formally sign their acceptance of such policies and ensure that they are aware of the consequences of violating them. AUPs should always contain a clause forbidding the use of anonymizing proxies, and state that controls are in place to monitor and detect their use. Formal AUPs do deter many students from trying to get around the rules, particularly if that information is part of a memo sent to parents.

Many schools also run internet safety classes as part of their computer curriculum, which can be utilized to explain more fully the dangers of anonymizing proxies and the thinking behind the AUP.

## Summary

Anonymizing proxies allow students to bypass their school's web filters to access inappropriate and blocked content. Their large and ever-changing numbers and ease-of-use make them difficult to block, and schools can find themselves legally liable if minors are accessing pornography and other sites from within the network. However, reputation and real-time detection will identify and block anonymizing proxies, and user education will ensure that students and parents are aware of the risks in bypassing web filters.

## Key questions to ask a security vendor

Schools need to identify and block anonymizing proxies quickly to ensure that students are not bypassing web filters to view pornography or social networking sites. IT administrators should ask their security vendors if their web security product can do the following:

- » Does it automatically detect and block anonymizing proxies?
- » Does it use a reputation service that scans proxy sites and related online forums to identify new anonymizing proxies as they appear?
- » Can it update its proxy list every 15 minutes or faster?
- » Can it detect private anonymizing proxies in real-time?
- » Can it decrypt complex encryptions of URLs?
- » How many new anonymizing proxy sites are catalogued every day?

## Sources

- 1 <http://www.sophos.com/pressoffice/news/articles/2008/04/secrep08q1.html>
- 2 <http://www.kcentv.com/news/c-article.php?cid=1&nid=14123>
- 3 [http://digg.com/security/Kids\\_Outsmart\\_Web\\_Filters\\_2](http://digg.com/security/Kids_Outsmart_Web_Filters_2)

---

## Sophos solution

Sophos Web Appliances, part of Web Security and Control, block spyware, viruses, phishing, malware and unwanted applications at the gateway, searching for and blocking anonymizing proxies, and enabling comprehensive web access control for safe, productive web browsing. They feature an innovative, full-spectrum scanning engine that detects all threats through a unique combination of reputation-based filtering, real-time predictive threat filtering, and content-based filtering. Their easy-to-use management console and powerful reporting tools deliver rapid insight into web traffic, threats and user behavior, enable secure browsing without the complexity of traditional web filters. As managed appliances, the Sophos Web Appliances feature remote “heartbeat” monitoring and on-demand remote assistance, ensuring they deliver the most dependable web security in the industry.

Boston, USA | Oxford, UK

© Copyright 2009. Sophos

All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

**SOPHOS**  
WWW.SOPHOS.COM