



Are Proxy Anonymizers Putting Your Enterprise in Peril?

By The Forsite Group

INTRODUCTION

Chances are, your company deploys Web filters to fight off the threats lurking in cyberspace. And chances are, some of your employees have no trouble bypassing them.

How are they undermining your best efforts to defend the enterprise? By accessing Web pages hosting proxy anonymizers, simple scripts that give surfers a way to get to sites that are officially off-limits. Also known as Web proxies, they're written in open source—allowing just about anyone to create them and making them more numerous than ever. They're easily available and almost always free. With so many new ones being created every day, ordinary filtering technology based on URL blocking just can't keep up. And because they don't raise red flags in log files the way unapproved sites do, they elude easy detection by IT security staff.

By essentially rendering ordinary filters useless, proxy anonymizers expose companies to all of the familiar downsides associated with unauthorized Web surfing. Malware, spyware, and viruses are more likely to make their way onto the corporate network, putting data at risk and performance in question. Employees are likely to spend more time on MySpace, LinkedIn, and other sites than in doing productive work. And legal liability is likely to grow, as inappropriate or offensive material lands in the wrong in-box or loads as wallpaper.

Like many modern threats to enterprise security, the use of proxy anonymizers is in large part a behavioral issue. Educating employees on the dangers, updating acceptable use policies to reflect the risks, and treating violations of the rules with the seriousness they deserve are all necessary steps in addressing it.

But defending against proxy anonymizers also means deploying the right technology. Enterprises need a solution that goes beyond URL blocking, that identifies and filters HTTPS requests, and that enables monitoring of the non-standard ports proxies can sometimes make use of.

Like many modern threats to enterprise security, the use of proxy anonymizers is in large part a behavioral issue.

THE COMING PLAGUE

Proxy anonymizers are easy to use—which means they pose a disproportionately large risk to your company. All an employee has to do is visit one of the numerous sites that make them available, download the software to a Web page he or she has created, then use that page as a launching pad to whatever unauthorized site is the real destination. The proxy anonymizer masks the IP address of the user's machine and essentially becomes the "system" that actually requests the page. Because this system isn't on the enterprise network, the Web filter can't flag any of the requests that are made from it.

As recently as a few years ago, there were only a handful of sites offering proxy anonymizers. Now tens of thousands.

Why?

- The software used to create proxy anonymizers is now open source and freely available
- The software is very easy to use
- Anyone can get a free Web page on which to post the newly created proxy anonymizer

The net result?

Because anyone, anywhere can create a proxy anonymizer at any time, there's no way to update a Web filter's URL list fast enough, which means the proxy goes undetected.

Why can't companies just compile black lists of the sites from which proxy anonymizers are available? Simply put, there's no way to keep up. As recently as five years ago, there were probably only a handful of proxy anonymizer sites, so few that simple URL blocking was an effective solution. But since then, the software used to write anonymizers has gone open source, enabling anyone to write and post them for anyone else to download. Proxy anonymizers probably number in the tens of thousands today, and more are coming online every minute, thanks to clearing-house sites dedicated to their creation and dissemination.

In fact, sites like Kortaz.com openly advertise the business they're in, with screaming graphics encouraging visitors to "bypass any filter at work, home, or school—be sure to bookmark, and tell your friends!" Over roughly four weeks in early 2008, more than five dozen new proxy anonymizers were posted on Kortaz.com. With names like InstantUnblock, Hide My Footprint, and PimpMyIP, they leave little doubt as to what they offer. And by boldly promising speed, reliability, and unfettered access to any site users want, their creators know just what their customers want.

While proxy anonymizers allow access to any unauthorized page, most seem to target users of social networking sites in particular.

That says something important about the culture that surrounds the use of proxy anonymizers: Many were originally intended for students seeking access to MySpace or Facebook from the computers in their school libraries and classrooms. Consequently, students have become adept at tracking down and using anonymizers—and creating their own.

So even as they conduct research for term papers and gain some useful computer skills, they're also getting an education in how to bypass filter technology.

How does that affect the enterprise? These students are now showing up in the workforce. And they see little wrong in making use of low- to no-tech tools to engage in what they view as their right to visit any Web site they want, even if they're at work.

At the same time, creators of Web anonymizers are turning their eyes to enterprise. While their main targets continue to be students, they recognize the potential of the employee population as a customer base. One even blogged about the enterprise opportunities for fellow developers of proxies, offering tips for offsetting the likely drop in business as the school year came to a close in 2007:

"The schools are off so hopefully you've got enough profit to still afford those servers when probably a large majority of your traffic is going to decrease. I'm not too worried but I'm prepared for my AdSense earnings to plummet. Good ways to counteract the school kids deficit is by going for the likes of office workers. So set up a proxy specifically for office workers ... keep some of your decent earnings from other months through this summer."

That would be enough to worry about without authorized sites functioning as de facto proxy anonymizers. For example, a simple hack can turn Google translator into a tool for accessing unauthorized sites. Employees simply type the following URL into their address bar:

<http://www.google.com/translate?langpair=enlen&u=www.forbiddensite.com> where "forbidden site" represents the URL of the unauthorized site. As easily as that, employees can get to a Web page that a filter would otherwise block.

THE PERILS OF PROXY

When employees have such easy access to such easy-to-use tools, companies are put in a tough position. They're more vulnerable to security threats, more susceptible to drops in productivity and network performance, and more exposed to legal liability.

Malware

Among the biggest danger to enterprises are the numerous strains of malware on the Web. Google researchers ran an analysis of 4.5 million URLs in 2007 and found that 450,000

(or 10%) of them engaged in drive-by downloads of malicious scripts; another 700,000 URLs were suspected of harboring malware.

Worse, the volume of malware is only growing; German testing facility AV-Test detected 5.49 million unique samples of malicious software in 2007, up from 972,606 in 2006. And increasingly, the hackers making use of the most sophisticated malware have much more than mischief on their minds; they're specifically targeting corporate data, either attempting to steal it outright or to block a company from using it—effectively holding it for ransom.

Social networking sites—among the most popular destinations of those who use proxy anonymizers—loom as particularly dangerous landing places when it comes to malware. TechTarget reported that in November 2007, the MySpace profiles of Alicia Keys and a number of other recording artists were found to be serving up malicious code. Another TechTarget story details a mysterious MySpace friend request that, when clicked, pops up an apparently legitimate "automatic update" window, which then attempts to download a mix of malware that includes additional downloaders, several Trojans, and a remote administration tool.

The SANS Institute notes a similar incident from September 2007, when a virus spread itself across Facebook by masquerading as a message from a trusted friend asking "Do you remember this girl?" Clicking on the photo that was alleged to be attached instead downloaded a host of infected files.

Reduced Productivity

The unregulated surfing enabled by proxy anonymizers also cuts into employee productivity. After all, when workers are clicking from Web page to Web page, they're not doing the job they're being paid to do.

This isn't news, but the impact of social networking sites in particular lends fresh perspective. A U.K. study recently found that employee visits to MySpace, Facebook, and similar sites costs businesses as much as \$15.5 billion a year in lost productivity. Just consider the attitude of a Goldman-Sachs employee—recently discovered to have been spending four hours of every workday on Facebook—to see how that's possible. Told by his bosses to stop, he instead posted the e-mail warning to his Facebook page, writing: "It's a measure of how warped I've become that, not only am I surprisingly proud of this, but losing my job worries me far less than losing Facebook."

Such behavior might also be indicative on what's emerging as a larger problem: The addictive nature of social networking.

According to UCLA's Higher Education Research Institute, more than 86 percent of incoming freshmen said they spend one to five hours a week on social networking sites such as Facebook and MySpace. These particular users may still be years away from entering the workforce, but companies should already be on watch for signs of such behavior among their employees, especially because of a direct side-effect of addiction to social networking: compromised enterprise security.

Phishing presents a particular threat. As users grow less wary of posting more personal information online, spammers are growing more capable of collecting it—and turning it back on users with much more personal e-mails that invite them to part with private (or corporate) data.

Poorer Network Performance

Just as with productivity, enterprises have also long had to contend with the impact of unregulated surfing on network performance. Proxy anonymizers obviously undo whatever efforts companies make to ensure that performance is humming—since they aid and abet in file sharing, video streaming, and other bandwidth-sapping activities.

Again, it's illustrative to look at the particular impact of social network sites. According to the same U.K. study cited above, workplace visits to social networking sites consume up to 20% of corporate bandwidth. That's no surprise, given all the photos, music clips, videos, and other huge files that are there for the downloading. And when those files are stored or sent on to others, the strain on the infrastructure grows even greater.

Further, unchecked downloading and transmitting wreaks havoc with capacity planning. The time and money spent on tuning networks for optimum performance thus goes to waste—even as network availability and response times grow worse.

Increased Legal Liability

When workers use proxy anonymizers to bypass filters, they can gain access to sites hosting inappropriate, offensive, or even potentially illegal content. And if that information comes into the workplace, it increases enterprise exposure to legal liability. Even though there are numerous, well-documented cases of litigation spawned by dissemination of these materials, workers continue to download jokes, gossip, and graphic images and send them through corporate e-mail or even display them on their desktops.

There's also the risk associated with information that leaves the premises. Complying with regulations like HIPAA and Sarbanes-Oxley, as well as with various Securities and Exchange Commission rules, means ensuring the privacy and confidentiality of personal, medical, and financial information. And disclosure of that information becomes more likely when employees are visiting unauthorized sites harboring malware, or even posting (intentionally or not) to their Facebook, MySpace, or LinkedIn profiles.

New questions of liability surround social networking in particular, as appropriate modes of behavior and responsibility are still being defined. A high-profile case in Missouri involving the suicide of a teenage girl allegedly harassed by neighbors via MySpace should raise a red flag for enterprises: What would happen if such activity occurred from within corporate premises on a company machine? Liability laws vary from state to state, and federal statutes are still taking shape, but the last thing a business needs is to be named as a co-defendant in a lawsuit charging harassment, defamation, fraud, or worse.

WHAT TO DO ABOUT PROXY ANONYMIZERS

A complete Web protection strategy involves more than blocking proxies. Clearly, the increased use of proxy anonymizers poses serious challenges for enterprises. With all the investment they've made in deploying and updating Web filters, they're essentially back where they've started once employees have learned to bypass them.

But as is always the case where Web surfing habits are concerned, the right combination of education and enforcement can go a long way. Companies need to inform their employees—in plain language—of the dangers of using proxy anonymizers. Highlight the security hazards to both the individual and the business, stressing that the two are essentially inseparable: what harms one is likely to harm the other. Point out that productivity—and thus employee performance reviews—might suffer. And remind them that they too are potentially liable for whatever allegations arise or whatever damages are incurred.

Simultaneously, make sure the acceptable use policy governing online activity is updated. And make sure to keep it updated, so that it reflects and addresses the latest actions, behaviors, and capabilities that social networking or other unauthorized sites enable. Finally, take a hard line on enforcement, so that employees know there really will be repercussions if policy is violated.

The next step in the strategy: select the right technology. When searching for a solution, enterprises need to keep the following critical issues in mind.

A complete Web protection strategy involves more than blocking proxies.

Blocking URLs isn't enough:

URL-based filtering built on blacklists of known sites doesn't work in defending against the dangers of proxy anonymizers, which appear and disappear on a continuous basis. What's needed is a proxy-pattern blocking feature that writes signatures against known proxies while providing zero-day protection against anonymous proxies.

Stopping HTTPS is essential:

Identifying and filtering HTTPS is a crucial step in blocking access to proxy packages that make use of easy-to-configure SSL connections.

Monitoring non-standard ports is a must:

Enterprise IT departments also need to look beyond HTTP and HTTPS to block the proxies that are found on non-standard ports.

With its Proxy Pattern Blocking solution, M86 addresses the specific challenges of enterprises seeking to defuse the dangers of proxy anonymizers. Proxy Pattern Blocking features Proxy-Pattern Detection—a unique signaturebased technology that identifies and blocks requests for anonymous proxies on the fly, giving companies the continuous, real-time protection they need.

Proxy Pattern Blocking also denies access to HTTPS or SSL sites that don't have valid certificates, identifies and shuts down proxies that aren't already in filtering lists, and maintains records of user attempts to circumvent filters. Further, it supplements pattern detection with a full, updatable library of URLs for known proxy sites.

But M866 knows that a complete Web protection strategy involves more than blocking proxies. Whether deployed in the Professional Edition Internet Filter Appliance or the ProxyBlocker Appliance, Proxy-Pattern Blocking also delivers the following important capabilities:

- Blocks instant messaging (IM) and peer-to-peer (P2P) sites
- Enforces Google and Yahoo safe-search
- Blocks inappropriate Google images
- Filters search engine key words to keep workers from accessing unauthorized sites
- Denies Internet access to users who exceed administrator-defined thresholds for requesting unauthorized/inappropriate URLs
- Can handle 100 to 30,000 or more users

CONCLUSION

The only way to guard against today's threats—and stay on top of new ones—is to deploy a comprehensive approach to Web filtering and reporting.

Traditional URL blocking isn't of any use in limiting access to proxy anonymizers—simple scripts that give workers a way to bypass filters and get to sites that are officially off-limits. Written in open source and almost always free, they're also much more numerous than they used to be. And they expose enterprises to all the downsides associated with unregulated Web access, from security threats and reduced productivity to poorer network performance and legal liabilities. Proxy anonymizers are especially dangerous because so many new ones are being created, outpacing the ability of enterprises to keep up and eluding easy detection by security staff.

Fortunately, by educating employees, applying acceptable use policies, and enforcing penalties, companies can limit the dangers posed by proxy anonymizers. And when those practices are supplemented with a comprehensive solution built on pattern-detection technology that detects requests for proxy anonymizers on the fly, enterprises can make sure employees are prevented from getting to unauthorized sites—thus limiting the potential damage to their business.

But defending against the dangers of proxy anonymizers is just one part of a solid Web protection strategy. The only way to guard against today's threats—and stay on top of new ones—is to deploy a comprehensive approach to Web filtering and reporting. With the ability to block access to unauthorized sites, prevent inappropriate downloads, and enforce acceptable use policies through monitoring and reporting, companies can secure their assets, limit their liability, and enhance employee productivity—all to the benefit of the business.

The only way to guard against today's threats—and stay on top of new ones—is to deploy a comprehensive approach to Web filtering and reporting.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09.01.09