

## ISP DNS, proxies and security

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-05/0481.html>

---

**From:** sponge (yosponge\_at\_yahoo.com)

**Date:** 05/28/03

Date: 27 May 2003 22:35:48 -0700

On 25 May 03 23:58:38 MDT, "My\_Cat\_will\_get\_you"  
<GuardCat\_bogus@lycos.com> wrote:

*>If I block dns lookups to my isp and use an "anon" http proxy to  
>do the lookups, am i enhancing or reducing my privacy/security. If  
>dns lookups are not done by the isp, is my home dynamic ip  
>broadcast such that sniffers can profile my surfing or usenet  
>group activities? Lately I get alot of alerts from various ips  
>trying to send packets to the same ports-445,80,137, and other  
>higher ports. These seem to be activated by visting certain  
>newsgroups or articles or certain web page urls, so I guess they  
>are the result of sniffers monitoring lookups to certain ips or  
>usenet groups. How can my privacy be best protected given the  
>above?*

The alerts you see are usually either the result of trojans looking for services, are due to misconfigured File & Print Sharing and NetBIOS access attempts, and -- probably most of all, are due to file-swapping software. Principally, you have little to worry about from any of them if you are behind a firewall and/or are not running any services on them; if File/Print Sharing is disabled, you are trojan-free, and you do not have P2P running, nothing will happen even without a firewall.

As far as DNS goes, that's a good question, but I do not know of DNS servers that log requests other than some spyware-related ones which are not "normal" ISP DNS, but rather hijack your own DNS settings and point them to their DNS servers (specifically, I'm talking about the C2Media/Lop.com spyware.)

Personally, I've tended to view with more suspicion people who USE anonymous proxies. I have never subscribed of the belief that people that use them usually have something to hide, but many people and probably ISPs do. I DO, for example, consider suspicious people who use products like Evidence Eliminator, in part because that particular product advertises itself as being intended for covering evidence of illegal activity. Keep this in mind.

>*From a technical aspect, I find anonymous proxies to be of extremely limited utility. So, the website you are visitng doesn't see your "real" IP; the proxy does. Someone has to, in order for communication to work. Can you be certain that the proxy itself isn't monitoring where you're going or mining your data streams?*

Moreover, such a proxy is really of no value whatsoever if you haven't ensured your own house is in order. Do you have spyware or trojans running on your system? If so, they will merrily collect data and send it home regardless of whether you use a proxy or not. Is your browser locked down? If not, you are vulnerable to "drive-by downloads" and various script exploits that a proxy probably won't fix. Do you have File & Print Sharing disabled (or are behind a router or suitable firewall if you require them) If not, then you are still at risk from various exploits of those, regardless of the perceived correlation between such scans and the newsgroups or page URLs you mentioned.

Some ISPs have been known to monitor users, like Comcast and AT&T. They do this with transparent proxies, however. Even a truly anonymous proxy offers no protection whatsoever, since these proxies exist at YOUR ISP and monitor data streams directly to and from groups of users. There is little that you can do besides carefully reading your Terms of Service Agreement and regularly questioning staff and management as to such practices.

While an anonymous proxy that offers genuine filtering services like porn, spyware, cookies, or malicious ActiveX and VBScripts might be useful to completely inexperienced users, you can achieve the same results by simply not using Internet Explorer/Outlook (or at least properly locking them down), and using filtering software proxies like Proxomitron or WebWasher. Moreover, such services are quite performance intensive on proxies that may serve many users, so you can expect to pay a hefty fee for such services.

My advice is not to bother with an anonymous proxy.

Sponge  
Sponge's Anti-Spyware Source  
[www.geocities.com/yosponge](http://www.geocities.com/yosponge)