

## Re: Scanned for open relay ?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-08/0148.html>

---

**From:** David ([davidwnh\\_at\\_adelphia.net](mailto:davidwnh_at_adelphia.net))

**Date:** 08/02/03

Date: Sat, 02 Aug 2003 03:35:33 GMT

They may very well be legit themselves and the quality of a website can lead to two very different conclusions.

Some people keep things simple because of time constraints, limited resources, or because "fancy" sometimes exposes vulnerabilities, but it can also point to the amount of time someone puts into an entire project, not just their site but the remainder of they are trying to accomplish. A well done web site can just as easily be used trick people into falsely assuming legitimacy so it is really hard to say sometimes. But take a closer look and you will find at least two ways to exploit their system. This tells me that they not only haven't put much time into their website, but also haven't put enough thought or care into how they are implementing their blacklist. Not to mention their overall methodologies are very inaccurate for the purpose they are intended for.

>

> *I don't see what the quality of the design of their website has to do with anything. Since this is a volunteer, not-for-profit organization, I guess they have other things to spend their time and money on than web design. And I don't blindly believe what anyone says. The only reason why I vouch for njabl.org, is that I've used their services in the past, their lists works, and it cuts down on spam.*

You simply have to implement the methods they have provided to start harvesting. The big problem I see is that they are not only providing you ip addresses, but also categorizing them for you as open relays, open proxies, script vulnerabilities, etc. IMHO these people have not completely thought about the negative implications of what they are doing. Or maybe they have? Even if their intentions are noble which I cannot prove either way, there is a huge downside to the way they are doing things.

One part of the system does id spammers, but for the most part they are identifying vulnerable systems that the spammers are using as opposed to the spammers themselves. In any case there are other methods which do not have such a high potential for innaccuracy and in particular do not expose certain systems to further compromise. It's an assinine approach at best.

>

> *The lists are not available for download. You'll either have to search using the online tool (one IP at a time), or by querying their DNS server.*

>

comp.security.firewalls: Re: Scanned for open relay ?

They certainly are. You may only be able to query a single address from their webpage, but the information is there explaining how to set up your system to get it automatically either little by little or in one fell swoop.

>

> *But, they're not publishing anything.*

> >

Like I said I'm not much for dshield but you have to take a look at what they are doing. Their main purpose is not to catch and report offenders however they do now have the "FightBack" program which is not an automated process. Their main function is to collect and analyze statistics which basically help to show mostly the spread and wane of worms and other automated exploits. I suspect their organization is well versed on the fact that many things are spoofed or come from the compromised machines of somewhat "innocent" victims. I suspect also that they are a group well versed on the methods used to determine such things and are not automatically reporting something without first doing a little "homework".

>

> *So, people who contribute to the blocking of spam are "policing" the web, while people who report (mostly) harmless port probes are not? What if the automated process of reporting was wrong? What if they reported the probe to the wrong ISP or to the wrong hosting company or the wrong domain? Are they still doing a good job?*

Are these people contributing to the blocking of spam? If these things aren't implemented carefully they are actually counterproductive. There a bunch of these "services" available, some which are just as poorly implemented and others which at least on the surface look less prone to abuse. I can't say whether this particular site is legit or not but I don't put it past the spammer or others to be doing something like this. I have seen a few spam blocking programs which are actually tools that allow certain spam to pass. And there are a couple which are either directly tied to well-known fortune 500 companies or they are at least clients of the software developers from the advertising side of these "scams". So these days you can't really assume that anything in this regard is what it appears to be on the surface...it's a big cat and mouse game. These systems can be used allow spam to pass as well as block it. So it's not a matter of RBL's as a whole being legit or not. It is a matter of which RBL's are totally legit and which have an ulterior motive.

> *RBL groups are not posers. They have identified spammers, and are*

> *allowing other people to block spam based on what they know. From where*

> *I'm sitting, that's a good thing.*

>

There is a fair amount of proxy scanning going on these days, and I have seen a few that trace back to these types of websites and more often maybe just a "friendly-looking" DNS name, but this is sometimes all just part of the game. Social engineering at its finest.

There may be a good reason, or maybe the OP missed some of the ports scanned, but I am forced to wonder why a group claiming such wouldn't have

Re: Scanned for open relay ?

comp.security.firewalls: Re: Scanned for open relay ?

scanned port 25 also? Maybe they do it separately because a followup script would be different, but you might expect that to show in someone's log somewhere in this case.