

## RE: [fw-wiz] The home user problem returns

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-09/0090.html>

---

*lordchariot\_at\_earthlink.net*

**Date:** 09/14/05

To: "'R. DuFresne'" <dufresne@sysinfo.com>, "'Mason Schmitt'" <mason@schmitt.ca>  
Date: Tue, 13 Sep 2005 20:34:00 -0400

> *beside ingress and egress filtering, how much might ISP's suffer for*  
> *correcting some of the windows network protocol errors by not passing*  
> *ports 135-139, 445 and 5000 etc across perimeters? Or even allowing*  
> *them to broadcast within the ISP's realm? Certainly would work to neuter*  
> *the M\$ issues to a low noise level would it not?*

In the last 20 minutes it took to read the last batch of posts, I got 8 probes to 445 or 139.

Of course, I'm denying all this so there is little threat to me, but I like to keep an eye on this kind of traffic to give me a feel for what's out there in the wild.

```
Sep 13 19:42:57 PF SRC=71.0.173.129 DST=192.168.2.10 PROTO=TCP SPT=2633
DPT=445
Sep 13 19:44:06 PF SRC=71.0.243.133 DST=192.168.2.10 PROTO=TCP SPT=3767
DPT=445
Sep 13 19:48:54 PF SRC=71.0.243.133 DST=192.168.2.10 PROTO=TCP SPT=2574
DPT=445
Sep 13 19:58:04 PF SRC=71.0.129.190 DST=192.168.2.10 DF PROTO=TCP SPT=1592
DPT=445
Sep 13 19:59:10 PF SRC=86.193.83.45 DST=192.168.2.10 DF PROTO=TCP SPT=3416
DPT=139
Sep 13 19:59:13 PF SRC=86.193.83.45 DST=192.168.2.10 DF PROTO=TCP SPT=3416
DPT=139
Sep 13 19:59:19 PF SRC=86.193.83.45 DST=192.168.2.10 DF PROTO=TCP SPT=3416
DPT=139
Sep 13 20:01:53 PF SRC=71.130.34.177 DST=192.168.2.10 PROTO=TCP SPT=37388
DPT=445
```

However, I think all ISPs should be filtering all the MS networking ports by default. I can think of no good business reason to allow it. This would go a long way to mitigate many of the threats out there and it would reduce the number of calls from relatives, friends, neighbors, strangers that want me to help them clean out their infected machines.

Now the question is, should the filtering be a premium service that users

Firewall-Wizards: RE: [fw-wiz] The home user problem returns

pay extra for, or is the UN-filtered traffic now premium that I have to pay extra for the privilege of having?

Kudos to Mason for having some of the basic port blocking in place. This and Anti-spoofing egress filtering should be must-haves for all ISPs.

erik

---

firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>