

## Re: They can break ZoneAlarm easily !

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/10856.html>

---

**From:**

**Date:** 10/06/02

Date: Sun, 6 Oct 2002 12:46:30 -0600

"Duane Arnold" <[darnold92@Insightbb.com](mailto:darnold92@Insightbb.com)> wrote in message  
news:oS\_n9.60640\$I5.11904@sccrnsc02...  
> > *What should I do then?*  
>  
> *You could run an Intrusion Detection System in conjunction with ZA to  
better  
> protect the machine.*  
>  
> *Snort/IDS is free software that can be installed on the machine. I don't  
> know if it will run on the Win 9x OS... check it out.*  
>  
> *You could also install BalckIce\IDS on the machine and run it in  
conjunction  
> with ZA You could turn off BlackIce's Application and Communication  
controls  
> on the 3.5 version and tell the BalckIce firewall to ACCEPT, not  
> ACCEPT/TRUST or TRUST, all IP(s) on TCP and UDP ports. By doing the  
ACCEPT  
> only, you enable BlackIce's IDS system, which will inspect the data in the  
> network traffic for attack patterns.*  
>  
> *You can also get an older version of BlackIce such as version 2.9 and  
below,  
> which doesn't have Application and Communication control features and put  
it  
> on the machine with ZA.*  
>  
> *I hope this helps*  
>  
> *Duane :)*  
>  
>  
> "Latet" <[NOSPAM\\_latet@poczta.onet.pl](mailto:NOSPAM_latet@poczta.onet.pl)> wrote in message  
> news:anppr7\$pf8\$I1@pippin.warman.nask.pl...  
> > > *How come ZA allowed that to happen?*  
> >  
> > *Someone just told me, that if a disk or folder is "shared" in LAN,*

comp.security.firewalls: Re: They can break ZoneAlarm easily !

> > *it is also possible to access it from the internet,*  
> > *even if ZoneAlarm is set up correctly.*  
> >  
> > *What should I do then?*  
> >  
> > *Thanks.*  
> >  
> > *Latet.*  
> >  
> >  
>  
>

I advise against intrusion detection systems. Usually they only complicate or reduce your firewall's effectiveness due to how they install and how they access certain system files. This was an issue raised a while back about people running two firewalls — they would conflict with each other. I would suggest turning off your shared folders and use TelNet over the LAN to share, if you're that worried.

Also, I'd be using only TCP/IP protocol, i.e. not NetBIOS, due to that also being raised a while back as an internet security issue.

However, also, if you're using ICS to share the DSL modem, I'd instead buy a broadband router, since most those include NAT "firewall" and either a packet filter firewall or a port mapper or some other additional security. For example, mine has stateful packet inspection. All the internet scans I can run have deemed my security safe.

But, however, I would suggest that you look that email thing up, since I think some emails can, as a script, create files on your desktop. If your outlook express settings are restricted zone (Tools > Options > Security), that should be sufficient.

Another issue, however, is your operating system. Compared to windows 2000/xp and linux, I'd say your operating system is one of your main vulnerabilities. Do you use windows update frequently?

Also, I'd try deleting your cookies, and then making sure in your internet security zones (all of them) that you go to the bottom in the custom settings and make sure your User Authentication > Logon is set to "Prompt for user name and password". Another thing would be to set your Microsoft VM > Java permissions to Disable Java (for LAN and restricted zone only) and High safety for all other zones.

Also, purge your zone sites.

Also, if you have IE 6, go set your privacy settings (under advanced) to Override automatic cookie handling checked, with first party cookies accepted but third party cookies blocked, and put a check in "Always allow session cookies". I don't trust ads nor their cookies, so I like to do that.

Honestly, if you're using ZA Pro, I'd be calling them and asking them why. But it could be your email settings, or a script from the email they sent. I've never heard of this.

The above are my opinions, and they are what I would do if it were me.

comp.security.firewalls: Re: They can break ZoneAlarm easily !

- *Next message:* [EricL: "Re: NBG800 Hackers Test."](#)
- *Previous message:* [: "Re: Alerts on McAfee firewall since downloading Windows Updates"](#)
- *In reply to:* [Duane Arnold: "Re: They can break ZoneAlarm easily !"](#)
- *Next in thread:* [Duane Arnold: "Re: They can break ZoneAlarm easily !"](#)
- *Reply:* [Duane Arnold: "Re: They can break ZoneAlarm easily !"](#)
- *Reply:* [ZZZZZZZ: "Re: They can break ZoneAlarm easily !"](#)
- *Reply:* [Latet: "Re: They can break ZoneAlarm easily !"](#)
- *Messages sorted by:* [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)