
Subject: Constant firewall violations

Posted by [Veyrdite](#) on Sat, 09 Feb 2008 01:32:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

I'm running zonealarm, and have found that nearly every day I use my computer, it blocks a supposed access attempt.

Half of them are simply because of me hosting my fds on lan, but the other half I haven't got a clue about.

I just want to know if this is entirely normal, or if the !PLECOS backdoor virus has got me.

Oh and no you can't hack me by that IP as I've just refreshed my router.

File Attachments

1) [firewall_log.gif](#), downloaded 552 times

| Rating | Date / Time ▾ | Type | Protocol | Program | Source IP | Destination IP | Direction | Action T... | C... |
|--------|--------------------------|----------|-----------------|---------|------------------|------------------|-----------|-------------|------|
| Medium | 2008/02/09 12:19:00+1... | Firewall | ICMP (type:8... | | 122.104.32.229 | 122.106.15.195 | Incoming | Blocked | 1 |
| Medium | 2008/02/09 12:12:14+1... | Firewall | ICMP (type:8... | | 122.107.230.86 | 122.106.15.195 | Incoming | Blocked | 1 |
| Medium | 2008/01/26 19:34:34+1... | Firewall | ICMP (type:3... | | 70.71.127.108 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2008/01/26 19:12:52+1... | Firewall | ICMP (type:3... | | 70.71.127.108 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2008/01/25 14:11:10+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/25 13:16:58+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/25 12:20:26+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/25 09:26:36+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/24 20:48:34+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/21 22:09:34+1... | Firewall | ICMP (type:3... | | 72.226.236.156 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2008/01/21 22:09:32+1... | Firewall | ICMP (type:3... | | 99.248.178.239 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2008/01/20 19:42:24+1... | Firewall | ICMP (type:3... | | 72.226.236.156 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2008/01/20 19:42:22+1... | Firewall | ICMP (type:3... | | 99.248.178.239 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2008/01/19 11:20:26+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/15 19:49:26+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/15 18:37:12+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/13 22:16:46+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/13 21:55:04+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/13 11:07:56+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/12 13:00:36+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.192.1... | Outgoing | Blocked | 1 |
| Medium | 2008/01/06 11:55:22+1... | Firewall | IGMP (type:3... | | 192.168.0.2 | 224.0.0.22 | Outgoing | Blocked | 1 |
| Medium | 2008/01/05 13:12:08+1... | Firewall | IGMP (type:3... | | 192.168.0.2 | 224.0.0.22 | Outgoing | Blocked | 1 |
| Medium | 2008/01/05 11:29:10+1... | Firewall | IGMP (type:3... | | 192.168.0.2 | 224.0.0.22 | Outgoing | Blocked | 1 |
| Medium | 2007/12/31 14:16:20+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.224.1... | Outgoing | Blocked | 1 |
| Medium | 2007/12/31 13:52:58+1... | Firewall | UDP | | 192.168.0.2:5... | 211.72.252.17... | Outgoing | Blocked | 2 |
| Medium | 2007/12/30 20:29:14+1... | Firewall | ICMP (type:3... | | 217.93.107.229 | 192.168.0.2 | Incoming | Blocked | 1 |
| Medium | 2007/12/30 18:36:50+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.160.1... | Outgoing | Blocked | 1 |
| Medium | 2007/12/27 16:03:22+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.160.1... | Outgoing | Blocked | 1 |
| Medium | 2007/12/27 16:00:10+1... | Firewall | UDP | | 192.168.0.2:5... | 159.153.235.2... | Outgoing | Blocked | 1 |

Subject: Re: Constant firewall violations
Posted by [Veyrdite](#) on Sat, 09 Feb 2008 01:44:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

Lol just now.

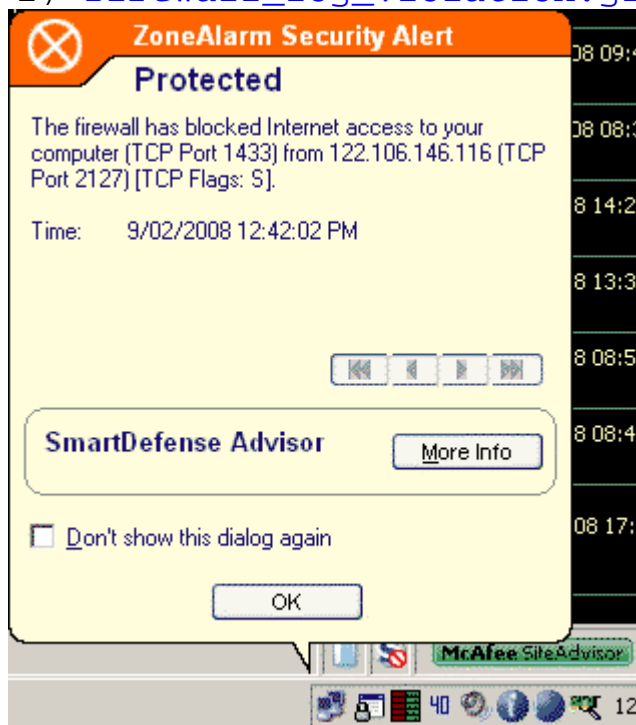
EDIT: Here we go again.

EDIT: Time to refresh my router again. Maybe it didn't change last time.

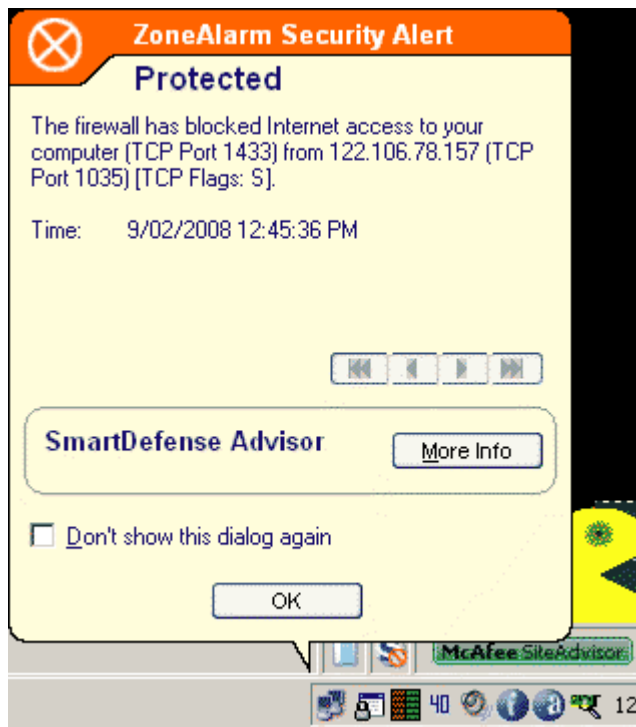
Sigh I think I'm infected with something today.

File Attachments

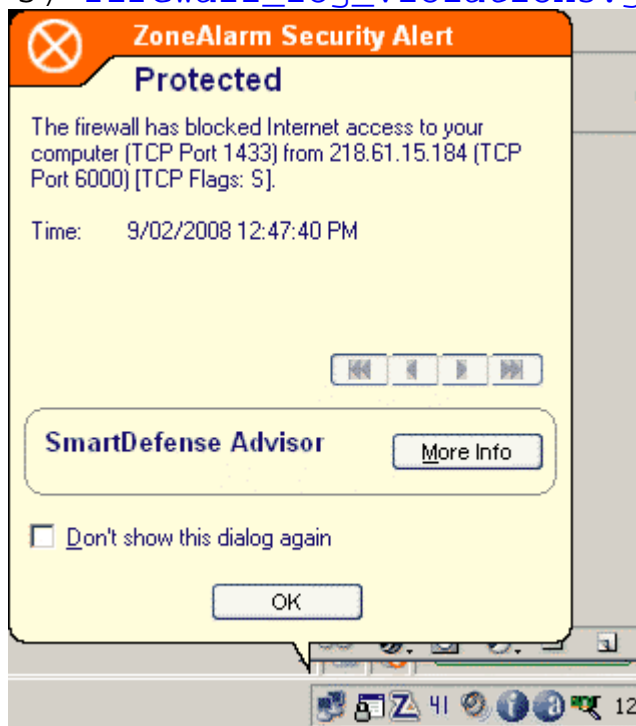
1) [firewall_log_violation.gif](#), downloaded 458 times



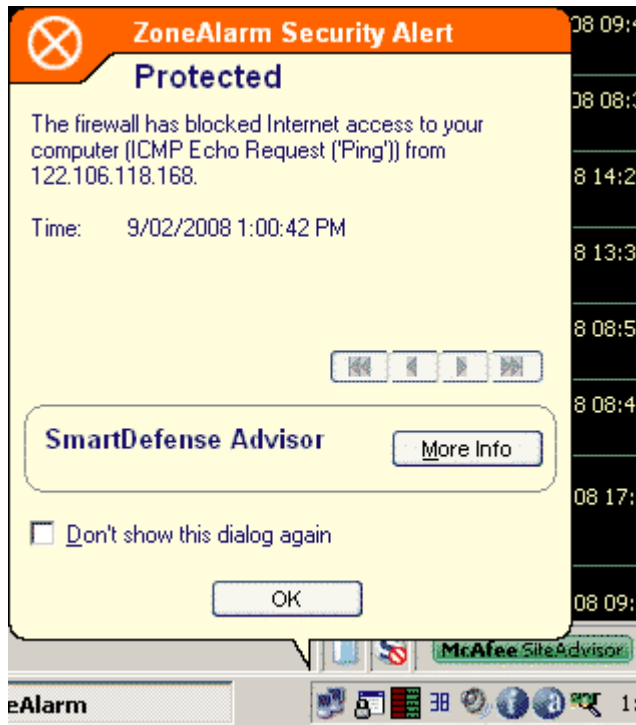
2) [firewall_log_violation2.gif](#), downloaded 450 times



3) [firewall_log_violation3.gif](#), downloaded 444 times



4) [firewall_log_violation4.gif](#), downloaded 440 times



Subject: Re: Constant firewall violations

Posted by [mrÅ£Å\\$Å-z](#) on Sat, 09 Feb 2008 02:04:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

A new Hacker Programm is out?

Subject: Re: Constant firewall violations

Posted by [Veyrdite](#) on Sat, 09 Feb 2008 03:17:44 GMT

[View Forum Message](#) <> [Reply to Message](#)

I've just had another 5. eek.

Subject: Re: Constant firewall violations

Posted by [Blazer](#) on Sat, 09 Feb 2008 04:35:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

If you are running an FDS on that PC, you probably do not want to block outgoing UDP, as the FDS uses that to negotiate NAT players (not to mention that all the renegade traffic is UDP).

Subject: Re: Constant firewall violations

Posted by [Veyrdite](#) on Sat, 09 Feb 2008 04:45:54 GMT

[View Forum Message](#) <> [Reply to Message](#)

Worked out why I keep getting so many violations today. I'm so stupid, should have thought of it earlier.

I bypassed my now dead router (which had a hardware firewall).

ticks "Do not show this dialog again button" and then presses ok

EDIT:

File Attachments

1) [firewall_log_violater.gif](#), downloaded 401 times

218.11.15.184

[Lookup this IP or website](#)

You can trace IP addresses and websites.

Examples: 213.86.83.116 (IP address) or msn.com (Host)

IP address location & IP address info:

| | |
|--------------------------------|---|
| IP address [?]: | 218.11.15.184 Copy Whois |
| IP address country: |  China |
| IP address state: | Shanxi |
| IP address city: | Shijiazhuang |
| IP address latitude: | 38.167198 |
| IP address longitude: | 113.116898 |
| ISP of this IP [?]: | CNCGROUP Hebei province network |
| Organization: | CNCGROUP Hebei province network |
| Local Time of this IP countrv: | 2008-02-09 12:49 |

Subject: Re: Constant firewall violations

Posted by [light](#) on Sat, 09 Feb 2008 09:04:21 GMT

[View Forum Message](#) <> [Reply to Message](#)

If you're directly connected to the net you'll be regularly scanned by other computers.

Having a NAT router/firewall will stop these because NAT just drops them and a firewall can be configured to ignore them.

Subject: Re: Constant firewall violations

Posted by [mrÃÄÄÄ-z](#) on Sat, 09 Feb 2008 11:28:28 GMT

[View Forum Message](#) <> [Reply to Message](#)

Try to get another Firewall (a diffrent) to have a bit more Security

Subject: Re: Constant firewall violations

Posted by [JPNOD](#) on Sat, 09 Feb 2008 19:50:31 GMT

[View Forum Message](#) <> [Reply to Message](#)

Blazer wrote on Fri, 08 February 2008 23:35 If you are running an FDS on that PC, you probably do not want to block outgoing UDP, as the FDS uses that to negotiate NAT players (not to mention that all the renegade traffic is UDP).

Indeed, and if I was the Topicstarter.

I would block all port's that you don't need, and just put the Server in DMZ. It's just wrong to open the ports for all PC's, you don't want that.

Subject: Re: Constant firewall violations

Posted by [Ryu](#) on Sat, 09 Feb 2008 21:39:47 GMT

[View Forum Message](#) <> [Reply to Message](#)

Why would a hacker waste his time trying to hack you..?

he wouldn't, so stop being paranoid.
