

Re: problems with sunbelt kerio firewall and Spy Sweeper from Webr

## Re: problems with sunbelt kerio firewall and Spy Sweeper from Webr

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00360.html>

---

- *From:* B. Nice <[b\\_nice@xxxxxxxxxxx](mailto:b_nice@xxxxxxxxxxx)>
  - *Date:* Wed, 09 Aug 2006 19:56:56 GMT
- 

On Wed, 09 Aug 2006 12:44:31 -0400, Elendil  
<[elendil.fairful-antispam@xxxxxxxxxxx](mailto:elendil.fairful-antispam@xxxxxxxxxxx)> wrote:

B. Nice wrote:

On Tue, 08 Aug 2006 20:39:07 -0400, Elendil  
<[elendil.fairful-antispam@xxxxxxxxxxx](mailto:elendil.fairful-antispam@xxxxxxxxxxx)> wrote:

ZA Free is also extremely powerful and effective.

Says who?

Let's see here: Myself, Millions of people around the world, Hundreds of people at several computer security/help forums such as BleepingComupter, Castle cops, etc., and many fair and honored software reviewers.

I believe you. Security software vendor's marketing departments are doing a great job.

The thing is, very few people are able to actually look underneath these products to see how they really work. And when they do they are not that impressed. When was the last time you yourself put it to a real test by throwing deliberate attacks at it (from the outside as well as from the inside) to see how it manages it?

I just put ZoneAlarm Free (the latest version 6.5.731.000) to a small leaktest myself. It didn't impress me much. But my findings fit the rating at [http://www.firewallleaktester.com/tests\\_overview.php](http://www.firewallleaktester.com/tests_overview.php) (press the "view results" button at the bottom and see for yourself how ZoneAlarm Free handles outbound connection tests). To put it nicely, it isn't very impressive. I would even go so far to say that it leaks like a sieve.

Re: problems with sunbelt kerio firewall and Spy Sweeper from Webr

Re: problems with sunbelt kerio firewall and Spy Sweeper from Webr

ZoneLabs themselves acknowledges that malware can take advantage of techniques that ZA free cannot cope with. And they don't intend to do anything about it.

Zonelabs even tries to make it look as it is nothing serious. They seem to have no idea what modern malware is capable of – or they are deliberately trying to calm it down.

[http://news.com.com/Malicious+code+could+trick+ZoneAlarm+firewall/2100-1002\\_3-5886488.html](http://news.com.com/Malicious+code+could+trick+ZoneAlarm+firewall/2100-1002_3-5886488.html)

So far, 200+ intrusion attempts have been blocked on my computer.

No. ZoneAlarm is just making a lot of fuss out of nothing to make itself look effective.

And you know that ZA is making a fuss about non-existent stuff when I'm the one who has the computer and firewall in question in front of me not you?

Yes, I can. Because that is what ZoneAlarm does. No matter where in the world it is installed. If ZoneAlarm was a serious security product it would just protect you and otherwise keep quiet like a normal good packet filter would do. It is really not the things it catches that is of interest, it is what it does not notice.

Please don't take this personally. I'm not trying to be a smartass in any way. It only worries me when people consider personal firewalls like ZoneAlarm Free powerful and effective or unbeatable, because technical evidence simply disproves this. And you should certainly not feel secure by using those, because at least as far as outbound connections are concerned they are simply not effective enough to be considered a reliable security measure.

Malware is something you stop at the gate (for example with a good anti-virus product – even though they are not too reliable either – or by using your common sense). It is not something you allow to run and then try to control. It's not called malware for nothing.

As far as inbound connection control is concerned there is no technical evidence that a personal firewall should do a better job than a good packet filter like the build-in windows XP SP2 firewall. In which case the windows firewall would be the preferred option in terms of security because it is a part of the OS (among other things making it possible to provide true protection at boot-time), and it is already there and therefore does not add any new attack vectors which the installation of an additional personal firewall does.

Re: problems with sunbelt kerio firewall and Spy Sweeper from Webr

Re: problems with sunbelt kerio firewall and Spy Sweeper from Webr

As far as outbound is concerned it cannot be done in a reliable way (which is most likely the reason why MS intentionally left it out). Within windows, there are simply too many ways for malware to connect out without a firewall noticing it. It is an arms race that cannot be won.

So the question one must ask oneself is, if it is worth it to install a big chunk of security code in order to control something that is highly uncontrollable or if one should just take responsibility for what one does, surf safely and not install/run all kinds of questionable software – in which case no security product can protect you anyway.