

Re: Why you should use a firewall on Win98

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-03/0737.html>

From: Gerald Vogt (vogt_at_spamcop.net)

Date: 03/15/05

Date: Tue, 15 Mar 2005 10:10:11 +0900

bassbag wrote:

> *I totally agree with you. A trojan doesn't care what operating system you
> have or what connection you have. It amuses me that many of the anti-
> application firewall brigade says you shouldn't need an out bound
> filtering firewall or indeed any firewall, because by being careful you
> won't get infected to stop any malware getting out. They then go on to*

No. If you like the outbound firewall you can use it. Just in average, for the average user, in my experience people tend rather to believe they are safe because they have a outbound firewall and it does not report anything instead of being careful. If you are very careful, you can add your outbound firewall if you think you need it. Just the blind advice "use this and you are safe" is just wrong. And the basic design to mix an outbound firewall with some inbound firewall and some intrusion detection system and some privacy control function and some parental control system and some more is just wrong. In most cases, if you knock out one of those things you knock out the whole thing. If it crashes it usually crashes completely. If you think, you need an outbound filter, get an outbound filter and run it separately from the inbound filter. Same results and you most likely think a little bit more about what you get for your money. With a PFW it's all there and nobody really thinks about what each part does and how reliable it actually works. (And no PFW maker will tell you...)

> *recommend AVs/adware progs etc that the "security conscious" should have*

None. I don't need any. No malware gets onto my computer. So why should I scan for some? My AV is the most useless thing on my computer and I only have it because I want to know how good it works as I have it running on some other people's computer as well. The last time it popped up was with some useless warning regarding a phishing e-mail before I even could read it. Jeez, how should someone learn to distinguish between a real and a fake email if they don't even see it. Someone recently wrote that he was so glad to have his AV because it prevented an infection of his computer with a Trojan./Phish.blablabla. It was just a simple phishing e-mail. A phishing e-mail is harmless until you click on the link which guides you somewhere else. Before that, it is harmless. (I played a little bit around with it and found the most disturbing

comp.security.firewalls: Re: Why you should use a firewall on Win98

message the warning that there is a phishing e-mail in my Trashbin once I moved it there. So you get a warning message for some really good practice like trashing a phishing e-mail instead of clicking on it...)

> *(mmmm seems a bit double standard there....why have an AV /adware prog if
> your that careful anyway?).And most amusing of all is they usually*

No double standard. You don't need one if you are careful.

> *recommend the worst possible AV.Of course my experience means nothing to*

Yes. None is the worst possible. ;-)

> *the security perfect here , but most people i know including myself (many
> moons ago as a newbie) have been infected by a trojan , and its been the
> firewall in many instances that has detected it and not the AV.Of course*

Good, then your firewall did have some purpose for you. Please allow me to ask how it happened and what your expectations have been of your firewall and AV before that and after that? Did they change?

> *perfect security conscious people dont get malware (though with no
> outbound filtering and possibly a crap AV , i doubt theyd even know if*

I know all my processes on my computer.

I install/recommend people AVs and PFWs only together with a long list of warnings that AV and PFW is just and only and nothing more than a backup net with huge holes in it. If you fall, it may or may not catch you. And you may never notice that you fell. (O.K. weird picture ;-;) I tell them, that if there is a warning message popping up, they have already lost. If they tell me, they got one, and it's a real one (not the phishing thing above still far far away from the real danger of clicking on it) I start using all those other adaware tools a.s.o on their computer to make sure that it was really the first and only time.

Occasionally (depending on how stubborn the user is) I just take the image of the first installation and restore it, telling them that to verify their computer is clean after they actually tried to open this PIF attachment takes a couple of hours and never is 100% sure. So you've lost your life. Game over. Start again... ;-;) If I found some malware despite the AV and PFW I always find some more drastic measures to lock down the computer further which is however a little bit more intrusive when they for instance cannot install any software anymore without consulting me first. I remove IE and OE/Outlook from their computers and replace them with Firefox and Thunderbird. That comes with a list of warnings, too, never to install an extension if the question pops up.

I am looking for a good, valuable replacement of the PFW part, though, that gives me satisfactory outbound filtering and good warnings and which is fully newbie usable, because I don't really see any good use for any of the other PFW features beyond the outgoing application filter

Re: Why you should use a firewall on Win98

comp.security.firewalls: Re: Why you should use a firewall on Win98

and a PFW is a hell complicated to configure to let it run without bigger problems (i.e. endless question dialogs) on a newbie computer.

Gerald