

Re: Recurrent question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-12/msg00479.html>

- *From:* Ansgar -59cobalt- Wiechers <usenet-2005@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* 16 Dec 2005 14:11:04 GMT
-

Kerodo wrote:

> In article <40dr6mF19hmiuU1@xxxxxxxxxxxxxxxx>, usenet-2005@xxxxxxxxxxxxxxxx says...

>> Kerodo wrote:

>>> In article <43a164e9@xxxxxxxxxxxxxxxx>, bumens@xxxxxxxx says...

>>>> Kerodo <loopback@xxxxxxxxxxxxxxxx> wrote:

>>>>> Yep, just because something isn't perfect 100% of the time doesn't

>>>>> mean it's useless.

>>>>

>>>> "Personal Firewalls" aren't "not 100% perfect". They're completely

>>>> useless because of being superseded by the Windows-Firewall,

>>>>

>>> That's completely ridiculous. They do entirely different things.

>>

>> No. Both filter inbound connections. That can be done reliably. The

>> Windows Firewall prevents applications from listening on ports. That

>> can be done reliably as well. Personal Firewalls try to prevent

>> applications from communicating outbound. That cannot be done

>> reliably. Which is why the Windows Firewall is sufficient.

>

> The key to your argument is the word "reliably".

Exactly. Security needs to be reliable otherwise you don't have security.

And IIRC this group is still comp.SECURITY.firewall rather than

comp.PROBABILITY.firewall, isn't it?

> So it depends on what exactly you mean by that.

Look it up in a dictionary.

> It goes back to that AV being useless argument. By your definition of

> "reliably" then all AVs are useless too because they don't catch 100%

> of the threats and hence are not "reliable". Yet we still use them

> don't we? Why?

Signature-based detection is reliable, it will detect every matching

pattern (though it will sometimes produce false-positives), hence I

consider AV software useful.

> Because they will and do catch a high percentage of the threats.

Re: Recurrent question

No. Because they are reliable in the scenarios they are made for. Why do people always come up with this "high percentage of the threats" bullshit? A security (counter-)measure does not have to be reliable for 100% of all imaginable scenarios, but it has to be reliable for 100% of the scenarios it is designed for, otherwise it is useless.

> And catching most is better than catching none.

Not from a security PoV.

> Also to say that the reason why Windows Firewall is sufficient is
> because Personal Firewalls can't catch all outbound, is another
> illogical and silly argument. What does one have to do with the
> other?

A security measure has to be reliable. Outbound control is not reliable, hence it cannot be a security measure. Period. Plus, once you run malicious code on your system, you're toast anyway.

> I would say that the Windows Firewall is not sufficient because it
> makes no attempt to try to catch outbound. Some attempt is better
> than none.

You are wrong.

> Why do you think people "try" at things?

Software isn't people. Software is not supposed to try, but to DO.

> Nobody is perfect, yet we keep trying simply because some success is
> better than none, and to give up entirely is unacceptable. You would
> have everyone give up the attempt to catch outbound simply because it
> might be difficult at times.

It's not "difficult at times", it's impossible unless Microsoft re-designs the IPC in Windows.

cu
59cobalt

—
"Der Computer ist da, um zu rechnen, nicht um Ausreden wie 'Kann nicht durch Null teilen' auf den Bildschirm zu schreiben."

—Marco Haschka in de.org.ccc

.

-
- *Follow-Ups:*
 - ◆ **Re: Recurrent question**
 - ◇ *From:* Kerodo

- **References:**
 - ◆ **Recurrent question**
 - ◇ *From: GRL*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Volker Birk*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Sla#s*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Volker Birk*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Ric*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Kerodo*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Volker Birk*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Kerodo*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Ansgar -59cobalt- Wiechers*
 - ◆ **Re: Recurrent question**
 - ◇ *From: Kerodo*
- Prev by Date: **Re: WinXP SP2 firewall**
- Next by Date: **Re: Recurrent question**
- Previous by thread: **Re: Recurrent question**
- Next by thread: **Re: Recurrent question**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**