

Re: MS to charge for security?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-05/msg07902.html>

- *From:* NoStop <nostop@xxxxxxxxxxxx>
 - *Date:* Sat, 14 May 2005 08:07:24 GMT
-

<Vanguard> wrote:

> "NoStop" <nostop@xxxxxxxxxxxx> wrote in message
> [news:sMbhe.1342827\\$Xk.768635@xxxxxxxxxxxx](mailto:news:sMbhe.1342827$Xk.768635@xxxxxxxxxxxx)
>> I can't figure out what you're rambling about, but just enough to
>> understand
>> that you can't visualize beyond a workstation computer like Windoze XP
>> and
>> really don't have a clue what you're talking about.
>>
>> If a Linux host is running a mail server that serves mail to other
>> clients
>> on the LAN and those clients happen to be Windoze computers, then
>> indeed an
>> AV program running on the Linux server can and does scan the incoming
>> email
>> for viruses before passing the email on to the Windoze clients. You
>> see
>> this all the time with ISPs and web hosting companies that offer
>> anti-virus
>> email scanning. Get it?
>
> Yeah, now that you've explained more than a one-line response that
> supposedly attempted to encompass everything of what you meant. You're
> talking about adding features to a mail or file server program for the
> benefit of **whatever** platform connects to it. So are you claiming that
> NO viruses actually execute and can harm platforms **other** than Windows?

I said Linux. I can't speak for **other** systems, as I don't use them, nor keep up with any security issues they may have.

> So is
>
> <http://securityresponse.symantec.com/avcenter/venc/data/freebsd.scalper.worm.html>
> a
> hoax? Um, where did rootkits start (hint: **ROOT*kit*)?
>
> A rootkit is not a virus. And that symantec security response refers to a

Re: MS to charge for security?

worm that affects FreeBSD, not Linux. That news is 3 years old anyways, and I'm sure FreeBSD has long since been patched for this worm.

> The AV software of which you speak is designed to function under those
> setups of using a server for transferring messages or files; i.e., the
> AV product protects that process. I'm not sure AV software incorporated
> or integrated into mail programs actually also protects the host itself
> on which the mail program executes. Explain the point of AV software
> that is designed ONLY for the Linux workstation (i.e., it is NOT an
> enterprise version nor is it a server add-on process for filtering
> messages or files). There are non-Windows AV products for servers,
> desktops, and laptops. You chose to focus on use of AV incorporated
> into a program running on a server.

>

Because that is the only place I've ever heard of other Linux users ever using an anti-virus program. I don't know of any Linux users that are concerned about viruses on their Linux boxes. Even if one did get there, the amount of damage it could do would be so minimal it would be a non-issue in terms of the OS itself. Unlike in Windoze, applications cannot install themselves by themselves and certainly can't affect the OS's main files.

> I chose the larger number of hosts where the AV is used on a desktop
> (workstation). I believe Sophos has a workstation version of their
> Linux AV program. BitDefender has a Linux version for workstations
> (freeware). BitDefender has their Mail Server anti-virus product which,
> as you say, protects WHATEVER platform connects to the mail server
> process to get messages from there. Does that mail server AV product
> actually protect the host on which the mail program executes, or do you
> still need to get a separate copy of BitDefender Linux Edition to
> protect the host? In any case, there are AV products to protect Linux
> workstations and servers.

>

A virus cannot just run by itself on a Linux system. It would have to have permission to run. It would have to be run by a user with permission to do so and if that user wasn't root, there would be no damage to the OS itself. I don't know what kind of AV products some commercial vendors are trying to market to Linux users. But I've not heard of any Linux users using such products or concerning themselves with viruses, unless they were total newbies coming from the Windoze world and thinking in the Windoze mindset or running Linux servers with Windoze clients as I stated earlier.

> There are far fewer viruses that target commercial *NIX platforms. The
> *NIX community is generally more intelligent than the Windows community,
> but that is because they have to be. Windows was designed to be a
> consumer OS which highly differentiates it from the history of evolution
> of *NIX platforms. There is some social engineering that has been
> present in *NIX platforms and their applications that lagged getting to
> Windows. But to say or even imply that *NIX platforms are virus proof
> is just a flat out lie.

Re: MS to charge for security?

Well give me some examples – recent ones – where a Linux system has been brought down by a virus. I'd like to hear about them, as that would be news to me.

Why don't you go and read this article that dispels much of the Windoze myths about Linux and security ...

http://www.theregister.co.uk/security/security_report_windows_vs_linux/#winvslinuxdesign

"Yes, worms for Apache have been known to exist, such as the Slapper worm. (Slapper actually exploited a known vulnerability in OpenSSL, not Apache). But Apache worms rarely make headlines because they have such a limited range of effect, and are easily eradicated. Target sites were already plugging the known OpenSSL hole. It was also trivially easy to clean and restore infected site with a few commands, and without as much as a reboot, thanks to the modular nature of Linux and UNIX.

Perhaps this is why, according to Netcraft, 47 of the top 50 web sites with the longest running uptime (times between reboots) run Apache. [2] None of the top 50 web sites runs Windows or Microsoft IIS. So if it is true that malicious hackers attack the most numerous software platforms, that raises the question as to why hackers are so successful at breaking into the most popular desktop software and operating system, infect 300,000 IIS servers, but are unable to do similar damage to the most popular web server and its operating systems?"

--

--[*Usenet FAQ*]--

A. Yes it is. It's called "Top Posting" and frowned on by the Usenet community.

Q. But isn't that backasswards?

A. If their reply comes BEFORE what they are quoting, they probably use Outlook Express under Windoze.

Q. How can I tell what OS a Usenet poster runs?

• References:

- ◆ **MS to charge for security?**
◇ From: Måç
- ◆ **Re: MS to charge for security?**
◇ From: Vanguard
- ◆ **Re: MS to charge for security?**
◇ From: NoStop
- ◆ **Re: MS to charge for security?**
◇ From: Vanguard
- ◆ **Re: MS to charge for security?**

Re: MS to charge for security?

◇ *From:* NoStop

◆ ***Re: MS to charge for security?***

◇ *From:* Vanguard

- Prev by Date: ***Re: dialing up net connection when starting windows and it won't stop!***
- Next by Date: ***Re: Checking PC health***
- Previous by thread: ***Re: MS to charge for security?***
- Next by thread: ***Re: MS to charge for security?***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***