

Re: OS related question

Source: <http://www.tech-archive.net/Archive/Publisher/microsoft.public.publisher/2005-03/1099.html>

From: albertv (*albert_at_verbrugh.net*)

Date: 03/22/05

Date: Mon, 21 Mar 2005 18:19:42 -0600

To: Frank <fb@nospam.com>

Frank wrote:

> *albertv* wrote:

>

>> *Frank* wrote:

>>

>>> *albertv* wrote:

>>>

>>>> *Ed Bennett* wrote:

>>>>

>>>>> *albertv* <*albert@verbrugh.net*> was very recently heard to utter:

>>>>>

>>>>>> *Windows 2000 and it's offspring have security issues which are not*

>>>>>> *enabled in win 98/Se/Me.*

>>>>>

>>>>>

>>>>>

>>>>>

>>>>>

>>>>>

>>>>> *Please feel free to delude yourself.*

>>>>>

>>>>> *I'll stick with an operating system that is supported by updates.*

>>>>>

>>>>

>>>> *A so you should, however, I'm surprise you lack knowledge about the*

>>>> *difference between OS98 and NT.*

>>>

>>>

>>>

>>> *I don't, but it's very obvious from your postings you do.*

>>> *Frank*

>>

>>

>>

>>

>> *Windows XP's new support of the full raw socket application*

>> *programming Interface (API) allows for the creation of fraudulent and*

>> *damaging Internet traffic. This has never been possible under Windows
>> without first modifying the operating system with third-party device
>> drivers — which has never been done by malicious programs.
>> The security features built into all other raw socket capable
>> operating systems (Windows 2000, Unix, Linux, etc.) deliberately
>> restrict raw socket access to applications running with full "root"
>> privilege. However, the Home Edition of Windows XP executes all
>> applications with full administrative ("root") privilege. Thus,
>> Windows XP eliminates the raw socket safety restrictions imposed by
>> all other operating systems.
>> For the first time ever, applications running under the Home
>> Edition of Windows XP — whether deliberately executed or running as
>> hidden "Trojan" programs — will be easily able, without modifying the
>> operating system in any way, to generate the most damaging forms of
>> Internet attacks.
>> Internet attacks launched from security-compromised Windows
>> systems are already common. (Because security-compromised Windows
>> systems are common.) However, the previous Internet API built into
>> Windows, prevented those attacks from being as damaging as those
>> launched by Unix and Linux systems. The sole reason for this
>> difference was Windows' previous lack of full raw socket support
>> (which was a blessing).
>> No previous version of Windows (9x, ME, or NT) had, or needed,
>> full raw socket support. Those systems worked seamlessly on the
>> Internet. While there are valid uses for advanced raw-IP packet
>> generation by system level processes (NAT routing, IPsec support,
>> etc.), there is no valid use for raw sockets by end-user software. The
>> only applications are Internet Research or the exercise of malice.
>> Therefore, this new danger is without justification.
>> Windows XP's security model, which has been seriously compromised
>> in order to accommodate the needs of Windows 9x legacy applications,
>> will not prevent the wholesale hijacking of Windows XP machines. These
>> compromised machines — with their needlessly potent full raw socket
>> support — will be used to attack and damage any chosen Internet user
>> or site.
>>
>> <http://www.grc.com/dos/xpsummary.htm>
>>
>> Still think I don't know what I talking about? Say good night!
>>
> That is such old news (Oct 6, 2003) as to no longer be relevant. We all
> knew about it over 2 years ago. No you don't know what you're talking
> about if you still think running any Win9x is more secure than any NT.
> Frank*

It maybe old news but nothing has changed Frank.

avast! Antivirus: Outbound message clean.
Virus Database (VPS): 0511-1, 03/17/2005
Tested on: 3/21/2005 6:19:43 PM
avast! - copyright (c) 1988-2004 ALWIL Software.

microsoft.public.publisher: Re: OS related question

<http://www.avast.com>