

Re: On connecting to the Internet

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-10/0627.html>

From: Mark Sykes (realnews_at_network.org)

Date: 10/08/03

Date: Thu, 09 Oct 2003 04:30:29 +1000

On Wed, 08 Oct 2003 13:41:49 GMT, "David" <davidwnh@adelphia.net> wrote:

>Its all laid out in RFC 1256 for the router discovery protocol.
>Here's a good link with a short explanation for the layman:
>http://www.networkcomputing.com/netdesign/1107icmp7.html?ls=NCJS_1107bt
>
>If you have the proper gateway address entered into the dial up connection's
>configuration you can probably filter these packet's with no adverse
>affects.
>
>Multicasting is not just for client applications to send IM or video
>streams, etc to groups. It is simply an addressing scheme that is more
>efficient than using unicast or broadcast addresses for certain things. So
>in your example when the OS is looking to update it's routing
>table(generally when you first initialize a network connection or if a
>router in your table doesn't seem to be responding) instead of using a
>broadcast address to look for local routers, it uses an address that
>specifically pertains to "all routers on the local subnet".
>
>So the real time networking role is simply that your machine has to know
>which router to use to send traffic whose destination is outside of the
>local subnet.
>> OK. What real-time networking role would cause a stand-alone dialup
>> box to need to do this query?
>>
>> Like, the only protocol used here is tcp. No ipx/spx, no netbios, no
>> netware and none of the rest.
>> Has it got anything to do with messaging or uploading ?
>>
>> regards

Thank you. That makes it clearer. So, it is reasonable to say that all operating systems with an internet capability would perform the same song and dance on connecting, is it not ?

Any windows user, or rather users of earlier versions of windows would not be concerned or curious about these 'background transactions'

comp.security.firewalls: Re: On connecting to the Internet

as they would be invisible, particularly if they run without a firewall.

I wonder what other processes might be taking place 'behind the scenes'. Take this for example ..

I writing application in kernel mode (driver) – WIndows XP
I want my (trojan or backdoor) was invisible
socket-----tcpip-----+-----firewalll-----+-----ndis

| 1.) |

2.)

+-----my driver -----+

1. Hook it
2. Read address from ndis.sys from hard disk

What you think about my idea?

Its a worry ! Trusted computing or misplaced trust.

regards