

Re: Is the Gaobot virus blocked with a firewall?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-05/8034.html>

From: Alan (*somewhere_at_nospam.pew*)

Date: 05/07/04

Date: Fri, 7 May 2004 19:20:57 -0400

So the answer is, "yes, a firewall will block the Gaobot virus."

Alan

"Steve Nielsen" <steve_nielsen@nospam.nowhere.net> wrote in message
news:eXBYTVINEHA.3016@tk2msftngp13.phx.gbl...

> *If you knew how a firewall works you'd have seen the answer in what I
wrote.*

>

> *Yes, block TCP ports 135 and 445.*

>

> *Steve*

>

> *Alan wrote:*

>

>> *And eventually, someone might actually answer the OP's question as to
>> whether the Gaobot virus is blocked by using a firewall.*

>>

>> *Alan*

>>

>> *"Steve Nielsen" <steve_nielsen@nospam.nowhere.net> wrote in message
>> news:ulfzblHNEHA.1272@tk2msftngp13.phx.gbl...*

>>

>>> *Ghostrider wrote:*

>>>

>>>

>>>> *Brian C wrote:*

>>>>

>>>>

>>>>> *Is the Gaobot virus blocked with a firewall?*

>>>>>

>>>>> *I was curious if anyone got the virus using a firewall? Since it is
>>>>> not detected by some virus programs.*

>>>>>

>>>>> *Brian C.*

>>>>

>>>>

microsoft.public.windowsxp.general: Re: Is the Gaobot virus blocked with a firewall?

> >>>

> >>>>A firewall is just one of the lines of defence for a computer
> >>>>system. Unless one keeps the computer completely off a network
> >>>>or does not accept any input from any untrusted, external source,
> >>>>including floppies, cdroms, websites, etc., then it is penetrable.
> >>>>But this is an improbable situation since users must e-mails, send
> >>>>files as attachments, do downloads, etc.

> >>>

> >>>>Gaobot, according to SARC, infects computers through an IRC
> >>>>channel. To have an IRC channel, there is an open port through
> >>>>the firewall, or it might exploit ports 135 and 445. Does this
> >>>>answer the question about it?

> >>>

> >>

> >>>You're confusing how it infects with how attackers can use an IRC
> >>>channel to control an infected machine.

> >>

> >>>It infects through the DCOM RPC vulnerability using TCP port 135 and the
> >>>RPC locator vulnerability using TCP port 445. This is different than
> >>>allowing an attacker to access an infected computer through an IRC

> >

> > channel.

> >

> >>>Steve

> >>

> >

> >

> >

>