

Re: WIN2000NT False prophets(!).

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-11/0443.html>

From: Martin Spencer-Ford (tpwuk.dash.zero.one_at_ntlworld.com)

Date: 11/20/05

Date: Sun, 20 Nov 2005 00:17:41 GMT

Bruce Chambers wrote:

> *Martin Spencer-Ford wrote:*

>

>>

>>

>> *Sorry, i didn't know that Blaster or Sasser were more threatening to a*

>> *system where the messenger service has been disabled.*

>>

>

>

> *The only thing turning off the messenger services does, beyond*

> *freeing an insignificantly minuscule amount of system resources, is*

> *disable a crude sort of security warning that your firewall has failed.*

> *All disabling the messenger service actually accomplishes is stop the*

> *messenger service (obviously) and the display of the messenger spams. Do*

> *so doesn't close the IP ports by which those messages arrived from the*

> *Internet. Those ports used by the messenger service are also used by*

> *the "black hats" to broadcast malware, such as Blaster, Welchia, and*

> *Sasser.*

>

I don't want to seem argumentative here, but if the service is disabled, then in my mind, the ports used by the service would no longer have a listening application to respond to he packets delivered to that port, please enlighten me if i am in error here.

>

>>

>>

>> *Agreed, May be i have the wrong impression here, but does not*

>> *disabling a service make it dead, what your statement suggests here is*

>> *that ok the warning signs are gone, but the underlying problem of the*

>> *service is still there as its not really disabled?*

>>

>

>

> *The *messenger* service may be "dead," but that doesn't close the IP*

> *ports exploited by other malware. The "warning" provided by the*

> messenger service is that those ports are wide-open and exploitable.
>
>

But at least the messenger service would be doing something useful for the stand alone windows based pc or laptop ... :) If it was left enabled that is.

>>
>>
>> *The OP in *my* opinion was just asking how to stop the damned adverts, not how to install and maintain a firewall, Mike stated that he had ran software that is normally good at stopping most scum ware, so I didn't feel the need to go into the needs of a security policy, as he is obviously to me, on the right approach to the runway. Your linking to a medical condition, is amusing in comparison, but i wouldn't have needed the doc to tell me "well don't do that" I would have figured that myself, which is like i say – i assumed that Mikes approach was.*
>>
>
>
> *But would you have accepted such medical advice as the sole solution to your problem? ;–} Wouldn't you, at some point in the future, want to be able to reach that top shelf again? And, if you don't like the medical analogy, how about this one: pulling the battery out of a noisy smoke detector, rather than looking for – and eliminating – the source of the smoke that set it off?*

Not my fault i am only five feet seven. But yes i do understand the comparison and yes i do appreciate all you have said in this thread, its been informative, and interesting, not a bad result from a loose post.

>
>
>>
>>>
>> *Agreed, but still suggests that disabling the service still leaves it active ?*
>
>
>
> *No, but it still leaves the true vulnerability in place. The problem is that turning off the Messenger Service does *not* block the wide open TCP and UDP ports that the spammers used to deliver the spam to the Messenger Service for display. With the Messenger Service disabled, those spam deliveries to the PC are still continuing, but they're simply not being displayed.*

See the above query with respect of turning off a service should also remove the listening application.

>

> *The danger of this "treat the symptoms" approach has been more than
> aptly demonstrated by the advent of the W32.Blaster.Worm, the
> W32.Welchia.Worm, the W32.Sasser.Worm, and their variants. These worms
> attack PCs via some of the very same open ports that the Messenger
> Service uses. Need I mention how many hundreds of thousands of PCs have
> been infected by these worms since August of 2003? To date, according
> to my records, I have personally responded to over 1000 Usenet posts
> concerning Blaster/Welchia/Sasser infections since then, and I can't
> possibly have seen and replied to every one that there's been posted in
> this period.*

No need to mention the havoc delivered by such worms, but even though this goes part way to answering my above query, (multi goto's yugh) then

I am going to have to read more as to what other services messenger service and alerter service tie into, or is it under the broad and heavily abused svchost.exe

>
> *Now, how many of those infected with Blaster/Welchia had turned off
> the Messenger Service to hide spam? I can't say, and I don't think
> anyone can. What I can say with absolutely certainty is that if they'd
> all had a properly configured firewall in place, they would have blocked
> the annoying spam _and_ been safe from a great many other dangers,
> particularly Blaster/Welchia/Sasser*

Agreed. :)

>
> *Of course, like the Messenger Service Buffer Overrun threat, there
> is also a patch available to fix a PC's vulnerability to
> Blaster/Welchia, which was available to the general public a full
> month before the first instances of Blaster/Welchia "in the wild." If
> people learned to stay aware of computer security issues and updated
> their systems as needed, a whole lot of grief could have been avoided.
> The problem with relying upon patches, however, is that they're
> sometimes not available until _after_ the exploit has become
> wide-spread. Antivirus software suffers from this same weakness; it's
> simply not always possible to provide protection from threats that
> have not yet been developed and/or discovered. Both approaches, while
> important, are re-active in nature.*
>

The average computer user is very ignorant of updates and patches until they become affected, and then many still don't learn, but as sad as that is, it is also a good source of income, ask any premium rate tech support company. I also agree whole heartedly that it is pretty much a biological response by security software, that is to say, you can't always have an anti-body for an infection, you sometimes have to wait for a cure.

>
>

>> I noted the tools that Mike was using, and yes i noticed there was not
>> a mention of a firewall, ok maybe i should have asked if there was one
>> installed, but for all i know, that may well have been his next plan
>> of action, and like i said in the other reply to Steve, Mike might be
>> doing things in the *wrong* order, but he is showing signs of going in
>> the right direction.

>>

>> I don't claim to be an "expert" and as much as i like to be corrected
>> if the information i have provided is wrong, and i certainly don't
>> wish to get involved in a shaming flame war as seen on other groups,
>> but the advice i have given in this case to *me* is accurate. The fact
>> that I offered the quick solution for someone who appeared to be
>> desperate to stop the ads, as valid as your point is about revealing
>> underlying problems, i felt no need to flood the poor chap with what
>> he should and should not do, which is another reason why I liked your
>> post, you did not show any bias with any tools for securing up his
>> remaining issues

>>

>

>

> Your subsequent posts in this thread (the ones I should have read
> before I "scolded" you – for which I apologize) do indicate that you do
> indeed know better and meant well. Your intent and reasoning is noted.
> I tend to be over-sensitive on this issue of offering a "quick
> solution", primarily because I've had to spend more hours that i care to
> think about cleaning up behind others who used this and other "quick
> solutions" to make problems seem to go away. I prefer to fix things
> completely the first time. As my grandfather once told me, "If you can
> find the time to do it over, you had time to do it right in the first
> place."

No need for the apology, it has been informative, and your grandfather shows all the signs of wisdom that comes from experience, its a saying i will remember, and take to heart. Though you may not see it in use here, be certain it's on my mind.

>

> Now, as for the Messenger Service itself, it generally doesn't
> hurt any thing to turn it off, although I never recommend doing so.
> Granted, the service is of little or no use to most home PC users
> (Although I've had uses it on my home LAN.), and turning off
> unnecessary services is part of any standard computer security
> protocol. However, I feel that the potential benefits of leaving the
> Messenger Service enabled out-weigh any as-yet-theoretical risks that
> it presents. It will indirectly let the computer user know that
> his/her firewall has failed by displaying the Messenger Service spam.
> Think of it as the canary that miners used to take down into the
> mine shafts with them. There are others, of course, who disagree with
> me on this point and advise turning off the service because it isn't
> needed; you'll have to make up your own mind here.

>

microsoft.public.security.virus: Re: WIN2000NT False prophets(!).

>

I swing both ways on the argument to disable the service or not. On LAN it does indeed have its uses, but on the Internet side, i see little to no functionality for it to be there, so MS's new attitude towards this service is for me, the better one.

Many thanks Bruce for making this thread a pleasure...

Martin
(TpWUK)