

microsoft.public.win2000.security: Re: New Virus released, can anyone help identify it?

Re: New Virus released, can anyone help identify it?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-09/1077.html>

anonymous_at_discussions.microsoft.com

Date: 09/29/04

Date: Wed, 29 Sep 2004 00:02:51 -0700

Thanks for the info. Is this a new release? I have talked to over 20 people today that have recieved it. It spreads through the network like wildfire. Both my domain controllers, all my citrix servers, mail server, backup server, and 400 XP workstations, and htat was only at one location.

Plus, once it gets in, you cant access the 2000 desktop, not even through safe mode. Any way of preventing it? I think I got it removed, it was a bit of a pain, but i deleted the executable, and removed the registry entries.

>-----Original Message-----

>Here is some more info on your problem as reported by Trend Micro by

>searching their site for lsess.exe. --- Steve

>

>http://www.trendmicro.com/search/google/en-us/results.asp?lr=lang_en-us&q=LSESS.EXE

>

>WORM_SDBOT.CU - Description and solution

>.... It drops a copy of itself as the file LSESS.EXE in the Windows system

>folder. This malware runs on Windows 95, 98, ME, NT, 2000, and XP. ...

>www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SDBOT.CU... -

>49k

>

>

>

>"Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message

>news:Ffr6d.274838\$mD.133155@attbi_s02...

>> If your virus scanner does not pick it up with the latest definitions try

Re: New Virus released, can anyone help identify it?

microsoft.public.win2000.security: Re: New Virus released, can anyone help identify it?

>> *a second opinion and contact your antivirus vendor with the information*
>> *you supplied here to see what they recommend. Trend Micro has a free and*
>> *compact Sysclean download for malware detection and removal and pattern*
>> *file that you need to download to a common folder to execute from. Also*
>> *scan with something like AdAware or Pest Patrol. Pest Patrol is pretty*
>> *good and targets Trojans and parasites. They have a free download but I*
>> *think it will only detect and not remove. Also try some of the free tools*
>> *from SysInternals – TCPView, Process Explorer, and Autoruns to help*
>> *identify what is happening by mapping port use to processes, and showing*
>> *detailed info on what applications are configured to start up*
>> *automatically. Note that you can also use msinfo32/software*
>> *environment/running tasks to see process to path mapping in W2K and you*
>> *can also use it to view processes on remote computers. For computers that*
>> *do not need to offer resources on the network it may help to enable tcp/ip*
>> *filtering on the network adapter to block uninitiated inbound traffic. Be*
>> *sure to disable it when you are done as it may cause network connectivity*
>> *problems in the future. Of course XP and W2003 have the built in ICF*
>> *firewall. --- Steve*
>>
>> <http://www.trendmicro.com/download/dcs.asp> -- Sysclean
>> <http://www.trendmicro.com/download/pattern.asp> --
pattern file current as
>> *of today*
>>
<http://www.pestpatrol.com/Downloads/Eval/DownloadHomeEvalNew.asp> -- Pest
>> *Patrol*
>>
<http://www.sysinternals.com/ntw2k/source/tcpview.shtml> --
TCPView
>>
http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/sag_TCPIP_pro_TCPIPfilter

Re: New Virus released, can anyone help identify it?

microsoft.public.win2000.security: Re: New Virus released, can anyone help identify it?

r.htm

>>

>>

>> "Craig N." <anonymous@discussions.microsoft.com> wrote
in message

>> news:114d01c4a5c0\$d39f1aa0\$a601280a@phx.gbl...

>>> I am a consultant, and I have had 3 corporate netowrks,

>>> plus 20 servera t my colo facility nailed with a new

>>> virus. Virus sacns are not picking it up, and I have
the

>>> latest definitions.

>>>

>>> I have identified the culprit service to be

LSESS.EXE, not

>>> LSASS.exe, ans the sasser patch and removal tool does
not

>>> work. ALso, in the system32 folder, I locate the file.

>>>

>>> It appears as though this virus just comes right in,
not

>>> through e-mail or surfing. Since some of the machines

>>> affected are pure gaming servers, and dont have anyone

>>> accessing the net or receiving e-mail.

>>>

>>> Anyways, as far as effects, the first noticeable sign
is

>>> that once you log into 2000, you do not get a
desktop, it

>>> just sits with a blue screen for hours. Then the
machine

>>> starts rebooting constantly.

>>>

>>> I performed a format and reinstall of 2000, and got my

>>> desktop back, but within 2 minutes, I started getting

>>> svchost errors, and Windows would rebbot after 10
seconds.

>>>

>>> I finally did a clean 2003 install, and once again
got the

>>> virus, but it was attacking the RPC,causing a reboot
in 10

>>> seconds. I went into services, and disabled the action

>>> from reboot machine to take no action for RPC.

>>>

>>> I have noticed that if I restrict access to the file

>>> LSESS.EXE the machines apper to run fine. I have also

>>> encountered multiple instances of it inthe registry.

>>>

>>> It looks like blaster or maybe Sasser, but not exact.

It

>>> also appears t be a widespread infection. I originally

Re: New Virus released, can anyone help identify it?

microsoft.public.win2000.security: Re: New Virus released, can anyone help identify it?

>>> *caught it two days ago, and assumed it was blaster,*
but
>>> *then it nailed everypne today, and these are all*
seperate
>>> *corporations, and nothing on the security sites*
regarding
>>> *it.*
>>>
>>> *Anyways, anyone have any idea what it is?*
>>>
>>>
>>
>>
>
>
>
>