

Re: Sasser & Blaster problem

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-05/2127.html>

From: PA Bear (PABear_at_mvps.org)

Date: 05/25/04

Date: Tue, 25 May 2004 17:04:11 -0400

> *Can I safely assume that this means that all is
> well, or is there another way that I should check?*

Prolly but you can try running a couple of the the free online scans listed at <http://aumha.org/secure.php#freeav>.

Configure NAV to seek updates and run a full system scan daily at a time when the machine is normally running and connected. If necessary, do so manually or configure NAV to do so (in that order) at boot.

SysRestore should be re-enabled.

Glad to be able to help.

--

~PA Bear

soups wrote:

> Thank you so much, PA Bear. I followed the instructions to
> the letter, and everything seems to have worked. I was
> able to download/install/run every update/patch/tool that
> I needed. Blaster and Sasser were successfully removed
> according to the tool messages. I also managed to extract
> Welchia, Randex and Bobax following instructions from
> Symantec I think it was. What a mess: I would call what I
> had worse than an infestation.
> XP Firewall is on, Norton AV is updated and running, and
> all MS downloads in place. I do, however, have a few more
> questions if I may take more of your time.
> I have run the AV, and it no longer finds any infected
> files. Can I safely assume that this means that all is
> well, or is there another way that I should check?
> I take it that I should no enable System Restore again?
> And return the RPC to the original settings (if I can find
> the note I made as to what they were)? Anything else I
> should do?
> Thank you again very very much,
> soups

>

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

>> Instructions for patching and cleaning vulnerable Windows 2000 and

>> Windows XP systems:

>>

>> Vulnerable Windows 2000 and Windows XP machines may have the LSASS.EXE

Re: Sasser & Blaster problem

microsoft.public.security: Re: Sasser & Blaster problem

>> process crash every time a malicious worm packet targets the vulnerable
>> machine which can occur very shortly after the machine starts up and
>> initializes the network stack.
>>
>> When cleaning a machine that is vulnerable to the Sasser worm it is
>> necessary to first prevent the LSASS.EXE process from crashing, which in
>> turn causes the machine to reboot after a 60 second delay. This reboot
>> cannot be aborted on Windows 2000 platforms using the Shutdown.exe or
>> psshutdown.exe utilities and can interfere with the downloading and
>> installation of the patch as well as removal of the worm.
>>
>> 1. To prevent LSASS.EXE from shutting down the machine during the
>> cleaning process: a. Unplug the network cable from the machine b. If you
>> are running Windows XP you can enable the built-in Internet Connection
>> Firewall using the instructions found here: Windows XP
>> <http://support.microsoft.com/?id=283673> and then plug the machine back
>> into the network and go to step 2.
>>
>> c. If you are running Windows 2000, you won't have a built-in firewall
>> and must use the following work-around to prevent LSASS.EXE from
>> crashing. This workaroud involves creating a read-only file
> named 'dcpromo.log' in the
>> "%systemroot%\debug" directory. Creating this read-only file will
>> prevent the vulnerability used by this worm from crashing the LSASS.EXE
>> process. i. NOTE: %systemroot% is the variable that contains the name
>> of the Windows installation directory. For example if Windows was
>> installed to the "c:\winnt" directory the following command will create
>> a file called dcpromo.log in the c:\winnt\debug directory. The
>> following commands must be typed in a command prompt (i.e. cmd.exe)
>> exactly as they are written below.
>>
>> 1. To start a command shell, click Start and then click run and type
>> 'cmd.exe' and press enter.
>>
>> 2.Type the following command: echo dcpromo >%systemroot%
>> \debug\dcpromo.log
>>
>> For this workaroud to work properly you MUST make the file read-only by
>> typing the following command:
>>
>> 3. attrib +R %systemroot%\debug\dcpromo.log
>>
>>
>> 2. After enabling the Internet Connection Firewall or creating the
>> read-only dcpromo.log you can plug the network cable back in and you
>> must download and install the MS04-011 patch from the MS04-011 download
>> link for the affected machines operating system before cleaning the
>> system. If the system is cleaned before the patch is installed it is
>> possible that the system could get re-infected prior to installing the
>> patch. a. Here is the URL for the bulletin which contains the links to
>> the download location for each patch:
>> <http://www.microsoft.com/technet/security/bulletin/ms04-011.msp> b. If
>> your machine is acting sluggish or your Internet connection is slow you
>> should use Task Manager to kill the following processes and then try
>> downloading the patch again (press the Ctrl + Alt + Del keys
>> simultaneously and select Task Manager):
>>
>> i. Kill any process ending with '_up.exe' (i.e. 12345_up.exe) ii. Kill
>> any process starting with 'avserv' (i.e. avserve.exe, avserve2.exe) iii.
>> Kill any process starting with 'skynetave' (i.e.
> skynetave.exe) iv. Kill hkey.exe
>> v. Kill msiwin84.exe vi. Kill wmioprsvw.exe

microsoft.public.security: Re: Sasser & Blaster problem

>>
>>
>> 1. Note there is a legitimate system process
> called 'wmiprvse.exe' that does
>> NOT need to be killed. c. allow the system to reboot after the patch is
>> installed.
>>
>>
>> 3. Run the Sasser cleaner tool from the following URL: a. For the on-line
>> ActiveX control based version of the cleaner you can run it directly from
>> the following URL:
> <http://www.microsoft.com/security/incident/sasser.asp>
>>
>> b. For the stand-alone download version of the cleaner you can download
>> it from the following URL:
>>
>> [http://www.microsoft.com/downloads/details.aspx?](http://www.microsoft.com/downloads/details.aspx?FamilyId=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&displaylang=en)
> FamilyId=76C6DE7E-1B6B-4FC3-90D4-
> 9FA42D14CC17&displaylang=en
>>
>> 4. Determine if the machine has been infected with a variant of the
>> Agobot worm which can also get on the machine using the same method as
>> the Sasser worm. a. To do this run a full antivirus scan of your machine
>> after ensuring your antivirus signatures are up to date. b. If you do
>> NOT have an antivirus product installed you can visit HouseCall from
>> TrendMicro to perform a free scan using the following URL:
> <http://housecall.trendmicro.com/>
>>
>> If you have any questions regarding the security updates or its
>> implementation after reading the above listed bulletin you should contact
>> Product Support Services in the United States at 1-866- PCSafety
>> (1-866-727-2338). International customers should contact their local
>> subsidiary.
>> --
>> HTH - Please Reply to This Thread
>>
>> ~Robear Dyer (PA Bear)
>> MS MVP-Windows (IE/OE), AH-VSOP
>>
>> AumHa Forums
>> <http://forum.aumha.org>
>>
>> Protect Your PC
>> <http://www.microsoft.com/security/protect>
>>
>> Soups wrote:
>>> Without going into how it happened (a very long story),
>>> Sasser and Blaster both are occupying my notebook (HP
>>> ze4230/XP). In a nutshell, it's thanks to no firewall
>>> protection and a shocking (about 8 months worth) lack of
>>> patches/updates from MS.
>>> Right now, all downloads/installations of patches/updates
>>> from MS are blocked with the familiar NT message. I have
>>> tried instructions from Symantec, MS and countless others
>>> to stop the processes so that I can (maybe) download
>>> updates and a removal tool, but I cannot find any of these
>>> processes in Task Mgr. These include processes starting
>>> with 4 or more numbers to msiwin84.exe, all from a very
>>> recent list from Symantec. I never found Msblast.exe
>>> either. I have disabled System Restore. I have altered the
>>> RPC from first, second and subsequent failures to restart
>>> the service. In a nutshell, I have followed everything,

microsoft.public.security: Re: Sasser & Blaster problem

```
>>> but I cannot get rid of this mess.  
>>> Where else might I find Sasser/Blaster to stop the  
>>> processes?  
>>> Is it possible that I could do a System Recovery (not  
>>> restore--I can be dumb, but not that dumb!), add a  
>>> firewall and then go online to install what I need?  
>>> Thanks for the help.  
>>>  
>>> Soups  
>>  
>> .
```