

microsoft.public.windowsupdate: Re: Worm blaster remover program.

Re: Worm blaster remover program.

Source: <http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2004-06/0827.html>

From: Shenan Stanley (*news_helper_at_hushmail.com*)

Date: 06/05/04

Date: Fri, 4 Jun 2004 23:26:11 -0500

Gypsum 35 wrote:

> *Worm blaster remover will not load.*

BLASTER:

If you have Blaster, the Microsoft provided information on the matter can be found here:

<http://support.microsoft.com/?kbid=826955>

The Microsoft recovery tool to assist you in its removal can be found here:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e70a0d8b-fe98-493f-ad76-bf673a38b4cf&DisplayLang=en>

(Shorter Link: <http://snipurl.com/3rq0>)

The Symantec Repair utility and manual removal instructions can be found here:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html>

The McAfee "Stinger" utility to help remove the pest can be found here:

<http://vil.nai.com/vil/stinger/>

The patch that would have prevented this whole fiasco for you (XP):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=5fa055ae-a1ba-4d4a-b424-95d32cfc8cba&DisplayLang=en>

(Shorter Link: <http://snipurl.com/2d5x>)

SASSER:

If you have Sasser, the Microsoft provided information on the matter can be found here:

<http://www.microsoft.com/security/incident/sasser.asp>

The Microsoft recovery tool to assist you in its removal can be found here:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&DisplayLang=en>

(Shorter Link: <http://snipurl.com/63mw>)

The Symantec Repair utility and manual removal instructions can be found here:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.removal.tool.html>

The McAfee "Stinger" utility to help remove the pest can be found here:

<http://vil.nai.com/vil/stinger/>

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

The patch that would have prevented this whole fiasco for you(XP):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=3549EA9E-DA3F-43B9-A4F1-AF243B6168F3&disp>

(Shorter Link: <http://snipurl.com/64oy>)

** You MUST have Windows XP SP1a installed FIRST!

As far as Sasser removal, I have found Microsoft's instructions (posted on these newsgroups earlier) work wonders (particularly changing certain files to read-only) and the removal tool and subsequent patches seem to repair 95% of the problems. True, some people have to ask friends with CD burners for assistance, but it fixes their issues.

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.

--- Begin Microsoft Instructions given in Newsgroups Earlier ---

This workaround 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 workaround to work properly you MUST make the file read-only by typing the following command:

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

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 wmiprvsw.exe

– 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?FamilyId=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&disp>

(Short Link: <http://snipurl.com/63mw>)

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/>

-- End Microsoft Instructions given in Newsgroups Earlier --

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

Once you have rid yourself of which ever virus/worm you had (or if you had both, of both) then you need to make sure it never happens again. This means you need to learn to protect your PC and perform periodic maintenance to it in order to be sure this never happens again, or if it does, the damage is minimal.

Suggestions on what you can do to secure/clean your PC. I'm going to try and be general, I will assume a "Windows" operating system is what is being secured here.

UPDATES and PATCHES

This one is the most obvious. There is no perfect product and any company worth their salt will try to meet/exceed the needs of their customers and fix any problems they find along the way. I am not going to say Microsoft is the best company in the world about this but they do have an option available for you to use to keep your machine updated and patched from the problems and vulnerabilities (as well as product improvements in some cases) – and it's free to you.

Windows Update

<http://windowsupdate.microsoft.com/>

Go there and scan your machine for updates. Always get the critical ones as you see them. Write down the KB##### or Q##### you see when selecting the updates and if you have trouble over the next few days, go into your control panel (Add/Remove Programs), match up the latest numbers you downloaded recently (since you started noticing an issue) and uninstall them. If there was more than one (usually is), install them back one by one – with a few hours of use in between, to see if the problem returns. Yes – the process is not perfect (updating) and can cause trouble like I mentioned – but as you can see, the solution isn't that bad – and is MUCH better than the alternatives. (SASSER/BLASTER were SO preventable with just this step!)

Windows is not the only product you likely have on your PC. The manufacturers of the other products usually have updates as well. New versions of almost everything come out all the time – some are free, some are pay – some you can only download if you are registered – but it is best to check. Just go to their web pages and look under their support and download sections.

You also have hardware on your machine that requires drivers to interface with the operating system. You have a video card that allows you to see on your screen, a sound card that allows you to hear your PCs sound output and so on. Visit those manufacturer web sites for the latest downloadable drivers for your hardware/operating system. Always (IMO) get the manufacturers hardware driver over any Microsoft offers. On the Windows Update site I mentioned earlier, I suggest NOT getting their hardware drivers – no matter how tempting.

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

Have I mentioned that Microsoft has some stuff to help secure your computer available to the end-user for free? This seems as good of a time as any. They have a CD you can order (it's free) that contain all of the Windows patches through October 2003 and some trial products as well that they released in February 2004. Yeah – it's a little behind now, but it's better than nothing (and used in coordination with the information in this post, well worth the purchase price..)

Order the Windows Security Update CD
<http://www.microsoft.com/security/protect/cd/order.asp>

They also have a bunch of suggestions, some similar to these, on how to better protect your Windows system:

Protect your PC
<http://www.microsoft.com/security/protect/>

FIREWALL

Let's say you are up-to-date on the OS (operating system) and you have Windows XP.. You should at least turn on the built in firewall. That will do a lot to "hide" you from the random bad things flying around the Internet. Things like Sasser/Blaster enjoy just sitting out there in Cyberspace looking for an unprotected Windows Operating System and jumping on it, doing great damage in the process and then using that Unprotected OS to continue its dirty work of infecting others. If you have the Windows XP ICF turned on – default configuration – then they cannot see you! Think of it as Internet Stealth Mode at this point. It has other advantages, like actually locking the doors you didn't even (likely) know you had. Doing this is simple, the instructions you need to use your built in Windows XP firewall can be found here:

<http://support.microsoft.com/?kbid=320855>

If you read through that and look through the pages that are linked from it at the bottom of that page – I think you should have a firm grasp on the basics of the Windows XP Firewall as it is today. One thing to note RIGHT NOW – if you have AOL, you cannot use this nice firewall that came with your system. Thank AOL, not Microsoft. You HAVE to configure another one.. So we continue with our session on Firewalls..

But let's say you DON'T have Windows XP – you have some other OS like Windows 95, 98, 98SE, ME, NT, 2000. Well, you don't have the nifty built in firewall. My suggestion – upgrade. My next suggestion – look through your options. There are lots of free and pay firewalls out there for home users. Yes – you will have to decide on your own which to get. Yes, you will have to learn (oh no!) to use these firewalls and configure them so they don't interfere with what you want to do while continuing to provide the security you desire. It's just like anything else you want to protect – you have to do something to protect it. Here are some suggested applications. A lot of

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

people tout "ZoneAlarm" as being the best alternative to just using the Windows XP ICF, but truthfully – any of these alternatives are much better than the Windows XP ICF at what they do – because that is ALL they do.

ZoneAlarm (Free and up)

<http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp>

Kerio Personal Firewall (KPF) (Free and up)

http://www.kerio.com/kpf_download.html

Outpost Firewall from Agnitum (Free and up)

<http://www.agnitum.com/download/>

Sygate Personal Firewall (Free and up)

http://smb.sygate.com/buy/download_buy.htm

Symantec's Norton Personal Firewall (~\$25 and up)

<http://www.symantec.com/sabu/nis/npf/>

BlackICE PC Protection (\$39.95 and up)

<http://blackice.iss.net/>

Tiny Personal Firewall (~\$49.00 and up)

<http://www.tinysoftware.com/>

That list is not complete, but they are good firewall options, every one of them. Visit the web pages, read up, ask around if you like – make a decision and go with some firewall, any firewall. Also, maintain it. Sometimes new holes are discovered in even the best of these products and patches are released from the company to remedy this problem. However, if you don't get the patches (check the manufacturer web page on occasion), then you may never know you have the problem and/or are being used through this weakness. Also, don't stack these things. Running more than one firewall will not make you safer – it would likely (in fact) negate some protection you gleamed from one or the other firewalls you ran together.

ANTIVIRUS SOFTWARE

That's not all. That's one facet of a secure PC, but firewalls don't do everything. I saw one idiot posting on a newsgroup that "they had never had a virus and they never run any anti-virus software. Yep – I used to believe that way too – viruses were something everyone else seemed to get, were they just stupid? And for the average joe-user who is careful, uses their one-three family computers carefully, never opening unknown attachments, always visiting the same family safe web sites, never installing anything that did not come with their computer – maybe, just maybe they will never witness a virus. I, however, am a Network Systems Administrator. I see that AntiVirus software is an absolute necessity. You can be as careful as you want – will the next person be as careful? Will someone send you unknowingly the email that erases all the pictures of your

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

child/childhood? Possibly – why take the chance? ALWAYS RUN ANTIVIRUS SOFTWARE and KEEP IT UP TO DATE! Antivirus software comes in so many flavors, it's like walking into a Jelly Belly store – which one tastes like what?! Well, here are a few choices for you. Some of these are free (isn't that nice?) and some are not. Is one better than the other – MAYBE. I personally love Symantec AV.

Symantec (Norton) AntiVirus (~\$11 and up)
<http://www.symantec.com/>

Kaspersky Anti-Virus (~\$49.95 and up)
<http://www.kaspersky.com/products.html>

Panda Antivirus Titanium (~\$39.95 and up)
<http://www.pandasoftware.com/>
(Free Online Scanner: <http://www.pandasoftware.com/activescan/>)

AVG 6.0 Anti-Virus System (Free and up)
<http://www.grisoft.com/>

McAfee VirusScan (~\$11 and up)
<http://www.mcafee.com/>

AntiVir (Free and up)
<http://www.free-av.com/>

avast! 4 (Free and up)
<http://www.avast.com/>

Trend Micro (~\$49.95 and up)
<http://www.trendmicro.com/>
(Free Online Scanner:
http://housecall.trendmicro.com/housecall/start_corp.asp)

Did I mention you have to not only install this software, but also keep it updated? You do. Some of them (most) have automatic services to help you do this – I mean, it's not your job to keep up with the half-dozen or more new threats that come out daily, is it? Be sure to keep whichever one you choose up to date!

SPYWARE/ADWARE/POPUPS

So you must be thinking that the above two things got your back now – you are covered, safe and secure in your little fox hole. Wrong! There are more bad guys out there. There are annoyances out there you can get without trying. Your normal web surfing, maybe a wrong click on a web page, maybe just a momentary lack of judgment by installing some software packages without doing the research.. And all of a sudden your screen starts filling up with advertisements or your Internet seems much slower or your home page won't stay what you set it and goes someplace unfamiliar to you. This is

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

spyware. There are a whole SLEW of software packages out there to get rid of this crud and help prevent reinfection. Some of the products already mentioned might even have branched out into this arena. However, there are a few applications that seem to be the best at what they do, which is eradicating and immunizing your system from this crap. Strangely, the best products I have found in this category ARE generally free. That is a trend I like. I make donations to some of them, they deserve it!

Spybot Search and Destroy (Free!)

<http://www.safer-networking.net/>

Lavasoft AdAware (Free and up)

<http://www.lavasoft.de>

CWSShredder (Free!)

<http://www.spywareinfo.com/~merijn/downloads.html>

Hijack This! (Free)

<http://mjc1.com/mirror/hjt/>

(Tutorial: <http://www.spywareinfo.com/~merijn/htlogtutorial.html>)

SpywareBlaster (Free!)

<http://www.javacoolsoftware.com/>

IE-SPYAD (Free!)

<http://www.staff.uiuc.edu/~ehowes/resource.htm>

ToolbarCop (Free!)

<http://www.mvps.org/sramesh2k/toolbarcop.htm>

Bazooka Adware and Spyware Scanner (Free!)

<http://kephyr.sureshot.xaviermedia.net/spywarescanner/>

Browser Security Tests

<http://www.jasons-toolbox.com/BrowserSecurity/>

The Cleaner (49.95 and up)

<http://www.moosoft.com/>

That will clean up your machine of the spyware, given that you download and install several of them, update them regularly and scan with them when you update. Some (like SpywareBlaster and SpyBot Search and Destroy) have immunization features that will help you prevent your PC from being infected. Use these features!

Unfortunately, although that will lessen your popups on the Internet/while you are online, it won't eliminate them. I have looked at a lot of options, seen a lot of them used in production with people who seem to attract popups like a plague, and I only have one suggestion that end up serving double duty (search engine and popup stopper in one):

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

The Google Toolbar (Free!)

<http://toolbar.google.com/>

Yeah – it adds a bar to your Internet Explorer – but its a useful one. You can search from there anytime with one of the best search engines on the planet (IMO.) And the fact it stops most popups – wow – BONUS! If you don't like that suggestion, then I am just going to say you go to www.google.com and search for other options.

One more suggestion, although I will suggest this in a way later, is to disable your Windows Messenger service. This service is not used frequently (if at all) by the normal home user and in cooperation with a good firewall, is generally unnecessary. Microsoft has instructions on how to do this for Windows XP here:

<http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp>

SPAM EMAIL/JUNK MAIL

This one can get annoying, just like the rest. You get 50 emails in one sitting and 2 of them you wanted. NICE! (Not.) What can you do? Well, although there are services out there to help you, some email servers/services that actually do lower your spam with features built into their servers – I still like the methods that let you be the end–decision maker on what is spam and what isn't. If these things worked perfectly, we wouldn't need people and then there would be no spam anyway – vicious circle, eh? Anyway – I have two products to suggest to you, look at them and see if either of them suite your needs. Again, if they don't, Google is free and available for your perusal.

SpamBayes (Free!)

<http://spambayes.sourceforge.net/>

Spamihilator (Free!)

<http://www.spamihilator.com/>

As I said, those are not your only options, but are reliable ones I have seen function for hundreds+ people.

DISABLE (Set to Manual) UNUSED SERVICE/STARTUP APPS

I might get arguments on putting this one here, but it's my spill. There are lots of services on your PC that are probably turned on by default you don't use. Why have them on? Check out these web pages to see what all of the services you might find on your computer are and set them according to your personal needs. Be CAREFUL what you set to manual, and take heed and write down as you change things! Also, don't expect a large performance increase or anything – especially on todays 2+ GHz machines, however – I look at each service you set to manual as one less service you have to worry about someone exploiting. A year ago, I would have thought the Windows Messenger

Re: Worm blaster remover program.

microsoft.public.windowsupdate: Re: Worm blaster remover program.

service to be pretty safe, now I recommend (with addition of a firewall) that most home users disable it! Yeah – this is another one you have to work for, but your computer may speed up and/or be more secure because you took the time. And if you document what you do as you do it, next time, it goes MUCH faster! (or if you have to go back and re-enable things..)

Task List Programs

http://www.answerthatwork.com/Tasklist_pages/tasklist.htm

Black Viper's Service List and Opinions (XP)

<http://www.blackviper.com/WinXP/servicecfg.htm>

Processes in Windows NT/2000/XP

<http://www.reger24.de/prozesse/>

There are also applications that AREN'T services that startup when you start up the computer/logon. One of the better description on how to handle these I have found here:

Startups

http://www.pacs-portal.co.uk/startup_content.php

That's it. A small booklet on how to keep your computer secure, clean of scum and more user friendly. I am SURE I missed something, almost as I am sure you won't read all of it (anyone for that matter.) However, I also know that someone who followed all of the advice above would also have less problems with their PC, less problems with viruses, less problems with spam, less problems with spyware and better performance than someone who didn't.

Hope it helps.

--

<- Shenan ->

--

The information is provided "as is", with no guarantees of completeness, accuracy or timeliness, and without warranties of any kind, express or implied. In other words, read up before you take any advice - you are the one ultimately responsible for your actions.