

Re: Trojan horse Downloader.Stubby.A

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-12/0630.html>

From: Bill Sanderson (*Bill_Sanderson_at_msn.com.plugh.org*)

Date: 12/09/03

Date: Mon, 8 Dec 2003 22:56:10 -0500

I just ran HijackThis on my system.

It was useful—it allowed me to remove a couple of startups, one of which remained from a manual ripping out by the roots of some software, and another of which I was tired of seeing in my notification area.

OTOH, here's what was left. There's a lot here, and I believe it is all stuff that is reasonably safe and that I want. Sorting out the dross from this kind of list is going to take some real care, no?

Logfile of HijackThis v1.97.7

Scan saved at 10:54:36 PM, on 12/8/2003

Platform: Windows XP SP1 (WinNT 5.01.2600)

MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:

E:\WINDOWS\System32\smss.exe

E:\WINDOWS\system32\winlogon.exe

E:\WINDOWS\system32\services.exe

E:\WINDOWS\system32\lsass.exe

E:\WINDOWS\system32\svchost.exe

E:\WINDOWS\System32\svchost.exe

E:\WINDOWS\system32\spoolsv.exe

E:\WINDOWS\Explorer.EXE

E:\Program Files\Google\ggviewer67-34.exe

E:\Program Files\TZO\TZOClient.exe

E:\WINDOWS\System32\taskswitch.exe

E:\WINDOWS\System32\pool\drivers\w32x86\3\hpztsb04.exe

C:\PROGRA~1\CA\ETRUST~1\ETRUST~1\VetTray.exe

E:\WINDOWS\System32\ctfmon.exe

E:\WINDOWS\System32\devldr32.exe

E:\Program Files\MSN Messenger\MsnMsgr.Exe

E:\Program Files\AnalogX\TSDropCopy\tsdc.exe

E:\Program Files\United Devices\UD.exe

E:\Program Files\United Devices\ud_1706422.exe

E:\WINDOWS\System32\CTsvcCDA.EXE

E:\WINDOWS\System32\inetsrv\inetinfo.exe

Re: Trojan horse Downloader.Stubby.A

microsoft.public.security.virus: Re: Trojan horse Downloader.Stubby.A

E:\Program Files\United Devices\ud_1706422_0.dir\ud_ligfit_Release.exe
E:\WINDOWS\System32\ScsiAccess.EXE
E:\WINDOWS\System32\tcpsvcs.exe
E:\WINDOWS\System32\snmp.exe
E:\WINDOWS\System32\svchost.exe
E:\Program Files\TZO\TZO_NT_Service.exe
E:\WINDOWS\System32\VetMsgNT.exe
E:\WINDOWS\System32\MsPMSPSv.exe
E:\Program Files\Outlook Express\msimn.exe
E:\Program Files\SpamPal\spampal.exe
E:\Documents and Settings\billS\Desktop\hijackthis\HijackThis.exe

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Window Title = Bill Sanderson's Microsoft Internet Explorer
R1 – HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = gopher=127.0.0.1:80
O2 – BHO: (no name) – {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} – D:\Program Files\Adobe\Acrobat 6.0\Reader\ActiveX\AcroIEHelper.dll
O2 – BHO: (no name) – {AA58ED58-01DD-4d91-8333-CF10577473F7} – e:\program files\google\googletoolbar1.dll
O3 – Toolbar: &Radio – {8E718888-423F-11D2-876E-00A0C9082467} – E:\WINDOWS\System32\msdxm.ocx
O3 – Toolbar: &Google – {2318C2B1-4965-11d4-9B18-009027A5CD4F} – e:\program files\google\googletoolbar1.dll
O4 – HKLM\..\Run: [TZOCClient] E:\Program Files\TZO\TZOCClient.exe
O4 – HKLM\..\Run: [UpdReg] E:\WINDOWS\Updreg.exe
O4 – HKLM\..\Run: [AHQInit] E:\Program Files\Creative\SBLive2k\Program\AHQInit.exe
O4 – HKLM\..\Run: [CoolSwitch] E:\WINDOWS\System32\taskswitch.exe
O4 – HKLM\..\Run: [HPDJ Taskbar Utility] E:\WINDOWS\System32\spool\drivers\w32x86\3\hpztsb04.exe
O4 – HKLM\..\Run: [QuickTime Task] "D:\program files\quicktime\qttask.exe" –atboottime
O4 – HKLM\..\Run: [NeroCheck] E:\WINDOWS\system32\NeroCheck.exe
O4 – HKLM\..\Run: [Qwik-Fix] "E:\Program Files\PivX Qwik-Fix\QwikFix.exe" splash
O4 – HKLM\..\Run: [VetTray] c:\PROGRA~1\CA\ETRUST~1\ETRUST~1\VetTray.exe
O4 – HKCU\..\Run: [ctfmon.exe] E:\WINDOWS\System32\ctfmon.exe
O4 – HKCU\..\Run: [msnmsgr] "E:\Program Files\MSN Messenger\MsnMsgr.Exe" /background
O4 – Startup: SpamPal.lnk = E:\Program Files\SpamPal\spampal.exe
O4 – Startup: TSDropCopy.lnk = E:\Program Files\AnalogX\TSDropCopy\tsdc.exe
O4 – Startup: UD Agent.lnk = ?
O4 – Global Startup: Microsoft Broadband Networking.lnk = ?
O4 – Global Startup: Microsoft Office.lnk = D:\Program Files\Microsoft Office\Office10\OSA.EXE
O8 – Extra context menu item: &Google Search – res://E:\Program Files\Google\GoogleToolbar1.dll/cmsearch.html
O8 – Extra context menu item: Backward &Links – res://E:\Program Files\Google\GoogleToolbar1.dll/cmbacklinks.html
O8 – Extra context menu item: Cac&hed Snapshot of Page – res://E:\Program

Re: Trojan horse Downloader.Stubby.A

microsoft.public.security.virus: Re: Trojan horse Downloader.Stubby.A

Files\Google\GoogleToolbar1.dll\cmcache.html
O8 – Extra context menu item: Similar Pages – res://E:\Program
Files\Google\GoogleToolbar1.dll\cmsimilar.html
O8 – Extra context menu item: Translate Page – res://E:\Program
Files\Google\GoogleToolbar1.dll\cmtrans.html
O9 – Extra button: Related (HKLM)
O9 – Extra 'Tools' menuitem: Show & Related Links (HKLM)
O9 – Extra button: Messenger (HKLM)
O9 – Extra 'Tools' menuitem: Messenger (HKLM)
O16 – DPF: {01A88BB1-1174-41EC-ACCB-963509EAE56B} (SysProWmi Class) –
<http://support.dell.com/systemprofiler/SysPro.CAB>
O16 – DPF: {02BCC737-B171-4746-94C9-0D8A0B2C0089} (Microsoft Office Template
and Media Control) – <http://office.microsoft.com/templates/ieawscab>
O16 – DPF: {02BF25D5-8C17-4B23-BC80-D3488ABDDC6B} (QuickTime Object) –
<http://www.apple.com/qtactivex/qtplugin.cab>
O16 – DPF: {03F998B2-0E00-11D3-A498-00104B6EB52E} (MetaStreamCtl Class) –
<https://components.viewpoint.com/MTSInstallers/MetaStream3.cab?url=Compaq>
O16 – DPF: {11865A2A-649F-4FA1-8B99-B97DF8070B7C} (IWSsystemchecks Control) –
<http://msfm.interwise.com/msfm/English/ActiveX/IWsystemchecks.cab>
O16 – DPF: {11B2C0D3-DFFB-11D3-9253-00500498D7E2} (ShowSetupObj2 Class) –
<http://invite.mshow.com/ShowSetup2.dll>
O16 – DPF: {11B2C0D3-DFFB-11D3-9253-00500498D7E3} (ShowSetupObj3 Class) –
<http://invite.mshow.com/ShowSetup.cab>
O16 – DPF: {166B1BCA-3F9C-11CF-8075-444553540000} (Shockwave ActiveX
Control) – <http://download.macromedia.com/pub/shockwave/cabs/director/sw.cab>
O16 – DPF: {1954A4B1-9627-4CF2-A041-58AA2045CB35} (Brix6ie Control) –
<http://a19.g.akamai.net/7/19/7125/1269/ftp.coupons.com/v6/brix6ie.cab>
O16 – DPF: {19E28AFC-EAE3-4CE5-AC83-2407B42F57C9} (MSSecurityAdvisor
Class) –
<http://protect.microsoft.com/security/protect/WSA/shared/cab/x86/MSSecAdv.cab?1063205794992>
O16 – DPF: {2BC66F54-93A8-11D3-BEB6-00105AA9B6AE} (Symantec AntiVirus
scanner) –
<http://security.symantec.com/sscv6/SharedContent/vc/bin/AvSniff.cab>
O16 – DPF: {34805D32-AD89-469E-8503-A5666AEE4333} (RdxIE Class) –
<http://207.82.221.103/10085e868404f4209c21/netzip/RdxIE.cab>
O16 – DPF: {41E95AF7-BB7B-403D-8E8B-4162188943DE} (INVC Participant Console
1.51) – <http://66.228.194.114/in/clients/listener/bin/inlist151.cab>
O16 – DPF: {4BEE3896-4820-48D1-85EA-5A9A9ECD3D95} (OPUCatalog Class) –
<http://office.microsoft.com/productupdates/content/opuc.cab>
O16 – DPF: {4E330863-6A11-11D0-BFD8-006097237877} (InstallFromTheWeb ActiveX
Control) – <http://msfm.interwise.com/IWCampus/student/client/iftwclix.cab>
O16 – DPF: {4E888414-DB8F-11D1-9CD9-00C04F98436A} (Microsoft.WinRep) –
<https://webresponse.one.microsoft.com/oas/ActiveX/winrep.cab>
O16 – DPF: {4ED9DDF0-7479-4BBE-9335-5A1EDB1D8A21} (McAfee.com Operating
System Class) –
<http://bin.mcafee.com/molbin/shared/mcinsctl/en-us/4.0.0.56/mcinsctl.cab>
O16 – DPF: {4FAE30E1-EE9C-477D-8D06-BF8D3429B60F} (WebIQ Technology
Client) – <http://webiqonline.com/WebIQ/bin/WebIQ.cab>
O16 – DPF: {56336BCB-3D8A-11D6-A00B-0050DA18DE71} (RdxIE Class) –
<http://207.188.7.150/0503130719ab0a231c04/netzip/RdxIE6.cab>
O16 – DPF: {597C45C2-2D39-11D5-8D53-0050048383FE} (OPUCatalog Class) –

Re: Trojan horse Downloader.Stubby.A

microsoft.public.security.virus: Re: Trojan horse Downloader.Stubby.A

<http://office.microsoft.com/productupdates/content/opuc.cab>

O16 – DPF: {713AE1D4-897C-11D2-B2A0-00C04F94B4D5} (WUCorpSuppControl Class) – <http://corporate.windowsupdate.microsoft.com/en/wucorpct.CAB>

O16 – DPF: {74D05D43-3236-11D4-BDCD-00C04F9A3B61} (HouseCall Control) – <http://a840.g.akamai.net/7/840/537/2003031101/housecall.antivirus.com/housecall/xscan53.cab>

O16 – DPF: {7584C670-2274-4EFB-B00B-D6AABA6D3850} (Microsoft RDP Client Control (redist)) – <http://fgc2003/tsweb/msrdp.cab>

O16 – DPF: {776706AE-CACA-4EA3-93DF-BB83D9259DA9} (MailConfigure Class) – <http://supportservices.msn.com/us/smtptool/MailCfg.cab>

O16 – DPF: {80DD2229-B8E4-4C77-B72F-F22972D723EA} (AvxScanOnline Control) – <http://www.bitdefender.com/scan/Msie/bitdefender.cab>

O16 – DPF: {82774781-8F4E-11D1-AB1C-0000F8773BF0} (DLC Class) – <http://transfers.one.microsoft.com/FTM/TransferSource/grTransferCtrl.cab>

O16 – DPF: {928626A3-6B98-11CF-90B4-00AA00A4011F} (SurroundVideoCtrl Object) – <http://carpoint.msn.com/components/ocx/Survid/MSSurVid.cab>

O16 – DPF: {9A9307A0-7DA4-4DAF-B042-5009F29E09E1} (ActiveScan Installer Class) – <http://www.pandasoftware.com/activescan/as5/asinst.cab>

O16 – DPF: {9F1C11AA-197B-4942-BA54-47A8489BB47F} (Update Class) – <http://v4.windowsupdate.microsoft.com/CAB/x86/unicode/iucl.CAB?37575.7315856482>

O16 – DPF: {A3009861-330C-4E10-822B-39D16EC8829D} (CRAVOnline Object) – <http://www.ravantivirus.com/scan/ravonline.cab>

O16 – DPF: {A7E092C3-692A-11D0-A7E5-08002B322F3B} (WebResponseAttachments Control) – <https://webresponse.one.microsoft.com/oas/ActiveX/FileXfer.cab>

O16 – DPF: {BB47CA33-8B4D-11D0-9511-00C04FD9152D} (ExteriorSurround Object) – <http://carpoint.msn.com/Components/Ocx/Exterior/Outside.cab>

O16 – DPF: {BF116476-3238-4EDA-A2D7-6D6814EF0DEC} (Quicksilver Class) – <http://scpwbf.ops.placeware.com/etc/place/RCC-BETA/pws-ms-04/5100-zi/lib/quicksilver.cab>

O16 – DPF: {C2FCEF52-ACE9-11D3-BEBD-00105AA9B6AE} (Symantec RuFSI Registry Information Class) –

<http://security.symantec.com/sscv6/SharedContent/common/bin/cabsa.cab>

O16 – DPF: {C78AC153-1FB9-4198-986D-3613E49B152E} (ScanMe Class) – <http://download.microsoft.com/download/win2000platform/Utility/416/NT45XP/EN-US/mssecuredll.cab>

O16 – DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) – <http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>

O16 – DPF: {DF6A0F17-0B1E-11D4-829D-00C04F6843FE} (Microsoft Office Tools on the Web Control) –

<http://officeupdate.microsoft.com/TemplateGallery/downloads/outc.cab>

O16 – DPF: {F2A84794-EE6D-447B-8C21-3BA1DC77C5B4} (SDKInstall Class) – <http://activex.microsoft.com/activex/controls/sdkupdate/sdkinst.cab>

O16 – DPF: {F58E1CEF-A068-4C15-BA5E-587CAF3EE8C6} (MSN Chat Control 4.5) – <http://fdl.msn.com/public/chat/msnchat45.cab>

O16 – DPF: {F7DC2A2E-FC34-11D3-B1D9-00A0C99B41BB} (Zoom Class) – <http://www.zoomify.com/download/zoomify214.cab>

"Kent W. England [MVP]" <kwe@mvp.org> wrote in message news:%23srSe7QvDHA.3468@TK2MSFTNGP11.phx.gbl...

> I think we can deal with hijackthis reports in this forum, so long as

> users follow the recommendations that spywareinfo suggests:

>

Re: Trojan horse Downloader.Stubby.A

microsoft.public.security.virus: Re: Trojan horse Downloader.Stubby.A

> 1) download and run SpybotSD and/or Adaware and remove all known spyware
> 2) update your anti-virus, run it, and remove all known viruses
> 3) download and run hijackthis and create a report to post here
>
> That way the hijackthis report deals only with a possible new bug or a
> particularly difficult trojan or a new variant of CWS.
>
> --
> Kent W. England, Microsoft MVP for Windows Security
>
>
>
> "Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message
> news:%238Ph4VeuDHA.2168@TK2MSFTNGP10.phx.gbl...
>> OK – that's clear, and I agree that the tool is outstandingly well
> written
>> in terms of safe operation. I need to copy your canned description of
> what
>> to do for use in some other groups, I think.
>>
>> What I'm not comfortable with doing is promoting responses to the use
> of
>> this tool in this forum, I think. (meaning on my part--not on yours!)
> I'm
>> not clear we have the expertise to handle the volume of requests we'd
> get,
>> and I still feel that ad-aware and spybot handle the majority of
> issues
>> here--but I haven't kept a careful count, and since someone recommends
>> ad-aware for nearly every post here, it's clear there isn't always a
> lot of
>> careful analysis behind that recommendation, nor always feedback about
> the
>> result!
>>
>>
>> "Mike Burgess" <winhelp2002@spamthis.com> wrote in message
>> news:uMG1KBbuDHA.2508@TK2MSFTNGP12.phx.gbl...
>>> Bill,
>>> You are right that HT is a diagnostic tool.
>>> However on the link I provided the OP, it states to run HT, then
> visit
>>> their Forum, for expert assistance.
>>>
>>> When a user selects an option for HT to remove, it unloads any DLLs
>>> and EXEs involved, then deletes the needed values, etc.
>>>
>>> It is an outstanding tool for spotting/removing Trojans,
> spyware\adware,
>>> etc.
>>> <http://www.spywareinfo.com/~merijn/htlogtutorial.html>

> > >
> > > *As Ad-Aware and SpyBot S&D can no longer keep up with the increased*
> > > *amount of (almost daily) threats, HT can be used "with assistance".*
> > >
> > > *Give it a try, as it *only* scans on the first run, HT does NOT*
> *remove*
> > > *anything*
> > > *unless the user selects a option. Note: HT automatically creates a*
> *backup.*
> > >
> > > *Better yet, take a few minutes and read thru the postings at the SWI*
> *Forum*
> > > *or one of the many, many others, you'll be amazed at the amount of*
> > > *infections!*
> > > *<http://forums.spywareinfo.com/> (server down at the moment)*
> > > *<http://forums.tomcoyote.org>*
> > > *<http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi>*
> > > *<http://boards.cexx.org/>*
> > > *<http://www.computercops.biz/forums.html>*
> > >

> > > *Mike Burgess [MVP Windows Shell\User]*
> *<http://www.mvps.org/winhelp2002/>*
> > > *Blocking Spyware, Adware, Parasites, Hijackers, Trojans, with a*
> *HOSTS file*
> > > *<http://www.mvps.org/winhelp2002/hosts.htm> [updated 12-01-03]*
> > > *Please post replies to this Newsgroup, email address is invalid*
> > > --
> > >
> > > *"Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message*
> > > *news:uIDdGgluDHA.3116@tk2msftngp13.phx.gbl...*
> > > > *Hey Mike – I should have tested HijackThis myself--but can you*
> *give a*
> > > > *simple*
> > > > *explanation?*
> > > >
> > > > *I've been assuming that HijackThis is primarily a diagnostic tool.*
> *I'm*
> > > > *getting the feeling from this and similar posts that it is also an*
> > *active*
> > > > *removal tool--what's the story?*
> > > >
> > > > *"Mike Burgess" <winhelp2002@spamthis.com> wrote in message*
> > > > *news:uIGJbaIuDHA.1996@TK2MSFTNGP12.phx.gbl...*
> > > > > *MER-44,*
> > > > > *"Downloader.Stubby.A" is fairly easy to get rid of*
> > > > > *(abetterinternet*
> > > > > *parasite)*
> > > > > *AVG will only identify the culprit .dll*
> > > > >
> > > > > *Dealing with Unwanted Spyware, Parasites, Toolbars and Search*
> *Engines*

microsoft.public.security.virus: Re: Trojan horse Downloader.Stubby.A

>>>> <http://mvps.org/winhelp2002/unwanted.htm>
>>>> *Note: make *sure* to follow-up with HijackThis!*
>>>> _____
>>>> *Mike Burgess [MVP Windows Shell\User]*
>> <http://www.mvps.org/winhelp2002/>
>>>> *Blocking Spyware, Adware, Parasites, Hijackers, Trojans, with a*
> *HOSTS*
>>> *file*
>>>> <http://www.mvps.org/winhelp2002/hosts.htm> *[updated 12-01-03]*
>>>> *Please post replies to this Newsgroup, email address is invalid*
>>>> --
>>>>
>>>> *"MER-44" <anonymous@discussions.microsoft.com> wrote in message*
>>>> *news:060f01c3b882\$2afdef10\$a401280a@phx.gbl...*
>>>> *> I just got a trojan virus and can't get rid of it. The*
>>>> *> norton anti-virus software that I have didn't pick it up*
>>>> *> but a recently downloaded version of AVG Anti-Virus 7.0*
>>>> *> did. I can't figure out how to get rid of it and would*
>>>> *> like some help. The trojan is "Trojan horse*
>>>> *> Downloader.Stubby.A ". Thanks MER-44*
>>>>
>>>>
>>>>
>>>>
>>>
>>>
>>
>>
>>
>