

Re: Bloodhound.exploit.6 Trojan

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-08/1556.html>

From: Lon (*anonymous_at_discussions.microsoft.com*)

Date: 08/28/04

Date: Fri, 27 Aug 2004 18:27:58 -0700

Thanks for all who answered my post and thanks for copying/pasting message that I couldn't read. Yes, this was the first time I tried and hopefully removed a virus myself. Hope it is the last. Took me 3 hours to do because I wanted to make sure I did it right. Since first post I have updated Yahoo anti-spy definitions, downloaded Adware SE (made sure def. were up to date) and I have found Safe Mode. (F8). I ran Yahoo anti-spy, no problems found. I ran Adware SE and it found 9 criticals (7 registry's, 1 malware and 1 tracking). I quarantined them and then waited a day and deleted. I then went into safe mode and ran a full virus scan. Nothing came up. Still in safe mode, ran Adware SE and found 4 neglibible items, quarantined and deleted them. Then rebooted and it went back to normal screen. Hope from what I have done virus is gone. There is just one question that I have. Since I have gone into safe mode and then rebooted a screen comes up on my computer when it gets to desktop saying you have changed the configuration etc...(can't remember all it said). So I went back into safe mode and safe mode was highlited. I then arrowed down until Start Windows Normally was highlited and then hit enter. REbooted again and same screen came up so I just clicked don't show me this message again. Is there something else I need to do? I know that this is not a virus related problem but I ran into it trying to make sure I got rid of one. Any advice or help?

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

>Not bad for your first experience with virus... :-)

>

>I was told that when you disable and unable your system restore and follo

>the steps as you did virus disappear...

>

>

>"Lon" <anonymous@discussions.microsoft.com> escribió en el mensaje

microsoft.public.security.virus: Re: Bloodhound.exploit.6 Trojan

>news:a98001c487ff\$d93c6280\$a401280a@phx.gbl...
>> *I am using Windows XP Pro sp1 with IE6.0 and NSW2003 with
>> NAV and Yahoo Anti-spy and spyblocker. Today my NAV
>> program informed me I had a virus on my computer called
>> Bloodhound.exploit.6 that they could not fix. I found
the
>> site
>>
www.symantec.com/avcenter/venc/data/pf/trojan.trunlow.html
>> for the removal procedures, printed them off and
>> followed the steps given. This is what I did:
>> 1. Disabled System restore
>> 2. Updated my NAV definitions by running live update
>> 3. Ran a full system virus scan to check for
>> Trojan.Trunlow files and found none. (was told if any
>> trojan/trudlow files found to delete and if not to
delete
>> value in registry)
>> 4. Went off line and then backed up the entire registry
>> and placed it on my desktop
>> 5. went to start/run/type regedit and steps told me to
>> search for key
>>
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersi
>> on\Run and on the right side panel to delete the
>> value "Microsoft Eventlog" - "%Windir%\Winupdate.exe"
>>I got to this step but when I went into
>> start/run/type regedit I found the HKEY_LOCAL_MACHINE
>> folder on left side and on the right side the only
thing
>> it said was Default REG_SZ value not set. I didn't
do
>> anything or find anything just
>> 6. Exited registry, rebooted computer, and then enabled
>> system restore.
>> 7. Ran Hijackthis and analyzed log and there were no
red
>> items found and couldn't find anything with Trojan in
it.
>> I also wanted to run full scan again in safe mode
and
>> check regedit again, but I couldn't get my computer to
go
>> into safe mode. Mine says to hit F1 but when I did
there
>> was no selection for safe mode.
>> Questions:
>> a. From what I have said above, can someone tell me if
I
>> no longer have this bloodhound.exploit.6 virus? And*

how

>> *can I tell if it is gone or not? And if it is gone how*

>> *did I get rid of it when I didn't delete anything?*

>> *b. What does it mean when it said in regedit Default*

>> *REG_SZ no value set*

>> *c. How can I get my computer to go into safe mode?*

When I

>> *boot up it says to go to the BIOS click F1 but doesn't*

>> *list safe mode.*

>> *d. Do I need to run full scan again in safe mode (once*

>> *found) and go to regedit again in safe mode?*

>> *Didn't mean this to be so long, but have never tried to*

>> *get rid of a virus before and just wanted someone to*

let

>> *me know if steps I took were correct and if there is*

>> *something else I need to do. I just want to know if it*

is

>> *gone and what I can do to make sure it doesn't come*

>> *back. Any advice or help with this would be greatly*

>> *appreciated.*

>>

>

>

>

>

>