

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

Re: Bloodhound.exploit.6 Trojan

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-08/1573.html>

From: Cris (cris_at_notienecorreo.com)

Date: 08/28/04

Date: Sat, 28 Aug 2004 12:21:15 +0200

Hi Lon:

All my previous posts in this thread are:

08-27-04:

3:25

3:29

3:45

3:47

08-28-04:

4:18

Five posts but no post 08-27-04 at 7:18.

Apart from these posts, yours and Pauly's I can't see any more.

May you be having problems with your news reader program? I'm afraid it's possible. Are you using an updated version of Outlook Express? If your version is not updated you need to update your Windows OS to get your Outlook Express also updated.

Start/All programs/Windows update.

It's very important for everybody to do this regularly because it prevents us from many problems.

You can also compact or restore this group to "refresh" it. There are several ways to do that...

Please confirm you read this post.

"Lon" <anonymous@discussions.microsoft.com> escribió en el mensaje news:1ba301c48cb3\$ccad7190\$a501280a@phx.gbl...

Thanks Chris for getting back to me but again I can't seem to pull up and read your last post for 08-27-04 at 7:18. Don't know what is wrong. Would it be too much trouble to copy and paste again? Would really appreciate it as I am sure the answer to my question is in that

Re: Bloodhound.exploit.6 Trojan

post.

>-----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

>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.*
>>
>
>
>
>