

## Re: Bloodhound.exploit.6 Trojan

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-08/1475.html>

---

**From:** Cris (cris\_at\_notienecorreo.com)

**Date:** 08/27/04

Date: Fri, 27 Aug 2004 03:29:33 +0200

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

I was told that when you disable and unblock your system restore and follow the steps as you did virus disappeared...

"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](http://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.*
- >