

Re: W95.Henky.Gen

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-01/0695.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 01/08/04

Date: Thu, 8 Jan 2004 08:10:33 -0500

Symantec doesn't provide much info on this –

<http://securityresponse.symantec.com/avcenter/venc/dyn/28981.html>

But if it is a version of the Henky.Trojan –

<http://securityresponse.symantec.com/avcenter/venc/dyn/28992.html>

Than it mucks with the hard disk and chances are it may be unrecoverable.

- 1) If you are using WinME or WinXP, disable System Restore
<http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>
- 2) Reboot your PC into Safe Mode
- 3) Using your AV software, perform a Full Scan of your platform and clean/delete any
infectors found
- 4) Restart your PC and perform a "final" Full Scan of your platform
- 5) If you are using WinME or WinXP, re-enable System Restore, reboot the PC
- 6) If you are using WinME or WinXP, create a new Restore point
- 7) Please report back your results

Dave

"Tony" <anonymous@discussions.microsoft.com> wrote in message
news:044b01c3d5e0\$dbbe00c70\$a001280a@phx.gbl...

| I'm running WinXP Pro, NTFS with several users set up. I
| have Norton Internet Security and Anti-Virus installed and
| configured for auto-updates. I was logged on and then
| logged on a second user who needed to use the internet.
| When they logged off and I went back to my desktop there
| was a message from Norton that 'C:\Program
| Files\Messenger\msmsgs.exe' had a virus: 'W95.Henky.Gen'
| and could not be repaired. It would be disabled.
| According to Norton's web site, this virus attacks .EXE
| files. Not a good thing! But they had no further info on
| it. I then attempted a full system scan under windows
| which resulted in a blue screen/mem dump. When I tried to
| boot off the NAV CD I was told it couldn't check
| compressed files. After restarting normally, then
| checking in Explorer my second physical Hard Drive (D:,
| E:, F:) was apparently no longer formatted, I was asked if
| I wanted to format now. Also the C: drive went from being
| nearly fragmentation free to seriously fragmented. I

microsoft.public.security.virus: Re: W95.Henky.Gen

| removed the second drive. I've updated my virus
| definitions and re-run a full system scan. The system is
| apparently virus-free. Where did the virus go? Can I
| recover my data on the second drive?