

## Re: recovering from hack/trojan

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-04/1751.html>

---

**From:** S. Pidgorny (*slavickp\_at\_yahoo.com*)

**Date:** 04/25/04

Date: Sun, 25 Apr 2004 19:00:31 +1000

FAQ:

<http://securityadmin.info/faq.asp#hacked>

You might wish to make an image of the system for forensic purposes but you need to disconnect the system, reformat, reinstall, harden, protect with a firewall and audit your internal network and users before bringing the system back online.

--

Svyatoslav Pidgorny, MVP, MCSE

-- F1 is the key --

"L H" <manklub@hotmail.com> wrote in message  
news:3afa01c42a25\$1ed77610\$a401280a@phx.gbl...

Hi.

For the past 6 months, we have been struggling with a compromised network. There were many indicators that we were being monitored, such as the webcam coming on spontaneously, the audio would stop coming over the speakers, but diagnostics said that it was working. At one point I even got a splash screen that said "YOU ARE BEING WATCHED". Codecs for streaming audio and video appeared that were not removable. (ie: the Uninstall or Remove button was disabled.) The firewalls were having rules installed, and hidden remote access adapters and protocols would appear in command-line utilities such as netsh and netstat but were not removable. Group policies keep getting applied to our computers, which start out benign, but eventually lock us out of our computers entirely. By the time we start being denied access to our own network and internet connections, we also lose property sheets to many files, objects and folders. Other indicators or symptoms are that the contents of installation CDs change, and the hard drives never show more than 2 Gigabytes of used space. Evidently, the drives get redirected to virtual drives. The Distributed Transaction Tracking, Remote Registry, COM+, WBEM and DCOM services, among others, get reenabled shortly after we disable them. If (and we have been doing this at least 2 times a week per machine for 6 months) we reformat and reinstall (flashing the bios as a precaution), and use new Workgroup names, the old workgroup name comes back, eventually. Firewalls get changes or disabled, virus scanners don't detect anything and run way too quickly, in my opinion.

Re: recovering from hack/trojan

## microsoft.public.security: Re: recovering from hack/trojan

The following program groups show up almost every time, soon after an install: (I will try to build a tree) Keep in mind, we DO NOT INSTALL IIS! There is also older versions of Windows Media (4.2, i think), IE5 and 4 and FrontPage installed.

Folder PATH listing

-C:\Program Files

---Common Files

```
3   ---InstallShield
3     3   ---Engine
3     3     3   ÅÅÅÅ6
3     3     3     ---Intel 32
3     3   ---IScript
3   ---Microsoft Shared
3     3   ---DAO
3     3   ---Microsoft Plus!
3     3     3   ---1033
3     3     3   ---LaunchAppContent
3     3     3     ---1033
3     3   ---MSInfo
3     3   ---Speech
3     3     3   ---1033
3     3   ---Stationery
3     3   ---TextConv
3     3   ---Triedit
3     3   ---VGX
3     3   ---Web Folders
3     3   ---web server extensions
3     3     ---40
3     3     ---admcgi
3     3     3   ---scripts
3     3     ---admisapi
3     3     3   ---scripts
3     3     ---bin
3     3     3   ---1033
3     3     ---bots
3     3     3   ---vinavbar
3     3     ---isapi
3     3     3   ---_vti_adm
3     3     3   ---_vti_aut
3     3     ---servsupp
3     3     ---_vti_bin
3     3     ---_vti_adm
3     3     ---_vti_aut
3   ---MSSoap
3     3   ---Binaries
3     3     ---Resources
3     3     ---1033
3   ---ODBC
3     3   ---Data Sources
3   ---Services
3   ---SpeechEngines
3     3   ---Microsoft
3     3     ---Lexicon
3     3     3   ---1033
3     3     ---SR
3     3     3   ---1033
3     3     ---TTS
3     3     ---1033
3   ---System
3     ---ado
3     ---msadc
```

## microsoft.public.security: Re: recovering from hack/trojan

```
3      ---Ole DB
---ComPlus Applications
---Internet Explorer
3      ---Connection Wizard
3      ---PLUGINS
3      ---SIGNUP
3      ---Yahoo
---Messenger
---microsoft frontpage
3      ---version3.0
3      ---bin
---MSN Gaming Zone
3      ---Windows
---NetMeeting
---Online Services
---Outlook Express
---Windows Media Player
3      ---Skins
3      ---Visualizations
---Windows NT
3      ---Accessories
3      ---Pinball
---xerox
3      ---nwwia
```

There are many other things going on, such as IPX netbui, etc... file systems have changed from NTFS to FAT32, FAT12 and FAT16. Wowexec shows up running in taskmanager and filenames go from lower to upper case. Microsoft help desk personnel told us that all of this was impossible, yet for some reason Microsoft has now released service packs that address these issues, and others that I have not enumerated here. the service packs however do not appear to get the backdoors or trojans or hackers or whatever out of our compromised machines. Reformatting and reinstalling and changing hardware including mobos, cpus, etc. seems to do no good, nor does staying off the internet. we get something called "Microsoft Raw Channel Protocol" installed and bound to network adapters with a characterisitic of "NCF\_hidden". we have dlls and inf files that have suspicious misspellings and terminology in them, and deleting and/or disabling and/or uninstalling the suspicious items casue "session manager" blue screens or the system file monitor restores them.

I have lots more but this will sum it up -- HELP!