Spyware, Adware and Keyloggers

Spotting and Eradicating Crappy Traffic

Laura Chappell
Protocol Analysis Institute, LLC
Author, "Laura Chappell's Master Library"
www.packet-level.com

Novell

The Terminology of Trash

Adware	Intrusive
Trackers	Privacy concern – cookies with GUID
Spyware	Secretly transmits personal information
Malware	Malicious Code
Scumware	Planting kiddie porn, etc.
Keyloggers	Key capture

How many systems are infected?

Novell

Examining Spyware Infection (LLK6)

Stopguard – evilprogram.dmp (covered in BYOL Session)
Trojan downloader (vsb) – clientdying.dmp (see LLK6)

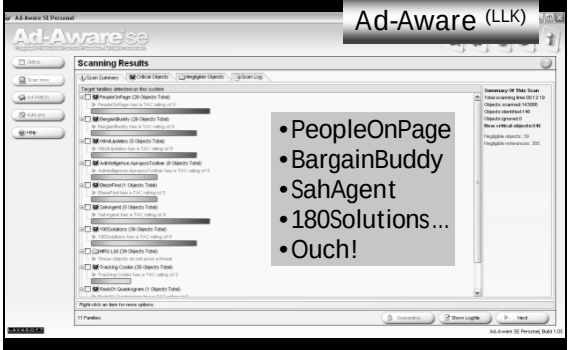
Novell

Spyware/Adware Removal

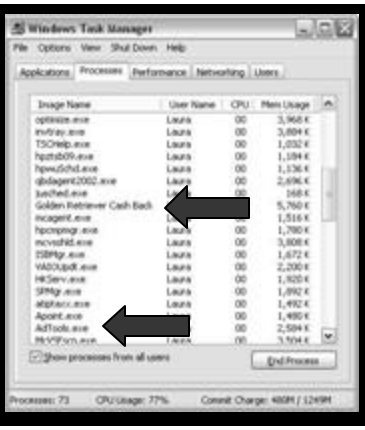
1. Run at least one of these free anti-spyware scanners; remove spyware/adware found
   - **Ad-aware Personal Edition (LLK6)**
   - **Spybot Search & Destroy**
2. Run your virus scanning program
3. Register at www.SpywareWarrior.com (free)
4. Run HijackThis (available online at www.spywarewarrior.com/files/hijackthis.exe and on the LLK6)

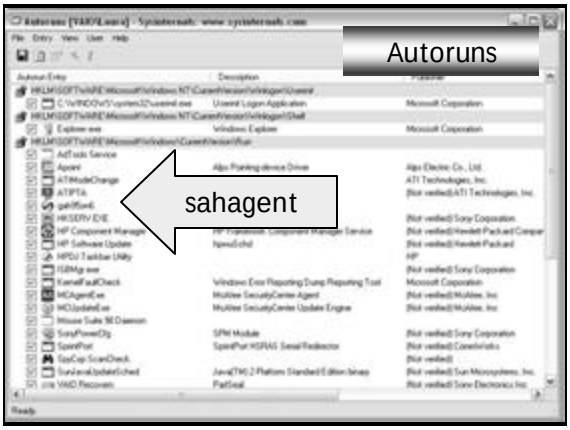
Novell

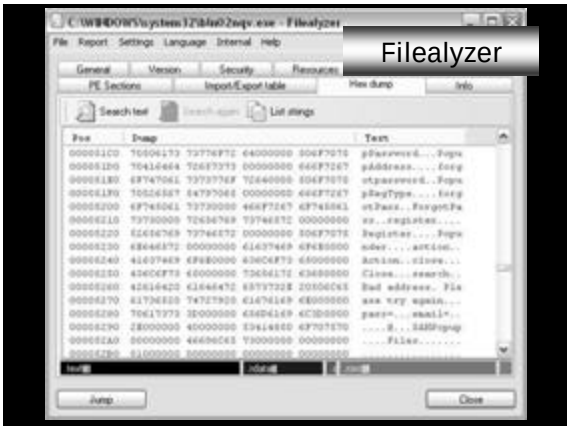
Ad-Aware (LLK)

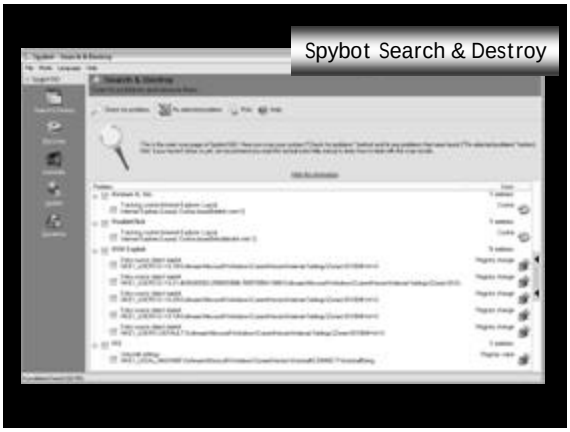


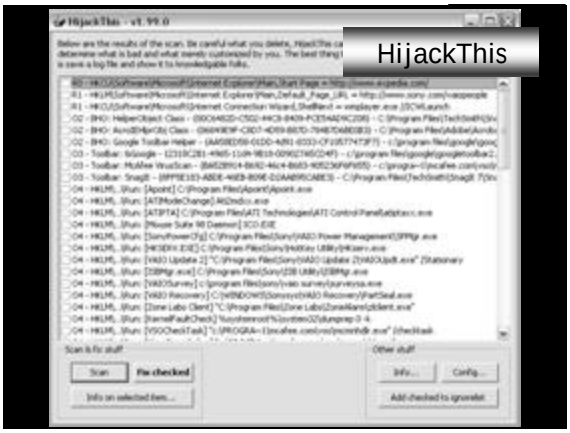
- PeopleOnPage
- BargainBuddy
- SahAgent
- 180Solutions…
- Ouch!











HijackThis Descriptions

R - Registry, StartPage/SearchPage changes
- **R0 - Changed registry value**
- **R1 - Created registry value**
- **R2 - Created registry key**
- **R3 - Created extra registry value where only one should be**

F - IniFiles, autoloading entries
- **F0 - Changed inifile value**
- **F1 - Created inifile value**
- **F2 - Changed inifile value, mapped to Registry**
- **F3 - Created inifile value, mapped to Registry**

N - Netscape/Mozilla StartPage/SearchPagechanges
- **N1 - Change in prefs.js of Netscape 4.x**
- **N2 - Change in prefs.js of Netscape 6**
- **N3 - Change in prefs.js of Netscape 7**
- **N4 - Change in prefs.js of Mozilla**

Novell

O - Other, several sections which represent:
- **O1 - Hijack of auto.search.msn.com with Hosts file**
- **O2 - Enumeration of existing MSIE BHO's**
- **O3 - Enumeration of existing MSIE toolbars**
- **O4 - Enumeration of suspicious autoloading Registry entries**
- **O5 - Blocking of loading Internet Options in Control Panel**
- **O6 - Disabling of 'Internet Options' Main tab with Policies**
- **O7 - Disabling of Regedit with Policies**
- **O8 - Extra MSIE context menu items**
- **O9 - Extra 'Tools' menuitems and buttons**
- **O10 - Breaking of Internet access by New.Net or WebHancer**
- **O11 - Extra options in MSIE 'Advanced' settings tab**
- **O12 - MSIE plugins for file extensions or MIME types**
- **O13 - Hijack of default URL prefixes**
- **O14 - Changing of IERESET.INF**
- **O15 - Trusted Zone Autoadd**
- **O16 - Download Program Files item**
- **O17 - Domain hijack**
- **O18 - Enumeration of existing protocols and filters**
- **O19 - User stylesheet hijack**
- **O20 - AppInit_DLLs autorun Registry value**
- **O21 - ShellServiceObjectDelayLoad (SSODL) autorun Registry key**
- **O22 - SharedTaskScheduler autorun Registry key**
- **O23 - Enumeration of NT Services**

HijackThis Steps

Post your HijackThis log

Be patient!

Follow removal instructions precisely

Protect your system from re-infection

Novell

```
Logfile of HijackThis v1.97.7
Scan saved at 11:53:26 AM, on 31/01/2005
Platform: Windows XP (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP1 (6.00.2600.0000)

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\System32\GEARSEC.EXE
C:\Program Files\Trend Micro\PC-cillin 2003\Tmntsrv.exe
C:\Program Files\Trend Micro\PC-cillin 2003\tmproxy.exe
C:\Program Files\Trend Micro\PC-cillin 2003\pccguide.exe
C:\Program Files\Trend Micro\PC-cillin 2003\PccPfw.exe
C:\Program Files\Trend Micro\PC-cillin 2003\PCCClient.exe
C:\Program Files\Trend Micro\PC-cillin 2003\Pop3trap.exe
C:\Program Files\MUSICMATCH\MUSICMATCH Jukebox\mm_tray.exe
```


Novell

```
C:\Program Files\QuickTime\qttask.exe
C:\Program Files\iTunes\iTunesHelper.exe
C:\Program Files\Common Files\Microsoft Shared\Work
Shared\WkUFind.exe
C:\Program Files\Ahead\InCD\InCD.exe
C:\Program Files\Java\j2re1.4.2_05\bin\jusched.exe
C:\WINDOWS\System32\tcmrxy.exe
C:\Program Files\AutoUpdate\AutoUpdate.exe
C:\WINDOWS\System32\ctfmon.exe
C:\Program Files\iPod\ bin\iPodService.exe
C:\WINDOWS\explorer.exe
C:\WINDOWS\system32\NOTEPAD.EXE
C:\WINDOWS\System32\wuauclt.exe
C:\Program Files\Internet Explorer\IEXPLORE.EXE
C:\Documents and Settings\Fred\My Documents\My Received
Files\hijackthis.exe
C:\Documents and Settings\Fred\My Documents\My Received
Files\hijackthis.exe
```

```
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
http://search.search-exe.com/nph-
search.cgi?tcode=exebar1&look=sbar1_srchbtn
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://search.search-exe.com/nph-
search.cgi?tcode=exesrch1&look=stmpl1&fw=
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
http://www.yahoo.com.au/
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://search.search-exe.com/nph-
search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar =
http://search.search-exe.com/nph-
search.cgi?tcode=exebar1&look=sbar1_srchbtn
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
http://search.search-exe.com/nph-
search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://search.search-exe.com/nph-
search.cgi?tcode=exesrch1&look=stmpl1&fw=
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://search.search-exe.com/nph-
search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
http://search.search-exe.com/nph-
search.cgi?tcode=exesrch1&look=stmpl1&fw=
R3 - URLSearchHook: WebSearch Class - {9368D063-44BE-49B9-BD14-
BB9663FD38FC} - C:\Program Files\se\v11\se.DLL
```

```
O1 - Hosts: 69.20.16.183 auto.search.msn.com
O1 - Hosts: 69.20.16.183 search.netscape.com
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O2 - BHO: (no name) - {00041A26-7033-432C-94C7-6371DE343822} -
C:\Program Files\se\v11\se.DLL
O3 - Toolbar: &Radio - {8E718888-423F-11D2-876E-00A0C9082467} -
C:\WINDOWS\System32\msdxm.ocx
O3 - Toolbar: Yahoo! Companion - {EF99BD32-C1FB-11D2-892F-
0090271D4F88} - C:\Program
Files\Yahoo!\Companion\Installs\cpn\ycomp5_5_7_0.dll
```


Novell

```
O4 - HKLM\..\Run: [pccguide.exe] "C:\Program Files\Trend Micro\PC-cillin
2003\pccguide.exe"
O4 - HKLM\..\Run: [PCCClient.exe] "C:\Program Files\Trend Micro\PC-cillin
2003\PCCClient.exe"
O4 - HKLM\..\Run: [Pop3trap.exe] "C:\Program Files\Trend Micro\PC-cillin
2003\Pop3trap.exe"
O4 - HKLM\..\Run: [MMTray] C:\Program Files\MUSICMATCH\MUSICMATCH
Jukebox\mm_tray.exe
O4 - HKLM\..\Run: [QuickTime Task] "C:\Program Files\QuickTime\qttask.exe" -
atboottime
O4 - HKLM\..\Run: [iTunesHelper] C:\Program Files\iTunes\iTunesHelper.exe
O4 - HKLM\..\Run: [WorksFUD] C:\Program Files\Microsoft Works\wkfud.exe
O4 - HKLM\..\Run: [Microsoft Works Portfolio] C:\Program Files\Microsoft
Works\WksSb.exe /AllUsers
O4 - HKLM\..\Run: [Microsoft Works Update Detection] C:\Program
Files\Common Files\Microsoft Shared\Works Shared\WkUFind.exe
O4 - HKLM\..\Run: [NeroCheck] C:\WINDOWS\system32\NeroCheck.exe
O4 - HKLM\..\Run: [InCD] C:\Program Files\Ahead\InCD\InCD.exe
O4 - HKLM\..\Run: [SunJavaUpdateSched] C:\Program
Files\Java\j2re1.4.2_05\bin\jusched.exe
O4 - HKLM\..\Run: [Search-Exe] "C:\Program Files\se\v11\se.EXE" /H
O4 - HKLM\..\Run: [3FrT3ng] tcmrxy.exe
O4 - HKLM\..\Run: [AutoUpdater] "C:\Program
Files\AutoUpdate\AutoUpdate.exe"
O4 - HKCU\..\Run: [CTFMON.EXE] C:\WINDOWS\System32\ctfmon.exe
```


Novell

O4 - HKCU\..\Run: [msnmsgr] "C:\Program Files\MSN Messenger\MsnMsgr.Exe" /background
O4 - HKCU\..\Run: [lo03RhMmR] ssdui.exe
O4 - Global Startup: Microsoft Office.lnk = C:\Program Files\Microsoft Office\Office\OSA9.EXE
O4 - Global Startup: Microsoft Works Calendar Reminders.lnk = ?
O9 - Extra 'Tools' menuitem: Sun Java Console (HKLM)
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Windows Messenger (HKLM)
O16 - DPF: {166B1BCA-3F9C-11CF-8075-444553540000} (Shockwave ActiveX Control) - http://download.macromedia.com/pub/shockwave/cabs/director/sw.cab
O16 - DPF: {4C39376E-FA9D-4349-BACC-D305C1750EF3} (EPUImageControl Class) - http://tools.ebayimg.com/eps/wl/activex/EPUWALControl_v1-0-3-17.cab
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab
O17 - HKLM\System\CCS\Services\Tcpip\..\{C6E89460-C870-48E8-9D29-1DFAD1416581}: NameServer = 203.134.64.66 203.134.65.66

Sample HijackThis Response

Place a checkmark next to these entries, close **all** browsers and windows, and have HijackThis fix them by clicking Fix Checked:

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://search.search-exe.com/nph-search.cgi?tcode=exebar1&look=sbar1_srchbtn
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://search.search-exe.com/nph-search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant = http://search.search-exe.com/nph-search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar = http://search.search-exe.com/nph-search.cgi?tcode=exebar1&look=sbar1_srchbtn
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://search.search-exe.com/nph-search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://search.search-exe.com/nph-search.cgi?tcode=exesrch1&look=stmpl1&fw=
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = http://search.search-exe.com/nph-search.cgi?tcode=exesrch1&look=stmpl1&fw=
R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) = http://search.search-exe.com/nph-search.cgi?tcode=exesrch1&look=stmpl1&fw=
R3 - URLSearchHook: WebSearch Class - {9368D063-44BE-49B9-BD14-BB9663FD38FC} - C:\Program Files\se\v11\se.DLL

Sample HijackThis Response (Cont.)

O1 - Hosts: 69.20.16.183 auto.search.msn.com
O1 - Hosts: 69.20.16.183 search.netscape.com
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O1 - Hosts: 69.20.16.183 ieautosearch
O2 - BHO: (no name) - {00041A26-7033-432C-94C7-6371DE343822} - C:\Program Files\se\v11\se.DLL
O4 - HKLM\..\Run: [Search-Exe] "C:\Program Files\se\v11\se.EXE" /H
O4 - HKLM\..\Run: [3FrT3ng] tcmrxy.exe
O4 - HKLM\..\Run: [AutoUpdater] "C:\Program Files\AutoUpdate\AutoUpdate.exe"
O4 - HKCU\..\Run: [lo03RhMmR] ssdui.exe

Sample HijackThis Response (Cont.)

Reconfigure Windows XP to show hidden files:

Click Start. Open My Computer.

Select the Tools menu and click Folder Options. Select the View Tab.

Under the Hidden files and folders heading select "**Show hidden files and folders**".

Uncheck the "**Hide protected operating system files (recommended)**" option.

Uncheck the "**Hide file extensions for known file types**" option.
Click Yes to confirm. Click OK.

Boot into Safe Mode:
Restart your computer and immediately begin tapping the F8 key on your keyboard. If done right a Windows Advanced Options menu will appear. Select the Safe Mode option and press Enter.
To return to normal mode just restart your computer as you normally would.

Sample HijackThis Response (Cont.)

Please delete these **folders** using Windows Explorer (if present):

C:\Program Files\AutoUpdate
C:\Program Files\se

We need to do a search. Start | Search | For Files and Folders.
Expand Search Options, check Advanced Options, check Search system folders, Search hidden files and folders, and Search Subfolders.
Paste this into the Search for files and folders named box:

"ssdui.exe","tcmrxy.exe"

If any of them are found delete them.

Now you can restart the computer normally.

Please run HijackThis again and post a fresh log, just so I can make sure that all the malware was deleted according to plan.

Adware/Spyware Prevention

1. Educate users
2. Install quality spyware/adware scanning software (see Eric Howes' comparisons at www.spywarewarrior.com) – note that no single program does it all right now – check out **Spybot Search & Destroy** and **Ad-aware** and **Pest Patrol**
3. Install quality anti-spyware protection (i.e., **Spyware Blaster** and **Spyware Guard** from JavaCool)

Adware/Spyware Prevention

4. Lock down Internet Explorer (Internet Zone, Privacy/Security Settings) or look into **Enough is Enough** (https://netfiles.uiuc.edu/ehowes/www/resource6.htm)
5. For IE, put bad sites on a restricted zone or check out **IE-SPYAD**
6. Consider another browser – such as Firefox or Opera
7. Consider outbound filtering/blocking (such as ZoneAlarm)

Novell

Adware/Spyware Prevention

8. Keep Windows updated
9. Read licenses and privacy policies – painful!
10. Check out **www.cleansoftware.org**
11. Get to know the Spyware Warrior folks well!

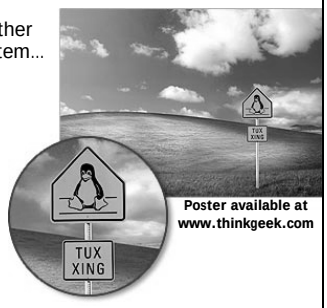
and finally…

Novell

Adware/Spyware Prevention

11. Consider another operating system…

like **Linux**!



Poster available at www.thinkgeek.com