Spyware Scan Details

Start Date: 9/5/2005 7:50:24 PM
End Date: 9/5/2005 7:53:46 PM
Total Time: 3 mins 22 secs

Detected Threats

ShopAtHome Spyware more information...

Details: ShopAtHome is a browser redirector that monitors your browsing behavior and online purchases.
Status: Ignored
Severe threat - Severe-risk items have an extreme potential for harm, such as a security exploit, and should be removed.

Infected registry keys/values detected

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run SAHBundle
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent BundleKey cdt1006.sah
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent BundlePackage setup4030.cab
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent PrefsServer www.shopathomeselect.com
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent PrefsPath agent2/
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent iniName setup4030.ini
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent PackageLocation downloads.shopathomeselect.com
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent PackageName agent/setup4030.cab
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent PrefsXML agent2/agentprefs2.sah
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent CookieUserAgent iexplorer
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent BrowserType Bundle
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent BundleProgress 0
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent CountKey 10
HKEY_LOCAL_MACHINE\software\vgroup
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent KeyExistNai Y
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent DllName C:\DOCUME~1\PAM~1.SOL\LOCALS~1\Temp\QEQAH3B8.dll
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent HtmlName C:\DOCUME~1\PAM~1.SOL\LOCALS~1\Temp\QSK2B3HO.html
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent EulaDate 2005-09-05 13:03:02
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent EulaStatus Displayed4002b
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent InstallLocation downloads.shopathomeselect.com
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent InstPath cdt/
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent KeyExistNai Y
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent BundleKey cdt1006.sah
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent BundlePackage setup4030.cab
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent PrefsServer www.shopathomeselect.com
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent PrefsPath agent2/
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent iniName setup4030.ini
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent PackageLocation downloads.shopathomeselect.com
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent PackageName agent/setup4030.cab
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent PrefsXML agent2/agentprefs2.sah
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent CookieUserAgent iexplorer
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent BrowserType Bundle
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent DllName C:\DOCUME~1\PAM~1.SOL\LOCALS~1\Temp\QEQAH3B8.dll
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent BundleProgress 0
HKEY_LOCAL_MACHINE\software\vgroup\SAHAgent CountKey 10
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent HtmlName C:\DOCUME~1\PAM~1.SOL\LOCALS~1\Temp\QSK2B3HO.html
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent EulaDate 2005-09-05 13:03:02
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent EulaStatus Displayed4002b
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent InstallLocation downloads.shopathomeselect.com
HKEY_LOCAL_MACHINE\SOFTWARE\VGroup\SAHAgent InstPath cdt/

MediaTickets CDT Spyware more information...

Details: Mediatickets is a spyware program that displays advertisements, reduces the security settings for the Trusted Sites zone in Internet Explorer, and attempts to fraudulently install trusted publishers.
Status: Ignored
Severe threat - Severe-risk items have an extreme potential for harm, such as a security exploit, and should be removed.

Infected files detected

C:\Documents and Settings\Pam.solutions\Local Settings\Temp\bundle_cdt1006.exe
C:\TEMP\bundle_cdt1006.exe

AvenueMedia.DyFuCA Browser Plug-in more information...

Details: AvenueMedia DyFuCA Internet Optimizer is adware that changes your browser error page. It periodically displays pop-up

advertisements from its remote sites and may update itself.
Status: Ignored
Severe threat - Severe-risk items have an extreme potential for harm, such as a security exploit, and should be removed.

Infected files detected
C:\RECYCLER\S-1-5-21-1922275950-1779413670-3725303808-1142\Dc359\optimize.exe
C:\TEMP\optimize.exe

180Solutions.SearchAssistant Adware more information...
Details: 180Solutions.SearchAssistant is adware that displays pop-up advertisements based on your browsing activity.
Status: Ignored
High threat - High-risk items have a large potential for harm, such as loss of computer control, and should be removed unless knowingly installed.

Infected files detected
C:\TEMP\180SAInstaller.exe

WindUpdates.MediaAccess Adware more information...
Details: WindUpdates is responsible for downloading adware.
Status: Ignored
High threat - High-risk items have a large potential for harm, such as loss of computer control, and should be removed unless knowingly installed.

Infected registry keys/values detected
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C}
HKEY_LOCAL_MACHINE\Software\Media Gateway param
7f08882a03b546111dab3967a015c9645cb0e0ca517cec9ccd551083ddd075faa1badb62f9d230a37bcc:3361363962663139346335613461
HKEY_LOCAL_MACHINE\Software\Media Gateway LastUpdate 1125939775
HKEY_LOCAL_MACHINE\Software\Media Gateway reqcount 42
HKEY_LOCAL_MACHINE\Software\Media Gateway track 0
HKEY_LOCAL_MACHINE\Software\Media Gateway DownloadPath \temp
HKEY_LOCAL_MACHINE\Software\Media Gateway Language en
HKEY_LOCAL_MACHINE\Software\Media Gateway
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
\Contains\Files C:\WINDOWS\Downloaded Program Files\MediaGatewayX.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
\DownloadInformation CODEBASE http://static.windupdates.com/cab/MediaAccessVerisign/ie/bridge-c18.cab
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C}\LocalServer32 C:\PROGRA~1\MEDIAG~1\MEDIAG~1.EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
\InstalledVersion 0,0,0,1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
\InstalledVersion LastModified Tue, 02 Aug 2005 18:23:17 GMT
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
SystemComponent 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
Installer MSICD
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C}\ProgID MediaGateway.Installer
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C}\TypeLib {15696AE2-6EA4-47F4-BEA6-A3D32693EFC7}
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C}\VersionIndependentProgID MediaGateway.Installer
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C} Installer Class
HKEY_CLASSES_ROOT\clsid\{1E5F0D38-214B-4085-AD2A-D2290E6A2D2C} AppID {735C5A0C-F79F-47A1-8CA1-2A2E482662A8}
HKEY_LOCAL_MACHINE\Software\Media Gateway
HKEY_LOCAL_MACHINE\Software\Media Gateway zuk 0

WindUpdates.MediaGateway Adware more information...
Details: WindUpdates is responsible for downloading adware.
Status: Ignored
High threat - High-risk items have a large potential for harm, such as loss of computer control, and should be removed unless knowingly installed.

Infected files detected
C:\Program Files\Media Gateway\MediaGateway.exe
c:\windows\downloaded program files\mediagatewayx.dll
c:\program files\media gateway\info.txt

Infected folders detected
c:\program files\media gateway

Infected registry keys/values detected
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Media Gateway
HKEY_CLASSES_ROOT\MediaGatewayX.Installer
HKEY_CLASSES_ROOT\MediaGatewayX.Installer\CLSID {15AD6789-CDB4-47E1-A9DA-992EE8E6BAD6}
HKEY_CLASSES_ROOT\MediaGatewayX.Installer MediaGatewayX.Installer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Media Gateway
HKEY_LOCAL_MACHINE\Software\microsoft\windows\currentversion\uninstall\Media Gateway
HKEY_LOCAL_MACHINE\Software\microsoft\windows\currentversion\uninstall\Media Gateway UninstallString C:\Program Files\Media Gateway\MediaGateway.exe /Remove
HKEY_LOCAL_MACHINE\Software\microsoft\windows\currentversion\uninstall\Media Gateway DisplayName Media Gateway
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Media Gateway
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Media Gateway
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Media Gateway
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Media Gateway
HKEY_CLASSES_ROOT\MediaGateway.Installer
HKEY_CLASSES_ROOT\MediaGateway.Installer\CLSID {1E5F0D38-214B-4085-AD2A-D2290E6A2D2C}
HKEY_CLASSES_ROOT\MediaGateway.Installer\CurVer MediaGateway.Installer
HKEY_CLASSES_ROOT\MediaGateway.Installer Installer Class

IBIS Toolbar Adware more information...

Details: IBIS Toolbar is an Internet Explorer search redirector.
Status: Ignored
High threat - High-risk items have a large potential for harm, such as loss of computer control, and should be removed unless knowingly installed.

Infected files detected
C:\TEMP\myEDowST3.exe

Detected Spyware Cookies

No spyware cookies were found during this scan.