Symantec Security Response
http://www.symantec.com/security_response/index.jsp

Adware.ClearSearch

Updated: February 13, 2007 11:34:10 AM
Type: Adware
Publisher: www.clrsch.com
Risk Impact: High
File Names: Loader.exe Delete me.exe CSP001.exe csLDRupdater.DLL csAOLinst.DLL CSIE.dll CSIEINST.dll CS
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

SUMMARY

Behavior

Adware.ClearSearch is an adware component that periodically contacts a Web site on the clrsch.com domain, for advertisement tracking purposes.

Symptoms

The files are detected as Adware.ClearSearch.

Transmission

This adware component must be manually installed, or may be installed as a component of another program.

Protection

Initial Rapid Release version September 23, 2003
Latest Rapid Release version January 2, 2009 revision 035
Initial Daily Certified version September 23, 2003
Latest Daily Certified version December 30, 2008 revision 004
Initial Weekly Certified release date September 24, 2003

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

TECHNICAL DETAILS

When Adware.ClearSearch is executed, it performs the following actions:
Creates the following folders:

%Temp%\ClrSch
%ProgramFiles%\ClearSearch
%ProgramFiles%\[RANDOM NAME]
%UserProfile%\Local Settings\Temp\clrsch

Notes:
%ProgramFiles% is a variable that refers to the program files folder. By default, this is C:\Program Files.
%Temp% is a variable that refers to the Windows temporary folder. By default, this is C:\Windows\TEMP (Windows 95/98/Me/XP) or C:\WINNT\Temp (Windows NT/2000).
%UserProfile% is a variable that refers to the current user's profile folder. By default, this is C:\Documents and Settings\[CURRENT USER] (Windows NT/2000/XP).

Adds the values:

```
"ClrSchLoader" = "[PATH TO THE ORIGINAL EXECUTABLE]"
"CSV10P1" =  "%ProgramFiles%\CSBB\CSP001.exe"
"CSV10P070" =  "%ProgramFiles%\CSBB\CSv10P070.exe"
"[RANDOM NAME]" = "%ProgramFiles%\[RANDOM NAME]\[RANDOM NAME].exe"
"5whgue21" = "%ProgramFiles%\5whgue21\5whgue21.exe"
```

to the registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Adds the following registry subkeys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ClrSch
HKEY_LOCAL_MACHINE\SOFTWARE\CSBB
HKEY_LOCAL_MACHINE\SOFTWARE\[ORIGINAL EXECUTABLE FOLDER NAME]
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00000000-0000-0000-0000-000000000221}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{0F2A4ADC-DABF-4980-8DB4-19F67D7B1F95}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{60494593-5408-447D-BD5E-A16640D6AF99}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CSIE.CSIECore
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CSIE.CSIECore.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{00000000-0000-0000-0000-000000000221}
HKEY_CLASSES_ROOT\CLSID\[RANDOM VALUE]
HKEY_LOCAL_MACHINE\SOFTWARE\[RANDOM VALUE]
```

Periodically updates itself by downloading control data from a Web site on the clrsch.com domain.

Contacts a Web site on the clrsch.com domain to track advertisements.

REMOVAL

Removal using the Adware.ClearSearch Removal Tool
Symantec Security Response has developed a removal tool for Adware.ClearSearch. Use this removal tool first, as it is the easiest way to remove this threat.

The current version of the tool will have a digital signature timestamp equivalent to **17/12/2004 03:28 PST**

Notes:

The date and time displayed will be adjusted to your time zone, if your computer is not set to the Pacific time zone.
Running the Adware.ClearSearch Removal Tool may cause other programs to function incorrectly, particularly those programs with which Adware.ClearSearch was installed. The uninstaller generally identifies the programs that will not work after uninstallation.

It has been reported that a computer on which Adware.ClearSearch is installed may also have other security risks. Symantec recommends that the following steps be carried out:
Apply the Adware.ClearSearch Tool.
Update the definitions by starting the Symantec program and running LiveUpdate.
Run a full system scan to detect any other security risks on the computer.
If the scan detects any further security risks, check for removal tools at http://securityresponse.symantec.com/avcenter/security.risks.tools.list.html.
If there are no removal tools for the security risks that are detected, follow the manual removal instructions listed in the threat report.

Manual Removal Instructions
The following instructions pertain to all Symantec antivirus products that support security risk detection.
Update the definitions.
Run a full system scan.
Delete any values added to the registry.
For specific details on each of these steps, read the following instructions.

1. To update the definitions
To obtain the most recent definitions, start your Symantec program and run LiveUpdate.

2. To run the scan
Start your Symantec antivirus program, and then run a full system scan.
If any files are detected, and depending on which software version you are using, you may see one or more of the following options:

Note: This applies only to versions of Norton AntiVirus that support security risk detection. If you are running a version of Symantec AntiVirus Corporate Edition that supports security risk detection, and security risk detection has been enabled, you will only see a message box that gives the results of the scan. If you have questions in this situation, contact your network administrator.
Exclude (Not recommended): If you click this button, it will set the risk so that it is no longer detectable. That is, the antivirus program will keep the security risk on your computer and will no longer detect it to remove from your computer.

Ignore or Skip: This option tells the scanner to ignore the risk for this scan only. It will be detected again the next time that you run a scan.

Cancel: This option is new to Norton Antivirus 2005. It is used when Norton Antivirus 2005 has determined that it cannot delete a security risk. This Cancel option tells the scanner to ignore the risk for this scan only, and thus, the risk will be detected again the next time that you run a scan.

To actually delete the security risk:
Click its file name (under the Filename column).
In the Item Information box that displays, write down the full path and file name.
Then use Windows Explorer to locate and delete the file.

If Windows reports that it cannot delete the file, this indicates that the file is in use. In this situation, complete the rest of the instructions on this page, restart the computer in Safe mode, and then delete the file using Windows Explorer. Restart the computer in Normal mode.

Delete: This option will attempt to delete the detected files. In some cases, the scanner will not be able to do this.
If you see a message, "Delete Failed" (or similar message), manually delete the file.
Click the file name of the risk that is under the Filename column.
In the Item Information box that displays, write down the full path and file name.
Then use Windows Explorer to locate and delete the file.

If Windows reports that it cannot delete the file, this indicates that the file is in use. In this situation, complete the rest of the instructions on this page, restart the computer in Safe mode, and then delete the file using Windows Explorer. Restart the computer in Normal mode.
Important: If your Symantec antivirus product reports that it cannot delete a detected file, Windows may be using the file. To fix this, run the scan in Safe mode. For instructions, read the document: How to start the computer in Safe Mode. Once you have restarted in Safe mode, run the scan again.

After the files are deleted, restart the computer in Normal mode and proceed with the next section.

Warning messages may be displayed when the computer is restarted, since the risk may not be fully removed at this point. You can ignore these messages and click OK. These messages will not appear when the computer is restarted after the removal instructions have been fully completed. The messages displayed may be similar to the following:

Title: `[File path]`
Message body: `Windows cannot find [file name]. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.`

3. To delete the value from the registry
Important: Symantec strongly recommends that you back up the registry before making any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify the specified subkeys only. Read the document: How to make a backup of the Windows registry.
Click **Start > Run**.
Type **`regedit`**

Then click **OK**.

Note: If the registry editor fails to open the risk may have modified the registry to prevent access to the registry editor. Security Response has developed a tool to resolve this problem. Download and run this tool, and then continue with the removal.

Navigate to the subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

In the right pane, delete the values:

```
"ClrSchLoader" = "[original executable path]"
"CSV10P1" =  "%ProgramFiles%\CSBB\CSP001.exe"
"5whgue21" = "%ProgramFiles%\5whgue21\5whgue21.exe"
"CSV10P070" =  "%ProgramFiles%\CSBB\CSv10P070.exe"
"[RANDOM NAME]" = "%ProgramFiles%\[RANDOM NAME]\[RANDOM NAME].exe"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\ClrSch
HKEY_LOCAL_MACHINE\SOFTWARE\CSBB
HKEY_LOCAL_MACHINE\SOFTWARE\[ORIGINAL EXECUTABLE FOLDER NAME]
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00000000-0000-0000-0000-000000000221}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{0F2A4ADC-DABF-4980-8DB4-19F67D7B1F95}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{60494593-5408-447D-BD5E-A16640D6AF99}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CSIE.CSIECore
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CSIE.CSIECore.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{00000000-0000-0000-0000-000000000221}
HKEY_CLASSES_ROOT\CLSID\[RANDOM VALUE]
HKEY_LOCAL_MACHINE\SOFTWARE\[RANDOM VALUE]
```

Exit the Registry Editor.