Miscellaneous: LNK Shortcuts

Problem Reported:
"Shortcut links" folder-like icon gets created which redirects to execute a hidden .scr, .exe files created by the virus itself on that particular drive and the Genuine files\folder gets hidden automatically".

For example, if you have a folder named "TEST" , then the virus will hide the folder and its sub-folder (if any) with SH attribute and creates shortcut folders with same name. User thinks that their folder are changed to shortcuts and cannot access any data. And if you check the properties of that shortcut folder, the Target path will be .scr, .exe file.

Solution:

Please be informed that this may happen due to a Vulnerability on the unpatched Operating System. Microsoft has released the hotfix (KB2286198) which will fix the vulnerability.

Please implement the hotfix on the affected Operating Systems specified on the link mentioned below.

"MS10-046: Vulnerability in Windows Shell could allow remote code execution"

http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx

Do note that having eScan installed and updated till date, you can download this patch and other Windows vulnerability patches using eScan on the respective systems.

To do this, open "**eScan Protection Center**", click on "**Tools**" and then click on "**Download Latest Hotfix (Microsoft Windows OS)** option.

Restart the pc once all the patches are installed properly.

As far as the virus cleaning routine is concerned, eScan detects the infection and the .scr, .exe files created by virus will be removed through scanning. Just scan all the drives of that system using "Quick scan your system".

To do this, click on Start - Programs - eScan for Windows - Quick Scan your system.

Now, Select the below options to Scan:

"Memory / Services", "Registry", "Startup Folders", "System Folders", "Scan Spyware", "Drive", "All Local Drives" , "Scan All files" and "Scan & Clean".

(Note: If you suspect any new infection, please do provide us the sample files in a password-protected zip format to support@escanav.com and to samples@escanav.com so that we can add the detection at the earliest).

How to Unhide the hidden files/folders:
Once the scan is completed, run the below command to unhide the files /folders of the respective drive.

For Example:
Execute the below command to unhide files/folders of a drive including sub-folders. Below example is for C drive.

Open CMD prompt and goto c:\program files\escan folder and type the below command:

mwavscan.com /unhideallfiles /folder=C: /subfolders

To specify a folder and its subfolder use the below command:(Below example will unhide files and sub-folders of "C:\ABC" folder.

mwavscan.com /unhideallfiles /folder=c:\abc /subfolders

Do note that some "shortcut link folders" left after scanning has to be deleted manually.
Unique solution ID: #1044
Author: Nitin
Last update: 2012-02-10 12:40