



香港電腦保安事故協調中心
Hong Kong Computer Emergency Response Team
Coordination Centre

“Marketscore” Removal Procedure Version 2.1

What is Marketscore?

Marketscore is a software that can direct user web network traffic, including SSL sessions, to route through Marketscore Inc.'s proxy server network. There may be a threat of personal information leakage of sensitive information like account number, user name and password.

Marketscore is promoted as an Internet accelerator and can be downloaded from the Marketscore web site. Alternatively it is bundled with some freeware or shareware programs and installed to your machine. Users may or may not be aware that the software is installed on their machine.

If you want to check whether this software is installed in your machine, or want to remove the installed Marketscore software, please follow the procedure below.

IMPORTANT NOTES

- This procedure is used for detecting and removing the Marketscore software. You should follow **ALL THE STEPS IN ORDER**.
- Before modifying the system, you should **backup your data** so that you can restore your system to the original state if there is any problem (e.g. copy document files, photos, address book, etc. to USB flash drive or CD-R/DVD-R.)
- All data and information provided in this procedure are for informational purpose only. The users should take full responsibility in deciding whether to follow the steps in the procedure and to remove the Marketscore software from their machines. HKCERT will not be liable for any errors or omissions in the content of this procedure, nor for any damages or losses arising from any actions taken in reliance on the information provided.
- If you have any query on this procedure, please contact HKCERT.
Tel: 81056060; Email: hkcert@hkcert.org

1. Detection

Some Marketscore variants bear distinctive characteristics that can be identified manually. However, some variants may possess characteristics that can only be detected using an anti-spyware software. We recommend all users to use an anti-spyware software to check for Marketscore after conducting the Manual Checks.

a. Manual Checks

- (i) Check from Control Panel if Marketscore software was installed.
 - From "Start" menu" choose "Settings" | "Control Panel". Double-click on "Add or Remove Programs"
 - From the list of currently installed program, search for either "Marketscore" or "Netsetter" or "RelevantKnowledge". If you can find either of these programs, you have Marketscore installed.
- (ii) Check from Internet Explorer if Marketscore certificates were installed.
 - Launch your Internet Explorer browser and select "Internet Options..." from the "Tools" menu. The Internet Options dialog box is displayed.
 - Click on the "Content" tab and then click on the "Certificates" button. The Certificates dialog box is displayed. Click on the "Trusted Root Certification Authorities" tab.
 - If the "Marketscore" and "Netsetter" certificates are in the list, you have Marketscore installed.

b. Scanning by an anti-spyware tool

In general, scanning by an anti-spyware tool may detect some other spyware software. Please download **ANY ONE** of the following anti-spyware program and install it on your machine.

Ad-aware SE Personal

<http://www.lavasoftusa.com/support/download/>

Microsoft Windows AntiSpyware (Beta)

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

Spybot Search and Destroy

<http://www.safer-networking.org/en/mirrors/>

- After installation, press "check for update now" button to update the spyware database.
- When updating completed, disconnect from the Internet and Select "Start" to scan the system.
- If Marketscore is found, you may follow the steps below to remove or quarantine the critical objects associated with the software.

2. Removal

With careful considerations, follow the steps suggested below to remove Marketscore and related files, and to remove the root certificates installed in your machine. You may need to take extra steps to restore the files corrupted in your machine.

a. Uninstall Marketscore software

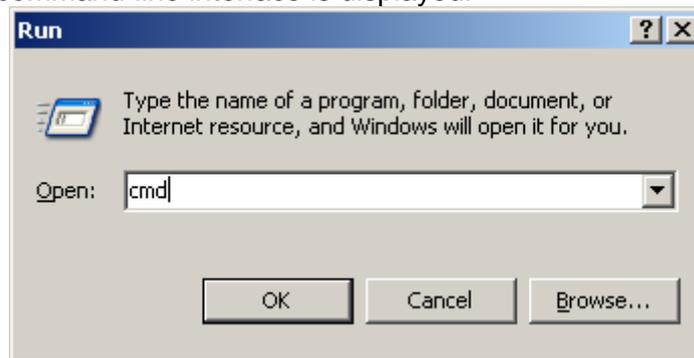
- (i) Uninstall using Control Panel

- In "Control Panels", double-click on "Add or Remove Programs" to open the list of programs installed on your computer.
- Find "Marketscore" or "Netsetter" or "RelevantKnowledge" or "Internet Accelerator" in the list of programs, and click on it and click the "Remove" button.
- When the uninstaller is finished, you MUST RESTART the computer normally.

(ii) Uninstall using Command Line

If you cannot find the programs in "Control Panel", try uninstall the software from command line

- Select "Run..." from the Windows Start menu and type "cmd" (without the quotes) in the "Open:" text box. Click the OK button. A window with a command-line interface is displayed.



- At the command line prompt, type the following to bring you to the system32 folder:

```
cd %SystemRoot%\system32
```

- At the command prompt, type each line below separately. (Note: usually, ONLY ONE of the commands will work while the other two will return errors stating that the file was not found.)

```
nscheck /uninstall  
ossproxy -bootremove -uninst:RelevantKnowledge  
mksc -bootremove -uninst:RelevantKnowledge
```

- Type "exit" (without the quotes) to close the command window.
- You MUST RESTART the computer normally and proceed to the next step.

b. Remove Marketscore software

- Download **ANY ONE** of the following anti-spyware program, and install it on your machine.

Ad-aware SE Personal

<http://www.lavasoftusa.com/support/download/>

Microsoft Windows AntiSpyware (Beta)

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

Spybot Search and Destroy

<http://www.safer-networking.org/en/mirrors/>

- After installation, press "check for update now" button to update the spyware database.
- When updating completed, disconnect from the Internet and Select "Start" to scan the system.
- Follow the instructions from the anti-spyware program to delete or to quarantine Marketscore and related files.

c. Remove the root certificates installed by Marketscore in browsers

Marketscore installed root certificates on your browser. When you access SSL web pages via their proxy servers, you will not be alerted that the certificate is not the original site certificate and that encryption has been broken. You must uninstall the Marketscore root certificates with the appropriate instructions below for the browser that you are using:

(i) Internet Explorer browser:

- Launch your Internet Explorer browser.
- Select "Internet Options..." from the "Tools" menu. The Internet Options dialog box will be displayed.
- Click on the "Content" tab,
- Click on the "Certificates" button. The Certificates dialog box is displayed.
- Click on the "Trusted Root Certification Authorities" tab.
- Find the "Marketscore" and "Netsetter" certificates in the list. For each certificate, click on the certificate and then click on the "Remove" button.
- Review to make sure they are deleted. Close all dialog boxes by clicking on OK.

(ii) Netscape Navigator or Mozilla browser:

- Launch your Netscape or Mozilla browser.
- Select "Preferences" from the "Edit" menu. The Preferences dialog box is displayed.
- Expand the "Privacy and Security" item in the list on the left side of the dialog box and then click on "Certificates".
- Click on the "Manage Certificates" button. The Certificate Manager dialog box will be displayed. Click on the "Authorities" tab.
- Find the "Marketscore" and "Netsetter" certificates in the list. For each certificate, click on the certificate, and then click on the "Delete" button.
- Review to make sure they are deleted. Close all dialog boxes by clicking on OK.

(iii) Mozilla Firefox browser:

- Launch your Firefox browser.
- Select "Options" from the "Tools" menu. The Options dialog box is displayed. Select "Advanced".
- In the "Advanced" window, expand the "Certificate" item in the list on the left side of the dialog box.
- Click on the "Manage Certificates" button. In the Certificate Manager dialog box, click on the "Authorities" tab.
- Find the "Marketscore" and "Netsetter" certificates in the list. For each certificate, click on the certificate, and then click on the "Delete" button.

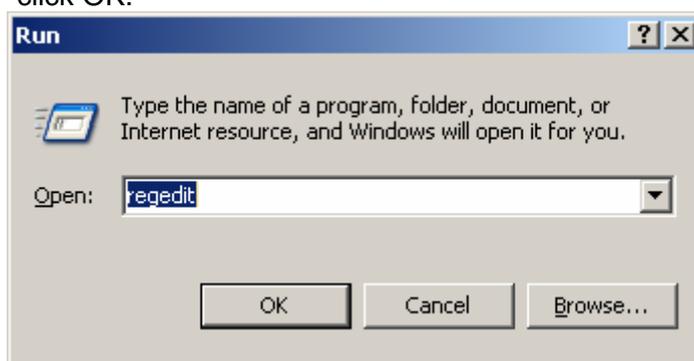
- Review to make sure they are deleted. Close all dialog boxes by clicking on OK.

d. Correct network connection (winsock) problem

Some users may experience network connection problems after the Marketscore software is removed, because the Winsock program (network driver) on the system was corrupted. If you cannot browse Internet, follow the steps below to restore Winsock on your machine.

(i) WinXP platform

- Delete the corrupted registry keys
 - Click Start, and then click Run. In the Open box, type regedit, and click OK.



- In Registry Editor, locate the following keys, right-click each key, and click "Delete":
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2
 - When you are prompted to confirm the deletion, click Yes.
 - You must RESTART Windows. The operating system will recreate the key entries.
- Re-install TCP/IP
 - After system restarted, open network connections and right-click the network icon, and then click "Properties".
 - Click "Install" button. Then choose "Protocol", and then click "Add" button.
 - Click "Have Disk". Type "C:\Windows\inf", and then click OK.
 - From the list of available protocols, click "Internet Protocol (TCP/IP)", and click OK.
 - Restart the computer. Test for Internet connection.

Warning: Programs that access or monitor the Internet such as antivirus, firewall or proxy clients may be affected. If you have a program that no longer functions correctly after you use this resolution, reinstall the program to restore functionality.

(ii) Windows platforms other than WinXP (Win95, Win98, WinME and Win2000)

- Remove corrupted TCP/IP
 - Open network connections and right-click the network icon, and then click "Properties".
 - Choose "Internet Protocol (TCP/IP)" and click "Uninstall" button. Click OK to confirm.

- You must RESTART Windows to have the system clean up the corrupted winsock.
- Re-install TCP/IP
 - After system restarted, open network connections again and right-click the network icon, and then click "Properties". You should see that "TCPIP" entry is gone.
 - Click "Install" button. Then choose "Protocol", and then click "Add" button.
 - From the list of available protocols, click "Internet Protocol (TCP/IP)" and click OK.
 - Restart the computer. Test for Internet connection.

e. Change the passwords for your online services

Note: If you have problem with this part please contact individual online services provider for assistance.

While you were running Marketscore, any credentials that you used to access websites may be captured by the software and stored as part of the data that they collect. For safety reasons, you should

- check your online transactions records for suspicious entries
- change your online services (web mail, online banking, etc.) passwords.

f. Remove residue Marketscore program files from your hard drive [Optional Removal Step]

Some Marketscore files might still be left on your hard disk after the above steps. Although they are not harmful to your system, you may consider removing all of them according to the following steps.

- Select "Run..." from the Windows Start menu and type "cmd" (without the quotes) in the "Open:" text box. Click the OK button. A window with a command-line interface is displayed.
- At the command line prompt, type the following to bring you to the system32 folder:

```
cd %SystemRoot%\system32
```

- At the command prompt, type each line below separately. (Note: usually, SOME of the commands will return errors stating that the file was not found.)

```
del csloa.dll
del csloa.dll
del cusnns.bak
del nscheck.exe
del nscheck.lgc
del nsconfig.dll
del nsconfig.dll
del nsconfig.inf
del okshook.dll
del osmim.dll
del osconfig.dll
del ossproxy.exe
```

- Type "exit" (without the quotes) to close the command window.

*** The End ***