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

移除 "Marketscore" 的程序
第 2.1 版

甚麼是 Marketsore?

Marketsore 是一個軟件，它能夠把用戶的訪問網站的交通（包括 SSL 會話）轉向，途經該公司管理的代理伺服器。它有可能帶來洩露用戶個人資料（如線上服務的帳戶編號、帳戶名稱和密碼等）的威脅。

Marketscore 公司宣傳該軟件可以增加網絡傳輸的速度。該軟件可以直接從 Marketscore 網站下載；此外，有些免費軟件或共享軟件工具的安裝程式，包含 Marketsore 在內，用戶在有意識或無意識的情況下，將 Marketscore 隨同下載的工具安裝到系統上去。

如果你想檢查電腦有否安裝 Marketscore，又或者你想移除已被安裝了的 Marketscore 軟件，請遵照以下步驟。

注意事項

- 這程序是專為偵測和移除"Marketscore"而設，請**按次序執行所有步驟**。
- 在執行移除程序之前，建議你先**備份電腦上的數據**（例如把文件、相片、地址簿等，備份到 USB 快閃記憶體，或燒錄至 CD-R 或 DVD-R 上），以確保系統一旦出現問題時，仍可復修至原來狀態。
- 本程序提供的數據和資訊祇作參考用途。用戶需要對是否遵循本程序、或移除機器上的 Marketscore 的決定承擔全部責任。HKCERT 對本程序的內容的錯誤、遺漏、及用戶因依據提供的資訊的所作的任何行為，而引起的任何損失，概不負責。
- 如果對此程序有任何問題，請聯絡 HKCERT。
  電話：81056060；電郵：hkcert@hkcert.org

1. 偵測

某些 Marketscore 變種有明顯的特徵，容易以人手測試確認。不過，另一些變種可能要使用反間諜軟件才能夠偵測得到。我們建議用戶先用人手測試，再使用反間諜軟件掃描。

a. 人手測試

(i) 從控制台檢查 Marketscore 軟件有否安裝

- 從"開始" 選擇 "設定" | "控制台"，雙擊 "新增/移除程式"。
- 從目前安裝的程式中，找尋 "Marketscore" 或 "Netsetter" 或 "RelevantKnowledge"。
- 倘找到任何一個，表示已安裝 Marketscore。

(ii) 從 Internet Explorer 檢查 Marketscore 根憑證有否安裝

- 開啟 Internet Explorer 瀏覽器，按選單表上 "工具"，選 "網際網路選項"。
- 在"網際網路選項"視窗，選"內容"分頁；在"內容"分頁，按"憑證"。
- 在"憑證"視窗，選"信任的根目錄憑證授權"分頁。
- 在"發給"一欄查看是否有任何 "**Marketscore Inc"** 憑證" 或 "**Netsetter**" 憑證。
- 倘找到任何一個，表示已安裝 Marketscore。

b. 反間諜軟件掃描

反間諜軟件掃描一般能偵測到其他的間諜軟件。從以下網址，下載**任何一個**反間諜軟件到電腦桌面。

Ad-aware SE Personal
http://www.lavasoftusa.com/support/download/

Microsoft Windows AntiSpyware (Beta)
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Spybot Search and Destroy
http://www.safer-networking.org/en/mirrors/

- 完成安裝後，按 "check for update now" 更新間諜軟件樣式資料庫。
- 完成更新後，可以中斷網絡連線，選擇 " start " 執行掃描。
- 若找到 Marketscore，你可以遵循下面的步驟移除或隔離。之後重新啟動電腦。

2. 移除

遵照以下步驟，經過小心判斷，移除或隔離 Marketscore 及有關的檔案，並移除被植入的根憑證。你可能需要額外的步驟重建受損的檔案。

a. 解除安裝 Marketscore

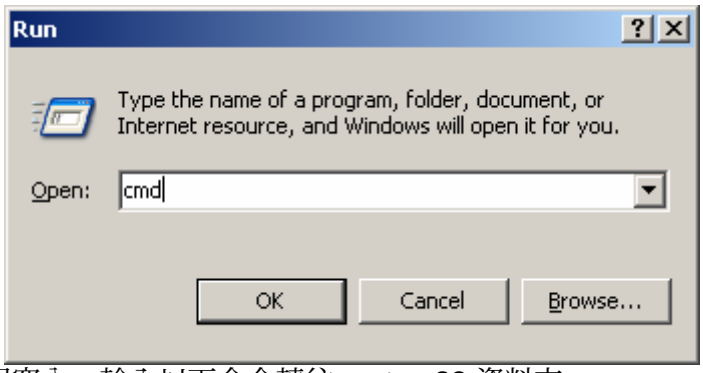
(i) 經控制台解除安裝 Marketscore

- 從"開始" 選擇 "設定" | "控制台"，雙擊"新增/移除程式"。
- 從"目前安裝的程式"中，找尋 "Marketscore" 或 "Netsetter" 或 "RelevantKnowledge"，點選並按"移除" 按鈕。
- 當移除完成，緊記要**重新啟動視窗**。

(ii) 人手解除安裝 Marketscore

如果你不能在控制台移除 Marketscore，可以執行這部分，直接輸入用命令。

- 從"開始" 選擇 "執行"，在"開始"文字匣中輸入 "cmd" (去掉引號"") 並按 "確定" 鈕。命令視窗開啟。



- 在命令視窗內，輸入以下命令轉往 system32 資料夾。

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

- 在命令視窗內，逐行輸入以下命令。（注意：通常祇有其中一行命令會有效移除軟件，其他的命令會產生錯誤" 找不到檔案"。）

```
nscheck /uninstall

ossproxy -bootremove -uninst:RelevantKnowledge

mksc -bootremove -uninst:RelevantKnowledge
```

- 輸入 "exit" (去掉引號"") 去關閉命令視窗。
- 當移除完成，緊記要**重新啟動視窗**，然後跳到下一個步驟。

b. 清除 Marketscore

- 從以下網址，下載**任何一個**反間諜軟件到電腦桌面。

  Ad-aware SE Personal
  http://www.lavasoftusa.com/support/download/

Microsoft Windows AntiSpyware (Beta)
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Spybot Search and Destroy
http://www.safer-networking.org/en/mirrors/

- 完成安裝後，按 "check for update now" 更新間諜軟件樣式資料庫。
- 完成更新後，可以中斷網絡連線，選擇 " start " 執行掃描。
- 遵循反間諜軟件給予的指示，移除或隔離 Marketscore 及有關的檔案。之後重新啟動電腦。

c. 移除 "Marketscore" 植入的根憑證 (Root Certificates)

Marketscore 會在瀏覽器植入的根憑證，使你經 Marketscore 的代理伺服器存取 SSL 網頁時，瀏覽器誤以為連線是可信的，不去警告你有敏感數據會被攔截。你必須遵照下面適用於你的瀏覽器的指示，移除 "Marketscore" 植入瀏覽器的根憑證。

(i) Internet Explorer 瀏覽器:

- 開啟 Internet Explorer 瀏覽器，按選單表上 "工具" ，選 "網際網路選項"。
- 在"網際網路選項"視窗，選"內容"分頁；在"內容"分頁，按"憑證"。
- 在"憑證"視窗，選"信任的根目錄憑證授權"分頁。
- 在"發給"一欄查看是否有任何 "**Marketscore Inc"** 憑證" 或 "**Netsetter**" 憑證。若發現，請移除之。
- 再檢查以確定憑證已被移除。按"關閉"完成。

(ii) Netscape/Mozilla 瀏覽器:

- 開啟 Netscape 或 Mozilla 瀏覽器。
- 按選單表上 "編輯"，選 "喜好"，"喜好"視窗會顯示。
- 在"喜好"視窗內，在"分類"，雙按"私隱和安全" ，然後按"憑證" (Certificate) 。
- 在"憑證"內，按 "管理憑證" 按鈕，在"憑證管理員視窗"內，按"授權"
- 在"憑證名稱"一欄查看是否有任何 "**Marketscore Inc**"憑證 或 "**Netsetter**"憑證。若發現，請移除之。
- 再檢查以確定憑證已被移除。按"關閉"完成。

(iii) Mozilla Firefox 瀏覽器:

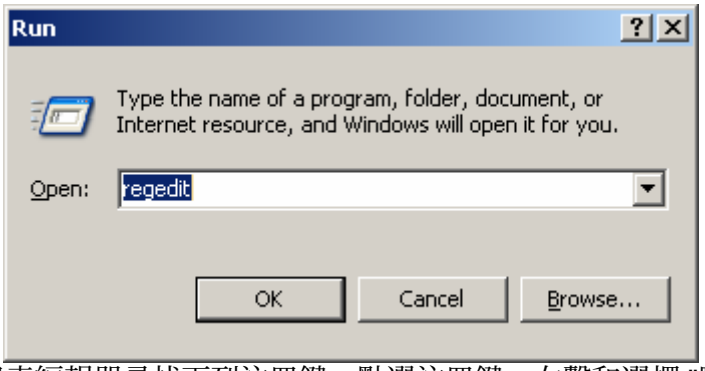
- 開啟 Mozilla Firefox 瀏覽器。
- 按選單表上 "工具"，選 "選項"。在"選項"視窗內，選"進階"。
- 在"進階"視窗內，按 (+) 憑證 (Certificate) 。
- 按 "管理憑證" 按鈕。在"憑證管理員視窗"內，按"授權" 按鈕。
- 在"憑證名稱"一欄查看是否有任何 "**Marketscore Inc**" 憑證 或 "**Netsetter**" 憑證。若發現，請移除之。
- 再檢查以確定憑證已被移除。按 "關閉" 完成。

d. 網絡連接 (winsock) 問題的解決辦法

有些用戶在移除 "Marketscore"時，可能會因為 Winsock 程式（網絡驅動器）受損，遇到不能連接 TCPIP 網絡的情況。倘若你不能上網，請遵循下面為不同視窗平台而設的步驟，重建 winsock。

(i) WinXP 視窗平台

- 刪除受損的注冊鍵
  - 從"開始" 選擇 "執行" ， 在"開始". 文字匣中輸入 "regedit" (去掉引號"")並按 "確定" 鈕。



  - 在注冊表編輯器尋找下列注冊鍵，點選注冊鍵，右擊和選擇 "刪除" ， 確認 "刪除" 。
    - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock
    - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2
  - 緊記要**重新啟動視窗，**視窗會再產生注冊鍵。

- 重裝 TCP/IP
  - 系統重新啟後，開啟 "網路和撥號連線" ， 右擊有關的網路圖示，選" 內容" 。
  - 按 "安裝" 按鈕，選 "通訊協定" ， 再按 "增加" 。
  - 按 "從磁片安裝" 按鈕，輸入 "C:\Windows\inf" ， 按 "確認" 按鈕。
  - 從網絡通訊協定列表，選"Internet Protocol (TCP/IP)" ， 按 "確認" 按鈕。
  - 重裝 TCP/IP 完成後，緊記要**重新啟動視窗，**測試網路連線。

警告：連接或監控網路的程式，如防病毒軟件、防火牆或代理伺服器客戶端在移除 Marketscore 後，均可能受影響。如果類似的情形發生，請重裝有任何應用程式。

(ii) 非 WinXP 的視窗平台（Win95、Win98 和 Win2000）

- 刪除受損的 TCPIP 設定
  - 開啟 "網路和撥號連線" ， 右擊有關的網路圖示，選 " 內容" 。
  - 選 "通訊協定" ， 再按 "解除安裝" ， 按 OK 按鈕。
  - 緊記要**重新啟動視窗，**視窗會刪除受損的 TCPIP 設定。
- 重裝 TCP/IP
  - 系統重新啟動後，開啟 "網路和撥號連線" ， 右擊有關的網路圖示，選 "內容" ， TCPIP 選項應該已消失。
  - 按 "安裝" 按鈕，選 "通訊協定" ， 再按 "增加" 按鈕。
  - 從網絡通訊協定列表，選 "Internet Protocol (TCP/IP)" ， 按 "確認" 按鈕。
  - 重裝 TCP/IP 完成後，緊記要**重新啟動視窗，**測試網路連線。

e. 更新線上服務的密碼

注意：若在更新線上服務的密碼方面有問題，請向個別線上服務供應商的支援尋求協助。

Marketscore 運行時，會擷取你在網站登錄的身份資料，收集和記錄下來。為安全計，你應該

- 檢查你的線上交易記錄，有否可疑項目。
- 更新線上服務（如網頁電郵、線上銀行等）的密碼。

f. 移除 Marketscore 的殘留檔案 [非指定的移除步驟]

經過上面的移除步驟後，硬碟上可能尚有一些 Marketscore 的殘留檔案，雖然它們都是無害的，但最好是完全清理。以下是人手的清理步驟。

- 從 ”開始” 選擇 “執行” ，在 ”開始”. 文字匣中輸入 ”cmd” (去掉引號””) 並按 ”確定” 鈕。命令視窗開啟。
- 在命令視窗內，輸入以下命令轉住 system32 資料夾。

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

- 在命令視窗內，逐行輸入以下命令。(注意：通常其中幾行命令會產生錯誤” 找不到檔案” 。

```
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
```

- 輸入 "exit" (去掉引號””) 去關閉命令視窗。

*** 完 ***