

Conficker Worm 電腦蠕蟲

簡介與建議解決方案

[此文件主要在於介紹 Conficker Worm 電腦蠕蟲攻擊方式，並提供偵測方法與解決工具，期能協助使用者解決 Conficker Worm 電腦蠕蟲的問題]





Conficker Worm 電腦蠕蟲

簡介與建議解決方案

目錄

一、蠕蟲出現時間：	2
二、影響平台：	2
三、事件分類：	2
四、Conficker Worm 簡介：	2
五、Conficker Worm 攻擊手法：	3
六、Conficker Worm 偵測方式：	4
1. 網頁檢測方式：	4
2. Microsoft Baseline Security Analyzer.....	4
3. McAfee Conficker Detection Tool 1.0.8.....	8
七、Conficker Worm 感染後解決方案.....	11
工具 1：Microsoft Windows Malicious Software Removal Tool(MSRT)	11
工具 2：NOD32 EConfickerRemover.....	15
工具 3：SysClean-WORM_DOWNAD.....	16
工具 4：Kidokiller.....	18
八、結論：	19
九、參考資料：	19



Conficker Worm 電腦蠕蟲

簡介與建議解決方案

一、蠕蟲出現時間：

2011 年 11 月 21 日 首次出現 Conficker A

二、影響平台：

Windows2000/2003/XP/Vista/2008

三、事件分類：

INT 對外攻擊

四、Conficker Worm 簡介：

Conficker 主要利用 Windows 平台的 MS08-067 漏洞感染主機，感染之後 Conficker 會將自己安裝成為主機的常駐程式，並且封鎖系統和防毒軟體的更新，感染 Conficker 的主機由於這個原因，會連不上 Windows 以及防毒的更新頁面，使得偵測上極為困難。

Conficker 特點：

目前產生 5 種變種分別定義為 Conficker A~E

1. 感染途徑：

- 網路感染：NetBIOS，使用 MS08-067 漏洞
- 可移動媒體：USB 隨身碟

2. 更新方式：

- Http 更新
- 網路更新：NetBIOS，使用 MS08-067 漏洞
- P2P 更新

五、Conficker Worm 攻擊手法：

感染途徑一開始只有 MS08-067 漏洞一種，隨著時間過去 Conficker 出現了很多變種。修補完 MS08-067 漏洞的主機並不能保證就不會被 Conficker 感染，某些 Conficker 變種能透過網路分享，對設定弱密碼的電腦進行密碼猜測，然後感染之，或是透過 USB 的自動播放進行感染。

電腦在感染 Conficker 後會連接到一個伺服器接收進一步傳播的命令、收集個人信息和下載並安裝附加的惡意程序到受害人的電腦中。它還會把自己添加到 Windows 中必須執行的程序中，像是 svchost.exe，explorer.exe 和 services.exe。

而 Conficker 的 B/C 變種則會開啟 Http 服務並打開一個 1024 到 10000 之間的 PORT。如果遠程機被利用成功的情況下，受害者將會連接這個 Http 服務並下載一個病毒副本，它將會重置系統還原點並下載文件到電腦中。Conficker 變種還會自行破解使用簡單密碼做保護的網路分享，然後將惡意程式複製到網路分享資料夾之後，再感染其他使用者。此外還會嘗試透過可攜式儲存設備（如 USB）擴大感染範圍。

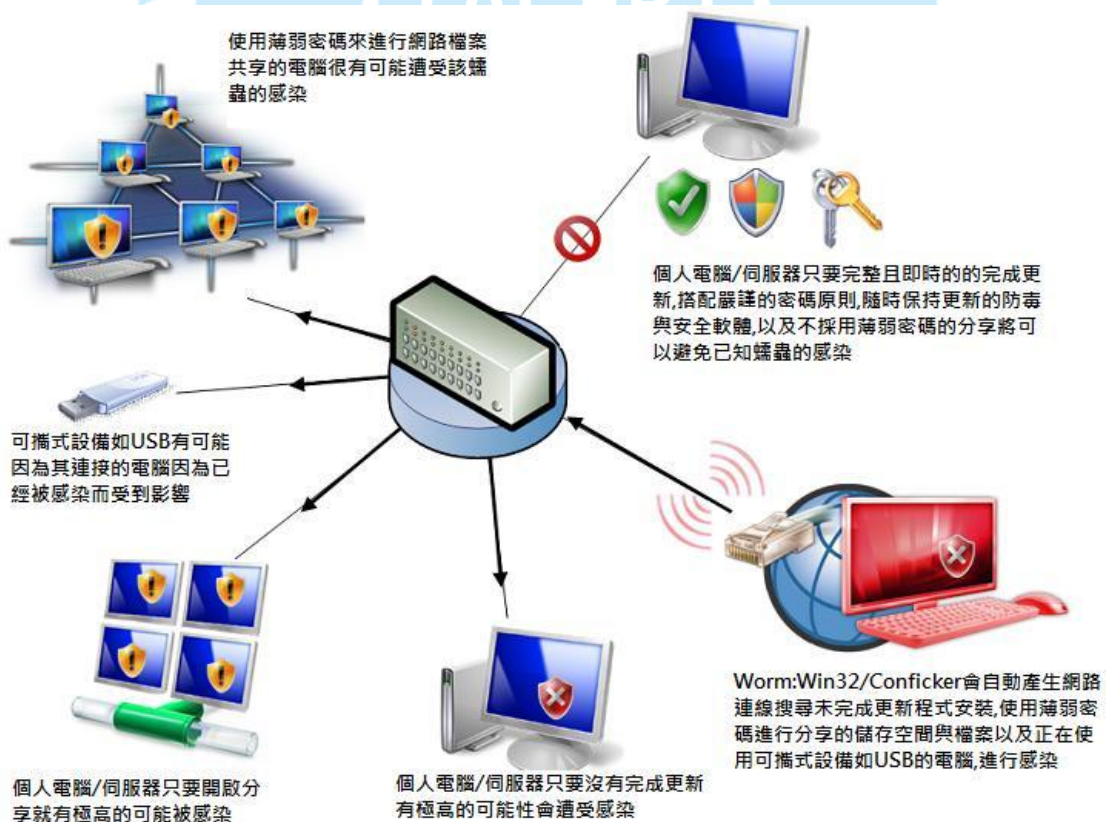


圖 1. Conficker 感染途徑說明圖(圖片來源：微軟網站)



六、Conficker Worm 偵測方式：

1. 網頁檢測方式：

網址：http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

說明：直接連線該網頁，透過網頁上面顯示之圖片可了解目前電腦感染狀況。如果上面三張圖片有全部無法顯示代表電腦可能感染 Conficker C 或更新變種，只能顯示部分圖片代表電腦可能感染 Conficker A/B。然而，若自身的電腦有使用 PROXY 的話，便無法非常準確的判別。

2. Microsoft Baseline Security Analyzer

網址：

<http://www.microsoft.com/en-us/download/details.aspx?id=7558>

說明：Microsoft Baseline Security Analyzer (MBSA) 能讓系統管理員掃描本機和遠端系統，偵查任何缺少安全性更新以及一般安全性設定錯誤的狀況。安裝說明：

Step1. 下載 MBSA

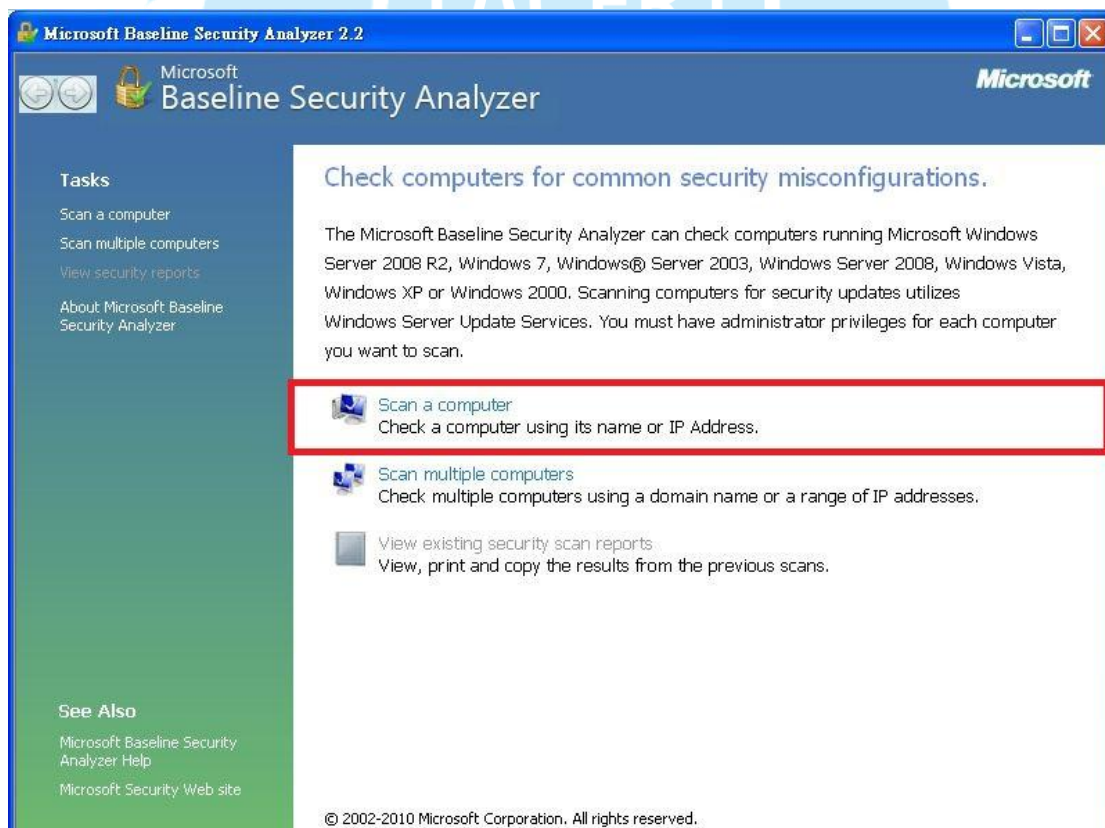
The screenshot shows the Microsoft Download Center page for Microsoft Baseline Security Analyzer 2.2 (for IT Professionals). The page includes a navigation bar with 'Microsoft', 'Search Download Center', and links for 'PRODUCTS', 'STORE', 'DOWNLOADS', and 'SUPPORT'. The main content area features the product title, a 'Quick details' section, and a 'Files in this download' table. The table lists various language and architecture versions of the installer, with the English versions for x64 and x86 highlighted with red boxes.

File name	Size	Download
MBSASetup-x64-DE.msi	1.7 MB	DOWNLOAD
MBSASetup-x64-EN.msi	1.7 MB	DOWNLOAD
MBSASetup-x64-FR.msi	1.7 MB	DOWNLOAD
MBSASetup-x64-JA.msi	1.7 MB	DOWNLOAD
MBSASetup-x86-DE.msi	1.6 MB	DOWNLOAD
MBSASetup-x86-EN.msi	1.6 MB	DOWNLOAD
MBSASetup-x86-FR.msi	1.6 MB	DOWNLOAD
MBSASetup-x86-JA.msi	1.6 MB	DOWNLOAD

Step2. 依指示安裝 MBSA

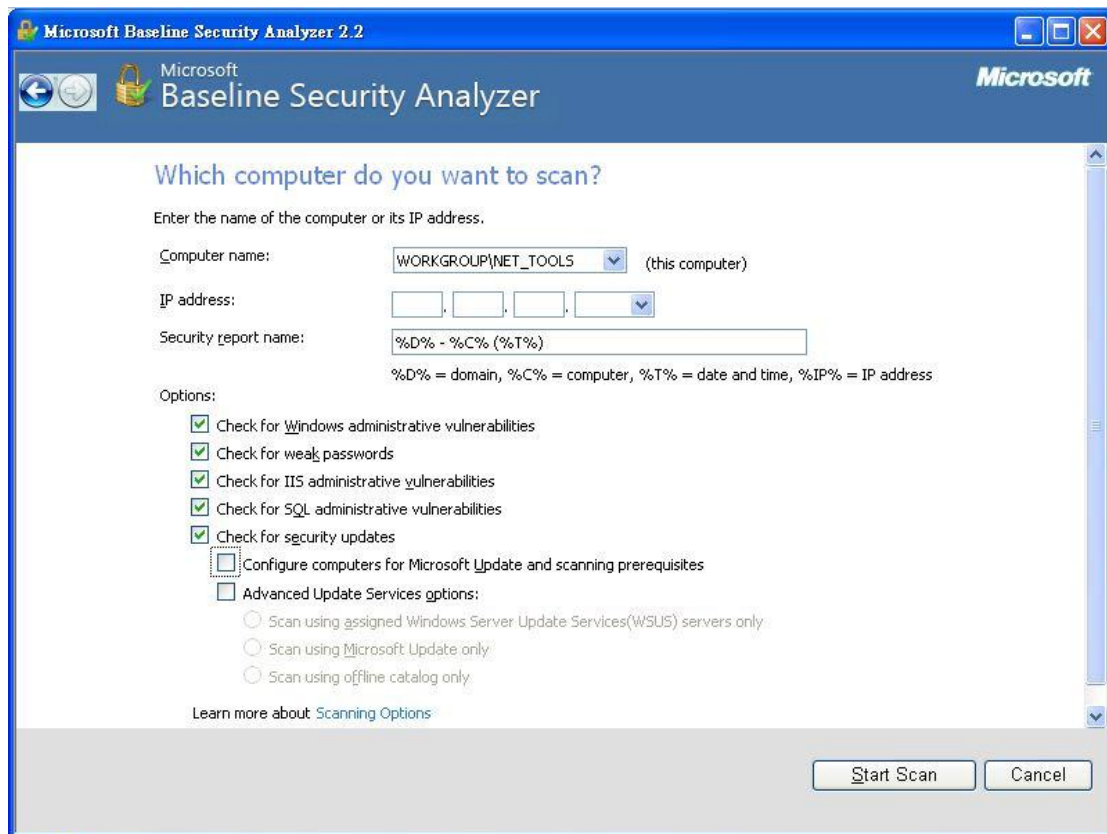


Step3-1. 執行 MBSA

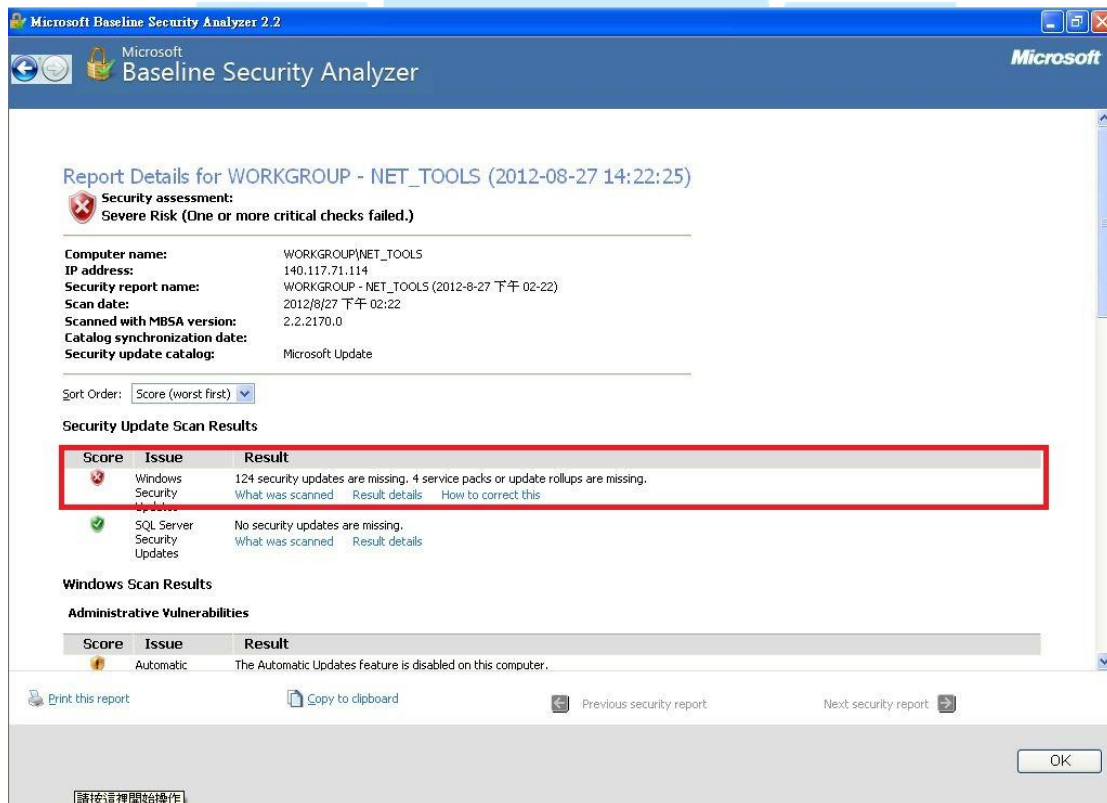




Step3-2. 使用預設掃描選項



Step3-3. 掃描完畢後，紅色為必要修正項目，點選「Result details」可看更詳細資訊





Step3-4. 點選「Description」能連結到各個修正項目詳細資訊並進行下載。

Microsoft Baseline Security Analyzer -- 網頁對話

Microsoft
Baseline Security Analyzer

124 security updates are missing. 4 service packs or update rollups are missing.

Result Details for Windows

Security Updates

Items marked with are confirmed missing. Items marked with are confirmed missing and are not approved by your system administrator.

Score	ID	Description	Maximum Severity
	MS07-009	Security Update for Windows XP (KB927779)	Critical
	MS08-030	Security Update for Windows XP (KB951376)	Critical
	MS08-046	Security Update for Windows XP (KB952954)	Critical
	MS07-061	Security Update for Windows XP (KB943460)	Critical
	MS09-061	Microsoft .NET Framework 2.0 Service Pack 2 Security Update for Windows 2000, Windows Server 2003, and Windows XP (KB974417)	Critical
	MS09-062	Security Update for Windows XP (KB958869)	Critical
	MS09-051	Security Update for Windows Media Format Runtime 9, 9.5 & 11 for Windows XP SP 2 (KB954155)	Critical
	MS10-034	Cumulative Security Update for ActiveX Killbits for Windows XP (KB980195)	Critical
	MS10-020	Security Update for Windows XP (KB980232)	Critical
	MS06-014	Security Update for Windows XP (KB911562)	Critical
	MS05-043	Security Update for Windows XP (KB896423)	Critical
	MS07-019	Security Update for Windows XP (KB931261)	Critical
	MS10-019	Security Update for Windows XP (KB980559)	Critical



3. McAfee Conficker Detection Tool 1.0.8

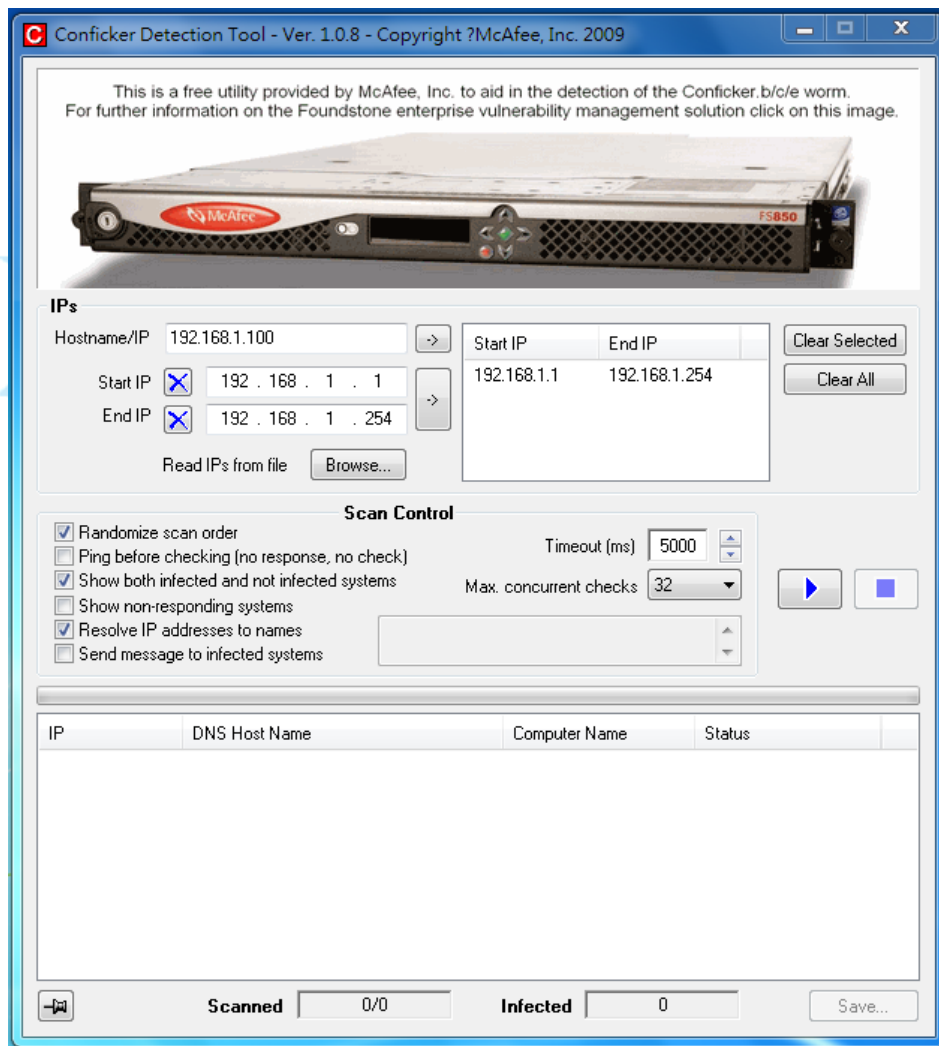
網址：

http://downloadcenter.mcafee.com/products/tools/foundstone/conficker_detection_tool_v108.zip

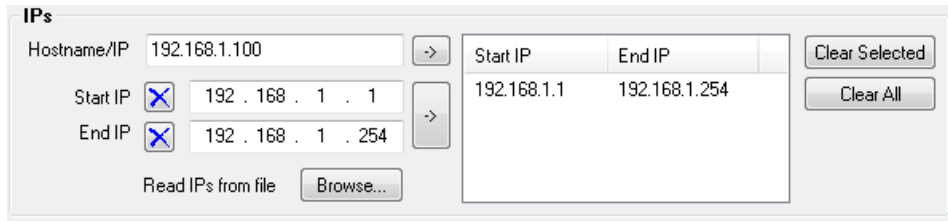
說明：掃描網域中是否有電腦感染 Conficker 蠕蟲的工具。其介面十分簡單，操作容易，可檢查出近期的.b/.c/.e 變種 Conficker。

使用說明：

Step1. 下載後解壓縮無需安裝直接執行



A. 首先是設定掃描的範圍，介面的中間部分有一個 IP 的區塊

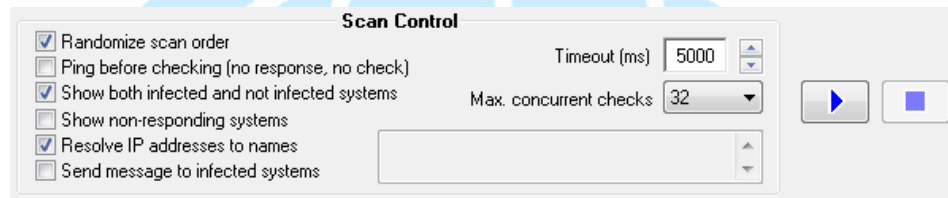


Start IP	End IP
192.168.1.1	192.168.1.254


1. Hostname/IP：此處基本上不用更改，軟體會自行偵測
2. Start IP：網域區段的起始 IP
3. End IP：網域區段的結束 IP

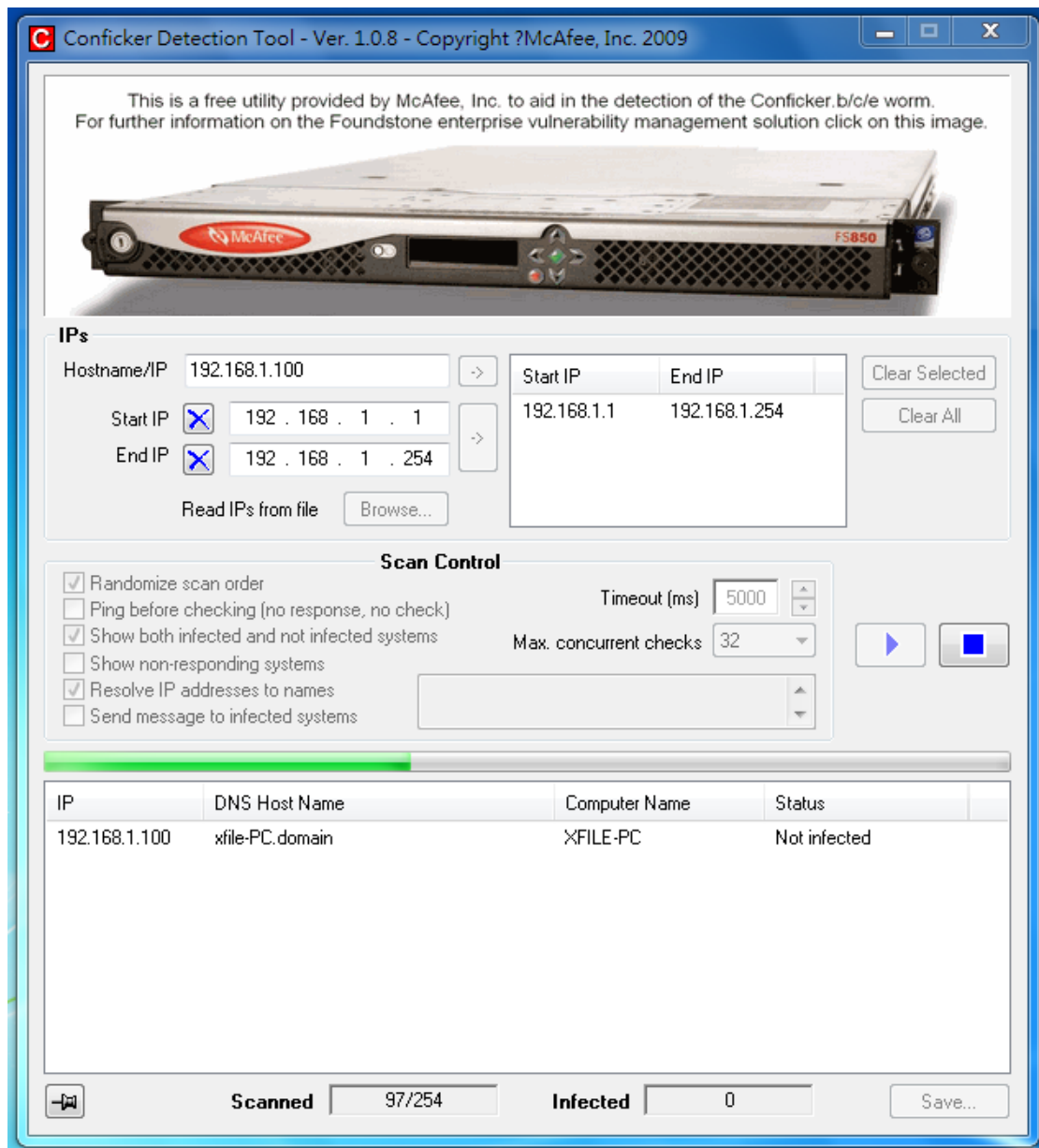
輸入完畢按右邊的「->」導入掃描範圍。您也可以將某些 IP 從掃描清單中移除，選擇清單中欲刪除的 IP 再按下 Clear Selected 的按鈕即可。若要全部清空，按下 Clear All 的按鈕。

B. 設定完 IP 後，就可以進行掃描，下面列出可供選擇的掃描選項：



1. Randomize scan order：掃描順序為隨機
2. Ping before checking (no response no check)：在檢查前先 Ping 這個 IP 看看有沒有反應，有回應則檢查，無回應則略過不檢查
3. Show both infected and not infected systems：將感染及未受感染的電腦都顯示出來。
4. Show non-responding systems：顯示對 Ping 封包沒有回應的電腦
5. Resolve IP addresses to names：將 IP 反解成主機名稱
6. Send message to infected systems：對受感染的電腦送出訊息。

C. 設定完成後，按下  的按鈕，就可以開始掃描了，下圖是它的掃描畫面：



七、Conficker Worm 感染後解決方案

1. 進行作業系統更新，建議更新作業系統至最新修正。如有更新限制，至少更新 [MS08-067](#) 漏洞。
2. 關閉共享資料夾或修改共享資料夾密碼（請注意使用符合密碼複雜性原則，如採用數字文字混雜的密碼，像是 A1H6，以避免過於簡單的密碼遭蠕蟲破解）
3. 使用工具進行清除，接下來將介紹幾種清除工具，協助清除 Conficker 蠕蟲。

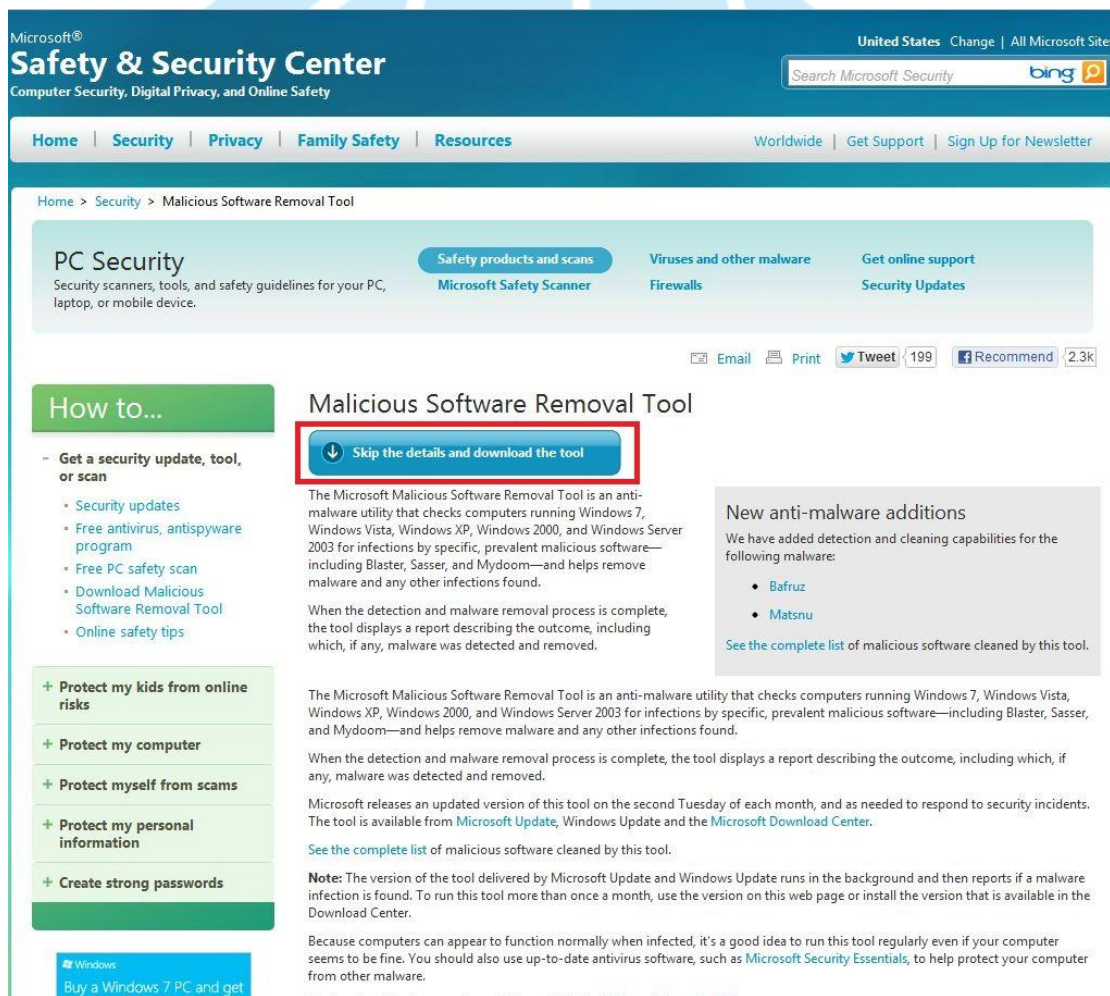
工具 1：Microsoft Windows Malicious Software Removal Tool(MSRT)

網址：<http://www.microsoft.com/security/pc-security/malware-removal.aspx>

適用平台：Windows 7/ Windows Server 2003/ Windows Vista/ Windows XP


使用說明：

Step1. 下載 MSRT



Microsoft®
Safety & Security Center
Computer Security, Digital Privacy, and Online Safety

United States | Change | All Microsoft Sites

Search Microsoft Security 

Home | Security | Privacy | Family Safety | Resources

Worldwide | Get Support | Sign Up for Newsletter

Home > Security > Malicious Software Removal Tool

PC Security
Security scanners, tools, and safety guidelines for your PC, laptop, or mobile device.

Safety products and scans
Microsoft Safety Scanner


Viruses and other malware
Firewalls

Get online support
Security Updates

Email Print Tweet 199 Recommend 2.3k

How to...

- Get a security update, tool, or scan
 - Security updates
 - Free antivirus, antispyware program
 - Free PC safety scan
 - Download Malicious Software Removal Tool
 - Online safety tips
- + Protect my kids from online risks
- + Protect my computer
- + Protect myself from scams
- + Protect my personal information
- + Create strong passwords

 Buy a Windows 7 PC and get

Malicious Software Removal Tool

[Skip the details and download the tool](#)

The Microsoft Malicious Software Removal Tool is an anti-malware utility that checks computers running Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove malware and any other infections found.

When the detection and malware removal process is complete, the tool displays a report describing the outcome, including which, if any, malware was detected and removed.

The Microsoft Malicious Software Removal Tool is an anti-malware utility that checks computers running Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove malware and any other infections found.

When the detection and malware removal process is complete, the tool displays a report describing the outcome, including which, if any, malware was detected and removed.

Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from [Microsoft Update](#), Windows Update and the [Microsoft Download Center](#).

See the [complete list](#) of malicious software cleaned by this tool.

Note: The version of the tool delivered by Microsoft Update and Windows Update runs in the background and then reports if a malware infection is found. To run this tool more than once a month, use the version on this web page or install the version that is available in the Download Center.

Because computers can appear to function normally when infected, it's a good idea to run this tool regularly even if your computer seems to be fine. You should also use up-to-date antivirus software, such as [Microsoft Security Essentials](#), to help protect your computer from other malware.

New anti-malware additions

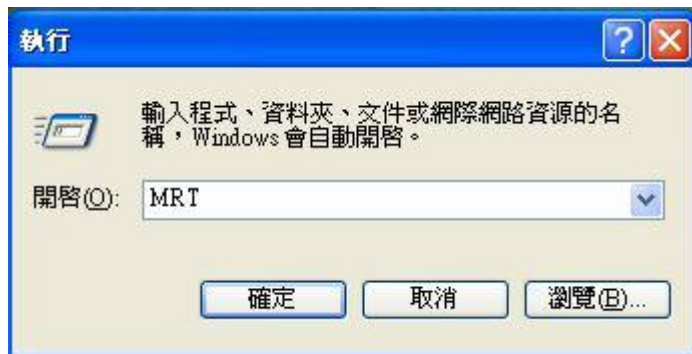
We have added detection and cleaning capabilities for the following malware:

- Bafruz
- Matsnu

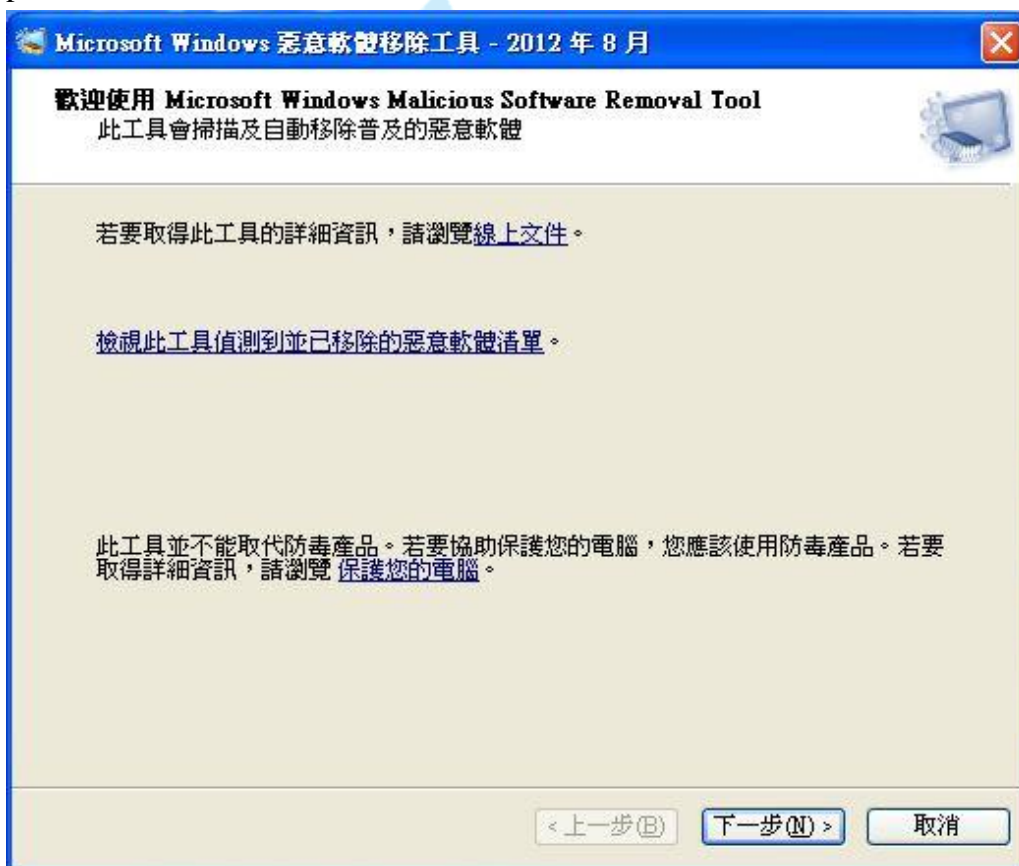
See the [complete list](#) of malicious software cleaned by this tool.



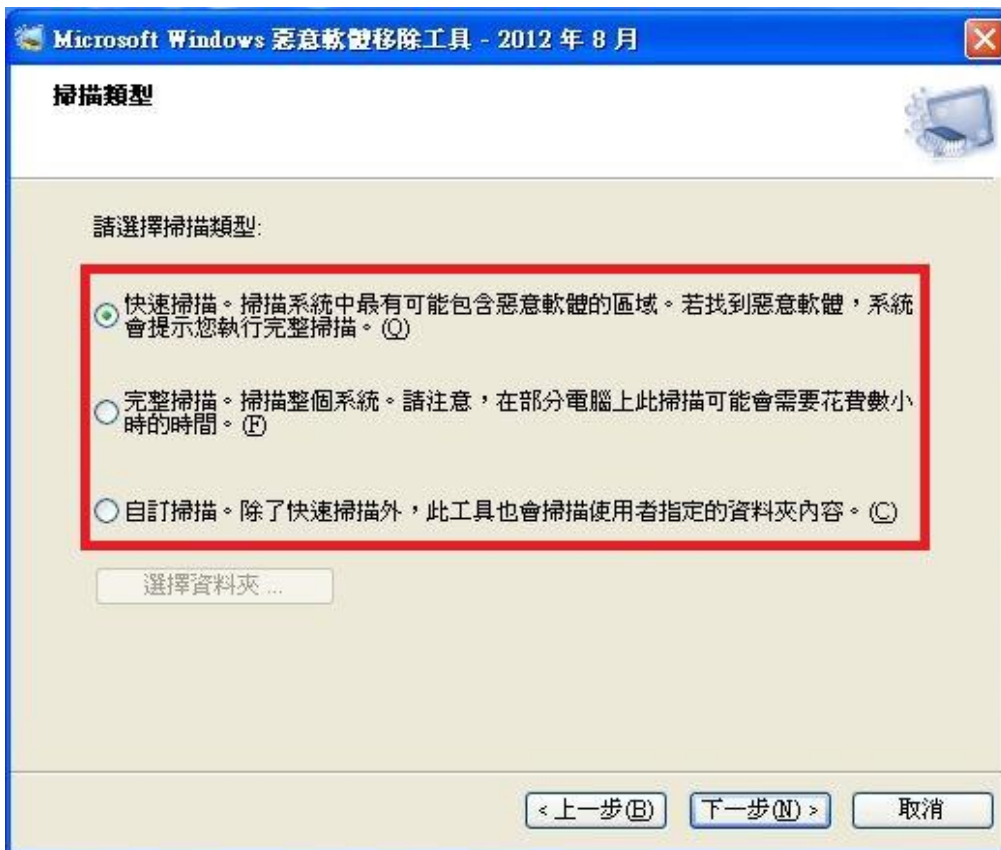
Step2-1. 執行 MSRT，於執行中輸入「MRT」即可執行 MSRT



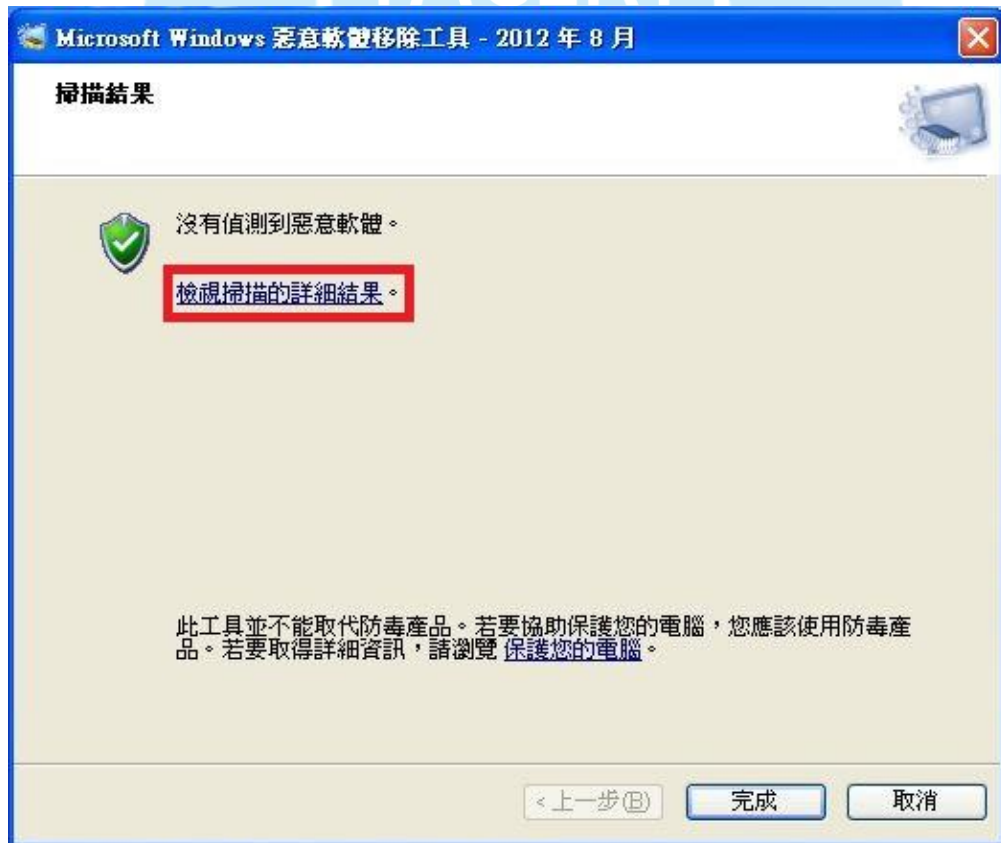
Step2-2. MSRT 執行畫面



Step2-3. 選擇掃描模式



Step2-4. 掃描結果，點選「檢視掃描的詳細結果」可得知相關訊息。



Step2-5. 從詳細結果中可得知此工具除可清除 Conficker 以外，尚可清除其他惡意程式。



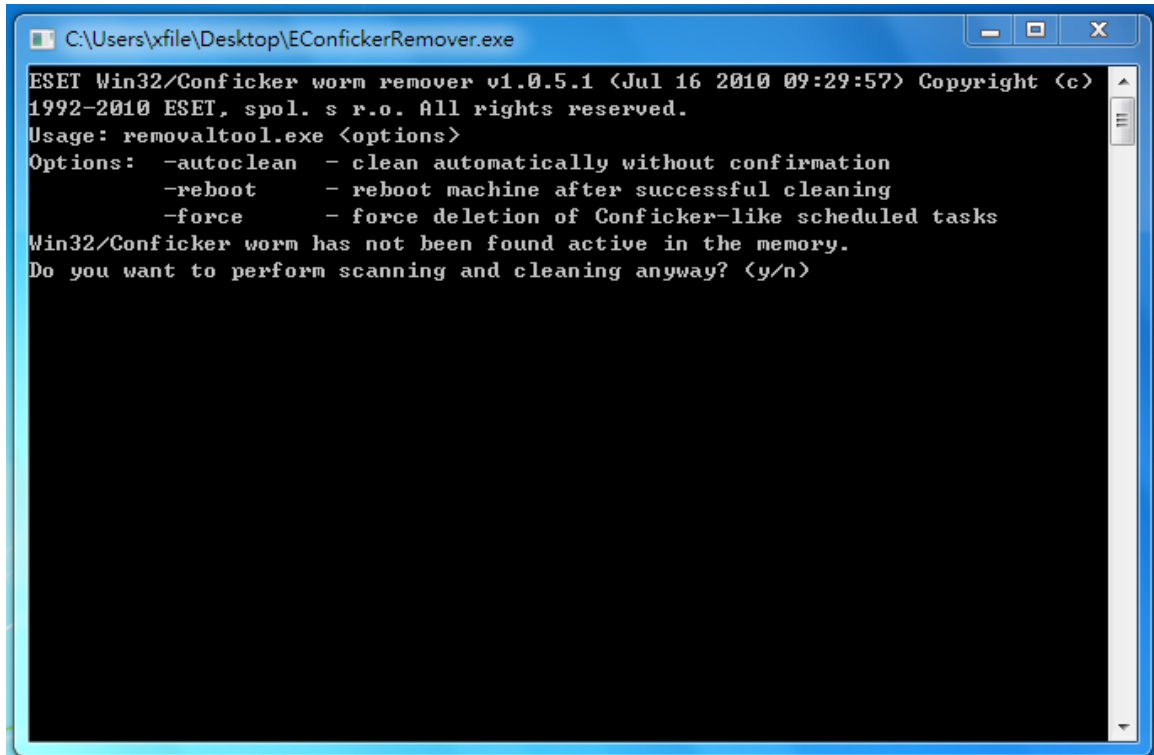
工具 2：NOD32 EConfickerRemover

網址：<http://download.eset.com/special/EConfickerRemover.exe>

適用平台：Windows XP/Windows Vista/Windows 7

使用說明：

Step1. 下載後無需安裝直接執行



```
C:\Users\xfile\Desktop\EConfickerRemover.exe
ESET Win32/Conficker worm remover v1.0.5.1 (Jul 16 2010 09:29:57) Copyright (c)
1992-2010 ESET, spol. s r.o. All rights reserved.
Usage: removaltool.exe <options>
Options:  -autoclean  - clean automatically without confirmation
          -reboot    - reboot machine after successful cleaning
          -force     - force deletion of Conficker-like scheduled tasks
Win32/Conficker worm has not been found active in the memory.
Do you want to perform scanning and cleaning anyway? <y/n>
```

此程式有參數可以使用，若要使用參數，必須自行開啟「命令提示字元」，並切換路徑到執行檔放置的位置，假設 removaltool.exe 放在 C 槽底下，切換到[C:]後，鍵入執行檔名稱，並在執行檔後面加上參數，例如：

```
C:\removaltool.exe -autoclean
```

表示在執行程式的時候自動清除，參數共有下面三種：

1. -autoclean：不再進行確認而直接進行清除的動作。
2. -reboot：清理完成後重新開機。
3. -force：強制將疑似為 Conficker 蠕蟲的執行序刪除。



工具 3：SysClean-WORM_DOWNAD

網址：

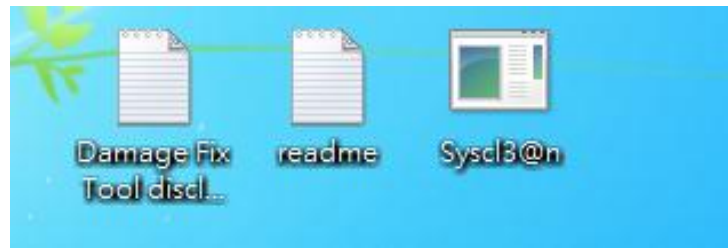
http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip

適用平台：

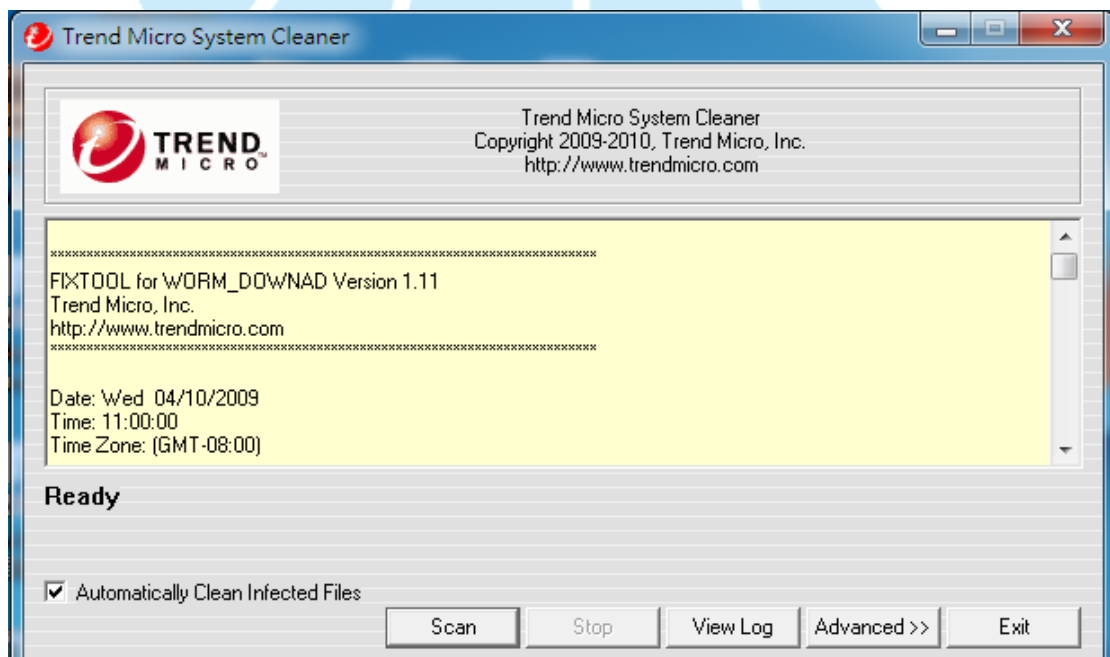
Windows 2000/Windows XP/Windows Server 2003/Windows Vista/Windows 7

使用說明：

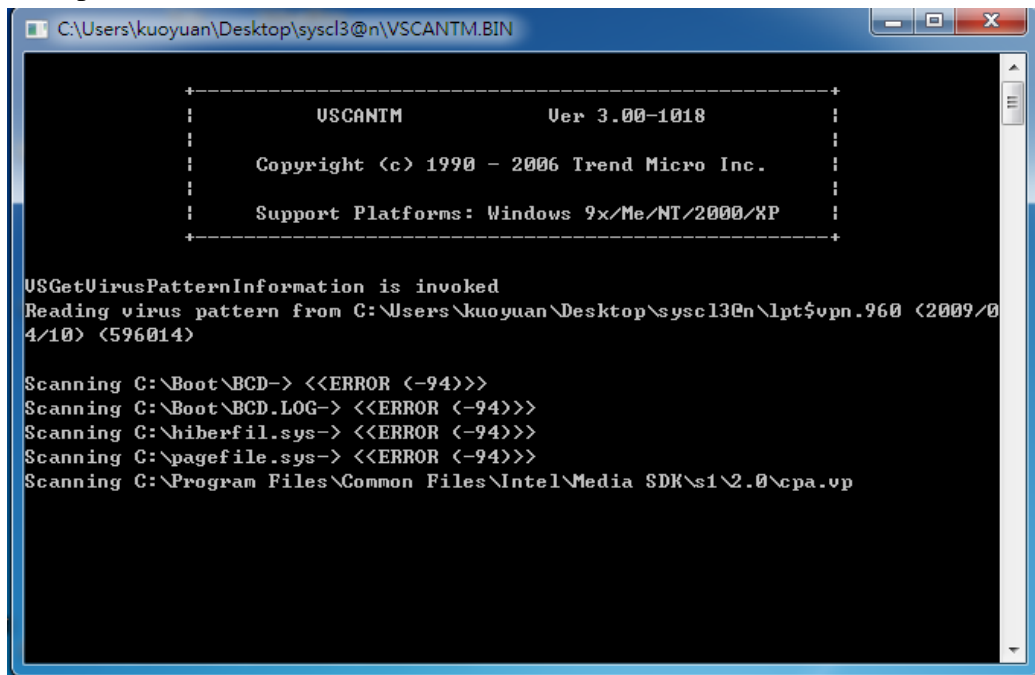
Step1. 下載後解壓縮後得到三個檔案無需安裝直接執行



Step2. 執行「Syscl3@n」



Step3. 按下 Scan 就會開始掃描



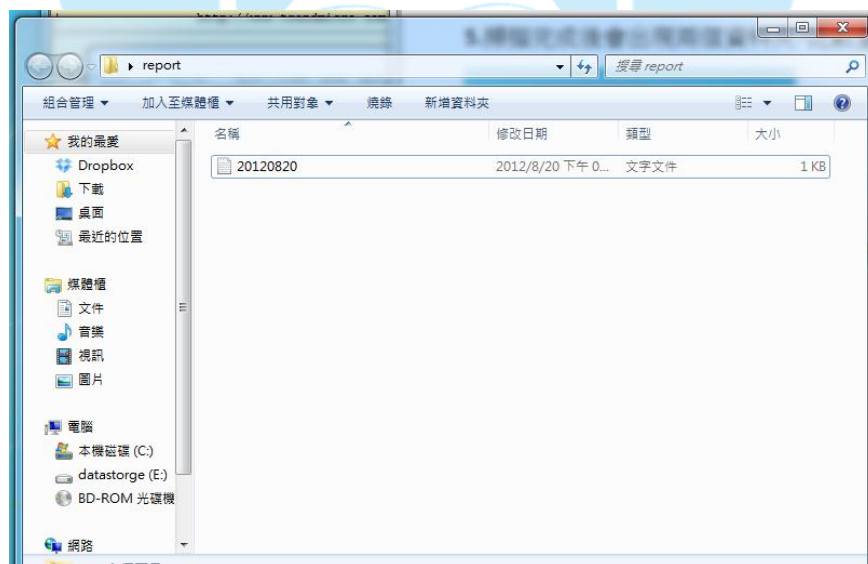
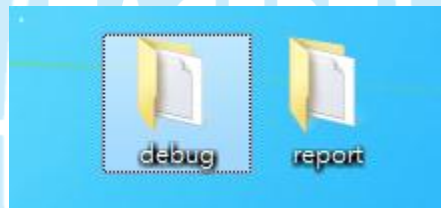
```
C:\Users\kuoyuan\Desktop\syscl3@n\VSCAN.TM.BIN

+-----+
|          USCANTM          Ver 3.00-1018          |
+-----+
|          Copyright (c) 1990 - 2006 Trend Micro Inc.          |
+-----+
|          Support Platforms: Windows 9x/Me/NT/2000/XP          |
+-----+

USGetVirusPatternInformation is invoked
Reading virus pattern from C:\Users\kuoyuan\Desktop\syscl3@n\lpt$vpn.960 (2009/04/10) (596014)

Scanning C:\Boot\BCD-> <<ERROR (-94)>>
Scanning C:\Boot\BCD.LOG-> <<ERROR (-94)>>
Scanning C:\hiberfil.sys-> <<ERROR (-94)>>
Scanning C:\pagefile.sys-> <<ERROR (-94)>>
Scanning C:\Program Files\Common Files\Intel\Media SDK\s1\2.0\cpa.vp
```

Step4. 掃描完成後會出現兩個資料夾「debug」和「report」，比較重要的是 Report 這個資料夾，裡面會有一份文件檔，內容空白的就是表示沒威脅。



工具 4：Kidokiller

網址：<http://www.kaspersky.com/virus-removal-tools>

適用平台：

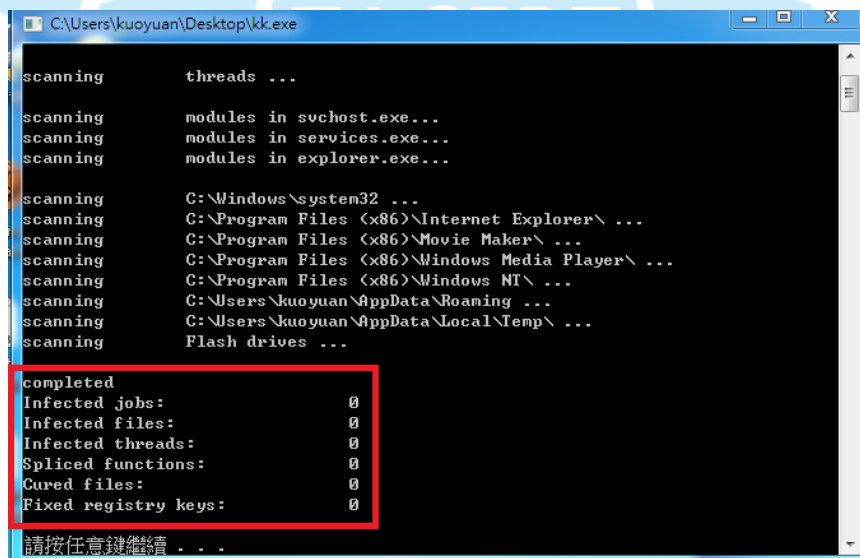
Windows 2000/Windows XP/Windows Server 2003/Windows Vista/Windows 7/Windows Server 2008

使用說明：

Step1. 下載程式後執行

XoristDecryptor	download [ZIP, 436 KB] [EXE, 497 KB] more information	2.2.75.0 New!	Trojan-Ransom.Win32.Xorist
RectorDecryptor	download [ZIP, 337 KB] [EXE, 398 KB] more information	2.4.3.0	Trojan-Ransom.Win32.Rector
KidoKiller	download [ZIP, 160 KB] [EXE, 167 KB] more information	3.4.14	Net-Worm.Win32.Kido
SalityKiller	download [ZIP, 160 KB] [EXE, 167 KB] more information	1.3.6.0	Virus.Win32.Sality.aa,ae,ag,bh
VirutKiller	download [ZIP, 128 KB] [EXE, 135 KB] more information	1.0.11.0	Virus.Win32.Virut.ce,q

Step2. 執行後會出現一個 DOS 畫面，程式會自動運行，運行完畢產生下列畫面



```
C:\Users\kuoyuan\Desktop\kk.exe
scanning      threads ...
scanning      modules in svchost.exe...
scanning      modules in services.exe...
scanning      modules in explorer.exe...
scanning      C:\Windows\system32 ...
scanning      C:\Program Files (x86)\Internet Explorer\ ...
scanning      C:\Program Files (x86)\Movie Maker\ ...
scanning      C:\Program Files (x86)\Windows Media Player\ ...
scanning      C:\Program Files (x86)\Windows NT\ ...
scanning      C:\Users\kuoyuan\AppData\Roaming ...
scanning      C:\Users\kuoyuan\AppData\Local\Temp\ ...
scanning      Flash drives ...
completed
Infected jobs:      0
Infected files:     0
Infected threads:   0
Spliced functions:  0
Cured files:        0
Fixed registry keys: 0
請按任意鍵繼續 . . .
```

要注意紅色框框裡的資訊，筆者目前的機器是沒有偵測出任何威脅，如果有偵測出的蠕蟲，數字就產生變動。



八、結論：

Conficker Worm 是一個行之有年的電腦蠕蟲，主要是透過網路分享和系統漏洞進行系統入侵的方式，且經過多年的傳播也產生多種變種。但平時如果能持續進行作業系統更新及安裝相關防護軟體，亦可避免該電腦蠕蟲感染及散播。

九、參考資料：

(一)[Conficker]

<http://en.wikipedia.org/wiki/Conficker>

(二)[針對近期的 Conficker 蠕蟲，微軟今天發佈最新的版本惡意軟體移除工具]

<http://www.microsoft.com/taiwan/security/articles/msrt0114.msp>

(三)[Microsoft Security Bulletin MS08-067 – 重大]

<http://technet.microsoft.com/zh-tw/security/bulletin/ms08-067>

(四)[Conficker Eye Chart]

http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

(五)[Microsoft Baseline Security Analyzer 2.2(for IT Professionals)]

<http://www.microsoft.com/en-us/download/details.aspx?id=7558>

(六)[McAfee Conficker Detection Tool]

http://downloadcenter.mcafee.com/products/tools/foundstone/conficker_detection_tool_v108.zip

(七) [Malicious Software Removal Tool]

<http://www.microsoft.com/security/pc-security/malware-removal.aspx>

(八)[NOD32 EConfickerRemover]

<http://download.eset.com/special/EConfickerRemover.exe>

(九)[SysClean-WORM_DOWNAD]

http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip

(十)[Kidokiller]

<http://www.kaspersky.com/virus-removal-tools>