

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]

TACERT 臺灣學術網路危機處理中心團隊製



101/9



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(MS	BRT)11
エ具2:NOD32 EConfickerRemover	15
工具3:SysClean-WORM_DOWNAD	16
工具4:Kidokiller	
八、結論:	19
九、參考資料:	

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



Download Center

Products Categories Security Support

> Microsoft Baseline Security Analyzer 2.2 (for IT Professionals)

<u>></u> لا

Quick links ↓ Overview ↓ System requi

↓ Instructions Additional information The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.2 is a minor upgrade to correct minor issues and add optional catalog support.

-		1.	1
()	1 1 1	CL	1



Quick det	ails		
Version: Change languag	2.2 English	Date published:	8/6/2010
Files in this do	ownload		
The links in this sect	ion correspond to files availabl	e for this download. Download the files ap	propriate for you.
File name		Size	
MBSASetup-x64-D	E.msi	1.7 MB	DOWNLOAD
MBSASetup-x64-El	J.msi	1.7 MB	DOWNLOAD
MBSASetup-x64-FF	l.msi	1.7 MB	DOWNLOAD
MBSASetup-x64-JA	umsi	1.7 MB	DOWNLOAD
MBSASetup-x86-D	E.msi	1.6 MB	DOWNLOAD
MBSASetup-x86-Ef	J.msi	1.6 MB	DOWNLOAD
MBSASetup-x86-FF	l.msi	1.6 MB	DOWNLOAD
	10025	1.6 MP	DOWNLOAD





Setp3-2. 使用預設掃瞄選項

🎒 Microsoft Baseline Security Analyzer	2.2	
👀 🔮 Microsoft Baseline Sec	curity Analyzer	Microsoft
Which compute Enter the name of the comp Computer name: IP address: Security report name: Options: Check for Window Check for sugary Check for SQL add Check for SQL add Check for security Check for security Check for security Check for security Check for security Configure com Advanced Upu Scan using Scan using	er do you want to scan? puter or its IP address. WORKGROUP!NET_TOOLS (this computer) , , , , , , , , , , , , , , , , , , ,	
Learn more about Sc	anning Options	<u>×</u>
	<u>S</u> tart Scan	Cancel

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

rosoft Baseli	ne Security A	inalyzer 2.2		
	_{licrosoft} Baseline	e Security Analyzer		Micro
Report	Details fo	or WORKGROUP - NET_TOG ent: or more critical checks failed)	DLS (2012-08-27 14:22:25)	
Computer IP address Security re Scan date: Scanned w Catalog sy Security u	name: : :port name: ith MBSA vers nchronization odate catalog	WORKGROUP(WET_TOOL5 140.117.71.114 WORKGROUP-NET_TOOL5 (20: 2012/8/27 下午 02:22 sion: 2.2.2170.0 h date: p: Microsoft Update	12-8-27 下午 02-22)	
∑ort Order: Security U	Score (worst f pdate Scan	irst) 🔽 Results		
Score	Issue Windows	Result 124 security updates are missing, 4 servic	e packs or update rollups are missing.	
	Security	What was scanned Result details Ho	ow to correct this	
	SQL Server Security Updates Scan Results ative Vulneral	No security updates are missing. What was scanned Result details		
Score	Issue	Result		
	Automatic	The Automatic Updates feature is disabled	d on this computer.	
Print this report		Copy to clipboard	Previous security report	Next security report

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

crosoft	Baseline S	ecurity Analyzer 網頁對話	
e	^{Microsoft} Baseli	ne Security Analyzer	
.24 sec Lesult (curity upo Details for	lates are missing. 4 service packs or update rollups are missing. Windows	
Security tems mar	Updates ked with 😵	are confirmed missing. Items marked with \star are confirmed missing and are not approved by your system	administrator.
Score	ID	Description	Maximum Severity
8	MS07-009	Security Update for Windows XP (KB927779)	Critical
3	<u>M508-030</u>	Security Update for Windows XP (KB951376)	Critical
3	M508-046	Security Update for Windows XP (KB952954)	Critical
3	MS07-061	Security Update for Windows XP (KB943460)	Critical
3	M509-061	Microsoft .NET Framework 2.0 Service Pack 2 Security Update for Windows 2000, Windows Server 2003, and Windows XP (KB974417)	Critical
3	M509-062	Security Update for Windows XP (KB958869)	Critical
8	MS09-051	Security Update for Windows Media Format Runtime 9, 9.5 & 11 for Windows XP SP 2 (KB954155)	Critical
3	MS10-034	Cumulative Security Update for ActiveX Killbits for Windows XP (KB980195)	Critical
3	M510-020	Security Update for Windows XP (KB980232)	Critical
3	M506-014	Security Update for Windows XP (KB911562)	Critical
3	MS05-043	Security Update for Windows XP (KB896423)	Critical
3	M507-019	Security Update for Windows XP (KB931261)	Critical
	The second second		1. S.



3. McAfee Conficker Detection Tool 1.0.8

網址:

 $\frac{http://downloadcenter.mcafee.com/products/tools/foundstone/conficker_detectio}{n_tool_v108.zip}$

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

C Conficker Detection Too	l - Ver. 1.0.8 - Copyrigł	nt ?McAfee, Inc. 2	009	– – X
This is a free utility For further information on	provided by McAfee, Inc the Foundstone enterpr	. to aid in the dete ise vulnerability m	ction of the Conficke anagement solution	er.b/c/e worm. a click on this image.
0 Medice	•			F5850
IPs			••••••••••	
Hostname/IP 192.168.1.10	0 ->	Start IP	EndIP	Clear Selected
Start IP 🔀 192 . End IP 🔀 192 .	168 . 1 . 1 168 . 1 . 254	192.168.1.1	192.168.1.254	Clear All
Read IPs from	file Browse			
Randomize scan order Ping before checking (no Show both infected and n Show non-responding sys Resolve IP addresses to n Send message to infected	Scan Contro response, no check) ot infected systems tems ames systems	Timeor Max. concurrent c	ut (ms) 5000 ×	
IP DNS Hos	t Name	Computer N	lame Statu	8
- Scann	ed 0/0	Infected	0	Save

A. 首先是設定掃描的範圍,介面的中間部分有一個 IPs 的區塊

Hostname/IP	192.168.1.100	\rightarrow	Start IP	EndIP	Clear Selected
Start IP	192.168.1.1		192.168.1.1	192.168.1.254	Clear All
End IP	192 . 168 . 1 . 254	Ú			
	Read IPs from file Browse]			

- 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:

Scan	Control			
Randomize scan order Ping before checking (no response, no chec Show both infected and not infected systems Show non-responding systems	k) ^s Max	Timeout (ms) . concurrent checks	5000 32	
Resolve IP addresses to names Send message to infected systems Image: Contract of the systems Image: Contract			* *	

- 1. Randomize scan order:掃描順序為隨機
- 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
- 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
C Conficker Detection Tool - Ver. 1.0.8 - Copyright ?McAfee, Inc. 2009	er.b/c/e worm.
For further information on the Foundstone enterprise vulnerability management solution	click on this image.
IPs Start IP Ind IP Hostname/IP 192.168.1.100 > Start IP End IP Start IP Ind IP Ind IP Ind IP Ind IP End IP Ind IP Ind IP Ind IP Ind IP Read IPs from file Browse Browse Ind IP Ind IP	Clear Selected Clear All
Scan Control Randomize scan order Ping before checking (no response, no check) Show both infected and not infected systems Show non-responding systems Resolve IP addresses to names Send message to infected systems	
IP DNS Host Name Computer Name Status 192.168.1.100 xfile-PC.domain XFILE-PC Not in	ifected
Scanned 97/254 Infected 0	Save

七、Conficker Worm 感染後解決方案

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

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

使用說明:

Step1. 下載 MSRT

rrosoft® afety & Security nputer Security, Digital Privacy, and Onlin	Center ^{se Safety}	United States Change All Microsoft Si Search Microsoft Security
Home Security Privacy	Family Safety Resources	Worldwide Get Support Sign Up for Newsletter
Home > Security > Malicious Software I	Removal Tool	
PC Security Security scanners, tools, and safety guin laptop, or mobile device.	Safety products and scans Viruses a lelines for your PC, Microsoft Safety Scanner Firewalk	and other malware Get online support s Security Updates
How to	□ Malicious Software Removal Tool	Email 🗏 Print 👿 Tweet (199) 🖪 Recommend (2.3k
or scan Security updates Free antivirus, antispyware program Free PC safety scan Download Malicious Software Removal Tool Online safety tips	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.	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.
+ Protect my kids from online risks	The Microsoft Malicious Software Removal Tool is an anti-malware u Windows XP, Windows 2000, and Windows Server 2003 for infections	utility that checks computers running Windows 7, Windows Vista, s by specific, prevalent malicious software—including Blaster, Sasser,
+ Protect my computer	and Mydoom—and helps remove malware and any other infections	found.
+ Protect myself from scams	any, malware was detected and removed.	oor asprays a report describing are obteome, menouning when, in
+ Protect my personal information	Microsoft releases an updated version of this tool on the second Tue The tool is available from Microsoft Update, Windows Update and th See the complete list of malicious software cleaned by this tool.	sday of each month, and as needed to respond to security incidents. e Microsoft Download Center.
+ Create strong passwords	Note: The version of the tool delivered by Microsoft Update and Wir infection is found. To run this tool more than once a month, use the Download Center.	dows Update runs in the background and then reports if a malware version on this web page or install the version that is available in the
8 Windows Buy a Windows 7 PC and get	Because computers can appear to function normally when infected, seems to be fine. You should also use up-to-date antivirus software, from other malware.	it's a good idea to run this tool regularly even if your computer such as Microsoft Security Essentials, to help protect your computer



Step2-1. 執行 MSRT,於執行中輸入「MRT」即可執行 MSRT

执行	动了积 <u>式,漆料本,</u> 女件式细胞细胞溶液。	<mark>?</mark> [X
· 開啓(<u>O</u>):	和大性式、其科交、文件式和Frankering 稱,Windows會自動開啓。 MRT	
	確定 取消 激	₹®

Step2-2. MSRT 執行畫面





```
Step2-3. 選擇掃瞄模式
```

Microsoft Windows 悉起熟世 [。] 副世 知 到	移床上具 - 2012 年 8 月
审 调税 经	
諸選擇掃描類型:	
●快速掃描。掃描系統中最 ● 骨提示您執行完整掃描。	有可能包含惡意軟體的區域。若找到惡意軟體,系統 (Q)
○完整掃描。掃描整個系統 ○時的時間。④	た。諸注意,在部分電腦上此掃描可能會需要花費數小
○自訂掃描。除了快速掃描	晶外,此工具也會掃描使用者指定的資料夾內容。(C)
選擇資料夾	
	《上一步图》 下一步图 》 取消

Step2-4. 掃瞄結果,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。

惡意程式碼	掃描結果	
Win32/Bugbear Win32/Busky	尚未感染 尚未感染	
Win32/Captiya	尚未感染	1
Win32/Carberp	尚未感染	
Win32ALeekat Win32AChir	向木感発 冶夫威迦	
Win32/Cissi	尚未感染	
Win32/Claretore	尚未感染	
Win32/Cleaman	尚未感染	
Win32/Clodpuntor Win32/Codbot	向木感発 尚未咸热	
Win32/Conficker	尚未感染	
Win32/Conhook	尚未感染	
Win32/CplLnk Win32/Cpidev	向禾感染 出土威犰	
Win32/Cutwail	尚未感染	
Win32/Cycbot	尚未感染	
Win32/Daurso	尚未感染	
Win32/Distigy	尚未感発	~
	確定	



エ具2:NOD32 EConfickerRemover

網址: <u>http://download.eset.com/special/EConfickerRemover.exe</u> 適用平台: Windows XP/Windows Vista/Windwos 7

使用說明:

Step1. 下載後無需安裝直接執行

C:\Users\xfile\Desktop\EConfickerRemover.exe		x
ESET Win32/Conficker worm remover v1.0.5.1 (Jul 16 2010 09:29:57) Copyrig 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)	ſht 〈	

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。

エ具3:SysClean-WORM_DOWNAD

網址:

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

M_DOWNAD.zip

適用平台:

Windows 2000/Windows XP/Windwos Server 2003/Windows Vista/Windwos 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

Damage Tool de	afix readine	SysciB@n		
Step2. 執行「Syscl3@	∮n _			
🥑 Trend Micro System Cleaner				
	Trend M Copyright 200 http://v	ficro System Cleaner 19-2010, Trend Micro, Inc. www.trendmicro.com		
Damage Fix reachne SysclD@n Step2. 執行「Syscl3@n」 Trend Micro System Cleaner 「Trend Micro System Cleaner 「Copyright 2009-2010, Trend Micro, Inc. Inter Micro System Cleaner 「Trend Micro, Inc. Inter Micro, Inc.				
Date: Wed_04/10/2009 Time: 11:00:00 Time Zone: (GMT-08:00)			•	
Ready				
Automatically Clean Infected Files	Scan S	top View Log Advanced	l>> Exit	





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。

	report ・ 49 度早での 加入至保證種・共用對象、 廃縣 新増資料次 臣 、 () 20120820 2012/8/20下午0 文字文件 1KB						
	_						
	đ		(CHOID)				
			-b-m				
			-				X
h report				提示 renort		01 970	
		the state where the state where where		acter op on			-
租台管理 ▼ 加入主媒	k腔恒 ▼ 共用對果 ▼ 月 2000 ^	I舔 新唱資科头	35 (72 #0	22.71	8== *		e
🗙 我的最愛	名稱	16	戊日期	頭型	大小	-	
Stopbox	20120820	20)12/8/20下午0	文字文件		1 KB	
12 收红的业主							
😭 煤體櫃							
文件 ■							
→ 音樂							
- 視訊							
■ 圖片							
■ 雷腦							
▲ 本機磁碟 (C:)							
datastorge (E:)							
● BD-ROM 光碟機							
Charles and the second s							

エ具4:Kidokiller

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

適用平台:

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

使用說明:

Stepl. 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\kuo	yuan\Desktop\kk.ex	e	Х
scanning	threads		
canning	modules in	svchost.exe	
canning	modules in	services.exe	
canning	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\k	uoyuan AppData Roaming	
scanning	C:\Users\k	uoyuan AppData Local Temp \	
scanning	Flash driv	es	
completed			
Infected job	S .	8	
Infected fil	es	С	
Infected thr	eads	9	
Spliced func	tions:	0	
Cured files:		0	
rixeu regist	ry keys:	U	
善按任音如辨	公吉		
时代工具建築	※頁		

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:

(-)[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.mspx

(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] <u>http://downloadcenter.mcafee.com/products/tools/foundstone/</u> conficker_detection_tool_v108.zip
- (七) [Malicious Software Removal Tool] http://www.microsoft.com/security/pc-security/malware-removal.aspx
- (/\)[NOD32 EConfickerRemover]
- <u>http://download.eset.com/special/EConfickerRemover.exe</u> (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