後門移除 SOP

ー・後門移除流程



後門移除 SOP 1/7 頁

二·後門檢視移除方法說明

檢視系統服務之方法:

Step1:在「我的電腦」按右鍵,選「管理」。

_				
	1			
640	<u> </u>			
2811	間間側			
0	2400 L			
	TR8			
F 10	waa waa waa			

	4-4.52			
52.	2.9.(4)			
	4 7 9:			

Step2:點選「服務」。

📮 電腦管理								
執行(Δ) 檢視(♡) ← → 🔁 📧 😰 🔂 😫 ▶ = ■>								
樹狀目錄	名稱 ∧	描述	狀態	啓動類型	登入身份			
1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	🇞 Alerter	將系		手動	LocalSystem			
	🎝 Application Manage	提供		手動	LocalSystem			
	🇞 Automatic Updates	啓用	啓動	自動	LocalSystem			
	🐉 Background Intellige	使用		手動	LocalSystem			
□ 🐺 效能記錄檔及警示	🗞 Check Point SecuRe		啓動	手動	LocalSystem			
田 🚋 共用資料夾	🗞 Check Point SecuRe		啓動	自動	LocalSystem			
	ClipBook 🗧	支援		手動	LocalSystem			
📃 🔄 🔣 本機使用者和群組	🖏 COM+ Event System	提供	啓動	手動	LocalSystem			
🖻 🖆 存放	🗞 Computer Browser	維護	啓動	自動	LocalSystem			
▲ 磁碟管理	DHCP Client	透過	啓動	自動	LocalSystem			
	Distributed Link Tra	在網…	啓動	自動	LocalSystem			
	🗞 Distributed Transacti	調整		手動	LocalSystem			
	DNS Client	網域	啓動	自動	LocalSystem			
E 版 73 久應用 住 25	🗞 DriverStudio Remote	Mana	啓動	自動	LocalSystem			
	Event Log	記錄	啓動	自動	LocalSystem			
	💫 Fax Service	幫助		手動	LocalSystem			
	💫 Indexing Service			手動	LocalSystem			
	Infrared Monitor	支援	啓動	自動	LocalSystem			
	Internet Connection	透過		手動	LocalSystem			
	IPSEC Policy Agent	管理	啓動	自動	LocalSystem			
	🔓 Logical Disk Manager	邏輯	啓動	自動	LocalSystem	-		

Step3:檢視服務名稱、顯示名稱及執行程式路徑。

Alana 四本 (本宗事業)	1 🗡
一张 倚天 前復 後在開業	
眼神谷 鲜 , a.m.m.	
\$4 4-5 社 (6) <u>25-5-</u>	
當在(D) 將於你這種等於最加強激散的使用者人電腦	
Win社式が注意① CANDEDのystem32serocks.com	
空动频和(L). [] th	◄
FB Texts Ass. (15-11)	
的可以指定堅耐多感;當然認道律堅斷服後時;這些指定的多易 會被問用。	*#
堅■\$\$\$\$(<u>M)</u> 。	
ište rate i	同島

執行步驟

後門名稱:KLGR_MSGina32

說 明

此為密碼截聽程式

檢 視

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Windows\AppInit_DLLs 的值。

* 該值的資料在正常情況下應該為 NULL (無資料),若不為 NULL,記錄該值內容中之檔案 路徑。

2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon\GinaDLL

* 該機碼在正常情況下應該不存在,若存在,則記錄該值內容中之檔案路徑。

<u>移除方法</u>

- 1. 設定 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs 的資料為 NULL (清成空白)
- 2. 刪除 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon\GinaDLL
- 3. 重新開機。
- 4. 删除 1、2 中機碼值所指向的檔案 (放在 %systemdir% 下)
- 5. 删除 regsvr.exe (放在 %systemdir% 下) PS.不一定會有這個檔案。
- 6. 更改系統上所有的密碼。

後門名稱:BKDR_RAC.A~D

檢視

服務名稱: Saes

顯示名稱: Security Accounts Events

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。

2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Saes 機碼。

3. 删除「執行程式路徑」中所指向的程式。

4. 重新開機。

檢視

服務名稱: Seae 顯示名稱: Security Accounts Event

<u>移除方法</u>

1. 點選「服務狀態:」下的「停止」按鈕。

2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Seae 機碼。

3. 删除「執行程式路徑」中所指向的程式。

4. 重新開機。

檢 視

服務名稱: SAE

顯示名稱: Security Accounts Events

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。

2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SAE 機碼。

3. 删除「執行程式路徑」中所指向的程式。

4. 重新開機。

檢視

服務名稱: Netconwork

顯示名稱: Network Connections Workstations

<u>移除方法</u>

1. 點選「服務狀態:」下的「停止」按鈕。

2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netconwork 機碼。

3. 刪除「執行程式路徑」中所指向的程式。

4. 重新開機。

<u>檢 視</u>

服務名稱: Remote Access

顯示名稱: Remote Access

<u>移除方法</u>

1. 點選「服務狀態:」下的「停止」按鈕。

2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Remote Access 機碼。

3. 刪除「執行程式路徑」中所指向的程式。

4. 重新開機。

檢視

服務名稱: WinMgts

顯示名稱: Windows Management Sessions

<u>移除方法</u>

1. 刪除 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\ 下的值: nethlpsvcs 資料: WinMgts

- 2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\ 下的值: DependOnService 資料: WinNgts
- 3. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinMgts 機碼。
- 4. 刪除 %windir%\system32\svchost.dll 檔案。
- 5. 重新開機。

後門名稱:BKDR_RAC.E

檢視

服務名稱: DhcpSvrView

顯示名稱: DHCP Client View

<u>移除方法</u>

- 1. 點選「服務狀態:」下的「停止」按鈕。
- 2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpSvrView 機碼。
- 3. 删除「執行程式路徑」中所指向的程式。
- 4. 重新開機。

後門名稱:BKDR_UMGR

檢 視

- 服務名稱: Multimedia Services
- 顯示名稱: Multimedia Services

移除方法

- 1. 點選「服務狀態:」下的「停止」按鈕。
- 2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Multimedia Services 機碼。
- 3. 删除「執行程式路徑」中所指向的程式。
- 4. 重新開機。

三. 執行後門移除程式

執行步驟

Step1:將 **AntiDoor20040108.zip** 解壓縮後,執行 **AntiDoor20040108.exe** 將開啟一個視窗,如以下畫面:

W Helds Dimit 200 Mic	
系統資料	調示結果
作業系统: Windows NT	1
版本 5.0 (Euld 2195)	
主機合解:	
P	
按學後門服務, 並自動活物 立即重新開機	
Made by ILST 行政使 [Executive Yuan]	
ELS: #() 思いていたい。 ELS: #() Els: #1 (National Information and Communication Security Taskforce)	n
技術服務中心 Information and Communication Security	

Step2:按下「搜尋後門服務,並自動清除」程式即自動進行搜尋及清除工作,並顯示結果於 右方文字框,如以下畫面:

冬時首問		Me (VAL) K	
作業系統 Várdovs NT		□F戸戸小山: Witholdwish1 版本 5.0 (Boild 2195)	
		主機名稱	
R2/4::5.0 (Build 2195)		IP:	
主播名稱		沒有發現後門服務1 12-10-10-10-10-10-10-10-10-10-10-10-10-10-	
		1993 现代在于1996 7952,目前18月1期 4996 8317 平 2996 点 24 月9日 25 25 20 月 14	
IP.		後門服務2書降成功	
		沒有說現狀門服務3	
		沒有發現後門服務4	
1077月月日日 第二日十年日		没有發現後門服務5	
196-4-1961 138 (cd. 31: 12 12 16 (cm. 16)	TE OF THE WING THE THE	被视波的服物5,日间状驱逐额行中	

Step3:清除工作完畢,需重新開機。按下「立即重新開機」重新啟動電腦。

四.後續處理

- 1. 檢查主機是否有不正常的帳號。
- 2. 變更所有帳號之密碼。
- 檢查主機上是否被安裝/開啟遠端控制程式(r_server、Terminal Service、Dameware Remote Control、VNC、PCAnywhere..);若無使用,請移除。

注意:上述服務可能被更名為其他服務名稱,檢視時請特別注意。