



# Windows 系統入侵檢測管 理流程

TACERT 臺灣學術網路危機處理中心團隊編譯

資料來源： CERT SOCIETE GENERALE

<http://cert.societegenerale.com/en/publications.html>



## 目錄

1. 準備(Preparation) .....	2
2. 確認(Identification) .....	3
3. 遏止(Containment) .....	6
4. 修正(Remediation).....	7
5. 復原(Recovery) .....	8
6. 後續情況(Aftermath).....	8

這份資安事件應變小抄，專給想要調查安全事件的網管人員。記住：面對事件時，跟著資安事件應變方法的流程，記下記錄不要驚慌。如果需要請立刻聯絡臺灣學術網路危機處理中心(TACERT)。



## 1. 準備(Preparation)

1-1. 執法調查員應該要能實際接觸可疑的系統。因為駭客可以偵測到調查痕跡，例如網路監聽，所以實際接觸會比遠端控制來的好

1-2. 為了當作法庭證據可能需要將硬碟做實體備份。最後，如果需要，切斷所有與可疑的機器接觸的網路連結。

1-3. 一台機器或是伺服器平常的網路活動知識是必要的，應該要在安全的地方保有一個記錄平時通訊埠活動的檔案，才能有效率的比較目前的情況。

1-4. 如果能具備平時在機器上運作服務的知識將會有很大的幫助。有需要時不要猶豫向 Windows 專家請求幫助。一個好意見對於機器上的服務或是執行的程序也能有所了解。

在使用者機器都是同樣的並且透過 Master CD 安裝的大型公司環境下工作會有很大的幫助。對於程序、服務與應用程式有所了解。在這樣的環境裡，使用者不被允許安裝軟體，任何額外的程序、服務與應用程式都是可疑的。

◇ 越了解一台乾淨機器的狀態，就越有機會發現一台機器裡正在執行的非法活動



## 2. 確認(Identification)

請注意 Sysinternals 疑難排解工具可以用來實行下面的任務

### ■ 不尋常的帳戶(Unusual Accounts)

尋找被新增的不尋常帳戶，特別是管理者群組(Administrators group)裡的不尋常帳戶：

```
C:\> lsrmgr.msc
```

or

```
C:\>net localgroup administrators or net localgroup  
administrateurs
```

### ■ 不尋常的檔案(Unusual Files)

在儲存裝置裡尋找不尋常的大檔案，大於 5MB 可以做為系統被置入了不合法內容的指標。

在系統資料夾裡尋找最近被加入的不尋常檔案，特別是

```
C:\WINDOWS\system32
```

- 使用”隱藏(hidden)” 屬性尋找檔案：

```
C:\> dir /S /A:H
```

- 如果可能，使用 “windirstat” (請參考[這裡](#))

### ■ 不尋常的註冊登記(Unusual Registry Entries)

在 Windows registry 裡尋找在開機時啟動的不尋常程式，特別是：



```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce  
HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
```

如果可能，使用”HiJackThis”(也會在你的啟動資料夾裡尋找，  
請參考[這裡](#))

#### ■ 不尋常的程序與服務(Unusual Processes and Services)

確認所有執行中的程度是否是不尋常或是不知名(unknown)

登記，特別使用者名稱是”SYSTEM”與”ADMINISTRATOR”  
的程序。

```
C:\> taskmgr.exe
```

(或 tlisk, tasklist 根據 Windows 版本選擇之)

如果可能，使用”psexplorer”(請參考[這裡](#))

#### ■ 確認使用者自動啟動資料夾

```
C:\Documents and Settings\user\Start Menu\Programs\Startup  
C:\WinNT\Profiles\user\Start Menu\Programs\Startup
```

#### ■ 尋找不尋常或是非預料中已安裝或啟動中的網路服務

```
C:\> services.msc  
C:\> net start
```

#### ■ 不尋常的網路活動

- 確認檔案分享與驗證每個都是與正常活動連結。

```
C:\> net view \\127.0.0.1
```

如果可能，使用”tcpview”(請參考[這裡](#))



- 尋找機器裡正開啟的網路連線

```
C:\> net session
```

- 查看機器與其它系統建立的連線

```
C:\> net use
```

- 確認所有可疑的 Netbios 連結

```
C:\> nbtstat -S
```

- 尋找在系統埠上任何不尋常的活動

```
C:\> netstat -na 5
```

(數字5 會讓他每5 秒更新一次，使用者可根據需求訂定)

使用 -o 旗誌(flag)可以在 Windows XP/2003 下看見每個程序的擁有者。

```
C:\> netstat -nao 5
```

如果可能，使用“fport” ([參考](#))

## ■ 不尋常自動化任務

尋找排程任務清單中任何不尋常的登記

```
C:\> at
```

若是 Windows 2003 或 XP:

```
C:\> schtasks
```

## ■ 瞧瞧事件檢視器是否有異樣

```
C:\> eventvwr.msc
```

如果可能，使用“Event Log Viewer” ([參考](#)) 或類似的工具。

◆ 尋找影響防火牆、防毒與檔案保護的事件，或是任何可疑



的服務

- ◆ 尋找大量的登入嘗試錯誤或是被封鎖的帳戶
- ◆ 檢視防火牆(如果有的話)記錄中的可疑活動。

### ■ 檢查 Rootkit

執行”[Rootkit Revealer](#)”、”Rootkit Hooker”、

”Ice Sword”、”[RkDetector](#)”、”SysInspector”、”Rootkit Buster”

最好能夠執行以上數個軟體，交互檢查。

### ■ 檢查惡意軟體

在全部的硬碟上執行至少一個防毒軟體，這些防毒軟體需確保是最新的。

## 3. 遏止(Containment)

如果這台機器對你公司營業活動很重要並且不能被切斷連結，備份所有重要的資料，免得駭客注意到你的調查活動而刪除檔案。複製一份系統的記憶體用來更進一步的分析。(使用像是 Memoryze, win32dd 的工具)

如果這台機器對你公司不是很重要並且可以被切斷連結，將機器關機移除他的插頭。如果是一台有電池的筆電，那就按著”off”的按鈕幾秒，直到電腦斷電。



如果線上分析沒有得到結果，就應該立刻進行離線調查。但是這台系統應該仍然是在被感染的情況下。

進行實體複製(逐位元複製)將整個硬碟複製到外部儲存裝置。可以使用 EnCase, X-WAYs, 或 dd, ddrescue 等

**嘗試找出駭客活動的證據：**

- **找到攻擊者使用過的檔案**，包含了被刪除的檔案(使用取證工具)與這些檔案用來做了什麼，至少要了解他的功能以用來評估威脅。
- **檢查最近被存取的所有檔案。**
- **檢查網路分享去看看是否有惡意軟體透過它來散播。**
- **嘗試找出攻擊者如何進入系統。**所有的線索都要考慮到。如果沒有找到電腦入侵的證據，千萬別忘記也有可能是透過實體接觸或是透過員工(共謀)竊取資料。
- **修正所有弱點(操作系統與應用程式)**，以免攻擊者使用已知的弱點。

#### **4. 修正(Remediation)**

**假使系統已經受到感染了：**





- 暫時移除所有有牽涉到此事件的帳戶。
- 移除所有攻擊者安裝的惡意檔案

## 5. 復原(Recovery)

不論駭客侵入系統到什麼程度以及你對於感染了解多少，只要系統被滲透過了，最好的方法就是用原始工具重新安裝系統，然後在新系統上安裝所有的補丁。

假使這個解決方法不能採用，那你應該：

- 改變所有系統帳戶的密碼，確保你的使用者們會遵從下列的安全方法：他們的密碼應該含有大小寫字母、特別字元、數字且至少 8 個字元。
- 復原所有檔案，復原那些已經被攻擊者改變過的檔案(例如 svchost.exe)

## 6. 後續情況(Aftermath)

### 報告

下列的主題應該要記錄下來：

- 初步檢測
- 每個重要事件的行為與時間軸
- 什麼是適當的行為



*Taiwan Academic Network Computer emergency Response Team(TACERT)*

- 什麼地方出了問題
- 事件成本

資料來源：**CERT SOCIETE GENERALE**

<http://cert.societegenerale.com/en/publications.html>

