# 系統管理員的急救包

你察覺你的伺服器上有隻病毒、或是你發現有不知名的 ID 在你的區網中但你卻無法刪除它們、或是網路日誌告訴你有人連線到財務主管的電腦且拷貝了主要財務報表、或是有位駭客寄電子郵件跟你說他們擁有你的信用憑證資料庫。這些案例任何一件都足以讓你事情大條。當這些事情已經發生了或是發現駭客們正在進行中，一定要保持冷靜且遵守正確的步驟來處理。

在我們的 First aid kit for sys admins 中，我們會教你面對一個被駭的系統、受感染的工作站、不懷好意的網路服務或是其他的緊急事項時該如何處理，這種狀況遲早都會發生在我們身上。以下有八個步驟來應付所有的緊急事件。

1. 不要驚慌
2. 了解狀況
3. 與其他組員保持聯絡
4. 將傷害降到最低
5. 採取適當的回復步驟
6. 針對狀況來做適當的回應
7. 記取教訓
8. 保持冷靜且小心操作

# 惡意程式的感染

即使是大公司也需要安裝防毒措施在他們的伺服器和工作站上，以防遇到惡意程式的感染。當你遇到零時差攻擊、過時的病毒資料庫、或是為了系統執行速度而關掉防毒軟體時，不管是哪一種網路都會因此而受到惡意程式的感染，且我們還沒提到夾帶在電子郵件中的或是隱藏在 USB 隨身碟中的惡意程式。微軟公司訂出六個步驟來讓大部分的公司可以應付這些危險狀況。

- 確認感染

並不是每次電腦只要怪怪的就一定是因為中毒了。可以透過防毒軟體來掃描或是預備開機硬碟來確認系統是否中毒了。如果無法 100%確定，那還是謹慎一點。

- 控制感染狀況

把系統的網路關掉。拔掉網路電纜、或是關掉 WI-FI 裝置，然後把系統關機直到你可以用安全的方式來開機作往後的處理。我們都不希望病毒去毀掉電腦上更多的資料或是散播到區往中的其他電腦或是寄發垃圾郵件。

- 確認處理步驟的方向

許多資訊部門的專家為了以防萬一，都希望採取清空整個系統來避免更多的傷害，而不想冒險只去清除受感染的檔案。但是硬碟中或許還存有重要的資料需要有人去備份。如果這個系統被格式化之後我們就無法重建了，那麼我們就需要好好考慮是否要整個清空或是先做備份。

- 嘗試清理系統

如果受感染的系統無法連上網路，那就要使用隨身碟或其他有安裝防毒軟體的媒體來做安全的開機。有些防毒軟體可以製作預備用的開機磁碟來清理受感染的系統，所以務必要小心選擇開機方式。要確定我們可以靠著安全的方式來開機，這樣才不會再度啟動那些已經受到感染的應用程式。

- 經常做還原點的儲存

如果你無法保證能把系統清理乾淨，但是你卻有作完整的還原紀錄。那就根據之前的還原紀錄來作系統還原。

- 重新建立系統

如果你無法清理乾淨或是還原，那麼你別無選擇只好從頭把系統重新建立起來。先備份重要資料，再把整個系統完全格式化後再作安裝。

- 記取教訓

解決問題後。找出一開始惡意程式之所以會穿越我們的防禦的原因，把我們的缺陷記錄下來然後減少以後再度發生的可能性。

你可以去仔細閱讀微軟的完整文章，裡頭有詳細的步驟，你可以下載有用的支援工具。你甚至可以了解如何去製作 windows 7 的開機用 USB 硬碟。

## 支援工具

以下是幾種有用的工具來幫助你處理受感染的系統。

- PsTool

這個軟體可以幫助你確認目前正在執行的程序，最重要的是它可以幫你停止那些你不想要卻又關不掉的程序。

- Netstat

這個方法或是有點傳統，但是使用 netstat 來確認哪些程序正在使用網路是最有效率的。

- What Process

這個網頁上有個相當有用的資料庫，可以讓你知道現在 windows 中所執行的那麼多程序的細節。

# 密碼破解

有很多方法可以去破解密碼，而且有些方法並不需要特殊的技術。使用者會把密碼寫下來、或是分享給其他人知道、或是選用簡單好猜的密碼。密碼破解軟體、鍵盤側錄程式和監聽未加密的流量都是使用者密碼的敵人。如果其中一名使用者知道其他人的密碼，那麼其他人將會失去他們的帳號保護能力，且將會處於隨時都會有人去擷取他們不應該知道的資料。以下為如何應付的步驟：

- 強迫所有可能有影響力的使用者去更改他們的密碼

可以在 AD(Active Directory)裡面去做相關的簡單設定，讓使用者再下次登入時強迫更改密碼。

- 訂定嚴謹的密碼設立規定

微軟公司強烈建議這項作法，嚴謹的密碼規則也一樣可以在 AD 裡面設定。

- 提醒使用者安全的密碼保護政策

這會需要更多的教育訓練手段，而不是口頭上的提醒。

- 考慮訂定登入審核方式來預防同樣的事情未來再度發生

微軟公司提供了如何執行的方法

# 支援工具

- 帳號鎖定工具

這種類型的工具包括 Event Log Parser、EventCombMT.exe 和其他可以用來找出哪個網域控制程式正在鎖定程序的工具，這讓我們可以找出惡意的來源。

- 如何設定嚴謹的密碼

使用簡單的步驟來幫助使用者訂定一個嚴謹又好記的密碼。

- KeePass

這是許多好用的開放原始碼的密碼工具之一，它可以讓使用者不再需要把密碼寫在紙上，它可以重複使用同一個密碼再不同帳戶卻又不影響安全性。

# 網頁破壞

這種情況就像是有人在你家的牆壁上畫上塗鴉，不過卻讓全世界都看的到。你會希望自己的網頁可以越快回復到正常狀態越好，不過你也希望這種情況不要再度發生。

- 將網頁伺服器離線且先暫時放上”維護中”的頁面來讓你的顧客們知道這很快就會回復正常。
- 對你的網頁執行弱點掃描來知道駭客們是如何在一開始就入侵你的系統的。
- 修復所有的漏洞且執行尚未安裝的更新檔。
- 從備份檔中來回復你的網頁內容。
- 回復到正常狀態後，在重新上線之前再重新掃描一次你的系統。
- 讓所有組員了解入侵事件的發生原因，讓下次再度發生的機率降低。

## 支援工具

- Wget

一個用來監控網頁的優秀命令列工具。它可以擷取你的網頁的所有狀態內容。

- Site 24x7

它不只可以用來監控你的網頁服務，還可以再你的網頁內容有所改變時警告你。

- Google Webmaster Tools

使用這些 Google 的免費工具來掃描你的網站以防惡意程式或其他的攻擊方式。

# 重要資料的未授權存取

不管是其中一個內部使用者再到處探聽或是一個駭客想對你的網路取得連線而想要竊取資料，當重要資料遭到未授權存取時，你需要快速且完整的做出應對。在某些案例中，你也需要依賴司法的力量。

- 確認哪些資料被存取過。使用連線的日誌來找出來些資料已經被看過、拷貝過或是更改過。

- 確認哪些資料被存取過之後要立刻做出應對。開放式的 FTP 伺服器、點對點的軟體、授權不嚴謹的網頁或是開放分享式的內部網路就可以讓駭客輕易利用漏洞來取得連線。

- 與資料負責人和擁有主要授權的主管一起討論並確認自己的發現。

- 確認哪些資料已經被駭客釘上了。如果已經被駭客存取過，就一定是有惡意的意圖。如果是被員工存取，就要向人力資源部門確認其相關意圖。

- 向你的法律顧問確認是否需要通知客戶、消費者或控管機構

- 掃描自己的網路確認其他事件中是否有相同的事件會造成未授權的連線，然後解決這些問題。

## 支援工具

- Logparser

這個強大的日誌探勘工具可以幫助你來監控、比較各種不同的日誌格式

- Cacls

這個工具可以拷貝或更改檔案系統的連線控制清單。

# 惡意 DNS 主機

這是有可能發生在大型組織最糟的情況之一，因為這代表了駭客可以間接看到你的所有電子郵件、網頁瀏覽紀錄和其他網路流量。因為這種情況在組織中影響可大可小，如果有駭客入侵了你的 DNS 主機，重要的是你要能隨時注意且快速應變。

- 立刻聯絡你的網路服務供應商或是註冊人員，馬上把 DNS 紀錄中未被授權的連線斷掉。
- 從你的備份中回復檔案
- 對於所發生的情況要公開且坦承通知你的客戶和廠商讓他們可以小心的預防接下來可能會發生的危險情況
- 確認這些未被授權的連線是如何發生的。是因為密碼被猜透、或是駭客用新的信用憑證重設系統來入侵信箱、或是寄送一封更改密碼的釣魚郵件？一旦發生了，要馬上採取正確的應對，以確保以後不會再度發生。

## 支援工具

- Dig for Windows

比 nslookup 還要功能強大

- DNS Stuff

一個網路上專業的 DNS 工具包

- DNS Lint

一個優秀的 DNS 診斷和測試工具，針對 AD 伺服器或其他目的

# 註冊碼破解

註冊碼的破解會讓使用者花很少的錢但卻讓相關公司損失數萬塊的成本來修復。當使用者安裝了某個軟體但卻沒有它的註冊碼，這樣就會讓相關公司陷入險境之中。

- 立刻解除安裝所有未被授權的軟體
- 如果使用者是透過網路來找到相關軟體，立刻關閉這種網路分享。
- 可以向相關公司索取軟體的註冊碼
- 訓練使用者有關使用合法軟體的重要性，然後訓練使用者用正確的方式來取得軟體註冊碼。

# 遭竊的硬體

硬碟竊取狀況需要公司撥一筆不小的數目納入預算項目中，但是這種狀況的發生可能會數個禮拜甚至數個月都不會被發現。維護一個完整、精確和通用的硬碟資產是非常重要的。在一個安全的封閉房間內安裝適當的安全伺服器，使用安全的電纜來讓終端機使用網路，而且確保使用者簽署保證書來確定他們會保管辦公室中的硬碟設備來減少損失

- 確保硬碟資產的購買能夠完整，包括註冊碼，還有確保硬碟資產的負責。
- 訓練使用者在車上或旅行時安全的使用桌上電腦、攜帶儲存硬碟和其他硬碟。
- 公佈有關硬碟竊取的法律制裁項目
- 確保所有硬碟媒體是有加密的來避免硬碟竊取後的資料遺失
- 鼓勵使用者使用背包或其他不明顯的方式來攜帶筆記型電腦，避免讓公司商標顯露來吸引他人的注意

# 結論

當然，預防勝於治療。在網路上使用適當的工具來更新你的系統，使用防毒軟體，經常執行安全掃描且維護，這樣至少可以預防大部分這份報告中提到的狀況。

*原文出處：GFI（CERT 譯）*
*http://landlanss.gfi.com/ebook-first-aid-kit?adv=62&loc=83*