預防間諜程式及其他不明軟件指南

簡介

大部份使用者都意識到病毒或蠕蟲可造成的衝擊，所以他們都會有措施去保護他們的電腦，例如使用防毒程式。但是，間諜程式及其他不明軟件通常都被忽略。這些程式靜靜地躲藏在系統上盜取資料，它們比病毒及蠕蟲難以發現，所以，實際的感染數字一定比報告的數字更大。

根據香港電腦保安事故協調中心(HKCERT)於 2005 年收到的事故報告統計，有 880 個報告是關於間諜程式感染，這個數字是比病毒或蠕蟲感染的數字爲高(圖 1)，顯示間諜程式變成另一個電腦系統的顯著的保安威脅。

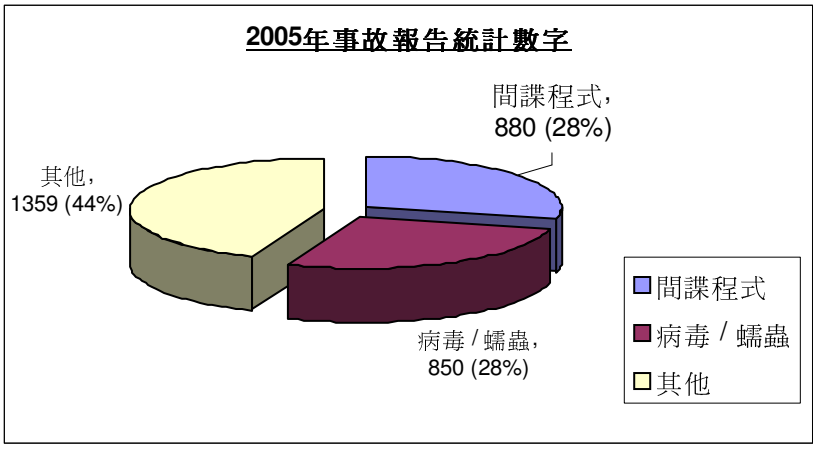

圖 1：HKCERT 2005 年事故報告統計數字

甚麼是間諜程式及其他不明軟件?

間諜程式及其他不明軟件(間諜程式及 PUS)是一些在未知會你或者未經你的同意的情況下被安裝的不明軟件，可能會帶來資料洩漏的威脅。它們與病毒或蠕蟲不同，病毒或蠕蟲會施展廣泛攻擊及對主機和網絡造成明顯的損害，間諜程式及 PUS 有時只會靜靜地隱藏在你的電腦，而且不易被系統保護程式如防毒程式偵測到。

間諜程式及 PUS 的主要功能是收集電腦或開放式網絡上的資料，然後透過網絡或互聯網傳送給第三者。這些資料可能是在你的硬碟內的檔案或個人資料如你在網上銀行網站輸入的登入名稱及密碼。

間諜程式及 PUS 的種類及威脅

「間諜程式及 PUS」其實是**惡意程式**的其中一類，它通常包括兩類程式：廣告程式及資料盜取程式。

廣告程式

廣告程式是一個套裝軟件，一旦它被安裝於你的電腦，便會在你的熒幕上自動顯示廣告資料，它不時會向你傳遞廣告訊息，並可能會收集你的網上瀏覽習慣的有關資料。有些廣告程式(瀏覽器騎劫程式)甚至可能改變你的瀏覽器設定如 Internet Explorer 的預設首頁及預設搜尋引擎，所以，瀏覽器可能會自動重新導向到你沒有打算瀏覽的網頁。另外，依附著廣告程式的幕後程式可能會消耗很多系統資源及網絡頻寬，最後，受感染的電腦的生產力可能會減低。

資料盜取程式

資料盜取程式是一個在未得你的同意下被安裝在你的電腦上的惡意程式，然後透過網絡如互聯網，把資料從你的個人電腦傳送給第三者，它可以帶來以下的威脅：

1. *資料洩漏*
   資料盜取程式會在受感染的電腦系統尋找「有用的」資料，它可以是任何檔案或程式，如業務計劃、原始碼、財務紀錄、在你的地址簿內的電郵地址及其他受版權保護的資料，這些被選取的資料可以透過內聯網或互聯網秘密地傳送給其他人。

2. *鍵盤輸入記錄及熒幕資料攫取*
   這可以是另一種資料洩漏，資料盜取程式的鍵盤輸入記錄功能可以記錄你的所有鍵盤輸入。被記錄的資料(如你在網上銀行輸入的登入名稱及密碼)可以在你不知情的情況下被傳送給第三者。雖然一些網上交易網站採用了動態鍵盤輸入，但是有些程式可以攫取網頁熒幕，然後紀錄鍵盤的輸入位置。

3. *中間人攻擊*
   中間人攻擊是可以允許攻擊者讀取、插入及更改訊息的攻擊。寄件者及收件者雙方都可能沒有察覺通訊管道的交通被第三者程式(有時叫作代理伺服器程式)偷看或攔截，攻擊者亦可以重播數據傳送過程而竄改部分數據，破壞資料的完整性。

間諜程式及其他不明軟件的來源

間諜程式及 PUS 可從多個途徑進入你的電腦，以下是其中一些令你的電腦受感染的方法。

- *附載於來歷不明的免費軟件或共享軟件*
  免費軟件及共享軟件如遊戲、熒幕保護程式及 P2P 客戶端可以容易地從互聯網下載，或從電腦商場派發的免費 CD-ROM 取得。多數人都沒有留意安裝的程式，在安裝時又沒有小心地閱讀使用者授權協議(EULA)，這樣給附載的惡意程式包括間諜程式及 PUS、病毒及蠕蟲有機可乘，「合法地」進入你的電腦，然後進行一些有害的行動。

- *僞冒的反間諜工具*
  一些程式聲稱有偵測及移除間諜程式及 PUS 的功能，但事實上，它們正是間諜程式及 PUS。在安裝後可能不停地要求你付款以提供一些功能，而且沒有任何正常的途徑去移除那些程式，其中一個聲名狼藉的例子是 SpyAxe。

  如欲知道可能是僞冒的反間諜工具，請瀏覽：
  http://www.spywarewarrior.com/rogue_anti-spyware.htm#products

- *安裝有害的瀏覽器協助物件或 ActiveX 元件*
  瀏覽器輔助物件 (BHO) 是一些爲了延伸瀏覽器功能而插入的元件，在開啓一個新的瀏覽器時載入，Yahoo 及 Google 工具列是 BHO 的例子；ActiveX 元件允許跨網絡(如互聯網)執行程式，ActiveX 技術使微軟電腦系統之間互相運作可行，例如在微軟 Internet Explorer 開啓 Word 或 PDF 文件和從遠端位置存取使用者硬碟內的資料。

本來設計它們的原意是好的，但是，一些惡意的人以這些功能的優點去發展間諜程式及 PUS，從安裝了惡意程式的使用者中得到好處。

- *彈出式視窗內的誤導選項*
  一些網站會使用彈出式的視窗去顯示服務或產品的廣告，這些彈出式的視窗邀請使用者訂閱或購買產品，它們通常會給「是」或「否」按鈕予使用者選擇。但是，在多數情況下，點擊其中任何一個按鈕都會有相同的效果，去允許間諜程式及 PUS 安裝於你的電腦。

- *在共享網絡內的病毒及蠕蟲*
  病毒及蠕蟲可以在家中或公司的網絡內快速傳播，所以，它們可以攜帶間諜程式及 PUS 或以代理身份去下載間諜程式及 PUS。如果你的電腦沒有足夠的防禦去對抗病毒及蠕蟲，被攻破的機會會相對地提高。這類攻擊的一個知名例子是 TrojanDownloader 及它的變種。

- *執行電郵附件或即時通訊器的有害的檔案*
  駭客可以模仿你的朋友或公司同事的身份，用電郵傳送間諜程式及 PUS 附件。你可能會容易地相信寄件者，開啓電郵附件，然後執行間諜程式及 PUS。幸好，大部份電郵伺服器所採用的電郵過濾服務發展成熟，可以減低這類攻擊的機會。

  另一方面，即時通訊器如 ICQ、MSN、Yahoo Messenger 越來越普及，但現時它們的保安仍然不足，這樣可能會導致電腦系統透過這些工具而感染惡意程式。

> 注意：
> 一旦間諜程式及 PUS 安裝在你的電腦，它們會確保在系統連線時能夠運作。它們可以當作啓動程式載入或與其他啓動服務或應用程式整合。所以，知道間諜程式及 PUS 的來源可以減低受感染的機會。

受感染電腦的徵狀

受感染的電腦可能有以下的徵狀：

1. 瀏覽器的預設首頁被改，不能被重設，又或者在重新設定後仍然顯示相同的網頁。
2. 瀏覽器被加入新的工具列、菜單或按鈕。
3. 「我的最愛」被加入可疑的網上連結或資料夾。

4. 彈出式的廣告視窗或陌生的對話盒不時出現。
5. 瀏覽器帶你到另一個網站，而不是你在網址欄位輸入的網站，例如它重新導向你到一個滿有市場資料的搜尋引擎。
6. 控制台的「新增/移除程式」列出不明的程式或在工作列不明的圖示，例如日歷或天氣資料。
7. 系統明顯地比正常慢，啓動時間亦較長。
8. 即使系統閒置，受感染電腦的往來網絡交通明顯地增加。

預防措施 / 良好習慣

1. *安裝反間諜程式*

   互聯網上有很多反間諜程式，有一些是免費，有一些則是收費的，以下列出電腦保安專家建議的三個免費常用的工具。

名稱 / 下載連結 Name / Download Link	**平台 Platform**
Windows Defender (Beta 2) http://www.microsoft.com/	視窗 2000(SP4)/XP(SP2)/2003(SP1)
Ad-aware SE Personal Edition http://www.lavasoft.de/	視窗 98/Me/NT/2000/XP
Spybot Search & Destroy http://spybot.safer-networking.de/	視窗 98/Me/NT/2000/XP

有關其他可信的反間諜產品，可瀏覽以下網址：
http://www.spywarewarrior.com/rogue_anti-spyware.htm#trustworthy

新的間諜程式及 PUS 不時被發現，故此應該定期更新定義檔(通常反間諜程式可自動更新)，確保即時保護處於啓動狀態及每星期最少掃瞄一次。

2. *安裝防毒程式*

   由於有些間諜程式及 PUS 透過病毒感染電腦，你的電腦應該安裝防毒程式及定時更新最新的病毒定義檔。

你可於 HKCERT 網站檢閱防毒程式試用版的列表：
http://www.hkcert.org/chinese/relinks/usefultoolcontent.htm
另外，HKCERT 的病毒預防指南可於以下網址下載：
http://www.hkcert.org/chinese/sguide_faq/sguide/secguide02.html

3. *定時更新操作系統及軟件*

   當相關的修補程式被發佈時，應爲操作系統及軟件進行更新，減低黑客利用已知的漏洞操控你的電腦的危機。

微軟 Windows update 可瀏覽下列網址：
http://windowsupdate.microsoft.com/

4. *使用個人防火牆*

個人防火牆就像你的電腦的護衛員，它可過濾經由互聯網嘗試進入你的電腦的惡意交通。微軟視窗 XP (SP2) 已預設開啓了 Windows 防火牆。

ZoneAlarm 是另一個支援其他版本的視窗的防火牆程式：
http://www.zonelabs.com/store/content/home.jsp

5. *確保你的瀏覽器達到安全性層級*

確保瀏覽器的網際網絡區域的安全層級設定最少爲「中安全性」(或「預設層級」)以避免不必要的或惡意的程式被自動下載(圖 2)。另外，要封鎖彈出式視窗(微軟稱爲「快顯視窗」)，這樣可以阻止多個廣告視窗同時顯示(圖 3)。

圖 2：微軟 Internet Explorer 的網際網路安全性層級設定

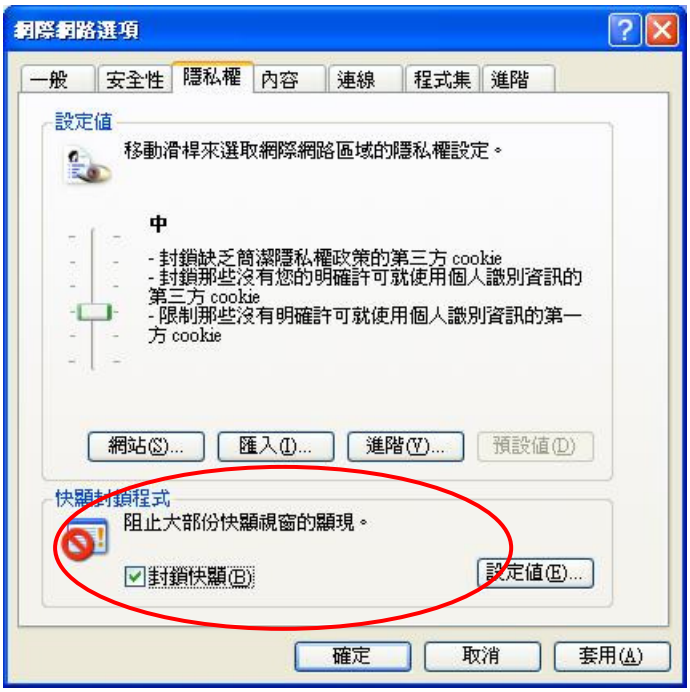

圖 3：微軟 Internet Explorer 快顯封鎖程式設定

(注意：其他瀏覽器的設定請參考相關供應商之使用者手冊。)

6. 安全地瀏覽互聯網

(i) 要關閉彈出的廣告視窗，要點擊右上角的「X」或同時按下鍵盤上的「Alt」及「F4」，不要點擊視窗內的連結或按鈕(即使是看似「X」或標記「否」的按鈕)，因爲它們可能是欺騙你去安裝不明的程式。

(ii) 留意安全警告，特別是在下載檔案或安裝 ActiveX 元件時和那些標記著「沒有簽署」的警告視窗(圖 4)。

圖 4：安全性警告視窗

(iii) 在下載或安裝任何軟件之前，特別是免費軟件及共享軟件，要小心地閱讀使用者授權協議(EULA)。如果 EULA 是難以找到或難以明白，你應該認真考慮是否安裝那個軟件。

7. *小心提防電郵附件或來自即時通訊器的檔案*

在互聯網上冒認身份是非常容易的，即使是所謂「你的朋友」傳送檔案給你，也不要輕易開啓。如果必須開啓檔案，建議先利用防毒及反間諜程式掃瞄它們，然後才執行。

參考(技術性文章)

1. *Spyware (US-CERT)*
   http://www.us-cert.gov/reading_room/spywarehome_0905.pdf
2. *The Spyware Epidemic: Dealing With "Legal" Malicious Code (Aladdin Knowledge Systems)*
   http://www.ajoomal.com/descargas/aladdin/esafe/esafe_spyware_wp.pdf
3. *Spyware: an annoying and dangerous problem you can eradicate (Secure Computing)*
   http://www.securecomputing.com/pdf/SpywareSC-TP.pdf
4. *Stopping Spyware at the Internet Gateway: Lessons from Real-World Spyware Attacks (CP Secure)*
   http://www.ccl.co.uk/downloads/Stopping-Spyware-At-The-Internet-Gateway.pdf

參考(網站)

1. *Microsoft Security at Home: Spyware*
   http://www.microsoft.com/athome/security/spyware/
2. *Anti-Spyware Coalition*
   http://www.antispywarecoalition.org/
3. *Stopbadware.org*
   http://www.stopbadware.org/
4. *Spywaretesting.org*
   http://www.spywaretesting.org/metadot/index.pl
5. *Preventing Spyware From GetNetWise*
   http://www.truste.org/articles/preventing_spyware.php
6. *Anti-Spyware Guide*
   http://www.firewallguide.com/spyware.htm
7. *Rogue/Suspect Anti-Spyware Products & Web Sites*
   http://www.spywarewarrior.com/rogue_anti-spyware.htm
8. *Spyware (From Wikipedia, the free encyclopedia)*
   http://en.wikipedia.org/wiki/Spyware