

隱形資訊竊匪：間諜軟件

間諜軟件已經成爲了現今互聯網上最危險和最普遍的威脅之一。全球三分之二的電腦已被植入各種間諜軟件，大部分電腦甚至被安裝了不只一種間諜軟件，但不少用戶卻懵然不知；而平均每部電腦因間諜軟件而導致的經濟損失高達三百美元。

間諜軟件入侵渠道千變萬化

間諜軟件是任何在電腦上安裝元件，企圖記錄互聯網瀏覽活動的軟件，通常都是在未經使用者許可或明確認知的情况下安裝到使用者的機器中。

間諜軟件的入侵渠道千變萬化，除了上網瀏覽外，還會隨著「免費程式」、「共享程式」一起下載（例如 P2P 軟件、軟件破解程式），又或者透過通訊媒介中的網站連結（例如 ICQ、電子郵件訊息）入侵。

黑客借間諜軟件偷取用戶資料

間諜軟件通常在背景中執行，沒有安裝任何防毒軟件的使用者初期完全不會察覺它們所進行的活動。黑客會利用間諜軟件偷取用戶的各種機密資料，例如登入名稱、密碼、銀行帳號、信用卡號碼或公司業務數據等。黑客甚至會盜用使用者的身份，開立他們「自己」的帳戶去進行詐騙活動。使用者除了蒙受龐大的金錢損失外，更可能會犯上官非。

如何判斷是否已被植入間諜軟件？

- 不斷跳出廣告
- 桌面或瀏覽器設定被更改，且無法恢復爲原來的設定
- 瀏覽器中出現未曾安裝的軟件
- 電腦效能變得很慢
- 程式經常異常終止

如何提防間諜軟件？

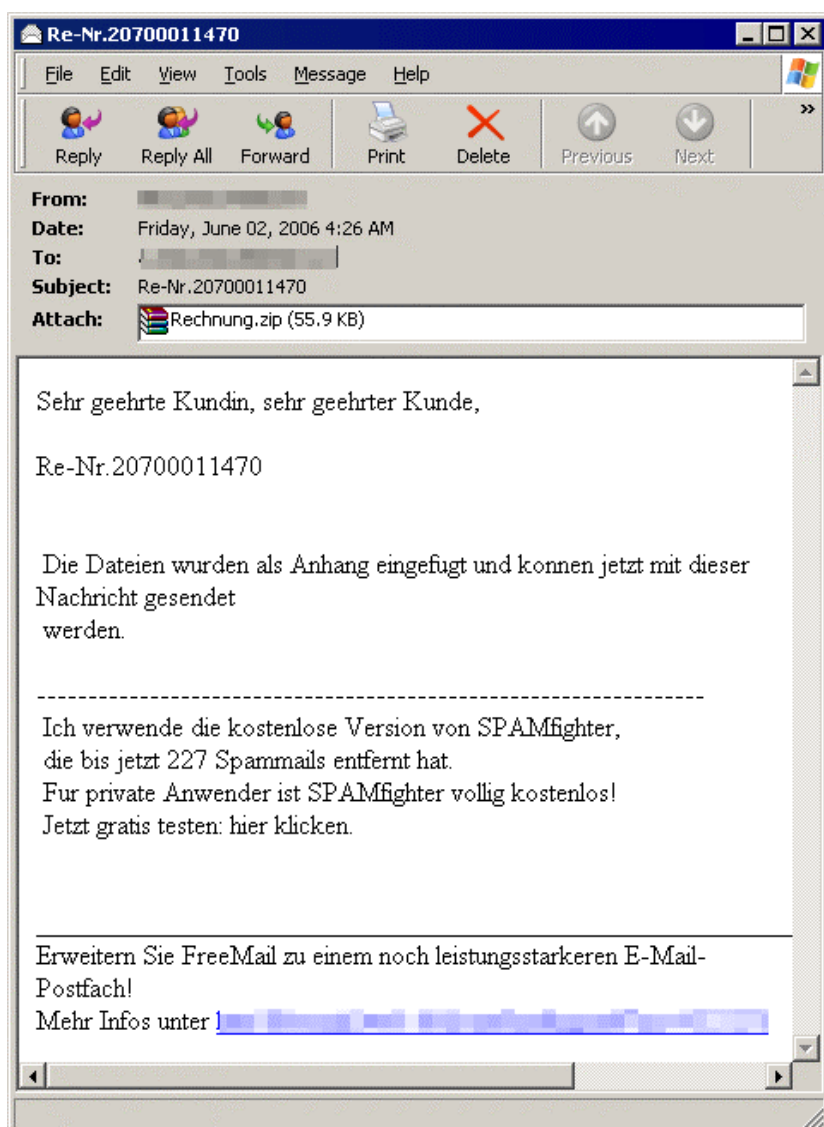
如果使用者懷疑電腦藏有間諜軟件，可以使用免費線上工具掃描及移除間諜軟件或病毒。使用者也應不時留意有關最新間諜軟件的公佈，提高警覺加以防範：

以下是保護電腦避免間諜軟件攻擊的建議：

- 1) 定期更新作業系統與瀏覽器，安裝最新的安全修補程式
- 2) 遵行電腦使用安全守則
- 3) 安裝具有反間諜功能的防毒/安全軟件，並更新至最新的病毒碼檔案



圖：間諜軟件透過電郵植入電腦



參考網址：

掃描及移除間諜軟件或病毒之免費線上工具：

<http://housecall.trendmicro.com/>

有關最新間諜軟件的公佈：

<http://www.trendmicro.com/vinfo/grayware/default.asp>

鳴謝資料提供：趨勢科技有限公司及怡和科技(香港)有限公司

©2006 版權為恒生銀行有限公司所有。

如若轉載本文，不論全部或節錄，均請註明來源。



恒生銀行
HANG SENG BANK



理財創富 專注為你