[請即發布]

Avira 警告用戶注意 Windows 的資訊安全漏洞

網路罪犯濫用所有 Windows 版本中的資訊安全漏洞，在電腦中植入惡意程式碼

2010 年 7 月 26 日，香港/台灣報導- 在 Windows 作業系統中目前有一個資訊安全漏洞，攻擊者可以濫用此漏洞混入病毒。 IT 資訊安全專家 Avira 警告，這足以開啓特別準備的 USB 裝置或其中包含 Windows 檔案總管操作連結的資料夾，Avira 的資訊安全軟體能保護您避免此威脅。

對於所有支援檔案連結的 Windows 作業系統，Microsoft 發佈了一項資訊安全公告有關處理檔案連結 (.lnk 檔) 中的資訊安全漏洞，不過，殲滅此資訊安全漏洞的更新尚未公佈。 該公司目前只提供停用 Windows 服務以及處理有缺陷的 .lnk 檔的常規操作的指導，對大多數用戶來說顯現太複雜的程序，並且有機會因爲一個小錯誤而造成系統無法使用的風險。 此外，啓動功能表和快速啓動功能表會在完成程序之後爲所有程式顯示標準圖示，這會明顯降低可用性。

Avira 的產品經理 Thorsten Sick 建議使用最新的防惡意程式碼軟體： 「Avira 利用啓發式分析偵測和阻止惡意程式碼濫用資訊安全漏洞，避免用戶遭遇這項威脅。 Avira 在此提供主動式防護避免用戶受此資訊安全漏洞所威脅，用戶無需爲此作特殊的病毒定義更新。」Avira 分別偵測這種惡意程式碼爲 EXP/CVE-2010-2568.A 和 EXP/CVE-2010-2568.B。

這個資訊安全漏洞起初爲特洛伊木馬程式濫用，Avira 偵測此程式爲 RKit/Stuxnet.A。 此程式可以透過 USB 裝置傳播， 而惡意程式碼利用 Windows 檔案總管開啓 USB 裝置，進而啓動惡意程式。 同時，網際網路上還有「概念證明」程式碼，網路罪犯可以將此程式碼輸入自己的惡意程式碼，以濫用資訊安全漏洞。 在未來幾天很可能會有更多的惡意程式碼出現，濫用這個資訊安全漏洞。

具備基本保護能力的 Avira AntiVir Personal 能偵測並阻止危險的惡意程式碼。 Avira AntiVir Premium 提供您更好的保護， 整合的 WebGuard 和 MailGuard 甚至能在惡意程式碼感染網頁瀏覽器或郵件程式之前先封鎖惡意程式碼。 Avira Premium Security Suite 也能保護用戶免受這些威脅，另外還包含防火牆、家長監控和備份解決方案 - 讓用戶能夠恢復重要的資料。

關於 Avira

Avira GmbH 爲全球領先的資訊科技安全方案供應商，產品廣泛應用於專業及個人領域。Avira 擁有超過二十年的網上防護經驗，是業界首屈一指的先驅。作爲宣揚「資訊安全，德國製造」的基礎成員(ITSMIG e.V.)，Avira 承諾提供能有效杜絕資料外泄的資訊安全產品。

德國資訊科技安全專家 Avira 總部設於波登湖畔的 Tettnang 市，並於世界各地設立多間辦事處。Avira 擁有超過 330 名員工，透過 Avira AntiVir Personal 的免費防毒保護，爲超過 1 億個人用戶的網絡安全作出貢獻。

Avira 的本地及國際用戶包括全球知名的上市公司、中小企、教育學府及政府機關。Avira 不但致力確保虛擬環境的安全，並成立奧厄巴赫基金（Auerbach Foundation），全力支持藝術、文化和科學等領域的慈善及社會項目，爲現實世界提供更大的保障。

傳媒查詢請聯絡：
吳加琪
Avira Ltd.
電話：2297 2284
傳真：2297 2215
電郵：amy.ng@avira.com