**有關電腦網路威脅的有用資訊**

**蔡明朗譯**

描述可能攻擊電腦之威脅類型的用語，通常令人感到困惑。以下是您將會在我們的報告中找到的威脅類型快速清單。您也可以在賽門鐵克安全機制應變中心[線上詞彙](http://www.symantec.com/zh/tw/norton/security_response/glossary.jsp)中找到更多有關安全詞彙的資訊。

* **偷渡式下載**：偷渡式下載是一種電腦代碼，會利用 Web 瀏覽器中的軟體錯誤，讓瀏覽器依照攻擊者的意願執行動作，例如執行[惡意程式碼](http://www.symantec.com/zh/tw/norton/security_response/malware.jsp)、損毀瀏覽器或讀取電腦的資料。無法阻擋瀏覽器攻擊的軟體錯誤又稱為[漏洞](http://www.symantec.com/zh/tw/norton/security_response/vulnerabilities.jsp)。
* **網路釣魚攻擊**：當攻擊者冒充來自受信任的公司來顯示網頁或傳送電子郵件時，就表示發生[網路釣魚](http://www.symantec.com/zh/tw/norton/security_response/phishing.jsp)攻擊。 這些網頁或電子郵件會向不知情的客戶索求敏感資訊。賽門鐵克安全機制應變中心於[此處](http://www.symantec.com/zh/tw/norton/security_response/phishing.jsp)提供有關網路釣魚的詳細資訊。
* **間諜軟體**：間諜程式是一種軟體封裝，能夠追蹤個人可識別資訊或機密資訊，並傳送給第三方。請造訪我們的「間諜程式主題中心」與[「間諜程式」](http://www.symantec.com/zh/tw/norton/security_response/spyware.jsp)區段 (在[「病毒與風險」](http://www.symantec.com/zh/tw/norton/security_response/index.jsp)區域中)。
* **病毒**：[病毒](http://www.symantec.com/zh/tw/norton/security_response/index.jsp%20)是一種惡意程式碼 (又稱為[惡意軟體](http://www.symantec.com/zh/tw/norton/security_response/malware.jsp))，通常是由其他電腦透過電子郵件、下載和不安全的網站來散播。 請參閱「惡意軟體主題中心」以取得更多詳細資訊。
* **以啟發式技術偵測到的病毒**：使用啟發式技術偵測到的[病毒](http://www.symantec.com/zh/tw/norton/security_response/index.jsp%20)是根據病毒本身表現出來的惡意行為而找到的。 這些行為可能包含嘗試竊取密碼或信用卡號碼之類的個人敏感資訊。
* **病蟲**：病蟲是另外一種惡意程式碼 (又稱為[惡意軟體](http://www.symantec.com/zh/tw/norton/security_response/malware.jsp))，主要目的是要散播到其他容易受到攻擊的電腦系統中。它通常是透過電子郵件、即時訊息或其他服務來傳送本身的複本，以散播到其他電腦中。請參閱「惡意軟體主題中心」以取得更多詳細資訊。
* **未經許可的瀏覽器變更**：未經許可的瀏覽器變更，其發生時機是網站或程式在未經使用者同意的情況下，變更Web瀏覽器的行為或設定。這樣可能會造成首頁或搜尋頁面變更為其他網站，通常是用來提供廣告或其他不必要的內容給使用者的網站。
* **可疑的瀏覽器變更**：可疑的瀏覽器變更，其發生時機是網站嘗試修改可信任網站的清單。網站可能會在未經您同意的情況下，嘗試讓您的Web瀏覽器自動下載並安裝可疑的應用程式。
* **撥號程式**：撥號程式是一種軟體封裝，能夠變更數據機設定，以撥打高成本的付費電話號碼，或要求付費以存取特定的內容。此攻擊的結果是電話線的擁有人必須支付從未授權的服務費用。
* **追蹤軟體**：追蹤軟體是一種軟體封裝，能夠追蹤系統活動、收集系統資訊，或追蹤客戶習慣，並將此資訊轉送給第三方組織。此類程式所收集到的資訊既非個人識別資訊亦非機密資訊。
* **駭客工具**：駭客工具是一種程式，讓駭客或未授權的使用者用來攻擊、取得不受歡迎的電腦存取權，或者執行您電腦的識別或特徵。某些[駭客工具](http://www.symantec.com/zh/tw/norton/products/library/article.jsp?aid=broadband_security)會被系統或網路管理員用於合法用途，但是這些工具提供的權利也可能會受到未授權使用者的誤用。
* **惡作劇程式**：惡作劇程式會修改或中斷您電腦的正常行為，並建立一般的干擾或麻煩。惡作劇程式是程式化來執行各種動作，例如使電腦的CD或DVD光碟機隨機開啟。
* **安全風險**：安全風險是指電腦較容易受到攻擊的狀況。 當其他無害的程式含有會降低電腦安全性的錯誤時，可能會建立此狀況。這些錯誤通常都是無意圖的。使用此類程式可能會增加電腦遭受攻擊的風險。
* **可疑的應用程式**：可疑的應用程式是指其行為對電腦具有潛在風險的應用程式。此類程式的行為已經過檢查，並判定為惡意的不必要行為。
* **網路蟑螂**：網路蟑螂是透過取得網站名稱，企圖以經營網站之組織的身分來欺騙他人之行為。網路蟑螂會實際安排一些欺騙內容來模仿受信賴的品牌，或者迷惑使用者。相近域名搶註是網路蟑螂的一種形式，使用拼字方式有些差異的名稱。
* **很難移除**：這些程式都很難移除。這些程式在移除之後，可能會留下一些檔案以及登錄機碼，好讓這些遺留的檔案在程式移除之後依然能夠執行。
* **電腦威脅**：直接載入到電腦上的項目，例如病毒和病蟲，這些項目可能會潛在地傷害您的電腦。
* **身分威脅**：間諜軟體或鍵盤側錄程式等項目，這些項目會嘗試從電腦竊取個人資訊。
* **電子商務安全威脅**：可疑的電子商務活動，例如出售仿冒品。
* **惱人的因素**：不會造成傷害、但會產生煩擾的項目，例如惡作劇程式或詐騙性網站。
* **點按付費的網站**：這表示該網站的網站名稱包含某品牌名稱，但該網站不是該品牌擁有者的關係網站，而且主要內容為廣告或通往廣告網頁的連結。網站的整體分級根據發現的威脅數除以分析的頁面數確定。