臺中市政府經濟發展局政風室

公務機密宣導專欄

惡意軟體的七大惡意行為

惡意軟體（Malware） – 結合了惡意（malicious）和軟體（software），代稱了所有會影響電子裝置正常行為的有害軟體。惡意軟體可以感染各種類型的運算裝置。個人電腦（包括 Mac）、智慧型手機、平板電腦、伺服器等。基本上，只要裝置具備運算能力，就有可能會感染惡意軟體。

不同類型的惡意軟體會以不同方式運作，但一般而言，惡意軟體會經由誘使使用者點擊或安裝惡意程式來感染裝置。一旦安裝，惡意軟體就能夠進行許多惡意操作，包括：

1. 安裝其他惡意程式。
2. 佔用運算資源，拖慢系統速度。
3. 鍵盤側錄（竊取密碼和其他敏感資料）。
4. 封鎖使用者使用檔案、資料夾甚至整個系統的能力。
5. 在受感染裝置上進行自我複製。
6. 讓瀏覽器或桌面不間斷地跳出廣告。
7. 刪除重要元件，讓裝置完全無法使用。

這份列表絕不算詳盡。惡意軟體作者一直在找尋新方法來傷害使用者。

六大惡意軟體

有許多不同類型的惡意軟體，包括：

1.病毒（Virus）

病毒的散播方式都一樣 – 感染乾淨檔案，然後再散播

臺中市政府經濟發展局
TAICHUNG CITY GOVERNMENT
ECONOMIC DEVELOPMENT BUREAU

創新 Innovation　服務 Service　活力 Dynamics

到其他乾淨的檔案。病毒能夠刪除或破壞檔案及資料夾，快速不受控地進行散播，導致整個系統無法使用。

你可能會想知道“病毒和惡意軟體有什麼區別？”病毒只是惡意軟體的一種。因此，所有的病毒都是惡意軟體，但並非所有的惡意軟體都是病毒。

2.蠕蟲（Worm）

蠕蟲與病毒類似，但它不需要宿主來運行。蠕蟲可以在整個網路散播，進行自我複製並在散播時感染越來越多的裝置。蠕蟲會利用軟體漏洞來竊取敏感資訊、損壞檔案、安裝後門程式並以許多其他方式造成傷害。

3.木馬程式（Trojan）

木馬程式是一種惡意軟體，它會將自己偽裝成合法程式，不讓使用者察覺其真實意圖。跟病毒或蠕蟲不同，木馬程式無法自我複製 - 它們需要由使用者安裝。木馬程式通常隱藏在郵件附加檔中或作為免費下載的檔案提供。一旦使用者在不知情下安裝了惡意程式，其惡意程式碼就會執行並進行設定好的工作。

4.間諜軟體（Spyware）

你可能已經猜到，間諜軟體可以讓網路犯罪分子監視他們的受害者。這類型的惡意軟體能夠讓犯罪分子取得受害者的個人資訊，包括使用者名稱、密碼、按鍵等等。

5.廣告軟體（Adware）

與其他惡意軟體相比，廣告軟體的危害最小，但它仍是種惡意軟體。廣告軟體會將廣告送到受害者裝置，為攻擊者帶來收入。雖然它的危害性相對較小，但廣告軟體經常與其他惡意軟體綁在一起，它產生的廣告也經常成為其他惡意軟體感染系統的快速管道。

6.殭屍網路（Botnet）

雖然殭屍網路（botnet）在技術上並不是惡意軟體，但它可能帶來災難性的後果。殭屍網路是由受感染電腦所組成的網路，接受網路犯罪分子控制來共同完成工作。它們被用來對網站或其他系統進行分散式阻斷服務（DDoS）攻擊。

【資料來源】☞臺中市政府政風處