Palo Alto Networks® 惡意程式分析技術

王仕豪

惡意程式一向是資訊安全事件發生的重要原因，一般用戶因個人疏忽或本身系統漏洞，造成電腦遭受惡意程式感染，因此導致重要資訊外洩。而在防護方面，因惡意程式的數量每年呈現爆炸性成長，且除了傳統個人電腦平台之外，行動裝置也成為惡意程式喜好的平台，並以 APT 之鎖定性的攻擊手法，惡意程式的判斷日漸困難。本文就針對惡意程式及其分析技術進行說明。

一、常見之惡意程式種類

一般來說只要非正常用途之程式通可稱為惡意程式，因其範圍廣大，一般我們會以其功能再來進行分類，一般來說大抵包含了以下幾類：

1. Backdoor

後門為一種繞開正常認證方式，供駭客在攻擊之後仍然可遠端存取電腦，並且控制的一種程式。常用的技術包含 Reverse Shells、Generic Listeners（圖一）。

Netcat Backdoor

```
# nc -l -p 8080 -e cmd.exe
```

圖一　傳統的 Netcat 後門：開啟一個監聽 TCP 8080 的連接埠，當駭客連接上後啟用命令提示字元供駭客操控

2. Bot

使受感染的機器主動連向駭客的命令主機接受命令，聽從攻擊者指示。這些指令可能包含複製電腦上的檔案至攻擊者的主機，嘗試感染同一內網的其它電腦，或加入其它已受感染的電腦群組內（Botnet），執行如分散式阻絕攻擊（DDos），傳遞垃圾郵件（Spam delivery），挖比特幣（Bitcoin Mining）等等。

3. Scareware

假借資訊安全產品之名以恐嚇受感染電腦之使用者，要求使用者付費購買其資料備份，或者攻擊者製作假的防毒產品，但實際上並沒有解決任何問題。如 Ransomware（圖二）。

4. Dropper、Downloader

(1) Dropper：執行時產行惡意程式碼並植入電腦內，通常用於單一惡意程式。