銀行及金融機構的目標式攻擊—Carbanak 惡意攻擊活動通知

資安警訊：

銀行及金融機構的目標式攻擊—Carbanak 惡意攻擊事件

威脅說明：

攻擊事件主要讓駭客能針對銀行能夠滲透公司網路修改銀行相關紀錄從而竊取高額鉅款，目前已知攻擊者能夠滲透 100 間位於不同國家的銀行，包括：俄羅斯、德國、中國、烏克蘭、美國。

威脅手法：

1. 透過魚叉式網路釣魚信件，並在信件內夾帶惡意檔案寄送給員工，當你點擊信件附檔後，將會在被攻擊者電腦植入 Carbanak 惡意程式到作業系統中。

2. Carbanak 介紹：

(1). 本身是一個後門程式，可以執行各種指令，包括：鍵盤側錄程式、擷取螢幕快照、檢查某些特定銀行應用程式（例如銀行轉帳軟體）。

(2). 駭客透過遠端管理工具利用 Carbanak 在內網中流竄直到找到可進行銀行交易的目標電腦為止，一旦成功入侵目標電腦，透過錄影方式記錄受害者銀行的交易流程，待竊取到所需資訊後，駭客即可進行銀行交易竊取金錢而不被發現。

建議措施：

1. 請留意勿開啟不明來源或偽冒來源之郵件附檔。

2. 隨時注意防毒軟體更新至最新病毒碼

資料來源：趨勢科技