駭客又出新招！

即使把電腦斷網、隔離也沒用，駭客照樣可以默默地竊取資料!

Reported: Jason
Date: June 10th 2020

Introduction

AENEAS

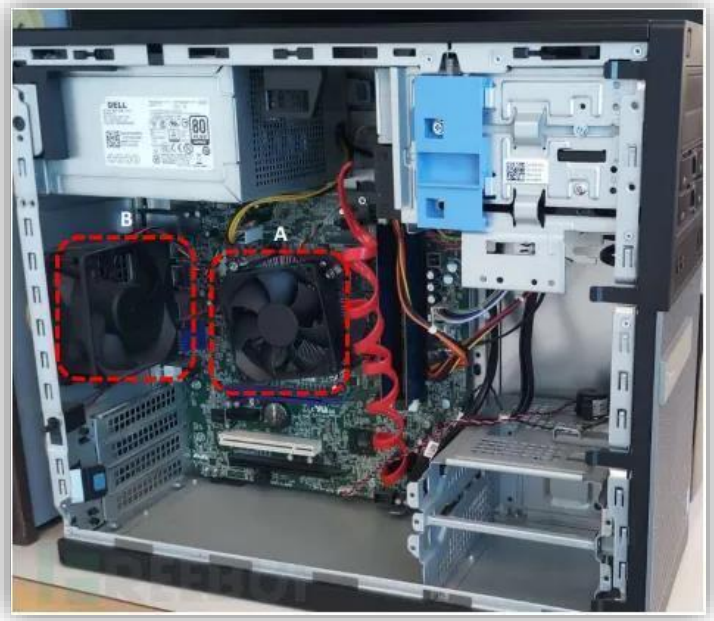
隨著時代演變，駭客盜走電腦資料的招數越來越多。

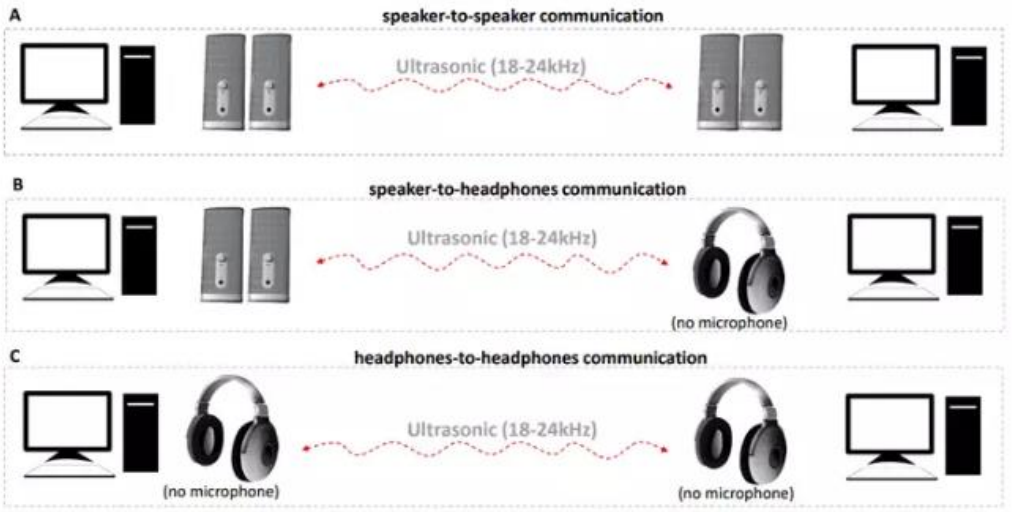
政府、軍方等單位要保護機密資料時，會將之儲存在永不連接網路的「氣隙電腦」（air-gapped computer），避免遭駭客入侵，竊走珍貴數據；但在駭客技術日新月異的現在，即使不連網路，

駭客仍有辦法隔空偷走電腦內的資料。

各種花式竊取招數，就怕你想不到。 AENEAS

利用電腦CPU風扇、硬碟 LED、螢幕亮度、電腦揚聲器、散發的熱量等，甚至利用電源線中的電流波動，都可以進行數據竊取。



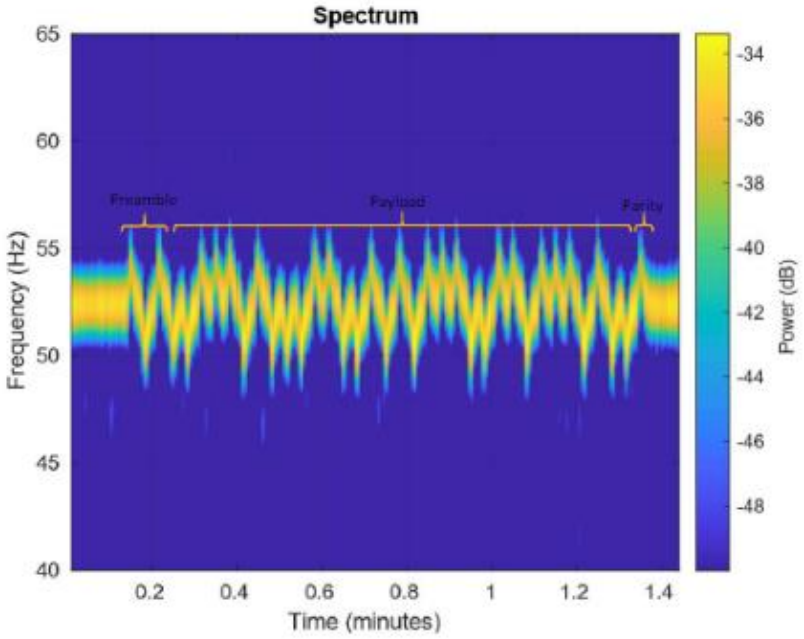


案例: 利用電腦風扇竊取資料

AENEAS

這種攻擊分為 3 個步驟。

首先，利用植入電腦中的惡意軟體來控制風扇轉速，以此來調節電腦產生的機械振動，數據會被編碼到這些振動中；



然後，將智慧手機放置在電腦桌上或靠近電腦主機的其他位置，手機中的加速度感測器可以用來收集振動訊號；

最後，透過 App 解碼獲取訊號。

入侵『氣隙設備』的各種技術

AENEAS

- PowerHammer 攻擊可透過**電源線**從氣隙電腦中竊取數據。
- MOSQUITO 技術透過**超音波**，可以將置於同一房間內的 2 台（或更多）氣隙電腦進行祕密地數據交換。
- eatCoin 技術可以使攻擊者從氣隙**加密貨幣錢包**中竊取私有加密密鑰。
- aIR-Jumper 攻擊藉助裝有夜視功能的**紅外線 CCTV 攝影機**，從氣隙電腦中獲取敏感資訊。
- MAGNETO 和 ODINI 技術使用 **CPU 產生的磁場**做為氣隙系統和附近智慧手機之間的祕密通道。
- USBee 攻擊可透過 **USB 連接器的射頻**傳輸從氣隙電腦上竊取數據。
- DiskFiltration 攻擊可以利用目標氣隙電腦的硬碟驅動器（HDD）發出的**聲音信號**來竊取數據。
- BitWhisper 依靠兩個電腦系統之間的**熱交換**來竊取虹吸密碼或安全密鑰。
- AirHopper 將電腦的**顯示卡轉換成 FM 發射器**來控制按鍵。
- Fansmitter 技術利用電腦**散熱器發出的噪音**獲取數據。

如何阻止？

AENEAS

一、在包含機密敏感信息的氣隙電腦上放置加速度傳感器，用以檢測異常振動。

二、風扇、溫度訪問監視器。

三、加裝隨機振動的組件連接到電腦上。

四、電腦進行物理隔離，把它放進特殊的抗微振機箱。

五、水冷系統代替原有的電腦風扇系統。

Thank You

AENEAS