

網路上最強大也是最具破壞性的勒索病毒

勒索病毒使用之資訊技術：

使用**2048**位元**RSA**和**AES**演算法，利用對稱與非對稱加解密技術，暗中將電腦上的文件或檔案加密，同時因為加密的關係，使受感染電腦無法正常上網、拒絕使用者開啓檔案並跳出付贖金之訊息通知受害者支付贖金。



感染途徑：

利用社交工程、釣魚網站、釣魚郵件、破解軟體、程式漏洞、受入侵被掛木馬程式之網站。

攻擊對象：

受感染電腦內Word (doc 、 docx) 、 Excel (xls 、 xlsx) 、 PowerPoint (ppt 、 pptx) 、 JPG 、 SQL 、 PDF及圖檔(png 、 jpg 、 gif)等近百種企業常見檔案格式。

攻擊範圍：

1. 受感染電腦內的檔案及文件。
2. 受感染電腦連結的網路芳鄰、網路磁碟機、檔案伺服器等，攻擊內部網路所有共享的文件或檔案。

受害程度：

1. 被感染的檔案及文件將無法開啟。
2. 檔案或文件被加密後，使用者無法自行復原。
3. 內部網路速度受影響，受感染的電腦效能也大幅度降低。

自保方式：

1. 重新格式化作業系統並從最近的備份回復資料。
2. 經常性更新作業系統及資安軟體、防毒軟體。
3. 經常性利用隨身碟或外接硬碟，將重要文件及檔案作離線備份。
4. 以及不要開啟來路不明的網站、郵件或檔案。