

臺中市政府經濟發展局政風室

公務機密宣導專欄

最容易被勒索病毒盯上的四種目標(節錄)

使用者會感染勒索病毒，大多經由不明來源的惡意電子郵件內的附件或連結下載到惡意程式。然而，由於勒索病毒的設計是為了盡可能長期躲藏而不被發現，因此受害者不太容易確切知道自己是何時感染。

兩大類型

1. 封鎖型勒索病毒

這類勒索病毒會將電腦鎖住，讓使用者無法使用。有可能是對電腦開機檔案動了手腳，讓使用者進不了桌面。一般來說，使用者還是能使用電腦來支付贖金，但除此之外就不能做其他事情。這類勒索病毒較為單純，造成的衝擊也不像第二種那麼嚴重。

2. 加密型勒索病毒

這類勒索病毒會將電腦上的重要資料加密（文件、相片、影片等等），但不會干擾電腦的功能。這種類型的勒索病毒通常會在勒索訊息當中加入倒數期限。如果沒有在期限內付款，就會將所有被加密的資料刪除。

四種對象

駭客主要的攻擊對象有 4 種：

1. 只有基本資安人員的單位

那些只有基本資安人員的機構，例如大學院校。

2. 能付出大筆贖金的企業、機關（構）

負擔得起大筆贖金且願意為了救回資料而支付贖金的企業。

例如政府機關、銀行、能源產業和醫療機構。



臺中市政府經濟發展局
TAICHUNG CITY GOVERNMENT
ECONOMIC DEVELOPMENT BUREAU

創新
Innovation

服務
Service

活力
Dynamics



這些機構要隨時都能存取他們的資料才能正常運作，而且通常會覺得支付贖金反而是兩害相權取其輕的作法。

3. 握有敏感資料, 怕被揭發資料外洩的機構

手上握有敏感資料的機構，例如法律事務所、社群媒體平台，以及身分認證相關的機構都屬於這類。駭客的想法是，這些機構會因為害怕被人知道其資料安全措施出了問題，進而衍生各種法律後果，所以會願意私下祕密支付贖金。

4. 因害怕而付錢的一般普羅大眾

這類是網路上的日常使用者，這類對象通常較缺乏相關常識，而且遇到事情也不知該如何處理，所以就容易因害怕而付錢。

不論是哪一類，一旦感染勒索病毒，基本上能做的事情只有 3 項：

1. **乖乖支付贖金**。一般來說，專家都會建議不要支付贖金，因為就算您付了錢，歹徒也可能會懶得幫您解開您的裝置或檔案。
2. 嘗試**將電腦上的勒索病毒清除**。
3. 如果不可能清除，必須將電腦**回復到出廠狀態**，並將一切資料清除乾淨。正是因為這樣，所以資料備份很重要。

不幸的是，勒索病毒似乎不可能消失。它的目標或許會改變，但這種犯罪本身不會消失。隨著生活越來越朝數位化發展，智慧家庭裝置與連網汽車都是它們的最新目標，如家用智慧門鎖和智慧溫控裝置，更別說像智慧心律調整器和植入晶片等連網醫療裝置。物聯網勢必將為網路犯罪集團帶來無限機會。

【資料來源】

👉 [資安人-最容易被勒索病毒盯上的四種目標](#)