勒索程式 第一課

定義、原理和後果

什麼是勒索程式？

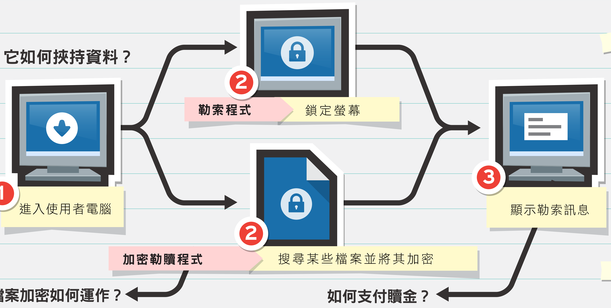
勒索程式是一種會挾持資料的嚴重資安威脅，它會讓檔案和系統功能無法使用，甚至讓整台電腦都無法使用。受害者必須支付一筆贖金來贖回自己的檔案和系統。

您如何感染？

您可能在不知情的狀況下經由下列其中一種管道感染到勒索程式：

- 遭到入侵的網站
- 垃圾郵件
- 其他惡意程式

它如何挾持資料？



檔案加密如何運作？

如何支付贖金？

它為何是一項資安威脅？

勒索程式早已從最初發現的那種沒有實質傷害性的恐嚇程式，演化成具備精密檔案加密能力的加密勒贖程式。

2006
俄羅斯出現一種可將受害者的**檔案壓縮**並加上密碼的勒索程式變種。

2011
出現一種要求受害者必須**發送高費率簡訊**到某個號碼的簡訊勒索程式。

2012
歐洲、美國和加拿大出現大量**假冒當地警察**而非留下勒索訊息的勒索程式。

2013
一種名為**CryptoLocker**的新型勒索程式出現，除了會鎖定系統之外，還會將檔案加密。

2014
所有 **48,000** 個偵測到的勒索程式當中有 **15,000** 個屬於**加密勒贖程式**，較首次發現以來成長了**27%**。

您如何保護自己？

感染勒索程式目前還沒有解藥，不過使用者可以藉由下列方法來防止自己感染：

定期備份資料
遵守 3-2-1 原則：3 份備份、2 種儲存媒體、1 個不同的安全存放地點。

將網站加入書籤
將您經常瀏覽及信任的網站加入書籤當中，可防止您意外打錯網址的風險。

檢查電子郵件來源
在開啟任何電子郵件中的連結或下載其中的檔案之前，務必先仔細核對寄件人的地址是否在您的通訊錄當中。

更新您的防護軟體
保持最新狀態的防護軟體可讓您多一層保障，因此請務必定期更新，讓您有防範最新勒索程式變種的能力。

資料來源：
whatis.techtarget.com
arstechnica.com

TREND MICRO

作者：TrendLabs,
趨勢科技全球技術支援與研發中心