資通安全危險案例
－勒索病毒

前言

資通安全的威脅日新月異，美國殖民管道公司、鴻海公司北美廠區與墨西哥廠區接連遭勒索病毒攻擊，就連如此資通安全防備的大公司都無法完全抵禦，各公務機關對於勒索病毒的防患未然實為必要之舉。

勒索軟體(Ransomware)是什麼？

- 勒索軟體(Ransomware)是一種透過破壞受駭者存取權限，並向受駭者要求贖金的惡意程式，目前可分類為「非加密型勒索軟體」與「加密型勒索軟體」。
  - ※**非加密型勒索軟體**：將受駭者的資訊設備鎖起來，破壞受駭者對設備的存取權。
  - ※**加密型勒索軟體**：加密受駭者硬碟上的檔案，破壞受駭者對資料的存取權，通常要求受駭者以加密貨幣支付贖金，以取回檔案的存取權。
- 個人、政府機關及企業組織皆可能成為被攻擊的對象，已逐漸成為嚴重的資安威脅之一，當遭受勒索軟體攻擊時，不建議支付贖金，因支付贖金並不能保證取回存取權限，且將助長勒索軟體更加猖獗。

攻擊跡象

勒索留言通常是 .txt 檔或是 .html 檔

發現文件被加密無法開啟

發現各目錄下開始出現奇怪副檔名的檔案，例如：.crypt、.VVV、.CCC、.ZZZ、.AAA、.ABC、.XXX、.TTT 等

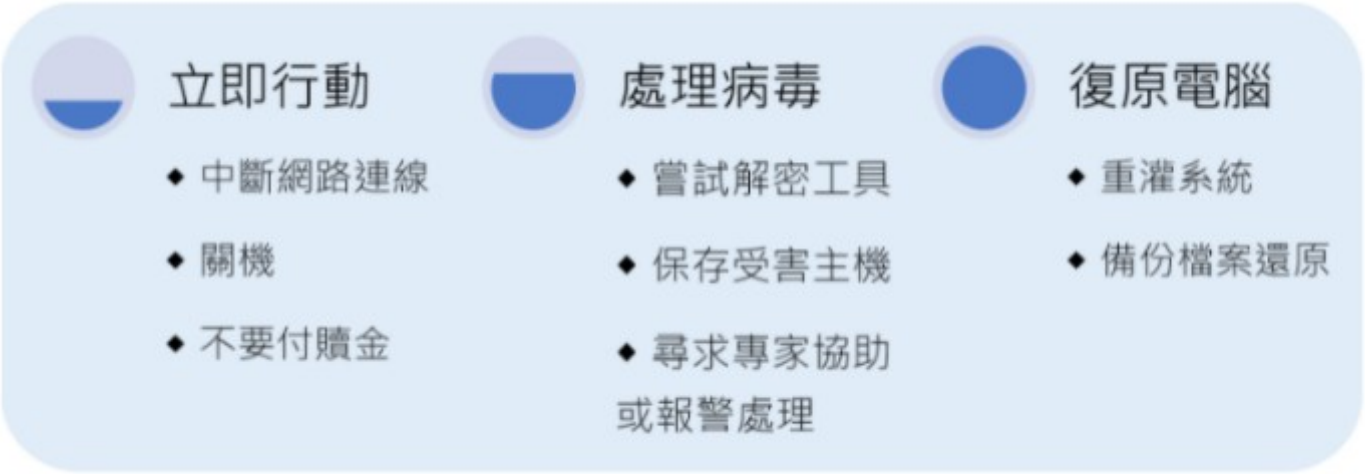
瀏覽器遭鎖定或瀏覽器工具列發現奇怪的捷徑。

畫面遭鎖定

電腦出現藍色當機畫面，在電腦重新開機時顯示勒索訊息。

感染勒索軟體的緊急處理

- 立即中斷受駭主機網路連線並隔離。
- 可嘗試使用信任來源的解密工具解密
- 系統重灌

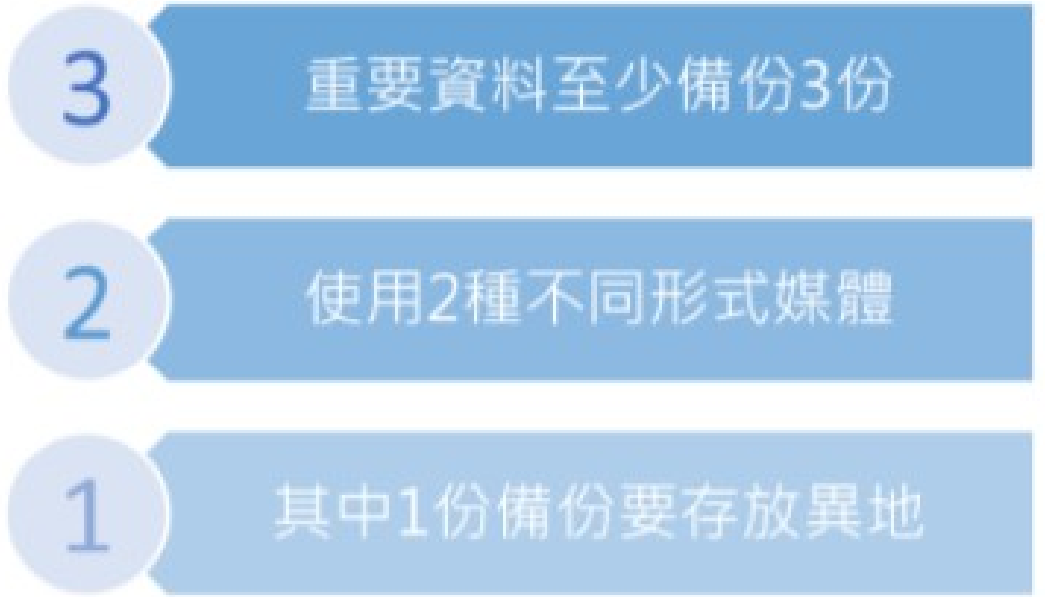


感染途徑

- 網站瀏覽
- 電子郵件感染
- 非法軟體感染
- 被已遭受勒索軟體攻擊的電腦或裝置感染（USB 磁碟等）

防護建議 1 — 定期備份檔案

- 採用「 3-2-1 原則」備份重要檔案
- 根據需求使用不同儲存媒體備份檔案
- 公有雲端備份



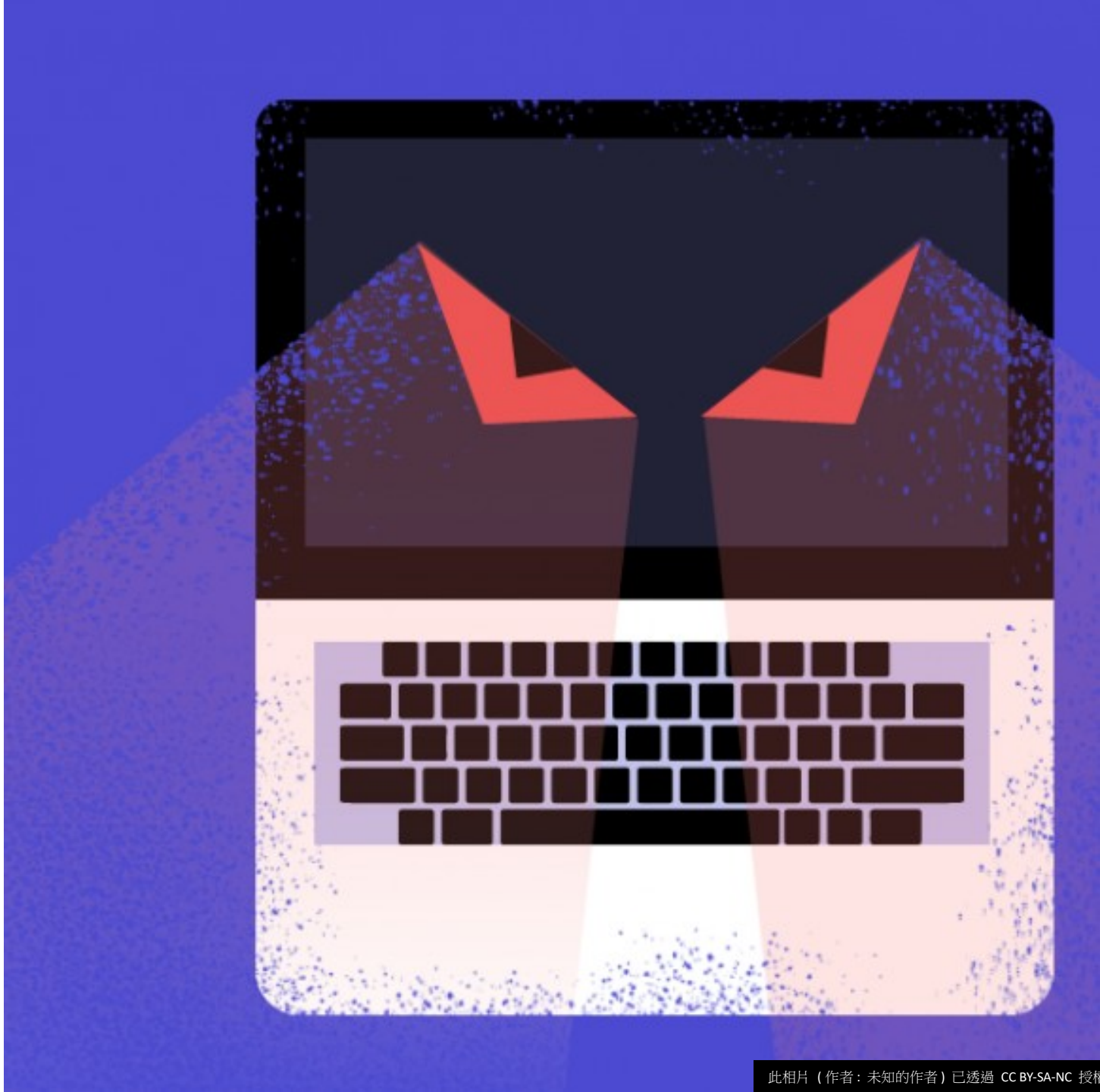
儲存媒體	特性
隨身碟/光碟片	適合小量資料備份
外接式硬碟/電腦	可儲存較大量資料
私有雲端備份- 網路儲存伺服器(NAS)	• 小型的雲端硬碟伺服器，接上網路，就可以透過網路存取這台NAS伺服器，如同建立一個私有雲端。 • 能把檔案異動都備份下來，而一些廠商提供的NAS產品，最高還能達上萬次歷史版本存取。若接有2顆硬碟， NAS會自動備份到另一顆硬碟，有資料備援之效。

防護建議 2 — 修補軟體漏洞

勒索軟體利用漏洞攻擊越來越常見，一般使用者平時應確保作業系統與常用應用程式（如：瀏覽器）維持在最新版本，減少因漏洞導致被入侵的風險。

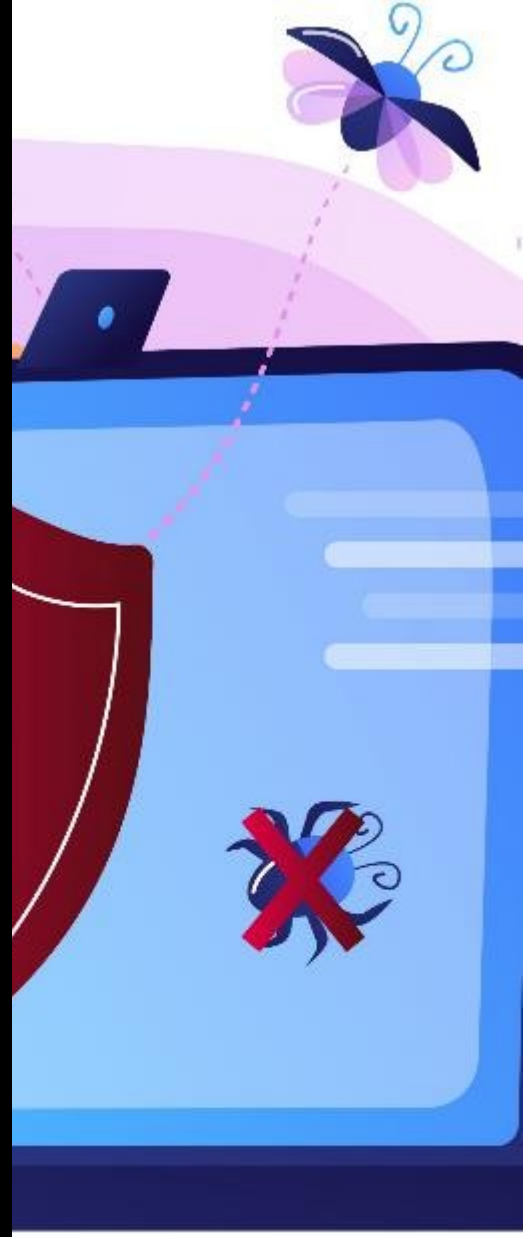
防護建議 3 — 謹慎開啟郵件，小心上網行為

- 不隨意打開來源不明的信件或點選信中的連結與附件。
- 不下載非法軟體或不明程式。
- 不要啟用 Office 文件的巨集，可考慮安裝 Office Viewer，因為它不支援巨集功能。
- 上網瀏覽時提高警覺，並使用較高安全性瀏覽器。
- 即時掌握已/預計停止支援更新的作業系統資訊，並盡速更換成更高版本或較高安全性的作業系統。
-



防護建議 4 — 安裝防毒軟體，隔離已知病毒

安裝防毒軟體是相當基本的防護策略，可增強端點資安防護，免於病毒及其他安全性威脅，更重要的是需時時更新病毒碼，並注意一些進階功能是否啟用，以增強未知病毒的防護能力。



資料來源：
行政院國家資通安全
會報技術服務中心