

An illustration depicting a ransomware attack. In the center, a large red skull and crossbones symbol is superimposed over a yellow background. Below this, the text '資通安全危險案例' (Information Security Risk Case) and '— 勒索病毒' (— Ransomware) is written in white. The background features several computer monitors with keyboards, some showing red exclamation marks. In the bottom left, a person is shown with their hands on their head, looking distressed, with a red exclamation mark above them. The overall color palette is dominated by red, yellow, and grey.

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，美國殖民地管道公司、鴻海公司北美廠區
與墨西無的廠區完全抵禦，勒索公毒機關對勒索病如毒資防安患未防然實為必
司都舉。要公必為實然未患防資毒如病索勒對機毒公務各，勒索公毒機關對勒索病如毒資防安患未防然實為必



勒索軟體 (Ransomware) 是什麼？

- 勒索軟體 (Ransomware) 是一種透過破壞者勒索，要求非勒索者支付贖金以恢復存取權的惡意程式。其目的與「勒索軟體」不同，勒索軟體是破壞受駭者的資訊，而非破壞受駭者的設備。
 - ※ 非加密型勒索軟體：將受駭者的資訊鎖起來，破壞受駭者對設備的存取權。勒索軟體受駭者以取得檔案，勒索受駭者支付贖金以取得檔案。
 - ※ 加密型勒索軟體：勒索受駭者支付贖金以取得受駭者硬碟上的資料。勒索軟體受駭者以取得受駭者硬碟上的資料。
- 個人、政府機關及企業組織皆可能成為勒索軟體的受害者。勒索軟體的攻擊對象，當其資料被勒索時，勒索軟體會攻擊其資料，勒索受駭者支付贖金以恢復存取權。勒索軟體的攻擊對象，當其資料被勒索時，勒索軟體會攻擊其資料，勒索受駭者支付贖金以恢復存取權。

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



立即行動

- ◆ 中斷網路連線
- ◆ 關機
- ◆ 不要付贖金



處理病毒

- ◆ 嘗試解密工具
- ◆ 保存受害主機
- ◆ 尋求專家協助或報警處理



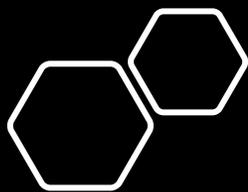
復原電腦

- ◆ 重灌系統
- ◆ 備份檔案還原

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

3

重要資料至少備份3份

2

使用2種不同形式媒體

1

其中1份備份要存放異地

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)	<ul style="list-style-type: none">• 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。



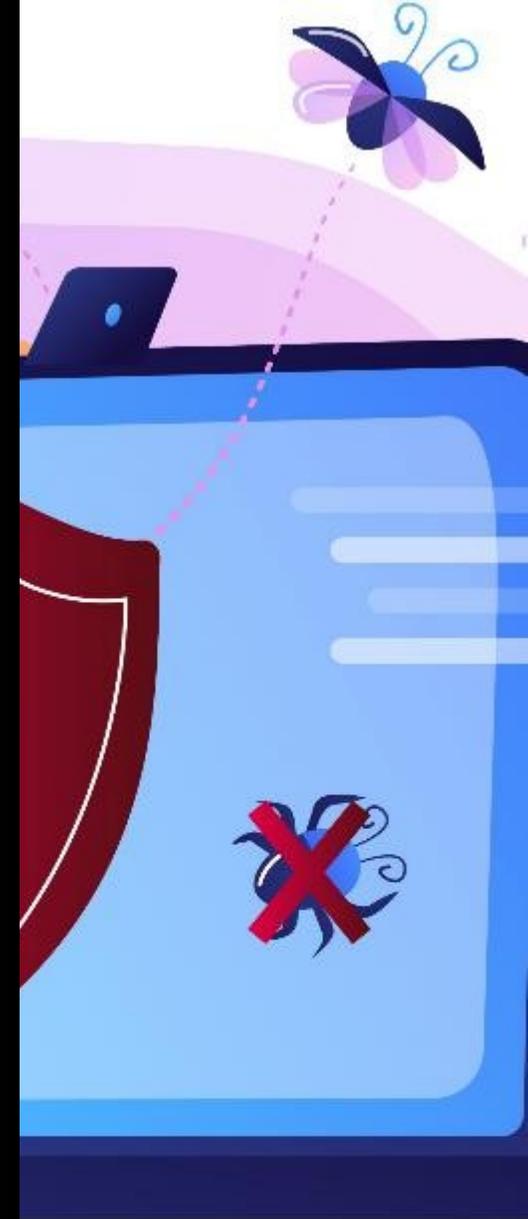
防護建議 3 — 謹慎開啟郵件， 小心上網行為

- 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

