面對全民公"駭"

勒索軟體防治

- 入侵手法
- 造成影響
- 處理程序
- 預防之道

長庚大學 資訊中心

入侵手法

- 釣魚郵件
- 惡意廣告、網頁木馬
- 共享文件
- 非法軟體

入侵手法 1

釣魚郵件-寄送附件或有害連結。

收到夾帶
惡意附件或
有害連結的
釣魚郵件。

執行附件
或點選
有害連結。

加密勒索軟體
連至C&C中繼站
取得金鑰。

開始加密，
完成後跳出
勒索贖金畫面。

入侵手法　造成影響　處理程序　預防之道

入侵手法 2

惡意廣告、網頁木馬-瀏覽器或裝置顯示出惡意廣告、網頁木馬。

利用Windows、Java、Flash或瀏覽器的漏洞。

瀏覽看似正常，卻遭植入惡意連結的網站。

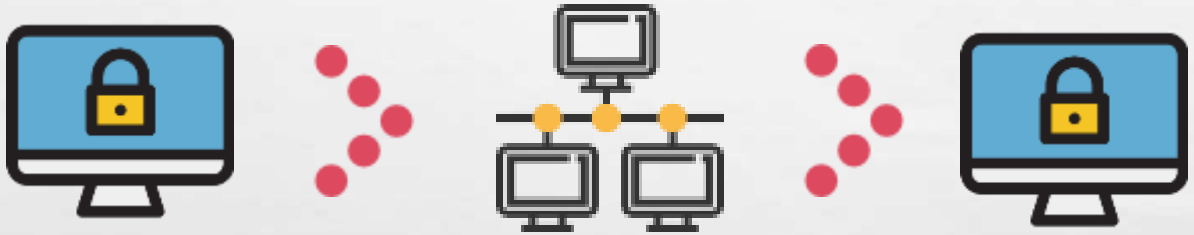
透過軟體漏洞，背景自動執行。

加密勒索軟體連至C&C中繼站取得金鑰。

開始加密，完成後跳出勒索贖金畫面。

入侵手法 3

共享資料夾



使用者感染勒索軟體卻不自知。

使用者具有共享資料夾存取權限。

共享資料夾的檔案也同時被勒索軟體加密。

入侵手法 4

非法軟體

從網站論壇
下載非法程式。

安裝及執行
非法程式。

加密勒索軟體
連至C&C中繼站
取得金鑰。

開始加密，
完成後跳出
勒索贖金畫面。

造成影響

目前可分為以下三類:

限制系統運作-無法正常使用電腦。

檔案加密-無法開啟文件與影音、照片。

磁碟加密-無法順利進入作業系統。

造成影響

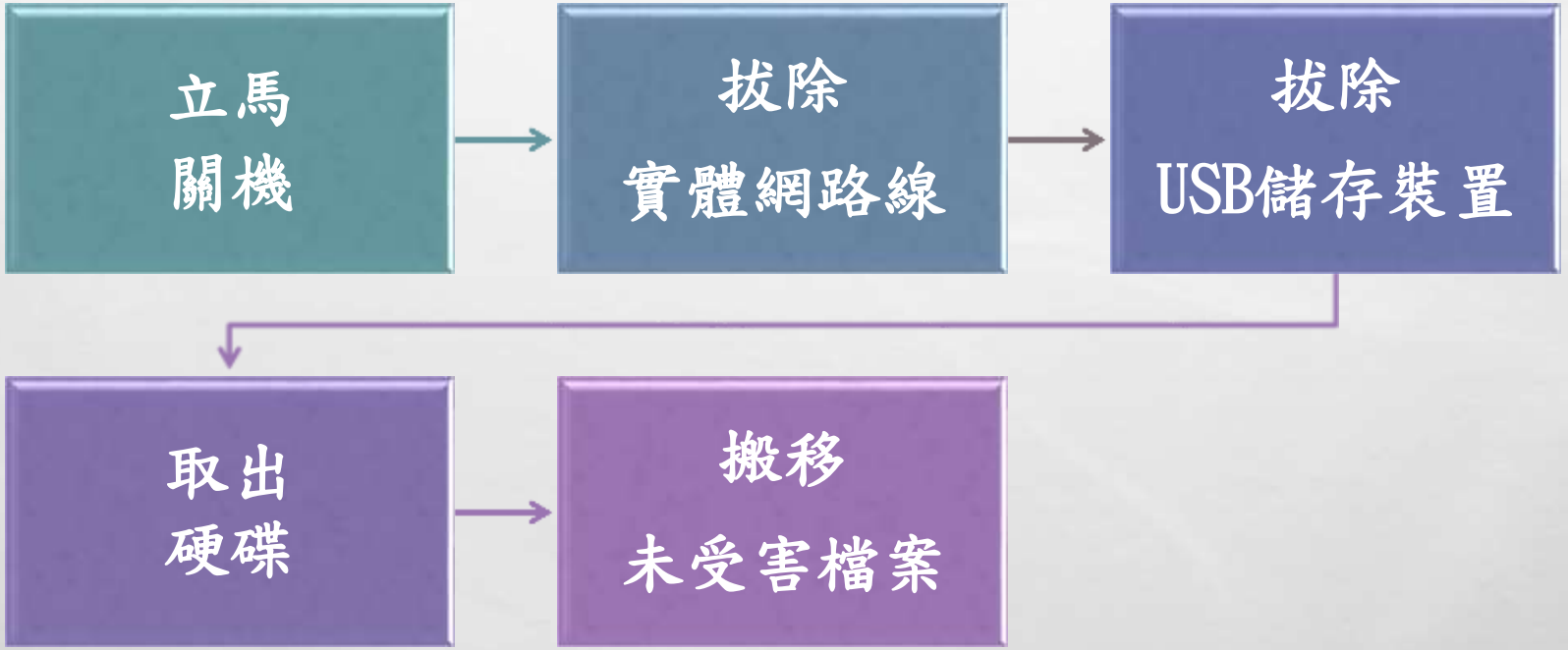
檔案加密的危害程度:

- 發出勒索訊息後，受害電腦無法上網。
- 無法開啟遭加密的文件，亦無法自行復原。
- 惡意程式加密內網共享文件時，會占用頻寬，導致內網速度超慢，受害電腦效能也會大減。
- 不只 WINDOWS 環境、連 LINUX 及 MACINTOSH 都已經有災情傳出。

處理程序

- 隔離
- 清查
- 救援
- 重灌

處理程序-隔離



處理程序-清查

盡速清查以下範圍是否有災情

- 受害主機的共享檔案
- 公用資料夾檔案
- 雲端空間檔案

★清查上述範圍後，再將各主機JAVA、Flash、PDF軟體、Silverlight、瀏覽器、Windows OS Update等更新至最新版本。

處理程序-救援

上策-使用備份檔案回復。

中策-尋找各防毒軟體廠商所提供的解密工具回復與刪除惡意檔案。

下下策-支付贖金。

★最後將已掃描檔案移至乾淨重建的作業環境使用！

處理程序-重灌

完成後請務必完成下列六點基本要求:

1.不使用來源不明之檔案與軟體。

2.執行作業系統更新，開啟自動更新功能。

3.安裝防毒軟體，開啟自動更新功能。

4.啟用防火牆功能。

5.帳號設定具複雜度之高安全性密碼。

6.公用電腦需設置保管人制度限制使用。

預防之道

- 三不三要
- 備份
- 更新
- 開啟UAC
- 系統還原
- 檔案唯讀
- 設定寫入權限
- 關閉WSH

★搭配防毒軟體進行防範之外，本身的操作意識是更有效率的防範機制!

預防之道-三不三要

不上鉤-標題特別吸引人的郵件及連結，務必停看聽

不打開-不隨便打開e-mail附件檔

不點擊-不隨點擊e-mail內的網址

要備份-重要資料要備份

要確認-開啟電子郵件前，要先確認寄件者身分

要更新-病毒碼一定要隨時更新

預防之道-備份

3-2-1完整備份黃金準則

3份完整-完整備份「3」份資料副本

2種不同-儲存於「2」種不同的媒體種類

1份異地-儲存「1」份副本於異地保存

★應定期對於備份檔案進行復原抽查，確保備份完整性與可用性!

預防之道-更新

以下軟體更新到最新，避免門戶大開。

- WINDOWS UPDATE
- JAVA
- ADOBE READER
- ADOBE FLASH PLAYER
- SILVERLIGHT
- 瀏覽器
- 防毒軟體

預防之道-開啟UAC

開啟 UAC 帳戶控制功能

作用-提升系統的安全性，當使用者進行軟體安裝或是調整系統帳戶權限時，跳出警告視窗來提醒使用者權限調整。

路徑-進入「控制台」的「使用者帳戶」之後，點選「變更使用者帳戶控制設定」。

設定-將設定調到最高，當應用程式嘗試安裝及變更電腦、或是有人試圖改變設定時會跳出警告通知。

步驟教學

預防之道-系統還原

可能有機會救回部分的檔案

作用-系統還原有機會恢復遭勒索病毒刪除的原始檔案，建議儘可能每個磁碟機都開啟。

路徑-進入「控制台」的「系統及安全性」的「系統」之後，點選「系統保護」。

設定-選擇磁碟機後點選「設定」選擇開啟系統保護。

步驟教學

預防之道-檔案唯讀

可防止「部分」勒索軟體

作用-當文件設為唯讀，則只有擁有者或具有寫入權限可以移除指定。 若某人嘗試變更唯讀文件，需製作文件複本並給予新名稱，才能儲存變更。

路徑-點選要保護的檔案右鍵，點選「內容」。

設定-勾選屬性「唯讀」方塊。

預防之道-設定寫入權限

可防止「部分」勒索軟體

作用-透過設定資料夾的寫入權限，可以防止勒索軟體未經同意，修改加密重要檔案。

路徑-在要保護的資料夾點選滑鼠右鍵，選擇屬性。之後點選「安全性」頁籤，在群組或使用者名稱按下「編輯」。

設定-在此將寫入的權限設定為「拒絕」。

步驟教學

預防之道-關閉WSH

可防止「部分」勒索軟體自動執行JScript指令

作用-關閉「Windows Script Host」可避免「部分」勒索軟體自動執行壓縮檔內的JScript指令。

路徑-同時按Windows 鍵及R鍵開啟執行視窗，輸入「regedit」。尋找「HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings」

設定-右鍵新增一個 DWORD 值為「Enabled」，數值資料設定為零。

步驟教學

參考資料

- 行動安全上網學習手冊(教育部)
- 「105 政府資通安全防護巡迴研討會」教材(行政院國家資通安全會報技術服務中心)
- 1分鐘學會預防勒索軟體 警製懶人包讓你電腦不被綁架(刑事警察局)
- 綁架勒索電腦檔案的惡意程式事件分析報告(臺灣學術網路危機處理中心團隊製)
- 加密勒索軟體捲土重來，大舉攻擊小型企業與個人用戶(ITHOME)
- 8個加密勒索軟體常見的問題(資安人)
- 2016 勒索軟體白皮書 (趨勢科技)
- 《資安漫畫》預防勒索軟體綁架-三不三要(趨勢科技)
- 恐怖的勒索軟體！ 有什麼解法與預防方式－ 目前沒有良好解藥，自我保護最重要(T客邦)
- 綁架電腦檔案勒索賺錢　簡單步驟預防檔案加密病毒《TORRENTLOCKER》及《CRYPT0L0CKER》(電腦阿達王)
- 勒索軟體預防針，停用 WINDOWS SCRIPT HOST 功能，不要放棄治療(綠色工廠)
- 拒絕勒索軟體系列(一)：實戰 3 大勒索軟體，WINDOWS 也能有效保護重要檔案(硬是要學)

入侵手法　造成影響　處理程序　預防之道

Thank You

長庚大學 資訊中心