

# 醫院面對勒索軟體攻擊的應變指南



衛生福利部資訊處

中華民國 114 年 3 月 5 日

## 版本資訊

版次	日期	修訂單位	說明
V0.1	114.3.3	衛生福利部資訊處	處長起草
V0.9	114.3.4	衛生福利部資訊處	資訊處、H-ISAC 團隊編輯
V1.0	114.3.5	衛生福利部資訊處	正式發布



勒索軟體攻擊對醫院構成重大威脅，可能干擾病人照護、洩露敏感數據，甚至危及生命。本指南提供分階段的應對方法——立即應對、遏制與診斷、恢復與重建，並附上詳細技術指引，以辨識勒索軟體、追溯其來源並減輕影響。

---

## 第一階段：立即應對（最初 1-2 小時）

初始應對對於「限制勒索軟體擴散」和「證據保全」至關重要，並依照規定完成通報。

### 1.1 隔離受感染系統

- **行動：**立即將受感染設備從所有網路（Wi-Fi、LAN、藍牙）中斷開。
  - 拔掉網路線並禁用無線連接。
  - 避免完全關閉系統，以保留易揮發性資料（如記憶體）以供取證分析。
- **額外步驟：**
  - 禁用遠端存取工具（例如遠端桌面協議 [RDP]、VPN），防止進一步入侵。
  - 若感染範圍不明確，隔離受影響的子網路。
  - 通知全院，勿開啟關機狀態的電腦，避免擴散感染。
  - 使用非內部網路通信方式（市話、手機、LINE、Signal 等）進行協調。避免使用內部可能已被監控的電子郵件或內部系統。
  - 若醫療相關系統受影響，考量啟動單機版或人工紙本作業。

### 1.2 啟動事件應變團隊

- **行動：**立即通知醫院的資安部門主管、資安專責(職)人員與資安長。
  - 遵循醫院事件應變計畫及組建應變小組。
- **關鍵角色：**
  - 醫院領導層(院長)：管理運營連續性和重大決策
  - 總指揮官(資安長)：協調跨單位資源、外部支援
  - 第一線指揮官(資訊/安主管)：負責損害控管、復原作業之指揮
  - 資安專(職)人員：通報聯繫作業，並應注意通報時效
  - 應變復原組(醫院資訊、醫工等及各設備、系統供應商)：執行復原與重建
  - 事件調查組(醫院資安 SOC 服務廠商)：事件調查及鑑識
  - 公關(醫院發言人)

### 1.3 證據保全

- **行動**：除非絕對必要，切勿重啟系統、刪除或清除檔案(如清理回收資料夾)。
  - 若遇到以下情形必須關機，則採用直接拔除電源方式。
    - 主機死當狀態、藍屏(Blue Screen of Death)無法操作
    - 作業系統異常影響操作功能
    - 系統繁忙資源耗盡無法操作
  - 拍攝勒索訊息、錯誤訊息或其他可疑活動的螢幕截圖。
  - 記錄檔案時間戳記和檔案詳情（例如加密文件的路徑、修改時間與建立時間、檔案擁有者等）。
- **工具**：使用手機或外部相機記錄，以免系統受損致證據佚失。

### 1.4 通報主管機關

- **行動**：於知悉事件一個小時內完成資安事件通報。
  - 公務醫院請至 N-CERT 通報，<https://www.ncert.nat.gov.tw/>
  - 非公務醫院請至 H-ISAC 通報，<https://hisac.nat.gov.tw/>【電話：03-4072132 (24 小時客服及緊急應變專線) | 電子郵件：[hisac-cs@mohw.gov.tw](mailto:hisac-cs@mohw.gov.tw)】  
若需外部支援可於通報單註明，並洽客服專線
  - 駭侵事件之犯罪調查，應向調查局資安工作站報案 (02) 29112241#8702。
- **額外步驟**：
  - 如個資外洩或損壞，請依「個人資料保護法」及「醫院個人資料檔案安全維護計畫實施辦法」辦理
    - 事故時起七十二小時內，填寫「個人資料侵害事故通報紀錄表」以書面通報地方衛生局、副知衛生福利部
    - 衛生福利部醫院個資保護窗口：醫事司沈約聘副研究員，(02)85907385，[mdblackcat168@mohw.gov.tw](mailto:mdblackcat168@mohw.gov.tw)
    - 於發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害事故時迅速處理，以保護當事人之權益，包含「查明事故發生原因及損害狀況，以適當方式通知當事人或其法定代理人」

### 1.5 保護備份

- **行動**：確認與驗證備份完整性。
  - 檢查備份文件是否已被加密或篡改。

- 將備份主機離線或是副本儲存在隔離媒體 ( 例如外部硬碟、磁帶 ) 。

---

## 第二階段：遏制與診斷 ( 最初 24 小時 )

此階段專注於「識別勒索軟體」、「追溯其進入點」並保護關鍵資產。(由資安 SOC 服務廠商協助執行)

### 2.1 識別惡意軟體類型

- **行動**：分析勒索軟體痕跡以確定其類型和來源。
  - **勒索訊息**：檢查檔案 ( 如 README.txt 或 DECRYPT\_INSTRUCTIONS.html ) 中的時間戳記、檔案名稱或 IP 位址。
  - **加密文件副檔名**：尋找特徵 ( 例如 .locky、.crypt、.WNCRY ) 。
  - **C2**：中繼站與攻擊者來源 IP 。
  - **惡意程式雜湊**：提供惡意程式雜湊值 ( MD5、SHA-1、SHA-256 )
    - 將雜湊值與威脅情報平台 ( 例如 VirusTotal、ID Ransomware、NoMoreRansom ) 比對。
    - ※ **注意**：不可將完整檔案上傳，避免造成資料外洩
  - **動態分析**：可在沙盒環境 ( 例如 Cuckoo Sandbox、Any.Run ) 中執行勒索軟體，觀察其行為。
- **目標**：識別勒索軟體類型 ( 例如 WannaCry、Ryuk、LockBit ) 並尋找已知的解密工具。

### 2.2 收集入侵指標 ( IOCs )

- **行動**：蒐集 IOCs 資料，並於 24 小時內提供 H-ISAC 客服信箱(hisac-cs@mohw.gov.tw)
  - 受害主機作業系統及用途
  - 惡意程式植入時間
  - 文件雜湊：勒索軟體文件的 MD5、SHA-1、SHA-256 。
  - 惡意 IP/域名：中繼站、攻擊來源及下載到惡意程式的網站。
  - 網路流量：從分析網路封包後發現的異常行為。
  - 檔案名稱/副檔名：.locked、.crypt 或隨機字串。
  - 機碼變更：開機啟動 ( 例如 HKLM\Software\Microsoft\Windows\CurrentVersion\Run ) 。

- 異常程序：非預期的 powershell.exe 或 cmd.exe 活動。
- 攻擊路徑：找出入侵的手法。(如利用弱點、工具、VPN 入口...等資訊)
- 額外步驟：若有取得惡意程式樣本，請將檔案加密壓縮寄送至 H-ISAC 客服信箱，壓縮密碼請設定為 virus。
- 目的：提供 IoC，以協助集體防禦

---

## 第三階段：恢復與重建 ( 接下來 72 小時+ )

此階段恢復運營，同時修補漏洞並強化防禦。

### 3.1 評估損壞與系統優先級

- 行動：識別關鍵核心 ( 例如 HIS、PACS、EMR、LIS、NIS 等 ) 。
  - 根據對病人照護的影響優先恢復。
  - 評估是否可進行備份復原(Online)，若不宜，則以單機作業或紙本作業。

### 3.2 清理與恢復系統

- 行動：從驗證過的乾淨備份重建受影響系統。
  - 重灌受感染設備(從可信來源重新安裝作業系統/軟體)。
  - 全院修補所有漏洞並更新軟體/硬體。

- 驗證：使用 EDR 工具持續監控，以確認系統處於安全狀態。

※ 參考國家資通安全研究院 EDR 連通測試通過清單：

[https://www.nics.nat.gov.tw/core\\_business/cybersecurity\\_defense/EDR/Related\\_Documents\\_and-Forms/](https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/EDR/Related_Documents_and-Forms/)

[https://download.nics.nat.gov.tw/api/v4/file-service/UploadFile/edr/EDR%E9%80%A3%E9%80%9A%E6%B8%AC%E8%A9%A6%E9%80%9A%E9%81%8E%E6%B8%85%E5%96%AE\\_1140115.pdf](https://download.nics.nat.gov.tw/api/v4/file-service/UploadFile/edr/EDR%E9%80%A3%E9%80%9A%E6%B8%AC%E8%A9%A6%E9%80%9A%E9%81%8E%E6%B8%85%E5%96%AE_1140115.pdf) 【請自行維護最新版本下載點】

### 3.3 透明溝通

- 內部：告知員工事件情況、恢復時間表和臨時程序。

- 外部：若病人資料受影響，應依「個人資料保護法」第 12 條規定通知當事人。
- 經驗教訓：根據調查結果更新安全政策。

### 3.4 文件記錄與分享

- 完成通報主管機關之續報：1、2 級事件要於 72 小時，3、4 級事件於 36 小時進行續報。
- 完成通報主管機關之結報：後續於 1 個月內進行結案，送交調查、處理及改善報告
- 召開調查檢討會議



## 事前預防措施

勒索軟體的攻擊路徑包含取得合法帳號、利用系統漏洞或植入惡意程式後，建立後門並試圖橫向擴散至其他系統或取得高權限帳號，再開始發動攻擊，唯有在每個環節導入防護措施，才能有效阻擋。

1. **帳號密碼控管**：加強密碼原則(例如至少 12 碼、包含英數大小寫及特殊符號)，並定期檢查高權限帳號是否有異常活動。
2. **落實資訊資產設備盤點**：應及時汰換或加強管制停止支援(EOS)及存在風險之設備。
3. **及時修補漏洞**：定期執行滲透測試及弱點掃描，漏洞修補完成後，仍應檢視修補期間是否已被零時差攻擊。
4. **提升同仁資安意識**：定期辦理資安教育訓練，並實施社交工程訓練，必免同仁誤觸惡意程式。
5. **制定通報應變程序並定期演練**。
6. **監控異常告警**：監控異常存取大量資料與未授權變更(如關閉防毒軟體)等行為，並啟用日誌記錄、異常告警、備份與刪除保護。
7. **建立網路架構圖及網段隔離**：記錄網路設備、IP 配置、通訊協定等資訊，並落實網段隔離避免橫向擴散。
8. **最小權限原則**：分配給使用者最低限度權限，禁止使用者自行安裝程式與使用 PowerShell，如需要額外權限應另行申請，且高權限帳號應有多重身分驗證保護。
9. **端點保護工具**：於端點設備安裝 EDR 及防毒軟體，阻止惡意程式並發出告警，並落實可攜式媒體控管，未授權裝置不得連接內部網路
10. **系統備份及備援**：
  - (1)重要資料至少備份 3 份，使用 2 種不同形式媒體，其中 1 份備份要存放異地，並定期進行測試還原演練。
  - (2)離線加密備份也很重要，因為大多數勒索軟體攻擊者會嘗試尋找並刪除可存取的備份或將勒索病毒放入備份中。
11. 如不慎遭到成功入侵，請盡速依本文辦理應變處置。