

**TLP:WHITE**



**勒索軟體攻擊案例分享—  
以勒索軟體組織 CrazyHunter  
之攻擊事件為例**

臺灣學術網路危機處理中心團隊(TACERT)製

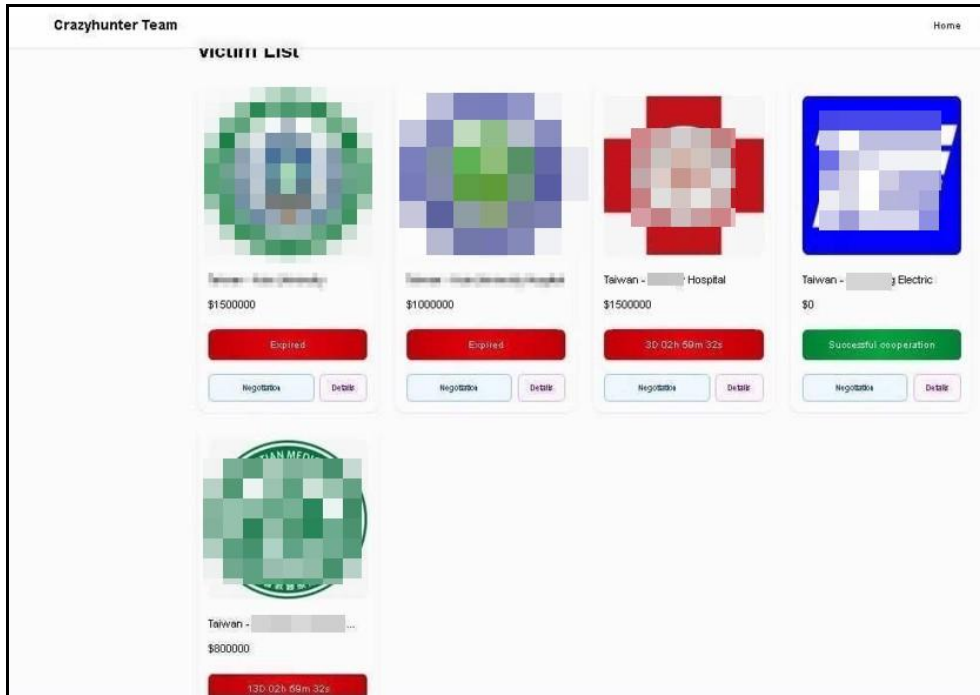
2025 年 09 月修訂 V2 版

## 一、事件簡介

1. 在連假期間學校人員接獲其外部附屬單位通知 A 系統主機疑似遭入侵做為跳板攻擊該單位系統之信件，之後兩天學校發現 A 系統主機與校園入口網站主機已被加密，兩天過後又發現備份主系統遭受攻擊無法直接進入系統，確認部分受害系統無法於可容忍中斷時間內使用系統備份復原。
2. 整個事件造成各資訊系統及網站（含官網、校務行政、DNS 主機等）的校級伺服器停止服務，無法於有可容忍中斷時間內恢復正常運作。經統計受影響主機高達五十台以上 VM 主機，其中有十多台核心系統主機，造成服務停止 6 天。
3. 該校多數系統因遭受攻擊造成服務中斷外，部分主機也遭加密，其中有多台主機是被透過 AD 網域派送勒索軟體後，執行加密。其中備份各系統 VM 的主機因部分備份 VM 遭加密導致這些系統需重建。

## 二、勒索軟體組織 CrazyHunter

1. CrazyHunter 為新的勒索軟體組織，自 114 年 1 月底起其攻擊活動不斷，其攻擊手法特徵有「使用開源工具、熟悉 AD 網域部署、善於隱匿 C2 與採用靈活戰術」等。
2. CrazyHunter 在暗網設立官方網站，詳細列出受害者名單、入侵證據以及相關「服務」資訊，而本案例受害學校也被列名於該網站上。
3. 在受害者列表（Victim List）上，受害機構僅來自台灣，涵蓋醫療（兩家醫院）、教育單位（某大學及其附屬醫院）與製造業。每個受害案例包含：勒索金額（最高可達 150 萬美元）、交易狀態（如 Expired 代表數據即將公開、Successful cooperation 代表已支付贖金）、倒數計時器等資訊，藉此對受害者施加心理壓力。



圖片:CrazyHunter 網站

### 三、事前預防

在勒索軟體攻擊事件發生之前，對於預防遭受攻擊方面，可由下列各項內容進行防護。

#### 1. 了解勒索軟體的散播管道

為了預防感染勒索軟體，建議管理者對勒索軟體的攻擊途徑有所了解。

##### (1) 網站瀏覽

瀏覽網站時，倘若使用者電腦存在 Java/Flash/Adobe/瀏覽器等軟體漏洞，當輪播到惡意廣告，便可能遭受勒索軟體入侵。點選到網站內的惡意連結(如：廣告、新聞)，便可能遭受勒索軟體入侵。誘騙使用者連到看似真正銀行或政府機關網站的假網站(山寨網站)。

##### (2) 電子郵件感染

當使用者點選或開啟電子郵件中的惡意連結或內嵌惡意程式的附件檔案，便可能遭受勒索軟體入侵，曾發生之勒索軟體電子郵件主旨

包含：退稅通知、電子帳單/電子發票、。假冒電子商務或購物網站  
訂單出貨通知(例如 Amazon.com)、Google Chrome 和 Facebook 重  
大更新和通知訊息、iPhone 中獎通知、求職信/履歷表、電子計聞、  
誘騙使用者連到看似真正銀行或政府機構網站的假網站、輸入驗證  
碼(CAPTCHA，一種防止機器人的程序)、您的帳戶欠款已過期。

### (3) 非法軟體感染

網路上非法軟體或小工具可能含有惡意程式，若使用者下載安裝這  
類非法軟體或小工具，惡意程式可能在安裝過程中讓使用者授權以  
存取機密資料或加密資料。許多勒索軟體會先利用 dropper 等惡意  
程式感染主機，在取得控制權後才會從惡意中繼站下載勒索軟體來  
執行。

### (4) 被已遭受勒索軟體攻擊的電腦或裝置感染

勒索軟體可能透過已遭受攻擊的電腦或裝置掃描使用者電腦所連結  
的磁碟機，包括本機的硬碟、連結電腦的 USB 磁碟、網路芳鄰磁碟  
機、雲端硬碟及檔案伺服器的檔案，只要能被循線找到，就都有可  
能遭受勒索軟體入侵。

### (5) 利用資安漏洞駭入系統感染

勒索軟體可利用產品漏洞或系統漏洞，如 NAS 存在弱密碼、  
WannaCry 之 SMB 協定漏洞，來駭入設備系統執行勒索軟體。

### (6) 透過 APT 攻擊感染

此為潛伏期長且深度隱藏的攻擊手法，入侵到內網後，取得管理者  
帳號與密碼等資訊，在內網橫向擴散勒索軟體。它通常以網域控制  
站為目標，並將其當作散播勒索軟體的中轉站。在攻擊者取得 AD  
伺服器的控制權後，會將勒索軟體散播到 AD 網路中所有的主機內。

### (7) 透過第三方的託管服務入侵

學校所委外使用的雲端託管服務建議來自可信賴的供應商，並且需

做好身分與密碼管理，因為攻擊者可能透過廠商連線管道來散播勒索軟體於內部網路中。

## 2. 保護系統免於感染勒索軟體

- (1) 定期更新防毒軟體病毒碼，並更新系統與軟體至最新版本。
  - a. 建議每周至少一次對全系統執行一次掃描。
  - b. 當連接儲存設備(如:隨身碟)時應先執行防毒軟體掃描作業。
- (2) 加強具有派送軟體功能之伺服器安全，例如:AD 伺服器、防毒軟體  
中控主機因具有派送軟體的功能，需更注意安全更新，與留意主機  
是否有不正常異動狀況。
- (3) 限制微軟 Office 巨集的啟用時機，因為勒索軟體可透過 office 檔案  
來啟用巨集的方式散播。
- (4) 限制開放使用的 port，因為勒索軟體可能利用開放的 port 或對外啟  
用的服務散播，因此確認 port 開放的必要性是很重要的。
- (5) 管控存取權限，提供最小權限給人員使用，例如:設定人員遠端登入  
時存取最低權限。定期檢視各帳號使用的情形，實施多因子的身份  
驗證，以及停用已不活動的帳號。
- (6) 定期提供人員教育訓練，以加強資安觀念。
- (7) 定期進行系統備援，針對重要的核心系統應規劃備援機制，以確保  
服務不中斷。
- (8) 啟動系統日誌功能，確保持續記錄系統故障或異常狀況。

## 3. 保護重要資料

- (1) 定期維護備份資料，並且保持存放資料主機的離線。
- (2) 對於重要或敏感資料進行加密，以防資料被竊時造成外洩。
- (3) 依資料重要性與使用範圍管控讀取權限。
- (4) 採用 3-2-1 備份原則，3 份備份、2 種儲存媒體、1 個不同的存放地  
點。

(5) 定期維護重要系統的映像檔，以便遭遇攻擊時能快速重建系統。

#### 4. 建立妥善的事件應變計畫

- (1) 擬定應變計畫進行演練，並檢視計畫之可行性。
- (2) 加入資安情資分享組織，以取得資安預警、資安威脅與資安弱點等情資。

### 四、事中應變

當發現遭受勒索軟體攻擊時，有下列處理措施提供參考。

1. 立即斷開與受感染主機的所有網路連線。若系統服務因為勒索軟體影響而中斷，確認是否有備援主機可運作，並在與感染主機隔絕狀態下，啟動備援機制，以維持系統服務不中斷。若系統服務無法短時間內恢復，可將所有連到受感染主機的連線導向系統修復中的網頁頁面。
2. 對受害主機進行證據保全作業，盡可能保留受感染主機的狀態與內部資料，如為虛擬主機建議當下執行快照或關機匯出該主機系統，以利後續鑑識所需。
3. 區段隔離受害主機所在實體網路，清查與確認受感染主機同一區域內的其他主機是否有感染現象。待盤點出可能受影響主機後，對這些主機進行預防性隔離與執行掃毒。
4. 清查受影響業務資料範圍，以本案件為例，包含所有行政業務的機敏資料，並研議若資料外洩或毀損時執行之因應對策。
5. 依照程序在法規規定時間內進行資安通報，啟動組織內資安事件應變措施。
6. 由於需確認感染哪一種勒索軟體，建議從主機上取出勒索通知信(ransom note)與兩個被加密的檔案，送至 ID Ransomware 勒索軟體識別網站(<https://id-ransomware.malwarehunterteam.com/>)檢測，以確認勒索

索軟體的類別與是否有解密工具的資訊。另外，也可在 no more ransom project 網站上( <https://www.nomoreransom.org/zh/index.html>)，尋找解密工具。若未能找到解密工具，可將被加密的檔案備份到安全的地方，以待未來出現解密工具時解密。

7. 尋找外部專業鑑識團隊，進行鑑識作業，找出攻擊手法與入侵管道。可將系統日誌檔進行備份，連同受感染主機的系統備份，交由鑑識團隊進行分析，以了解事件發生原因與避免再次遭受攻擊。
8. 可檢視檔案修改時間來判斷出駭客執行勒索軟體的時間，進而以此時間比對學校對外防火牆的連線紀錄，來追蹤可能的駭客來源 IP。
9. 檢視受害主機內的背景程式，確認勒索軟體是否仍在背景程式中執行。若仍執行中，需中止並移除該勒索軟體後，才可對受害主機執行檔案存取或系統修復作業，以免觸發第二次檔案加密攻擊，

## 五、事件分析

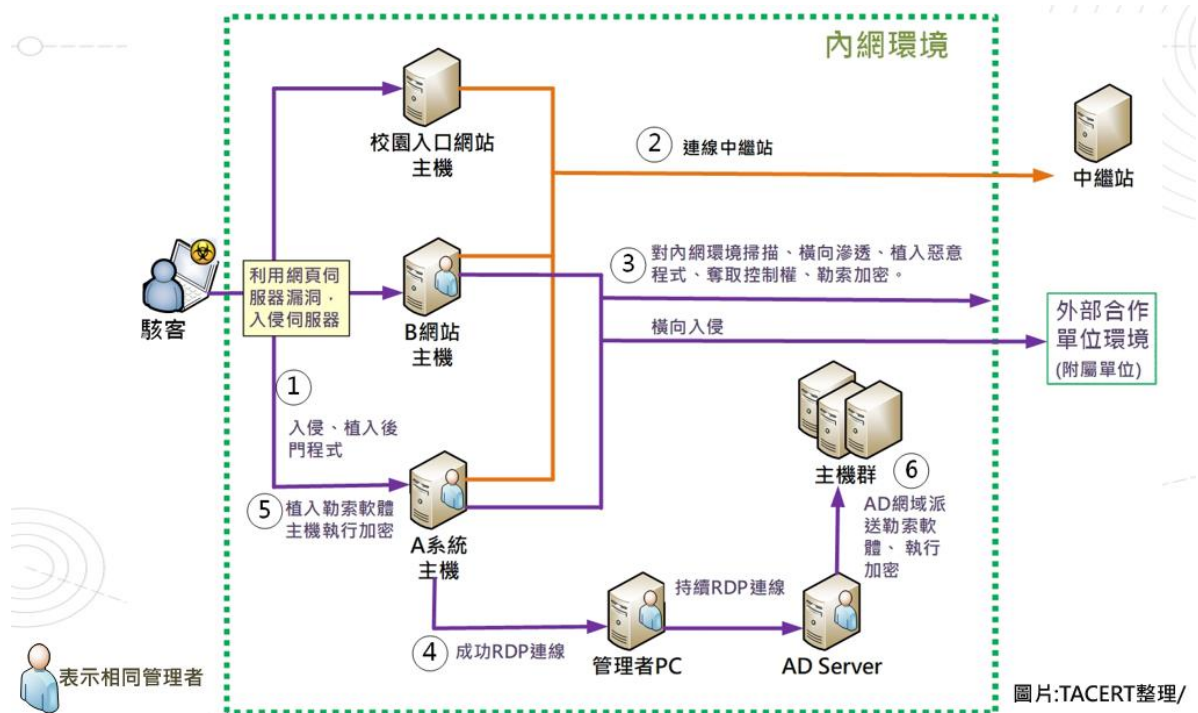
本案例在經由資安公司進行鑑識作業取證後，透過分析得知本案駭客的攻擊手法與入侵管道如下所述。

1. 駭客於發動勒索軟體攻擊前一個半月入侵 A 系統主機後植入後門程式，之後再開始發動一系列攻擊。
  - (1) 利用網頁伺服器漏洞入侵 B 網站主機。
  - (2) 使用校園入口網站主機、A 系統主機與 B 網站主機陸續連線中繼站。
  - (3) A 系統主機與 B 網站主機對內網環境掃描、橫向滲透、植入惡意程式、奪取控制權與勒索加密，同時也開始橫向入侵其外部附屬單位的系統。
  - (4) 取得學校人員的通訊軟體帳號，對學校進行恐嚇。

2. 造成本次多台主機被勒索軟體加密的主要原因為駭客在駭入 A 系統主機後，RDP 遠端連線登入管理者個人主機，取得大量主機連線資訊與帳號密碼列表相關文件，同時該主機也遠端連線登入 AD 伺服器中，因該 AD 伺服器自攻擊事件發生前一週與管理者個人主機建立連線後就沒斷線。接著駭客利用 AD 伺服器派送勒索軟體給 AD 網域中各受害主機，最後導致這些主機被加密。

## 六、事件攻擊行為

本事件一開始起於駭客利用網頁伺服器漏洞入侵主機、植入後門程式，在潛伏一個半月後開始發動一系列攻擊。駭客使用已經被入侵的校園入口網站主機、A 系統主機與 B 網站主機來連線中繼站，接著利用 B 網站主機與 A 系統主機對內網環境進行掃描、橫向滲透、植入惡意程式、取得主機控制權與執行勒索軟體的加密作業等，同時也對外入侵外部合作單位的主機。這期間 A 系統主機成功 RDP 連線到管理者電腦，而管理者電腦本身與 AD 伺服器連線中，因此駭客透過 A 系統主機將勒索軟體一路送至 AD 伺服器中，最後使用 AD 網域派送勒索軟體至其網域內各主機中，並且執行檔案加密作業。



## 七、事後復原

在事件發生應變處理後，緊接著進行後續的復原作業與改善措施。針對本案例有下列事後處理事項提供參考。

1. 使用系統備份檔案還原受害主機，恢復系統服務。在利用備份進行還原之前，需確認該備份有無任何惡意軟體或存在任何系統漏洞。在確認該主機備份與連接主機的設備是乾淨狀態下，才可進行還原作業。
2. 將主機連接至安全的網路，以利下載、安裝與更新作業系統與應用軟體。
3. 定期更新與執行防毒軟體掃毒作業。
4. 根據調查出的事件發生原因，進行改善措施，確保不會再次發生相同事件。針對本案有下列的改善措施，提供參考。
  - (1) 提升學校人員處理資安事件的敏感度與積極性。
  - (2) 各網站主機可安裝 MDR 主動式端點偵測系統，來隨時監測主機狀態。
  - (3) 建議對上線之網站主機定期進行弱點掃描等安全檢測，以降低可能

存在的風險。

- (4) 加強遠端連線作業之管理，例如：限制連線的時段與連線的來源 IP。
  - (5) 定期更新各主機的系統與修補漏洞。
  - (6) 建議系統管理者勿使用同一組帳號與密碼來同時管理多台主機。
  - (7) 對於主機內重要資料的保存作業，建議壓縮加密後才存於主機內。
  - (8) 定期備份各網站主機資料，資料備份所存放的設備可平時離線，視需要上線。
  - (9) 落實密碼安全原則，定期變更密碼。
  - (10) 加強具有派送軟體功能之 AD 伺服器安全性。
5. 調查勒索軟體攻擊後是否有資料外洩情況，例如：調查公開資料或暗網等地方。可利用 haveibeenpwned、Firefox monitor 或 OSRFramework 等工具調查，也可尋求外部資安公司協助。若有資料外洩事實，應確認外洩資料欄位與外洩資料筆數，並根據資料受影響範圍，通知相關利害關係人。

## 八、總結

本案為近幾年中學校遭受勒索軟體攻擊受害最嚴重的事件，導致該校核心系統服務停止長達 6 天。造成許多台主機感染勒索軟體的原因是因駭客使用 AD 伺服器派送它，而 AD 伺服器因為管理者登入後長期未中斷連線，以致於管理者電腦被駭入後，讓駭客直接入侵到 AD 伺服器。又駭客發動攻擊時間為連假期間，學校在內部人員溝通與事件應變反應方面比較遲緩，加上存放系統備份的主機也遭受攻擊，導致在事件應變與事後復原方面需花較多時間來恢復所有服務。