

TLP:WHITE



**勒索軟體組織 CrazyHunter
攻擊學校事件分析報告**

臺灣學術網路危機處理中心團隊(TACERT)製

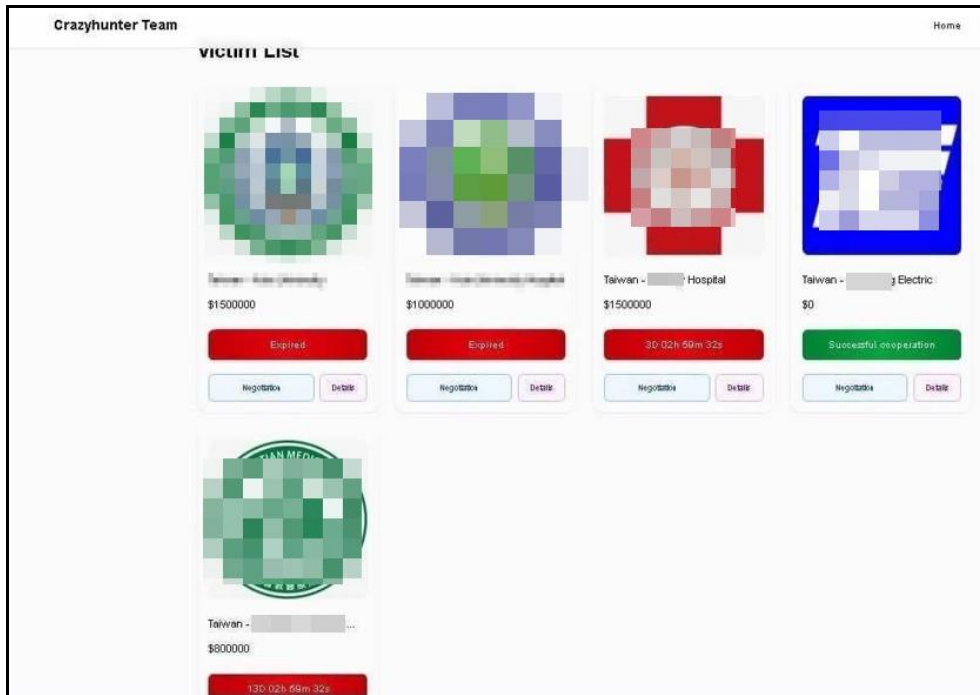
2025 年 05 月

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

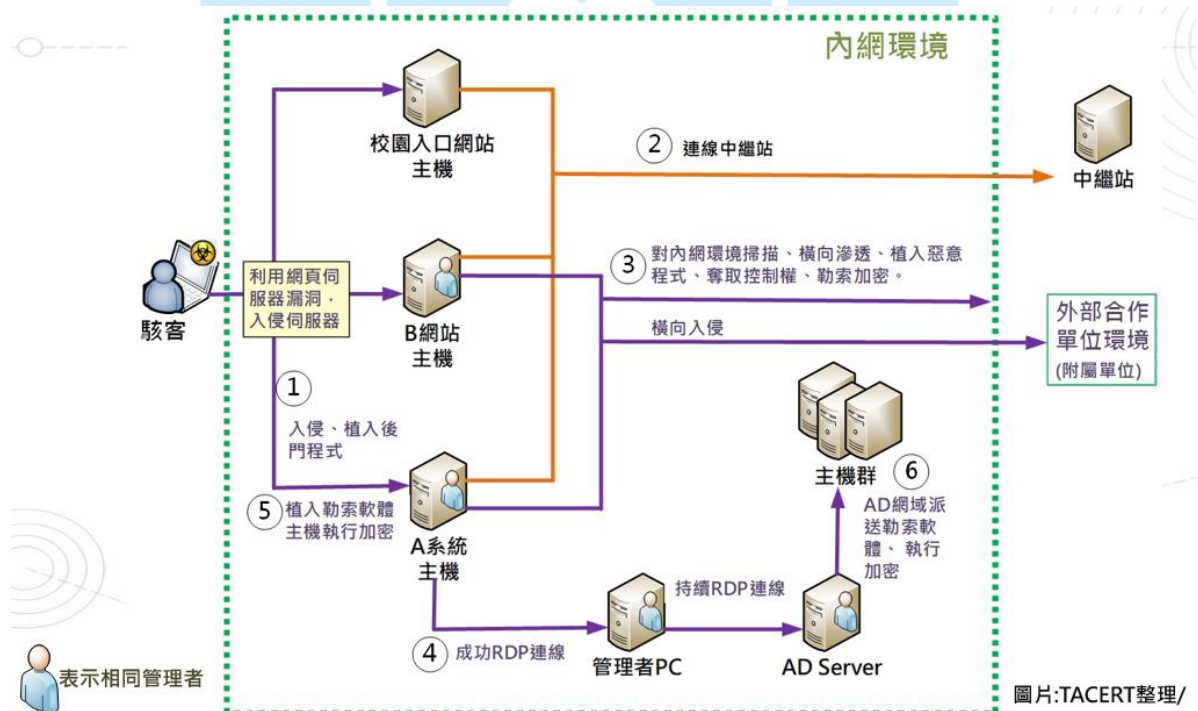
三、事件分析

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。

四、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。



五、總結與建議

1. 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。
2. 在處理勒索軟體的攻擊事件方面有下列的處理方式，提供學校參考。
 - (1) 封鎖受害主機所在網段之網路。
 - (2) 清查網段內各主機感染勒索軟體的情形。
 - (3) 對受害主機進行證據保全作業，以利後續執行鑑識所需。
 - (4) 可取出 2 個被加密檔案與勒索通知信檔案至 ID Ransomware 網站 (<https://id-ransomware.malwarehunterteam.com/index.php>) 或 No More Ransom 網站 (<https://www.nomoreransom.org/crypto-sheriff.php>) 判斷勒索軟體的類別。
 - (5) 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。
 - (6) 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。
 - (7) 使用系統備份檔案還原受害主機，恢復系統服務。
3. 針對本案例有下列建議的防範措施，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。

