勒索軟體防護指南

2. 事中 – 遭受勒索軟體攻擊時的應變措施

2.1 如何識別遭受勒索軟體攻擊?

受到勒索軟體攻擊，初期特徵是因為對大量檔案做加密運算，所以會發現硬碟、CPU 或記憶體使用率會大幅提升，另外，受影響的檔案通常會被修改副檔名。

檔案被加密結束後，在大多數的狀況下，因勒索軟體需要向受害者要求贖金，所以會將勒索訊息顯示在設備螢幕上，亦或是留下相關文件，也會有連絡方式，讓受害者可以與攻擊者溝通付款的議題。

攻擊者甚至可能威脅要在網上發布數據以迫使受害者支付贖金，例如：MAZE 勒索軟體的攻擊者，公佈了 Hammersmith Medicines Research 的醫療檔案以迫使他們支付贖金。

2.2 應變措施

(1) 損害降低

- 立即斷開受感染設備與所有網路的連接，無論是有線、無線還是基於行動網路。在非常嚴重的情況下，可考慮關閉 Wi-Fi、禁用任何核心網路連接（包括交換機）以及斷開 internet 連接。
- 若系統服務遭受勒索軟體影響而中斷，在確認備援機已與感染網路隔絕，並正常運行後，即可啟動系統備援機制，以維持系統服務不間斷。

(2) 報案與通報

- 依內部通報程序進行通報，啟動相關應變措施。
- 向就近的派出所報案並提供受駭侵佐證資料，或尋求法務部調查局/內政部刑事警察局的協助。
- 透過 TWCERT/CC 官網(twcert.org.tw)或 Email(twcert@cert.org.tw) 進行資安事件通報。
- 尋求外部資安專業單位協助事件處理。

(3) 損害評估

- 區段隔離實體網路並監控流量以確認感染範圍。

- 盤點可能受影響設備，將這些設備進行預防性的隔離，並對這些設備執行防毒軟體掃描。
- 盤點受影響資料範圍，包括: 設計開發、測試、財務、客戶、供應商、帳號密碼等機敏資料，以備研議資料毀損或外洩之因應措施。

(4) 識別病毒及備份加密檔案

- 大多數被勒索軟體加密的資料難以被破解，但仍可嘗試透過勒索軟體名稱、副檔名等資訊，檢閱該病毒的類型，在 no more ransom project[1] 的網站上，尋找可信任資安單位提供的解密工具。
- 針對未能找到解密工具的檔案，可以先將這些檔案備份到安全的地方，當未來出現解密工具時就可以使用。
- 將系統日誌檔進行備份，交由外部資安團隊進行分析，可以了解事件發生原因，進行降低二次感染的機會。

[1] https://www.nomoreransom.org/zht_Hant/decryption-tools.html

參考資料

[1]https://jenner.com/system/assets/assets/11480/original/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.pdf
[2]https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
[3] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks