勒索軟體處理指南

事中 – 被勒索軟體攻擊時的應變措施

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，也會有連路方式，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. 應變措施

(1) 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。

(2) 向調查局/刑事局報案，尋求協助。

(3) 透過 TWCERT/CC 官網(twcert.org.tw)或 Email(twcert@cert.org.tw) 進行資安事件通報。

(4) 尋求外部資安專業單位協助事件處理。

(5) 依內部通報程序進行通報，啟動相關應變措施。

(6) 監控網路流量並執行防毒掃描以確定是否仍有感染。

(7) 盤點可能受影響設備，並對這些設備執行防毒軟體掃描

(8) 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。

[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