

勒索軟體處理指南

事中 - 被勒索感染後的應變措施

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，並通報 TWCERT/CC。
- (3) 尋求外部資安專業單位協助事件處理。
- (4) 依內部通報程序進行通報，啟動相關應變措施。
- (5) 監控網路流量並執行防毒掃描以確定是否仍有感染。
- (6) 盤點可能受影響設備，並對這些設備執行防毒軟體掃描
- (7) 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 project¹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