

勒索軟體事後回復指南

事後 – 回復階段的作法

- (1) 重置包括密碼在內的權限憑證。
- (2) 確認受感染設備已完全的清除並重新安裝作業系統。
- (3) 在利用備份進行還原之前，需確認該備份沒有任何惡意軟體，如果已非常確認備份和連接它的設備是乾淨的，則恢復工作應該只從備份進行。
- (4) 將設備連接到乾淨的網路，以便下載、安裝和更新作業系統和所有其他軟體。
- (5) 安裝、更新和執行防毒軟體。
- (6) 建議將攻擊事件資訊藉由 TWCERT/CC 分享(去識別化)，以幫助國內外其它企業組織防範相關攻擊，減少勒索軟體的影響。
- (7) 依受駭原因，規劃改善措施並執行。

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>