◎資訊安全宣導

—網路安全事件：勒索軟體的發展階段—

RaaS 已成為新興的商業模式，因為它允許任何人利用漏洞並發起攻擊，它也被證明是一種有利可圖的商業模式；如同 Colonial Pipeline 與水廠事件，當營運中斷或遭惡意入侵時都可能危及生命。攻擊者瞭解到關鍵基礎設施組織是有利可圖的目標，他們不僅有足夠財力，且他們將不惜一切代價以恢復營運。

趨勢公司研究後得出以下結論

1. 勒索病毒是存在已久卻仍在持續演進的威脅：從 DarkSide 最近活動就能看出，今日勒索病毒在許多方面都已進化，包括更大的攻擊目標與更進階的勒索技巧。
2. 勒索集團不再只滿足於將電腦鎖死，讓企業無法動彈來獲得贖金;現在，他們還會深入挖掘企業網路以找到更多獲利方法。例如，遭駭客入侵的雲端伺服器可能再經歷另外的攻擊流程，資料遭竊轉賣。已遭入侵的企業資產，在地下市場可說是暴利商品。
3. 趨勢科技總監 Jon Clay 列出勒索病毒發展階段：。

第 1 階段：單純只有勒索病毒。將檔案加密，留下一封勒索訊息，然後等著收錢。

第 2 階段：雙重勒索。第 1 階段＋將資料外傳然後威脅公開資料。Maze 是第一個採用此手法的已知案例。

第 3 階段:三重勒索。第 1 階段＋第 2 階段＋DDoS 攻擊威脅。SunCrypt、RagnarLocker 和 Avaddon 是率先採用此手法的已知案例。

第 4 階段:三重勒索。第 1 階段＋第 2 階段＋DDoS 攻擊威脅。SunCrypt、RagnarLocker 和 Avaddon 是率先採用此手法的已知案例。

【文章擷取-法務部調查局清流雙月刊】

臺中榮民總醫院提醒你!也關心你!