美東燃油輸油管系統運營商「殖民管線」遭駭客勒贖軟體攻擊，被迫暫停所有管道運作，凸顯勒贖軟體對基礎設施的威脅。華爾街日報從以下幾個方面說明企業如何應對勒贖軟體攻擊。

•勒贖軟體如何運作？

勒贖軟體使用加密程式鎖住受害者的重要資料，勒索受害者支付贖金來解開加密系統。資安公司 Coveware 表示，今年第一季駭客要求的贖金平均為 22 萬零 298 美元（約台幣 611 萬元

•勒贖軟體對企業的威脅有多大？

美國國土安全部長梅奧卡斯 5 日說，勒贖軟體威脅國家安全，去年發生的勒贖軟體攻擊中，約有七成五受害者是小企業，這些企業總共付了 3 億 5 千萬美元（約台幣 97 億元）贖金。一些駭客組織除了會用勒贖軟體鎖住檔案之外，還會威脅公布敏感資料。

•如何降低被勒贖軟體攻擊的風險？

資安分析師指出，許多勒贖軟體攻擊是從普遍的資安漏洞牟利。美國國土安全部旗下的網路安全及基礎設施安全局建議，企業應多管齊下預防被駭客勒贖，包括勤於更新軟體、定期修補安全漏洞等。

•被勒贖軟體攻擊後該怎麼辦？

美國聯邦調查局、特勤局等執法機關表示，被駭客勒贖的公司應向治安單位求助。

•要從勒贖軟體攻擊復原，有哪些選項？

網路安全及基礎設施安全局執行助理主任戈德斯坦指出，適當備份資料，能使企業在被駭客勒贖後，無須駭客破解加密程式就恢復系統正常運作，「這是從勒贖軟體攻擊復原最有效的方法」。

•被勒贖軟體攻擊該付贖嗎？

•被勒贖軟體攻擊該付贖嗎？

聯邦調查局建議受害者不要付贖。處理過駭客勒贖事件的資安專家往往指出，駭客拿到贖金後不見得會破解加密系統，而且駭客得逞一次後很可能食髓知味，再度勒贖。

•在遏制勒贖軟體攻擊方面，美國政府做了哪些努力？

美國司法部最近設立一個任務小組，研究如何遏制勒贖軟體攻擊。另外，美國政府官員和微軟、亞馬遜、火眼等科技公司共組的「勒贖軟體任務小組」，4 月 29 日發布報告，建議拜登政府，由白宮主導設立跨部會工作小組，加強管制加密貨幣，因為駭客往往要求受害者用加密貨幣付贖。

Scripted from : 2021-05-10 23:00 聯合報 / 編譯李京倫 /