KASEYA: IT SOFTWARE MANAGEMENT

Kaseya主要的業務是為向託管服務提供商提供IT管理軟體，協助沒有自己IT部門的小型企業管理系統、防範IT意外。然而其中一個管理軟體Kaseya VSA卻在美國7月2日下午遭受駭客組織攻擊，使全球上千家中小企業被勒索軟體威脅。

這次攻擊中使用的是REvil勒索軟體，主要攻擊便是MSP業者。駭客利用前幾週Kaseya VSA才被資安人員發現的缺陷，對此發動零日攻擊。Kaseya強調他們已經確認被駭客利用的漏洞，正在對此進行補救當中。

後續Kaseya也通知所有VSA客戶關閉伺服器，防止災害進一步擴大。

最早發現這次攻擊的資安公司Huntress Labs高級資安研究人員約翰．哈蒙德指出，約有30家IT外包服務廠商在這次攻擊中受到影響，導致勒索軟體的攻擊範圍擴散至全球至少17個國家、地區，可能有上千家企業受害。

而Kaseya執行長佛萊德．沃克拉透露，由於主要受害的是「客戶的客戶」，因此很難確切評估實際的影響，但他們估計約有800至1,500家企業在這次事件中受到影響。

不過沃克拉表示，Kaseya本身並沒有受到任何傷害，自從攻擊事件爆發後，員工們整個週末都在努力搶修恢復服務，並計畫向所有客戶發布更新，填補被駭客利用的漏洞。

聲稱執行這次攻擊的駭客組織，則公開聲稱他們已經加密了超過100萬個系統，並對這次攻擊要求7,000萬美元的贖金，並以比特幣的方式支付，強調只要收到贖金，所有被鎖定的系統都會在一小時內恢復。倘若駭客組織拿到贖金，這將成為史上金額最高的勒索軟體攻擊事件。

勒索軟體攻擊爆發後，Kaseya也積極與聯邦調查局、美國國土安全部合作，著手對這次事件進行調查。沃克拉表示，他已經與白宮、FBI、CISA就漏洞問題進行過討論，但目前沒辦法對外透露相關事宜，僅強調當一切安全時，才會公開漏洞的細節。

這次攻擊也驚動了美國總統拜登，在週末便下令要求調查這次攻擊的幕後黑手。外界推測這次攻擊背後可能與俄羅斯有關。

美國政府擔憂，這次攻擊可能不僅僅傷害全球各個中小型企業，甚至可能對國安造成威脅。不過沃克拉目前指出，他們沒有發現任何國家重要單位受到攻擊，也沒有參與任何大規模的基礎設施。