案例分享–某企業OT產線長期受勒索病毒感染，無法根除

- 12月 12, 2022

雲智維科技
Cloud Intelligent Operation, CIO

某企業OT產線長期受勒索病毒感染，無法根除

一、案例故事

某企業客戶於某日下午OT產線數台主機遭受到WannaCry勒索病毒感染，其嚴重影響產線運作，企業透過多方管道購買相關SOC服務以及防毒軟體，仍無法找到真正來源並根除，該企業藉由「雲智維資訊顧問代管代維方案」主動找出企業內部資安問題，並根除長期無法解決的困擾。

註：WannaCry勒索病毒於2017年開始肆虐全世界各地，其勒索病毒是利用作業系統漏洞主動進行攻擊，只要電腦開著且聯網，以及尚未修補Windows EternalBlue【永恆之藍】漏洞就可能遭到入侵並將系統檔案進行加密。

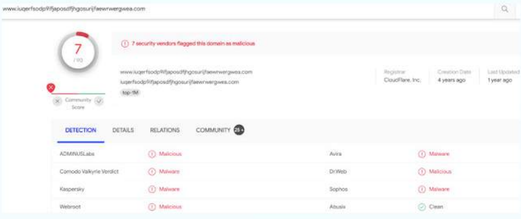
二、解決方法

使用「雲智維資訊顧問代管代維方案」，收集客戶單位中各種網路設備syslog、資安設備syslog、Flow及SNMP，從各式數據搭配AI即時分析，從中查找出重要的關鍵數據，找出客戶內部環境網路、資安問題所在。

該企業使用「雲智維資訊顧問代管代維方案」，從該企業所收集到的DNS和AD數據中發現數台OT產線主機對WannaCry勒索病毒惡意網域【www[.]iuqerfsodp9ifjaposdfihgosurijfaewrwergwea[.]com】連線以及對其他在線的OT產線主機進行帳號和密碼猜測行為。

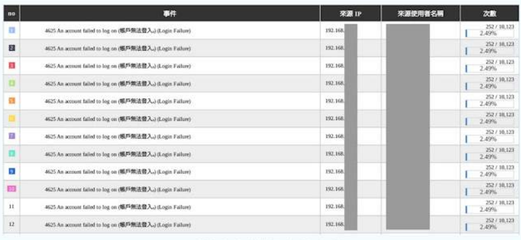
該企業某日下午導入OT產線DNS數據後，立即發現數台已中毒的產線主機主動對外發起大量連線，其連線的目的主機皆為WannaCry勒索病毒網域。

OT產線中毒主機連線WannaCry勒索病毒網域



WannaCry惡意網域驗證

產線中毒主機不僅對惡意網域連線，也對內部其他在線產線主機進行帳號和密碼猜測，共嘗試44組帳號，意圖橫向感染其他電腦。



OT產線中毒主機暴力破解紀錄

建議改善措施：

1. 產線機台已遭植入惡意程式，故建議立即隔離該台主機並重新安裝。
2. 如因業務需求無法立即重新安裝，則建議啟用備援設備並針對該台有問題之主機進行防毒軟體掃描作業，於啟用後立即重新安裝該台主機。
3. 產線機台正常運行為企業重要核心業務，須進行實體隔離，管控進出流量，預防各類網路惡意程式的感染，降低資安風險。

三、結論

該企業使用「雲智維資訊顧問代管代維方案」，解決長期無法根除的勒索病毒問題，從企業導入的數據中發現數台OT產線持續發起大量連線至惡意網域，且也嘗試對其他在線的產線主機進行帳號和密碼猜測，其意圖橫向感染其他主機，使用「雲智維資訊顧問代管代維方案」，能夠主動幫企業找出問題點所在，並給予企業相關建議，而該企業逐步進行處理後，將此主機進行處置，成功預防內部資安事件擴大。

案例分享 勒索病毒

位置： 雲智維科技