ThreatSonar
APT威脅鑑識及回應工具

駭客威脅持續發生，進階持續威脅(APT)攻擊機會也不斷升高，企業每年投注愈來愈多的設備與人力預算，仍難以有效地發覺或阻止APT攻擊。當攻擊事件確認時，企業機敏資料往往已經被竊取。

有鑑於此，專注全球威脅情資分析與研究的TeamT5團隊，將獨特APT追蹤分析、數位鑑識方法，結合數千真實惡意程式和事件反應案例經驗，發展出【ThreatSonar APT威脅鑑識及回應工具】。

截至2021年10月，ThreatSonar已成功偵測超過350起確認的新APT事件，其中至少70%攻擊成功避開受害單位既有資安設備偵測，更有20%以上事件採用全球未知、全新的攻擊手法，針對遭受威脅情況與範圍，強化客戶資安範疇，降低同質威脅事件發生機會。

產品特色：

- ✓ 威脅報告簡單易懂，快速事件反應(Incident Response)，掌握每個端點狀況，視覺化的威脅獵捕工具。
- ✓ 架構彈性部署容易，不論是On-Premise、AWS雲端甚至筆記電腦，相容於多種虛擬化架構。
- ✓ 無需安裝常駐程式，派送後於背景掃描，平時不佔用端點硬體資源，無驅動程式，無相容性問題。
- ✓ 支援自訂惡意程式規則Yara rule與外部威脅情資Threat Intelligence匯入，可快速帶到每個端點比對。
- ✓ 快速高效率鑑識工作，平均每台端點檢測30分鐘，硬體資源充足下，可達到每小時5,000台端點以上大規模鑑識。

多層次威脅防禦：

- ✓ 第一層威脅模型：能夠透過3,000種以上動靜態特徵偵測已知威脅。
- ✓ 第二層威脅情資：以自行研究情資，與匯入外部第三方情資，有效偵測已知但我方未知的威脅。
- ✓ 第三層威脅狩獵：透過統計關連分析比對行為特徵，主動找出未知威脅。

ThreatSonar

The Last Line of Cyber Defense

獨特技術：

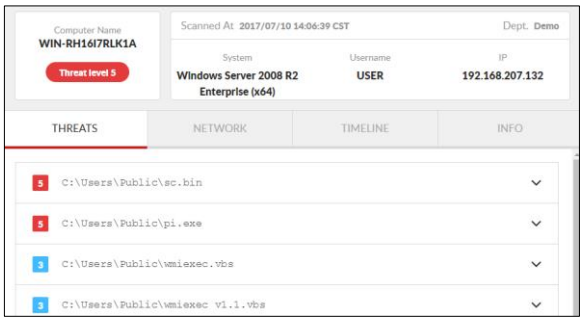
✓ 智能鑑識（Compromise Assessment）
- 真實案例訓練的APT風險模型
- 自動鑑定數百種動態行為異常
- 動/靜態混合偵測分析惡意程式
- 如記憶體、檔案、網路連線、系統登錄檔、機碼、啟動程序、執行程序、檔案、動態連結函式庫。

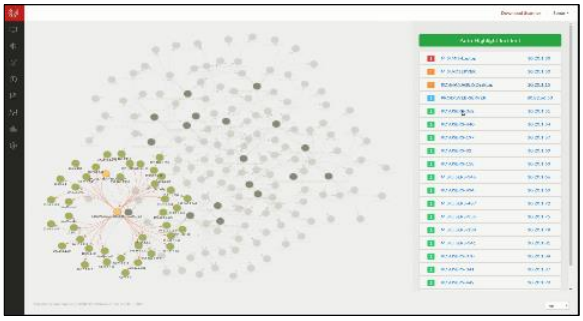
✓ 情資驅動（Threat Intelligence）
- 將第三方情資帶到每個端點
- 內建數千種亞洲APT後門特徵
- 匯入hash、IP、domain外部情資
- Yara rule動態IoC掃描所有端點
- 可雲端情資比對或離線斷網運作

✓ 自動調查（Auto Investigation ）
- 發掘攻擊事件起源及過程
- 追溯內網移動足跡
- 發掘資料外流路徑
- 時間軸Timeline呈現先後
- Graph Auto Analysis自動展開
- 調查各種攻擊手法TTP情境

✓ 威脅狩獵（Threat Hunting）
- 統計關聯分析找出未知手法
- 建立基準線鎖定Outlier
- 組織中稀有程式或目錄
- 合法系統工具遭到濫用
- 具數位簽章的惡意程式

✓ 自動聯防（Orchestration ）
- 開放API整合既有防護設備
- 自動化傳遞告警及更新情資
- 發送告警到SIEM設定規則阻擋
- Restful API下載報告及樣本
- 程式化更新情資調整偵測規則





用戶肯定：

TeamT5團隊由致力於全球資安攻防研究的白帽安全專家組成，長期研析各類駭客行為、手法與攻擊工具，追蹤監控隱匿幕後的攻擊團體。成員多數曾任職知名國際資安大廠，擅長亞太區網路間諜防護，HITCON台灣駭客年會中擔任長期義工，並於多個國際頂尖資安研討會中發表研究成果（Black Hat、TROOPERS、CODE BLUE等）。

產品服務遍及全球百大企業，如日本大型電信集團、電機製造商、綜合商社；並結盟美國、韓國、歐洲知名資安大廠；在台灣也獲得國防、金融、高科技產業、政府機關、大型SOC與資安顧問業者採用。

採購資訊：

☐ ThreatSonar APT威脅鑑識及回應工具包
(5端點/1年授權/支援Windows、Linux及Mac)
- ThreatSonar管理平台安裝
- 端點掃描程式軟體設定
- 協助遭到入侵端點清除威脅及調查是否有其他威脅

端點掃描程式系統需求

Windows：XP SP3及Server 2003 SP2以上；Linux：Kernel 2.6以上；Mac：MacOS 10.13以上

TEAMT5 杜浦數位安全

Website https://teamt5.org/ | Facebook TeamT5.org | E-mail sales@teamt5.org | Tel +886-2-7706-1299