技術優勢

即時回溯追蹤惡意威脅通訊行為解析 1500 萬+ (攻台) 靜態特徵碼
AI 未知惡意威脅程式行為解析 3000 萬+ 駭客 IP 與短期網域
沙箱惡意超連結下載解析 APT 攻擊連線反制
沙箱惡意程式行為解析 雙認證白名單

即時回溯追蹤惡意威脅通訊行為解析

APT (Advanced Persistent Threat) 進階持續威脅常見攻擊手法為鎖定目標後，蒐集情資、設計誘餌與執行任務；其中設計誘餌常見手法為假冒客戶、政府單位與知名服務提供者，例如 Apple、Google、國稅局、健保局與國際快遞等。此類社交工程信件由於郵件內容並無廣告嫌疑，再加上利用傳統電子郵件閘道弱點，將往來單位的電子信箱設定為系統或個人白名單，使得這類商業假冒郵件詐騙橫行無阻。本系統具備全球最前瞻假冒郵件辨識技術，提供獨家雙驗證白名單機制，意即寄件者信箱加上寄件者主機同時符合才可放行；以及獨家 SMTP 延遲反制，佔據駭客系統資源不予回覆，迫使轉戰他方。

新世代 AI 未知惡意威脅程式行為解析

惡意程式也是程式，站在程式開發者觀點，模擬程式客製化，且可辨識與自動分類程式語言庫，並定義各類型項目的評分，包含

1. 附件型態：附件加密、偽造副檔名、炸彈壓縮 (Zip Bomb)、解壓縮次數
2. 特徵資料庫：完整(MD5)、多段(Ssdeep)、載入(Imphash) 取樣、原廠資料庫
3. 程式行為：反偵測行為(Antidebug Antivm)、CVE 弱點漏洞偵測(CVE Vulnerability)、加密演算行為、嵌入漏洞檢查套件(Exploit Kits)、隱藏包裝(Packers Hidden)、文字命令程式(Webshells)、郵件識別、惡意文件、惡意程式、手機惡意程式、惡意網址
4. 沙箱分析(可選購獨立動態沙箱模擬系統)：行為分析、網路分析

APT 攻擊目的與手法

目的與手法	加密勒索	交易詐騙	操控系統	竊取情資	癱瘓勒索
蒐集情資	●	●	●	●	●
設計誘餌	●	●	●	●	
建立中繼站			●	●	
CALL Home			●	●	
植入程式			●	●	
執行任務	●	●	●	●	
網路綜合攻擊					●

設計誘餌 目的為找出組織弱點與寄送惡意超連結或附件；
Call Home 以取得更多惡意程式；
BEC 交易詐騙 滲透階段目的為取得郵件系統使用者的帳號與密碼，詐騙階段目的為取得匯款。

APT 技術比較

方式	攔截成效
即時回溯追蹤惡意威脅通訊行為解析 AI 未知惡意威脅程式行為解析	85-95%
動態沙箱鑑識 即時靜態特徵碼	10-30%

先發性濫發者通訊行為解析

運用全球獨家專利技術「SMTP 即時回溯追蹤」與「SMTP 駭客行為解析」，在 SMTP 交握階段即可有效辨識濫發、非法、匿名、偽造等寄件行為，「有依據、決定性、高效率」攔截 90% 以上的垃圾郵件；搭配雲端信譽黑名單、國際黑名單、DNSRBL、內容權重運算等，為企業帶來極高與最佳防護成效。

完善功能與組織型報表

SpamTrap 提供自我學習、政策比照、黑名單檢舉、白名單反饋、個人與群組政策制定與黑白名單、逾期未讀管理、代理人、隔離不發報告、重送報告、化名與群組合併處理等貼心機制。

SpamTrap 提供各種統計圖表與排行榜，並可依照組織架構定時寄送統計報告給部門主管。

鑑識日誌

排程可以立即發送或指定月、周、日、時；內容包含期間(起訖、今日、昨日、本週、上周、本月、上月、今年、去年)與風險等級，正規式比對輸入寄件者、收件者、主旨、來源路由、訊息代號；收件者可自行新增，自訂報表格式(支援網頁、文字、PDF)。

隔離報告

隔離中心

排程報表

ArmorX 鎧睿全球科技
Intelligent Security • Elite Customization
睿智安防 頂級訂製

鎧睿全球科技股份有限公司
業務信箱 sales@armorxgt.com
客服信箱 service@armorxgt.com

台北 | 新竹 | 台中 | 高雄 | 海外
總公司 | 30264 新竹縣竹北市自強南路 8 號 21 樓之 3
T 03-621-6700 F 03-621-6799