電子郵件為企業對外開放的主要通訊管道之一，無時無刻不遭受猛烈的 APT 攻擊。這些攻擊會嚴重影響政府、企業與個人的工作環境、財務風險，甚至營運信心。APT 攻擊手段包含 BEC 交易詐騙、加密勒索、操控系統、竊取情資、癱瘓勒索等，APT 攻擊勢力來自各方力量，涵蓋黑道、軍方、國家等，APT 攻擊總額 2017 年起已正式超越全球資安產值，其中 BEC 交易詐騙佔 APT 攻擊總額 50% 以上，受災對象涵蓋政府單位與民間企業，受災者追討無門，在在凸顯自我資安防衛的重要性。

80% 以上 APT 攻擊從電子郵件進入，Mail APT 攻擊防禦成為當前最重要課題。ArmorX 運用最先進 AI 人工智慧與 Cloud 雲端掃描技術，打造地表最強大、最全面 SMTP(s) 四項安全防護：流量清洗、APT 攻擊防禦、BEC 詐騙防禦、(選購) BEC 滲透防禦 (Exchange 安全代理)，能大幅降低攻擊流量與打造最佳安全防線。

流量清洗

APT 集團日益獲利增長與資源擴張，「密碼會被猜中」成為基本假設，「流量清洗」為必要手段。假設駭客成功連線 100 萬次會猜中，阻斷連線 90% 會讓駭客基於成效不彰而轉戰。本系統提供 ArmorX 雲端聯防機制，輔以主動偵測與學習攻擊與滲透來源，制敵防護於封包接收前，大幅降低攻擊與垃圾郵件量。

APT 攻擊防禦

本系統運用 AI 人工智慧技術，強化惡意程式行為解析，包含反偵測行為、CVE 弱點漏洞偵測、加密演算行為 (勒索病毒)、嵌入漏洞檢查套件、隱藏包裝、文字命令程式等，可執行加密附件本封與他封密碼檢測，(選購) 硬體式動態沙箱鑑識，可強化置換網址連線檢測與排程網址安全檢測。

BEC 詐騙防禦

常見 APT 釣魚信件 (假冒知名單位) 與 BEC 詐騙信件 (假冒廠商) 不包含惡意程式，而是用“騙”的。本系統運用假冒、匿名、濫發、非法解析等，強化變臉詐騙防禦，包含假冒自己、外部、知名業者、電信服務業者等，同時降低電子郵件系統遭受中間人收信滲透的風險。

(選購) 獨家 Exchange 安全代理

BEC 交易詐騙分為兩個階段，滲透階段與詐騙階段，滲透階段主要目的就是取得電子郵件系統內的使用者信件。本系統可作為 Https 與 Exchange 安全代理，支援 ROH、OWA、ActiveSync 等協定，執行流量清洗防止駭客猜密碼與弱掃，以及帳號/群組國別存取控管。

全球獨家專利技術

SMTP 即時回溯追蹤
SMTP 攻擊連線反制
SMTP 通訊行為解析
　　MUA+MTA 路由
MTA 防偽來源路由
　　FQDN[IP]/來源國別
雙認證白名單
　　MTA+Email 或 Domain

3000 萬+

APT 駭客 IP 與短期網域

4000 萬+

已知惡意程式特徵碼

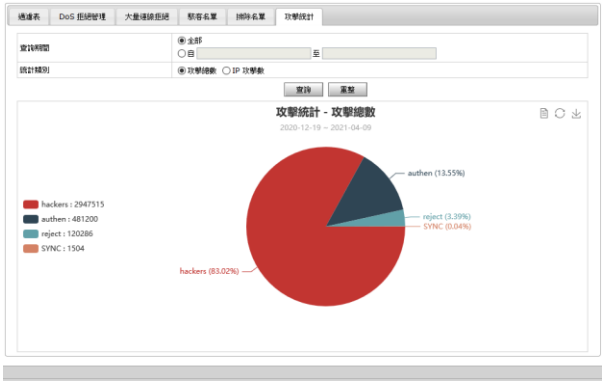
國際情資引用列舉

- 美國國家漏洞數據庫
- 中國國家訊息安全漏洞庫
- Japan Vulnerability Notes
- CVE Common Vulnerabilities and Exposures
- OWASP Foundation
- MISP - Malware Information Sharing Platform, Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing
- Openphish
- PhishTank
- ClamAV
- 卡巴斯基訊息安全網站
- Google Safe Browsing®

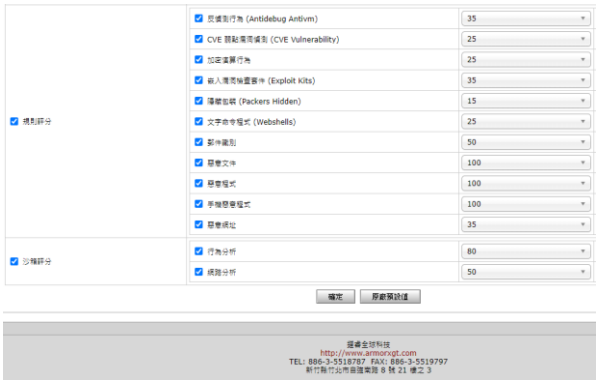
ArmorX APT 操作介面

流量清洗

攔截統計

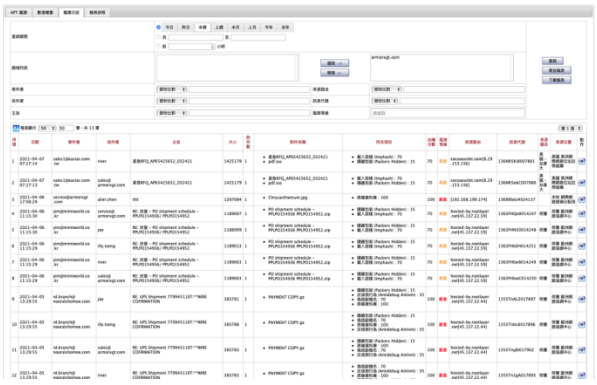


程式行為



釣魚行為

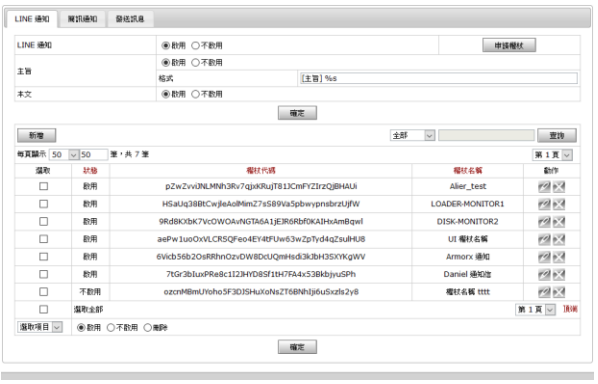
鑑識日誌



鑑識報告

報表排程

資安事件 Line 通知



鎧睿全球科技 ArmorX
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