型錄

趨勢科技

趨勢社交工程攻擊防護組合方案

(內含目標式攻擊與社交攻擊行為偵測模組）

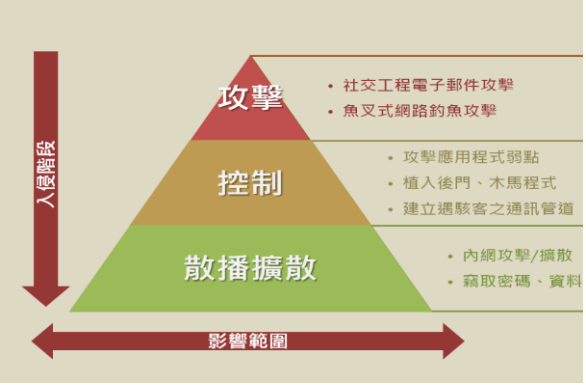
主要功能

趨勢科技研發，採用靜態分析引擎技術，針對透過社交工程攻擊的 APT 惡意信件，可即時偵測攔截，阻擋惡意社交信件進入內部信箱，此引擎

- **不需要透過病毒碼更新即可偵測 APT 惡意信**件，
- 不需考慮文件的弱點
- 不需辨識惡意程式
- 可偵測 Zero-Day Exploit
- 支援各種格式惡意文件附檔均可偵測
- 可快速且準確攔截夾帶惡意附件之電子郵件
- 可主動阻擋 APT 目標式惡意社交攻擊信件
- 不會影響郵件傳遞，造成郵件佇列影響郵件正常使用
- 支援針對組織型駭客/網軍使用的攻擊手法: 例如使用文檔開啟程式的弱點、檔案架構 / 格式遭　到竄改、被增加了特殊的編碼、嵌入 Binary code、遭植入有害的 Shell Code 等 APT 手法
- 利用雲端安全技術更快攔截零時差(zero-day) 威脅
- 即時檢查郵件內嵌及附件檔案的連結，封鎖挾帶惡意連結的電子郵件
- 運用特徵比對、行為偵測和即時雲端查詢來防止垃圾郵件和網路釣魚
- 直覺的介面以及集中的記錄檔和報表，簡化群組設定與管理功能
- 透用雲端安全技術封鎖來自不良或可疑寄件人的郵件，無需仰賴內容檢查功能

主要效益

利用趨勢科技專門研發的靜態分析引擎，可結合於趨勢科技的匣道防毒軟體：IWSVA 或 IMSVA 平台，及電子郵件信譽評等服務等，在目標式攻擊惡意郵件進入閘道時予以攔截；並可結合動態分析系統，分析惡意信件來源，將有用資訊回饋給使用單位，使其能即時攔阻單位內部對外惡意連線。搭配安裝環境為：在客戶已安裝趨勢科技郵件匣道防護軟體及網頁匣道防護軟體的客戶硬體上，需另外啟動趨勢社交工程攻擊防護組合的目標式攻擊與社交攻擊行為偵測模組 。



TREND MICRO

Securing Your Journey to the Cloud

趨勢科技官方網站：www.trendmicro.com.tw
趨勢科技企業專線：(02)2378-9666