Softnext

企業威脅防禦方案

Email X Malicious Analyzation X IR Solution

90% 的滲透攻擊以惡意威脅郵件為進入管道

60% 的APT事件，受駭單位在第三方通知後才察覺

71% 的惡意軟體是被新創造出來的，並只被使用一次

企業威脅防禦方案

Email X Malicious Analyzation X IR Solution

> **企業只分為兩種：已經被駭與即將被駭**
> **甚至正融合為一個類別 - 已經被駭並將再度被駭**
>
> There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.
>
> Robert Muller, Former FBI Director
> 前美國聯邦調查局局長

企業不論規模大小，皆面臨駭客威脅攻擊的嚴峻考驗

網路安全議題已從垃圾郵件、破壞目的病毒郵件轉變為追求利益的攻擊議題，例如自2013年開始廣泛出現至今仍難以扼止的勒索病毒、企業匯款詐騙、以及APT攻擊。為了能夠得到更好的收益，駭客攻擊的對象也不再侷限於政府單位或大型企業，取而代之的，人人都是勒索病毒的攻擊目標；只要有貿易行為，就是駭客眼中詐騙匯款的肥羊；資安防護相較大型企業弱的中小企業也成為APT攻擊目標，因為只要能夠入侵中小企業，要滲透攻擊合作的上下游大型企業就不是什麼難事了。

鎖定從事跨國貿易的中小企業　攻擊轉向防護相較不完善的中小企業　人人都是駭客目標

上述威脅大多利用電子郵件搭配社交工程發起攻擊，再透過惡意程式、惡意網頁、中繼站等多種工具的運行達成入侵的目的。

為何防毒軟體無法攔阻進階式郵件攻擊？

既然郵件威脅大多透過電子郵件遞送惡意程式發起攻擊，為何防毒軟體無法攔阻進階式郵件攻擊？

最大的關鍵在於病毒與APT有著不同的攻擊目的：無差別病毒攻擊與客製化針對型攻擊。無差別病毒攻擊不分對象，目的在短時間內造成大規模的破壞與感染，快速為攻擊者帶來利益。客製化針對型攻擊，則是駭客鎖定明確目標而量身打造，這類攻擊手法複雜且隱匿性高不易被誘捕，因此一般的防毒機制無法在短時間內攔截，受駭者難以肉眼察覺分辨。

> **單一防禦技術已無法抵禦現今攻擊管道複合、多變、不易歸納出固定模式的攻擊，面對不同的攻擊手法，應採取不同的防禦技術來因應**

Softnext以先進思維開發防禦技術，提供企業威脅防禦對策

Softnext中華數位科技長期觀察郵件網路安全趨勢，領先業界以先進思維開發防禦技術，提供企業威脅防禦對策，除了可防護來自電子郵件與網頁等惡意攻擊，留存相關攻擊記錄外，當滲透攻擊事件發生時，亦提供資安事件處理諮詢與專家顧問服務。

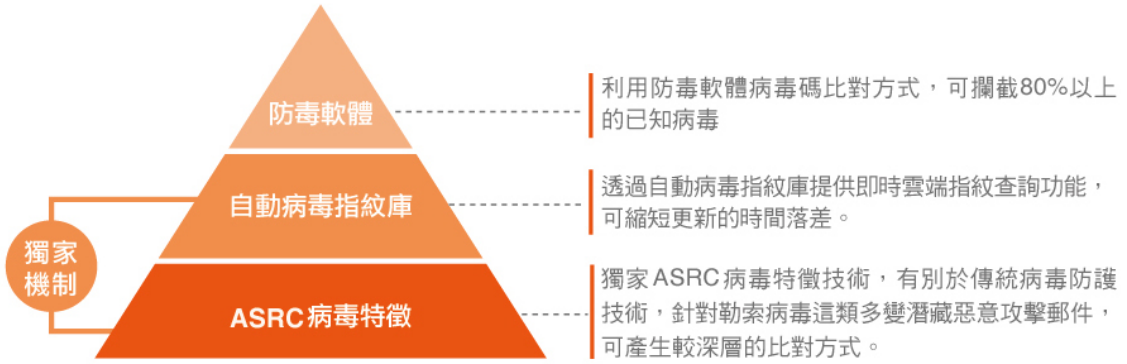
面對不同的攻擊手法，採取不同的防禦技術因應

攻擊手法	無差別病毒攻擊 一般病毒、Rootkit、間諜軟體、蠕蟲、後門程式及勒索病毒	客製化/針對型攻擊 詐騙、針對型魚叉攻擊、APT攻擊
事前防範	SPAM SQR 標準防毒功能 ｜ 雙重防毒模組	SPAM SQR ADM進階防禦模組
聯合防禦	動態沙箱 內建多重分析引擎	
事後處理照護	資安架構強化顧問服務	BEC 鑑識服務 / IR Solution 資安事件處理服務

SPAM SQR病毒防禦機制，防範無差別病毒攻擊

SPAM SQR可同時掛載多防毒引擎，並結合自動指紋辨識與ASRC病毒特徵防護，達到較好的攔截效果。

SPAM SQR 病毒防禦機制



靜態特徵聯合動態沙箱分析，防護更全面

進階持續性攻擊的目的在於以各種方法擊潰企業的安全防線，然而這些方法為成功達成目的盡其所能地避開現有的防禦機制。SPAM SQR 透過多層式過濾技術，可先行分類垃圾郵件及可疑威脅郵件，再將特定格式附檔拆離傳送至沙箱進行比對，於虛擬平台進行程式運作狀態分析。透過分析軟體的模擬，再將監測程式運作過程所產生的行為回傳至SPAM SQR，將動態沙箱分析結果統一整合於SPAM SQR，揭露風險一目了然且更易於管理。

SPAM SQR ADM & 動態沙箱聯防特色

良好的分析速度
分類掃瞄 節省資源消耗

動靜態交叉分析
增加入侵的困難

單一系統整合報表
風險揭露 易於追蹤

SPAM SQR靜態特徵防禦，先期抵禦新型態攻擊

ADM(Advanced Defense Module)進階防禦模組，透過長時間的追蹤並模擬駭客攻擊行為，利用雲端差分技術更新靜態特徵。程式會自動解封裝檔案進行掃描，可發掘潛在代碼、隱藏的邏輯路徑及反組譯程式碼，以利進行進階惡意程式比對。可攔截附件及檔案夾帶零時差(Zero-day)惡意程式、使用APT攻擊工具及含有文件漏洞的攻擊附件等攻擊手法的威脅郵件。

ADM 機制特色

特徵分析
有別於一般防毒商以被動式蜜罐捕獲，採主動追蹤攻擊族群並產出特徵

風險揭露
同時揭露漏洞編碼、攻擊工具及攻擊族群等資訊

快速反應
線上回報機制縮短反應時間

SPAM SQR搭配動態沙箱分析偵測模擬複雜多變的攻擊

透過創新的分層方法，結合了防毒特徵碼、信用評價、即時模擬防禦、深層程式碼及動態分析(沙箱作業)。一方面使用特徵碼和即時模擬這類分析強度較低的方法找出已知的惡意軟體，進而確保高效能分析；另一方面也為沙箱作業新增深層程式碼分析功能，針對高度偽裝、擅於規避的威脅提供更完善的防護。

動態沙箱 特色

強大的分析能力
結合深層程式碼分析與動態分析，提供更精準的偵測功能

平衡的處理效能
動靜態交叉比對，提升分析速度

客制化環境部署
最廣的作業系統支援，以滿足企業伺服器環境

SPAM SQR層層過濾郵件威脅，降低企業受駭風險

防毒引擎
直接隔離已知病毒，防止不當轉發降低中毒的風險

惡意檔案分析引擎
逐層解封裝檔案進行掃描，可發掘潛在惡意程式及漏洞編碼

威脅感知引擎
偵測郵件行為及頻率，阻絕惡意癱瘓郵件系統等行為

智能詐騙偵測
檢查郵件偽造痕跡並分析來源，當郵件放行至使用者端時加強警示，藉以提高使用者警覺

動態沙箱
執行檔案並檢測程式造成的影響以及相關的行為，提供詳細的歷程和分析報告

事後處理與資安顧問服務，降低再度受駭的風險

◤資安架構強化顧問服務

透過ISO27001、弱點掃描與滲透測試，強化資安防護

針對無差別攻擊的防禦，企業應當注重企業安全體質的提升，如遵循國際資安標準 ISO27001，強化存取控制、實體安全、運作安全、通訊安全、系統開發安全、事件應變等安全控制措施。此外，提升資訊機房的日常安全維運也能增強企業防禦攻擊的能力，可藉由中華數位弱點掃描服務偵測威脅，並透過符合 OWASP、NIST SP 800-115 的滲透測試指南來檢查漏洞，持續協助系統修補、套件管理、安全參數設定等強化工作。

◤BEC鑑識服務

當企業懷疑遭到BEC詐騙或不幸被騙時，BEC鑑識服務可協助企業清查鑑識受害電腦與關聯網路，調查駭客入侵與資訊洩漏的可能管道，提供防護諮詢建議與人員教育訓練，改善企業資安問題，避免再度遭受駭客攻擊。

- 可協助介接法界調查單位協助
- 協助調查駭客入侵、資訊洩漏的可能管道
- 清理受害電腦與關聯網路，避免再度受駭
- 防護顧問諮詢
- 人員教育訓練

◤IR Solution資安事件處理服務

透過調查與鑑識分析，降低再度受駭的風險

因為攻擊目的不同，APT攻擊相較其他資安入侵攻擊更難被察覺，企業從APT攻擊入侵成功至察覺有異平均長達200天以上，發生原因與入侵管道相當複雜。

當企業確認或懷疑內部遭到APT攻擊時，可透過IR Solution資安事件處理服務，由專業顧問介入實行鑑識與清理並強化保護措施，降低再度受駭的風險。

掃瞄

運用工具搭配資產管理或AD，全面佈署掃瞄，快速定位問題電腦

清理

鑑識後協助清除受感染電腦上的後門程式，防止入侵者繼續掌控遭到入侵的電腦

鑑識

透過鑑識確認入侵的時間、範圍規模與洩資的情況，並可以此結果做為事後進行資安工事補強的參考

資安照護

面對進階持續性滲透攻擊，需要長期持續的資安照護，遭到鎖定的目標，經過清理後仍可能再次遭到入侵。中華數位提供長期的資安照護服務，在訂閱此服務後，可在服務合約期間收到防護建議，與不定時特徵及疫苗，提高入侵者再次嘗試入侵的門檻。

SPAM SQR 全方位郵件安全防護

200型	500型
● 處理流量：2G以內 ● 1U可上19吋標準機架	● 處理流量：2~5G ● 1U可上19吋標準機架
1000型	**2000型**
● 處理流量：5~10G ● 1U可上19吋標準機架	● 處理流量：10G以上 ● 2U可上19吋標準機架

含一年系統維護、版本更新、硬體保固

IR Solution資安事件處理服務

服務項目	掃瞄服務	清除、顧問服務	資安照護服務
計價級距	100U、1000U	專案顧問分析服務 依人工以天計價	1000U、2000U
服務內容	企業單位Windows電腦全面掃瞄檢測，並提供掃瞄報告 此為一次性服務	● 重要主機後門清除 ● 隔絕非預期遠端操作 ● 入侵時間點、攻擊族群、洩資規模分析並提供報告 執行項目將依客戶購買的人工天數預估	● 根據企業單位樣本回饋，每一季提供簡要分析報告 ● 動態提供針對企業單位的防護特徵 服務區間以年為單位計價

Softnext 中華數位科技
TEL:+886-2-25422526 FAX:+886-2-25424838
Email: service@softnext.com.tw
www.softnext.com.tw