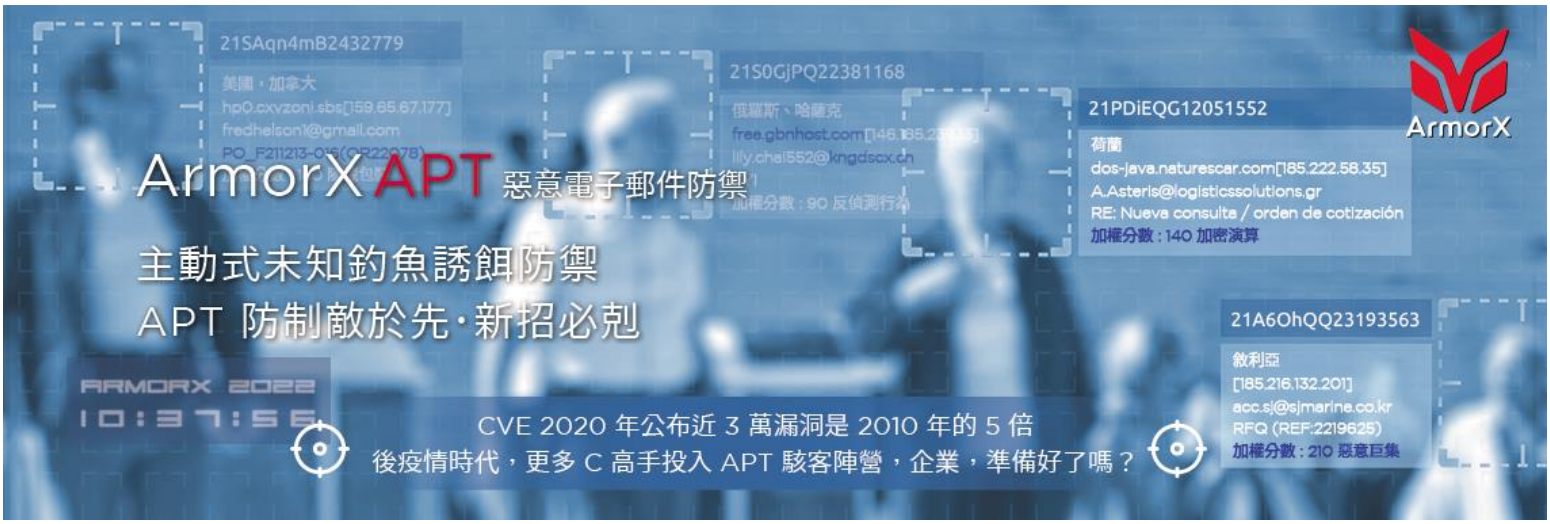
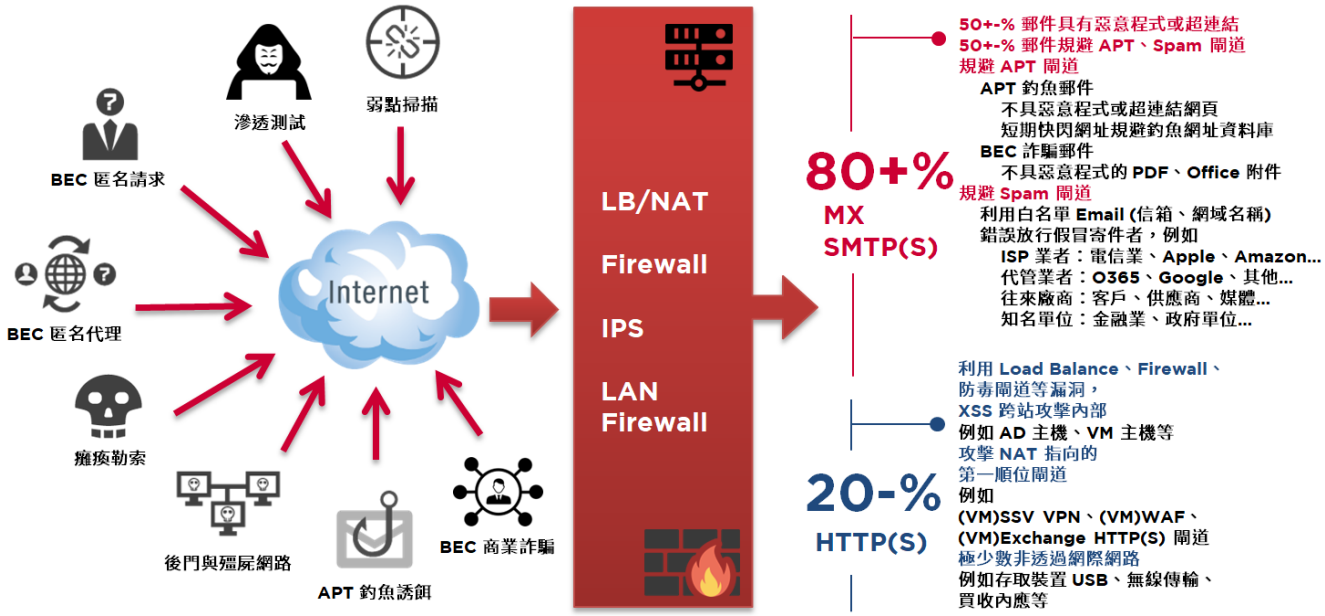


APT 電子郵件進階滲透攻擊 80+% 藉由入侵 MX SMTP(S)，例如 BEC 商業詐騙、加密勒索、竊取情資(雙重勒索)、操控系統(ATM、匯款、網銀等)、癱瘓勒索。20-% 藉由滲透電子郵件系統或使用者信箱。其中，BEC 商業詐騙佔 APT 整體營收的 50% 以上，其手法為先滲透電子郵件系統，取得精準個資與情資，再穿透 Spam、APT 閘道，寄送詐騙郵件。結論：Mail 滲透防禦與 APT 攻擊防禦是企業 APT 防禦的重中之重。

Cyber Security
BC Best Choice AWARD
第一屆 BC 資安產品獎
2022 Computex Taipei



ArmorX APT 零信任資安防禦

網路連線攻擊 ◆ 未知釣魚誘餌通訊 ◆ 垃圾郵件 ◆ 病毒蠕蟲 ◆ 惡意程式或超連結

流量清洗	主動式未知釣魚誘餌防禦	垃圾郵件 病毒蠕蟲	靜態惡意程式特徵解析	動態沙箱程式行為解析
3000+ 萬筆	未知釣魚誘餌	攔截	4000+ 萬筆	零時差攻擊防護
信譽阻擋黑名單	新興詐騙網址	垃圾郵件	已知惡意特徵碼	動態程式解析
(排除跳板受害者)	偽造(他人)	廣告郵件	釣魚網址資料庫	動態網頁解析
ArmorX MTA	濫發(跳板)		零時差攻擊防護	網頁時差攻擊防護
反駭客滲透偵測	匿名、非法	攔截	反偵測、加密演算	網址置換解析
APT 攻擊連線反制	亂數、時差	病毒郵件	CVE 漏洞、隱藏包裝	排程網址解析
SMTP 即時回溯追蹤	中間人商業詐騙	蠕蟲郵件	文字命令、巨集腳本	
SMTP 認證陷阱捕捉	公有雲短期詐騙	後門郵件	加密附件嘗試解密	

ArmorX APT 來源路由 FQDN[IP] 身份辨識 ◆ 全球獨家 MTA+Email 雙驗證白名單

LDAP/SQL 整合 ◆ SoC 日誌整合 ◆ 異常 Email/Line 通知

ArmorX APT 和 Others 同時具備 APT 防禦技術，流量清洗：包含駭客 IP、釣魚網址、惡意特徵碼，惡意程式行為解析：包含靜態程式特徵解析、動態程式沙箱行為解析，占整體 APT 攻擊防禦力 70+-%。ArmorX APT 獨家具備主動式未知釣魚誘餌防禦：包含假冒、匿名、濫發、非法、亂數、中間人、共用、公有雲、行為解析，占整體 APT 攻擊防禦力 30+-%。

APT 攻擊防禦解決方案比較表_1/2

防禦類型	防禦技術	佔整體防禦力	ArmorX	Others
流量清洗	駭客 IP		O	O
	釣魚網址		O	O
惡意程式行為解析	惡意特徵碼	70+-%	O	O
	靜態程式特徵解析		O	O
	動態程式沙箱行為解析		O	O
主動式未知釣魚誘餌防禦	假冒、匿名行為解析	30+-%	O	X
	濫發、非法行為解析		O	X
	亂數、中間人行為解析		O	X
	共用、公有雲行為解析		O	X

全球企業 APT 攻擊 80+% 透過 MX SMTP(S)，其中 50+-% 郵件具有惡意程式或超連結，50+-% 郵件試圖規避 APT 閘道，例如 APT 釣魚郵件不具惡意程式或超連結網頁，或者使用短期快閃網址規避釣魚網址資料庫，BEC 詐騙郵件不具惡意程式的 PDF、Office 附件。規避 Spam 閘道，例如利用白名單 Email (信箱、網域名稱) 錯誤放行假冒寄件者，例如 ISP 業者：電信業、Apple、Amazon...，代管業者：O365、Google、其他...，往來廠商：客戶、供應商、媒體...，知名單位：金融業、政府單位...

20-% 透過 HTTP(S)，利用 Load Balance、Firewall、防毒閘道等漏洞，XSS 跨站攻擊內部，例如 AD 主機、VM 主機等，或者攻擊 NAT 指向的第一順位閘道，例如 SSV VPN、VM 主機、Exchange HTTP(S) 閘道，以及極少數非透過網際網路，例如存取裝置 USB、無線傳輸、買收內應等。

市面 APT 解決方案 SMTP 郵件日誌提供日期、寄件者、主旨、來源 IP、郵件標題、內文、附件。ArmorX APT 獨家提供來源路由 FQDN[IP]、來源 IP 隸屬國家、SMTP 認證帳號、MTA 詳細傳輸資訊，可避免誤設公有雲 IP 為白名單或黑名單。

市面 APT 解決方案白名單設定方式提供來源 IP 與 Email (信箱、網域名稱)，近年駭客所註冊的數十萬短期快閃網址越來越多藏身公有雲，O365、Google、Amazon 等公有雲 IP 無法設定為白名單，致使系統管理者採用 Email (信箱、網域名稱) 為白名單，由於寄件者 Email 可以假冒，此錯誤放行儼然成為近年 BEC 商業詐騙的巨大資安漏洞。ArmorX APT 全球獨家提供 MTA+Email 雙驗證白名單，需兩筆資訊同時符合方可放行，否則視為假冒，例如 .google.com:abc.com，是企業建立精準白名單的正確工具。

APT 攻擊防禦解決方案比較表_2/2

管理工具		ArmorX	Others
SMTP 郵件日誌	日期、寄件者、主旨、來源 IP 郵件標題、內文、附件	O	O
	來源路由 FQDN[IP] 可避免誤設公有雲 IP 為白名單或黑名單	**O**	**X**
	來源 IP 隸屬國家	**O**	**X**
	SMTP 認證帳號	**O**	**X**
	MTA 詳細傳輸資訊	**O**	**X**
白名單設定方式	來源 IP O365、Google 等公有雲無法使用	O	O
	Email (信箱、網域名稱) 由於寄件者 Email 可以假冒 成為 BEC 商業詐騙的巨大資安漏洞	O	O
	全球獨家 MTA+Email 雙驗證白名單 需兩筆資訊同時符合方可放行 否則視為假冒 例如 .google.com:abc.com 是企業建立精準白名單的正確工具	**O**	**X**

(選購)獨家 APT 滲透攻擊防禦

作為 Exchange 安全代理，適用版本：2010、2013、2016、2019，支援協定：OWA、ECP、ActiveSync，執行流量清洗、反駭客滲透偵測、帳號存取國別控管，正向表列帳號允許連線國家，用來大量收集針對企業發動的攻擊 IP，是企業近身防禦最快速反應與最犀利的蜜網捕捉工具。

上述自動學習黑名單可反饋至 APT 攻擊防禦閘道執行流量清洗，大幅降低未知新興駭客 IP 與釣魚網址的危害。

ArmorX 鎧睿全球科技
Security Defense + Collaboration Platform
極智防護 + 全球最佳 + 資安防禦暨溝通協作

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