臺中市議會第4屆第5次定期會

市政府因應近期勒索軟體攻擊案件防制作為專案報告

臺中市政府
TAICHUNG CITY GOVERNMENT

報告人
臺中市政府警察局　　局長 李文章
臺中市政府數位發展局　　局長 林谷隆

中華民國114年4月15日

目　錄

壹、警察局報告

一、前言

近期勒索軟體攻擊頻傳，其犯罪手法係透過侵入系統加密被害人的檔案或鎖定系統，限制資料存取，導致無法開啟檔案或系統，要求支付贖金以換取解密金鑰。其攻擊方式多樣，常藉由釣魚郵件、程式漏洞或下載惡意軟體入侵被害人工作系統進行勒索，被害人通常具有資訊安全不足、內部管理不當、資安人員欠缺等特性，並於發生後始向警方報案，喪失機先防制、被害歷程蒐證等先機。本專案報告探討本市勒索軟體案件的發生現況、偵查作為與遭遇困境，並提出相關防制策略與作為。

二、發生現況

(一)案件統計

1. 本市受理勒索軟體案件 112 年共 12 件、113 年共 3 件、114 年迄今未接獲報案，共計 15 件。

2. 初步分析案件逐年降低原因，近年新聞媒體報導有關勒索軟體資訊，政府單位亦有向大眾宣導資訊安全，增加民眾加強防範之意識，此外，本局受理是類案件時，除積極偵辦外，亦會給予被害人資安方面之建議，如員工資安訓練、添購資安設備、加強安全監控或委託專業資安公司等，避免其再次遭受勒索軟體攻擊。

(二)被害特徵分析

1. 被害人特性：分析 112 年至 114 年 15 件案件，如表 1。

被害人特性分析			
特性	**類別**	**件數**	**比例**
被害人身分	私立	14	93%
	公立	1	7%
勒索金額（換算新臺幣）	未註明金額	9	60%
	500 萬以上	5	33%
	未達 500 萬	1	7%
攻擊來源	境外	15	100%
	境內	0	0%
交款方式	虛擬貨幣	13	86%
	未指定	2	14%
是否交款	否(註)	15	100%
	是	0	0%
攻擊態樣	資料加密	14	93%
	資料外洩	1	7%

（註：部分被害人後續未告知是否交付贖金）

表 1

2. 被害原因分析：

(1) 資安能量不足：

i. 設備不足：缺乏防火牆、入侵偵測系統等資安防護設備，或設備系統版本過舊易受攻擊。

ii. 制度管理不足：未建立系統權限控管、日誌稽核等相關資安機制。

iii. 人員專業度不足：無設置專責資安人員，或兼任資訊人員缺乏資安專業；例如學校由行政人員兼任資訊人員，或公司雖有設置資訊部門，但主要功能為資訊管理而無資安能力。

(2) 系統漏洞：系統廠商未即時修補漏洞，造成使用者遭受攻擊。

(3) 使用者資安觀念不足：資安宣導不足導致使用者遭受社交工程、誤擊釣魚網站、密碼強度過低遭暴力破解或交叉使用感染病毒之 USB 等。

被害原因分析		
原因	**件數**	**比例**
資安能量不足	10	67%
系統漏洞	3	20%
使用者資安觀念不足	2	13%

表 2

三、偵查作為

(一)受理通報

被害人至警察機關報案，本局即依規定通報刑事局科技犯罪防制中心，若被害人為公務機關、公營事業或關鍵基礎設施提供者，則由其自行通報數位發展部資通安全署。

(二)數位鑑識

刑大科偵隊及轄區分局科偵小隊至現場會同資訊人員進行數位取證，透過分析網路拓撲釐清受駭系統或設備的最初攻擊時間與路徑，並製作映像檔備份以利數位鑑識，後續由受駭方提供完整網路架構及網路設備 LOG，以分析案發前後網路流量異常及可疑 IP，確認勒索軟體入侵軌跡。

(三)幣流追查

藉由犯嫌留下的贖金錢包位址，利用公開帳本追蹤加密貨幣交易紀錄，以找出贖金流向，嘗試尋找交易所以調閱資料個化嫌疑人。

(四)國際協查

追查勒索軟體入侵軌跡、贖金後續流向多源自境外，需透過刑事局啟動協查機制，並等待境外執法機關回復結果，始能續行偵查作為。

四、偵查困境

(一)被害人不願提供資訊

被害人鑑於商業名譽、客戶權益保密或使用系統之急迫性，不願配合警方調查及提供關鍵資訊，造成辦案人員偵辦困難。

(二)資安應處能力不足導致未保留證據

因未設置資安專責單位、欠缺資安專業人力，以及委外系統廠商資安專業不足，甚至委外資安廠商未善盡防護責任，導致無法提供完整設備或 LOG 紀錄(如：網路設備架構或相關日誌、路徑等 LOG 紀錄)，無法進一步溯源分析。

(三) 虛擬貨幣查緝困難

虛擬貨幣系統具高度匿名與開放性，任何人皆可輕易創建錢包，並透過線下交易或無須實名制平臺取得資產。駭客常利用此特性，提供受害者難以追查的錢包地址作為支付方式，導致贖金流向產生大量無法確認持有者身分的錢包節點，增加溯源難度。

(四) 境外犯罪難以追查

經追查勒索軟體之攻擊源頭與贖金流向為境外時，僅能透過刑事局進行跨國協查機制，實務上甚難以取得後續追查情資，此現況致使警方遭遇偵查瓶頸，追查攻擊源頭與贖金流向的努力常徒勞無功，突顯勒索軟體偵辦中的國際協查困境，地方警察機關可著力之處確實有限。

五、策進作為

為有效防範與偵辦勒索軟體攻擊案件，應從加強資安能量、網路控管機制、加強虛擬貨幣控管及國際合作執法等四大面向推動策進作為：

(一) 加強資安能量

地方警察機關受理案件均依規定通報中央，已善盡通報責任，惟目前中央針對資安政策欠缺完善的法令規範及分級機制，使得公私立機構、民間企業形成嚴重的資安落差，如數位發展部訂定之「資通安全管理法」僅要求公務機關及關鍵基礎設施之資安防護；而金融監督管理委員會訂定之「公開發行公司建立內部控制制度處理準則」僅要求上市櫃公司需設置資安專責單位。造成非

屬規範內之中小型企業、公司、商家，甚至個人用戶，完全忽視資安風險，鑒此，建議中央應採「產、官、學」合作方式，邀集各領域之政府機關、專家學者、業界廠商，共同研議出完整的資安政策，包含法令規範、資安防護分級、認證標準、基礎建設等，如公司資本額多少規模，應達到何種資安防護等級、導入資安設備、通過檢測認證，且資安人員應取得何種證照、定期完成資安訓練等，並應提供合格資安廠商名單協助落實執行資安政策。

(二)網路控管機制

應針對駭客常利用之匿名通道連線（如 VPN、Tor）所形成之斷點類型與模式，建議中央研議修法或制定相關規範，以強化高風險網路連線行為之監管與責任機制，提升網路連線控管及溯源能力，有效防堵資安事件發生。

(三)加強虛擬貨幣控管

除提升執法機關技術能量，強化贖金路徑的分析與追查效率外，建議中央主管機關可推動境內虛擬貨幣交易全面實名制，提升透明度，同時建立監控機制，即時標記可疑錢包阻止其繼續交易，另可與各國政府建立跨境區塊鏈情資共享平臺，讓犯罪者無法匿名收取贖金，壓制犯罪氣焰。

(四)國際合作執法

建議中央在逐步強化網路連線控管並提升駭客入侵路徑可追溯性的基礎上，進一步強化與國際資安組織及執法機關之合作，積極參與全球資安聯防機制，推動資安情報共享、跨國資料調閱、司法互助及引渡協議，以追蹤勒索軟體犯罪網絡，提升跨境追查與打擊能力，強化我國在國際資安合作中的應變能量。

六、結語

面對勒索軟體攻擊手法日益進化，未來除持續強化警政機關偵查能量外，政府部門應建立完善的資安政策及規範，全面提升民眾及中小企業員工資安意識、強化網路及虛擬貨幣控管機制及深化國際合作執法，全面提升資安意識與應變能力，並透過國際聯防與情報共享機制，強化跨境追查與打擊效能，共同守護本市整體數位安全。

貳、數位發展局報告

一、 前言

勒索軟體的發展始於1989年的實驗性攻擊，並在數位化與加密技術進步下演化為全球性威脅。早期攻擊以簡單加密為主，2010年後結合非對稱加密與比特幣支付形成成熟犯罪模式，近年更發展出雙重勒索、RaaS 服務等進階型態，造成全球數十億美元的經濟損失。

表 1 犯罪型態演進

階段	技術特徵	勒索支付方式
實驗期 (1989)	可逆加密、物理支付追蹤	郵寄現金/匯款
技術突破期 (2010)	非對稱加密、自動化傳播	預付卡/電子支付
全球化攻擊 (2013)	比特錢包匿名支付、漏洞利用	比特幣
定向攻擊 (2019)	雙重勒索（加密+資料外洩威脅）	門羅幣等隱私幣
服務化犯罪 (2021)	RaaS 平臺、供應鏈攻擊	多重加密貨幣

在本國積極推展數位化的同時，網路的開放性以及資料的數位化不可避免的成為全球駭客攻擊的對象，從2019年多家醫院的應用系統檔案被加密、2023年對中油的相關支付系統加密，影響範圍擴及全國最受關注，今年臺北及彰化2家醫療院所受到的勒索軟體攻擊，顯示勒索軟體的攻擊威脅仍未停歇

表 1 本國遭遭勒索軟體攻擊的重大矚目事件列表

時間	組織 名稱	勒索病毒 名稱	損害 情形
2019年 8月31日	臺灣多家醫院	Globelmposter 3.0勒索病毒的變種	多達66間醫院受影響，醫療檔案遭加密
2020年 5月4日	中油、台塑	未公布勒索病毒名稱，調查局研判攻擊與 Winnti Group 駭客組織相關	影響客戶使用支付卡購買汽油
2025年 2月9日	馬偕紀念醫院	CrazyHunter	超過500臺電腦當機，病患資料無法開啟
2025年 3月1日	彰化基督教醫院	CrazyHunter	醫院系統受影響，病患資料安全未受影響

二、 本府因應勒索軟體攻擊的應對措施

(一)本府因應措施

面對勒索軟體的攻擊方式，本府也就各方面進行相關因應作為：

1. 導入資訊安全管理系統(ISMS)

本府中央資訊機房及本府共構骨幹網路已完成導入國際標準ISO 27001並通過第三方驗證，透過4大控制面向(組織面、人員面、實體面及技術面)與5項控制屬性(控制類型、資安屬性、網路安全概念、運作能力及安全領域)，建立資安管理程序及文件供各機關轄管系統在本府共構網路的運作有所依循，藉由 PDCA 的循環持續確保本府資安管理措施的有效性。

2. 技術面防護

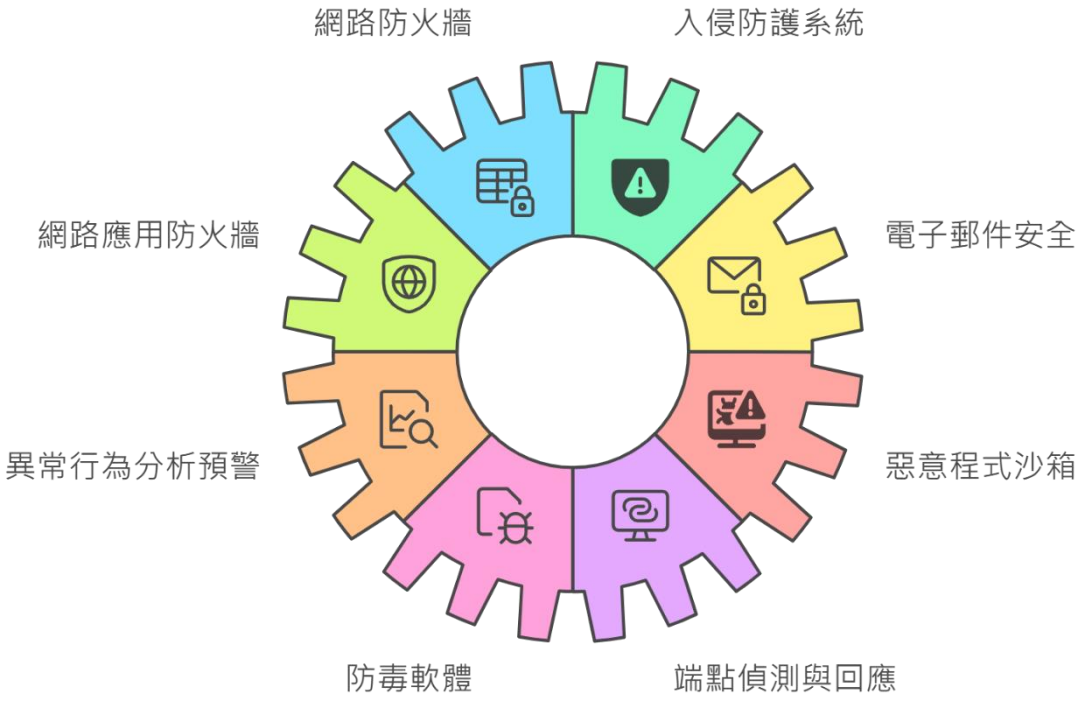
面對本府多達1萬8,000餘臺的連線設備，為避免因單點突破造成全面擴散，採用以下措施：

(1) 網路架構規劃:透過網路設備將本府同仁公務電腦、資通系統網路環境適當區隔，將本府各機關與網站系統分置於不同的網路作業環境,配合骨幹網路的閘道控管,當發生攻擊擴散行為時，可藉由網段隔離的方式使勒索軟體駭侵範圍受到侷限而能避免災情擴大。

(2) 資安設備防護：藉由本府於骨幹網路關鍵節點建置的各項資安設備，透過連線控管(網路防火牆)、威脅行為阻擋(IPS)、網站服務攻擊阻擋(WAF)、電子郵件防護系統、異常行為分析預警、惡意程式沙箱分析、防毒軟體安裝、伺服器系統端點偵測(EDR)等方式協同防護。本府於共構網路環境下對所有伺服器系統與同仁電腦更是全面佈署防毒軟體並統一管控，並於本府中央資訊機房所有網站系統提供端點威脅偵測機制，配合 SOC 的24小時不中斷監控服務，使本府網路連線由外而內、伺服器系統到使用者設備,能在資安攻擊前有一定的預警與阻擋,提高資安防護的門檻,並能在攻擊發生時，提早得到通知而能快速發現受攻擊的設備進行應對，降低對本府網路連線設備帶來的損害。

(3) 外部情資協防：資安即國安，在察覺外部有資安攻擊的情勢發生時，能馬上透過相關入侵威脅指標(IoC)的取得，匯入本府資安設備使攻擊防護生效，本府資安防護設備也藉由導入中央黑名單自動部署服務系統，與中央分享的資安威脅清單同步，以避免成為駭客潛在的攻擊標的。

圖 1 本府縱深防護機制

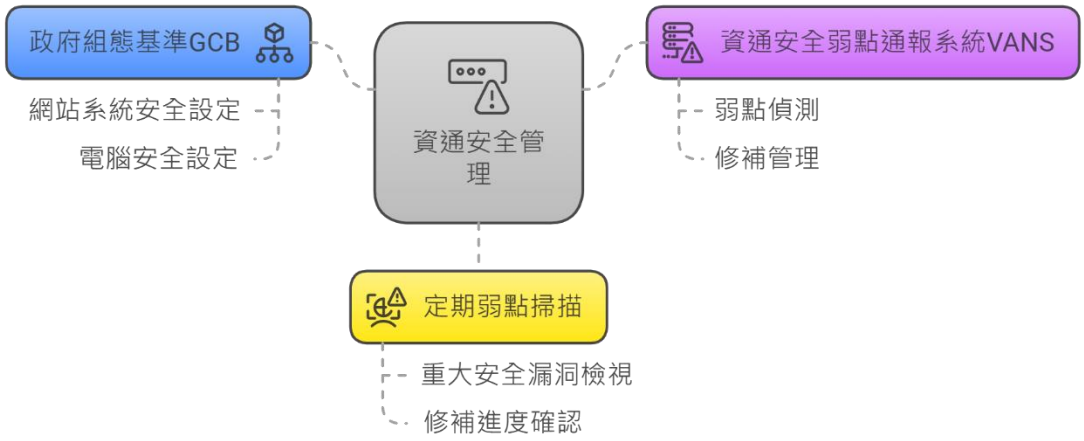


3. 系統漏洞與弱點修補

依據資通安全責任等級分級辦法，各級機關應建置政府組態基準 GCB(B 級機關)與資通安全弱點通報機制 VANS(B、C 級機關)，範圍須涵蓋轄管網站系統與同仁電腦，為避免本府共構網路環境的電腦作業系統與應用程式因系統的設定所生漏洞或程式缺陷未及更新導致勒索軟體的入侵，依據國家資通安全研究院規範的組態基準，提供本府共構網路環境所有的電

腦一致的安全性設定，並建置資通安全弱點通報系統提供本府轄管網站系統弱點偵測修補管理，強化本府資訊系統的穩定與韌性。

圖 2 系統漏洞/弱點修補



4. 帳號管理系統的強化

依據資通安全責任等級分級辦法的資通系統防護基準規範，各級(普/中/高)的資通系統在存取控制措施中，皆須建立帳號管理機制，國家資通安全研究院亦為各種系統作業環境提供各別一致性安全設定(GCB)，為使同仁帳號管理系統的安全能更進一步的強化，透過登入權限的管控避免未經許可對帳號的存取，並佈署虛擬修補程式以因應尚未釋出的弱點更新防護需求，透過每日 SOC 對系統的監控，以及定期執行系統安全性更新，確保同仁帳號不易被勒索軟體竊取或加密。

5. 人員教育訓練

市府的資安是由本府所有同仁一起維護，面對科技發展與網路攻擊變化，數位局加強辦理全府資安通識教育訓練、社交工程演練、資安通報應變演練與系統管理人員教育訓練等方式，不只開課頻率增加，課程的內容實用性也增加，共同提升本府

同仁對勒索軟體攻擊的防護及應變的素養，避免在受到勒索軟體攻擊時錯失緊急應變的時機。

圖 3　本府安全防護策略

三、 結語

市府落實並時時檢討資安措施的縱深防禦，以及培養市府同仁「資訊安全、人人有責」的素養，由上到下統一對市府資安防護的共識，才能有效降低事故發生的機率，加速資安事件應變處置以降低帶來的損害。

勒索軟體攻擊對政府機關、國營企業與關鍵基礎設施的威脅逐步升級，醫療與能源業成為主要目標。本府持續強化備分備援機制、跨機關協作及員工訓練等方式。也會因應時代趨勢持續關注未來防禦策略，並配合中央資安防護策略逐步評估與導入，如整合零信任架構或 AI 偵測，建立快速應變流程以降低攻擊影響。