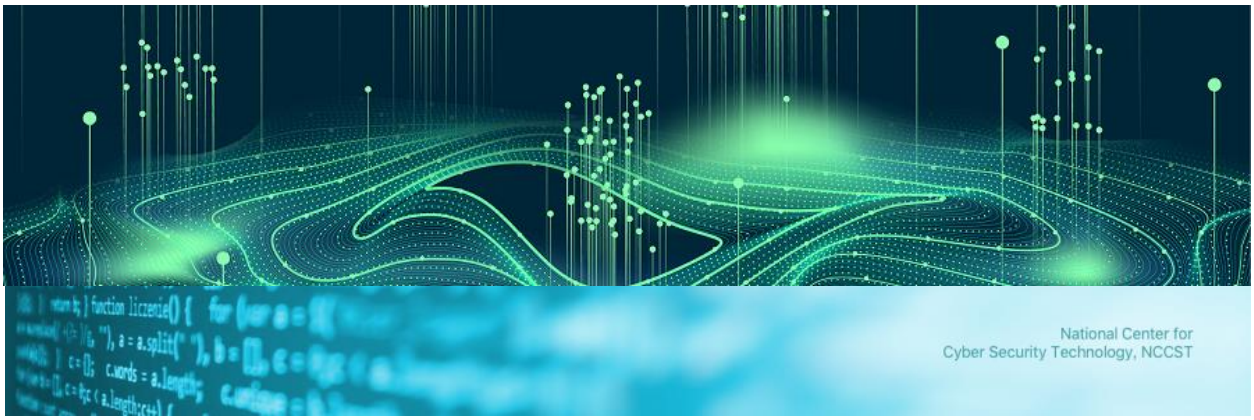
109年第4季資通安全技術報告

Quarterly Technical Report



目　次

圖 目 次

摘要

「第 4 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關最新資安風險之關注重點。

「第 4 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為駭侵組織 Lazarus 以軟體供應鏈手法攻擊南韓用戶；第 2 起案例為駭客於暗網拍賣 25 萬個竊取之 MySQL 資料庫。

分析政府資安威脅現況，發現政府機關通報事件分類，以「非法入侵」(占 56.39%) 類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 12.78 %)」與「網頁攻擊(占 6.77%)」為主要通報類型。

●2.資安專題分享

資安專題分享主題為量子破密技術研究，隨著量子處理器技術逐漸成熟，現有許多密碼系統，如 RSA 與 ECC(Elliptic Curve Cryptography)已面臨被破解之威脅。藉著量子破密技術研究，持續關注量子運算之基礎環境與破密技術發展，以掌握可能之威脅並提前部署。

●3.資安技術研析

資安技術研析主題為 Zerologon 漏洞研析，該漏洞已被視為影響重大之漏洞。利用 Zerologon 攻擊，駭客會先駭進某內網使用者電腦後，再經連線發現此電腦若連至內網主網域控制站 DC，即可成功發動 Zerologon 攻擊，再企圖控制整個網域。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享量子破密技術研究，以量子破密技術，設計量子電路進行破密手法實作。此外，資安技術研析主題為 Zerologon 漏洞研析，整理其攻擊手法與原廠更新計畫，提醒機關檢視安全設定與準備因應方案。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因與可能之衝擊與影響。109 年第 4 季(以下簡稱本季)探討供應鍊安全與如何加強資通系統防護，以避免遭受攻擊致資料暴露。

本章節之事件與議題皆配合整理相關之資安防護重點，提供機關就相關資安風險或議題進行評估，並依循資安防護重點進行強化。

1.1 全球資安威脅現況

面對詭譎多變的資安威脅與不斷推陳出新的資通訊科技，資安挑戰也持續升級，從資通安全強調縱深防禦，提升整體防護韌性，到主動式防禦以積極精進的風險管理概念，都顯示全面防禦，提升戰備的決心。從全球資安威脅案例可以看出駭侵手法不再單一，駭客利用供應鍊脆弱點找尋突破點，再加上暗網推波助瀾的憑證與個資外洩情況，都讓資通安防護相關不確定性課題加劇。

本季具指標性案例為駭侵組織 Lazarus 以軟體供應鏈手法攻擊南韓用戶；另一起案例為駭客於暗網拍賣 25 萬個竊取之 MySQL 資料庫。

首先，探討案例為駭侵組織 Lazarus 以軟體供應鏈手法攻擊南韓用戶。資安業者 ESET 揭露，駭侵組織 Lazarus 針對南韓用戶發起供應鏈攻擊行動，透過南韓資安監控驗證軟體 WIZVERA VeraPort，再利用竊取得來之合法數位憑證，將惡意程式植入受駭者電腦。

WIZVERA VeraPort 為南韓政府指定之資安監控驗證軟體，當存取政府或銀行網路服務時，該軟體會自動安裝政府或金融機構網站所需之系統元件與資安軟體，然而 WIZVERA VeraPort 驗證網站數位憑證時，僅會檢查數位憑證有效性，不會檢查其擁有者是否為真。駭侵團體 Lazarus 利用此一漏洞，將須下載之系統元件或資安軟體置換為惡意程式，並利用竊取之合

法數位憑證於惡意程式中加入數位簽章，將惡意程式偽冒為合法程式，爾後植入遭駭網站中，待已安裝 VeraPort 之受害者電腦連線至該遭駭網站，即自動下載並安裝含有合法數位簽章之惡意程式。

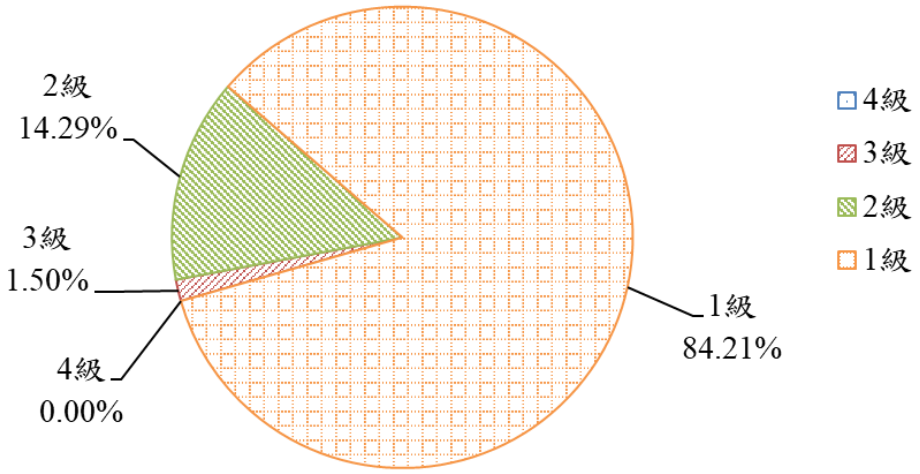
第 2 起案例為駭客於暗網拍賣 25 萬個竊取之 MySQL 資料庫，據資安業者 Guardicore 研究報告指出，駭客針對暴露於公開網路之 MySQL 資料庫發動攻擊，透過暴力破解手法駭侵 MySQL 資料庫，藉此進行資料庫內容竊取、加密及勒索攻擊，勒索失敗時，便於暗網出售資料。

駭客成功入侵 MySQL 資料庫後，便會將其內容封裝為壓縮檔，傳至駭客伺服器，並刪除原資料庫內容。此外，駭客亦於資料庫中新增一個表格，並放入勒索內容，要求受害者支付約 500 美元之贖金，若受害者不願支付贖金，駭客便將其所竊取之資料庫轉移至位於暗網之公開拍賣網站，供外界競標。目前此一公開拍賣網站已存放來自 8.5 萬個 MySQL 伺服器，共計 25 萬個資料庫，數據資料容量總計 7 TB。

綜覽本季重大資安事件，除加強供應廠商在選商前之風險評估外，亦應善盡監督管理之責。同時持續加強使用者端之資安防護概念，避免在社群網路盛行時，不經意洩漏自己個人資訊，造成有心組織利用蒐集而來資訊藉機謀利或干擾資通訊服務。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成之衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 84.21%為大宗，2 級事件占 14.29%次之，3 級事件僅占 1.50%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

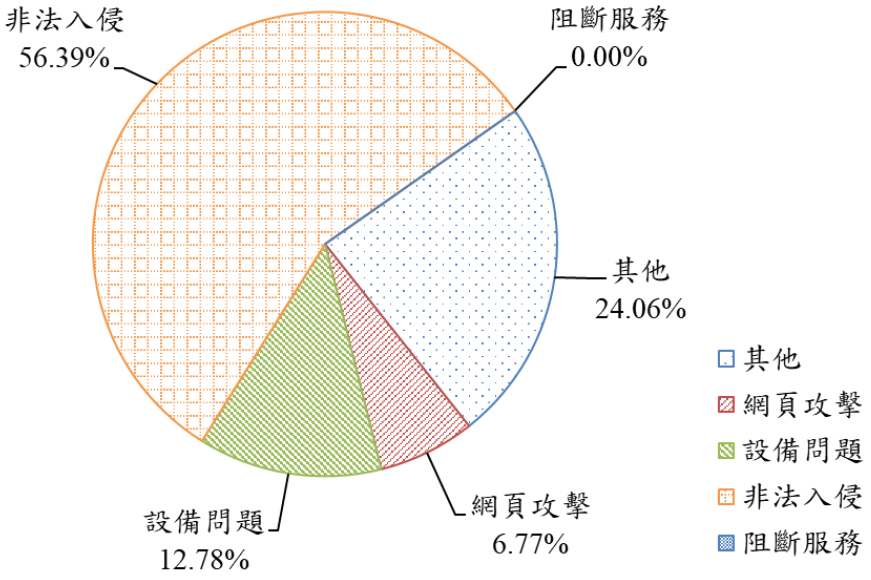


資料來源：本報告整理

圖1　109 年第 4 季通報事件影響等級比率圖

本季接獲 2 件 3 級重要通報事件，某機關因系統設定錯誤，致使用者上網讀取自己資料時，會帶出其他人個資；另一起事件為新進人員不慎將含有個人資料檔案夾帶於電子郵件中誤寄出，致多筆涉及當事人之姓名、身分證字號及手機等聯絡方式資料外洩。這些案例由於外洩資料內容包含民眾個人資料，因此通報為 3 級重要資安事件。

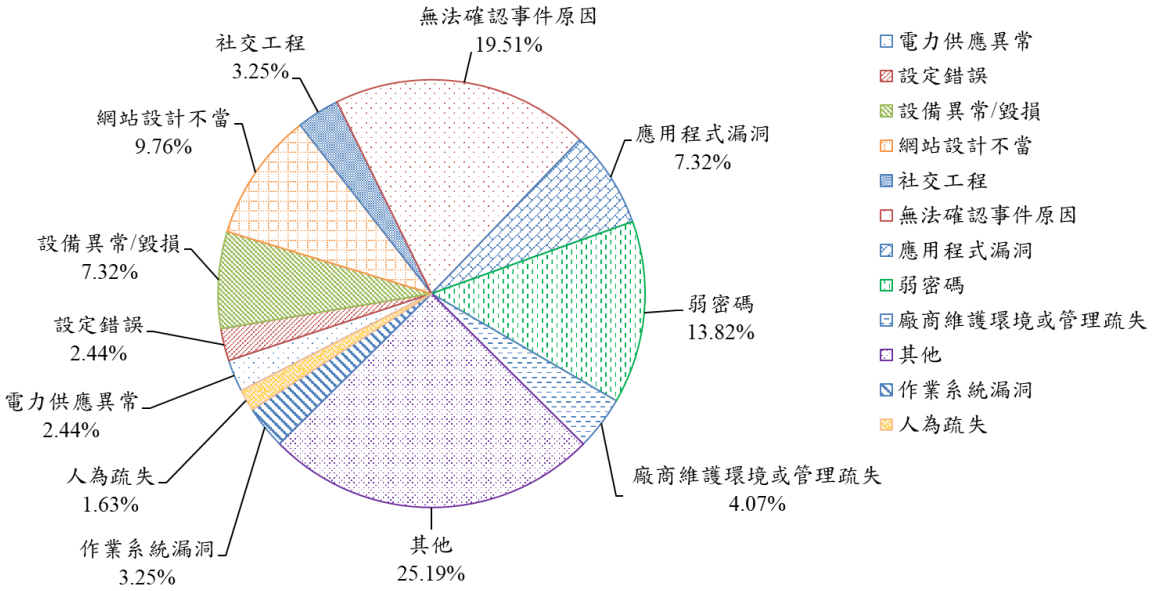
除上述資安事件外，本季通報案件發現發現部分機關網站管理後台因使用弱密碼，再加上外部存取權限設定寬鬆，遭駭客利用上傳可疑程式。本季非法入侵在事件比率，相較於上一季(52.39%)之通報比率有略為上升之趨勢。整體事件比率，以「非法入侵」(占 56.39%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　109 年第 4 季通報類型比率圖

接續，分析通報事件發生之各項原因(詳見圖 3)，發現事件原因以其他(25.19%)為主，其次分別為無法確認事件原因(19.51%)、弱密碼(13.82%)、網站設計不當(9.76%)、應用程式漏洞(7.32%)、設備異常/毀損(7.32%)、廠商維護環境或管理疏失(4.07%)、社交工程(3.25%)、作業系統漏洞(3.25%)、設定錯誤(2.44%)、電力供應異常(2.44%)及人為疏失(1.63%)。本季一般事件發生原因多為尚未歸屬到特定主題之資安事件通報，如發生因核心系統所使用之通訊電信線路故障，且又無法於可容忍中斷時間內回復正常運作；或因設備資源配置容量不足，致系統運作緩慢甚至出現無法連線及接獲入侵事件警訊進行通報，但內部調閱防火牆或 DNS Server 紀錄卻查無連線紀錄等，亦以「其他」進行結報。



資料來源：本計畫整理

圖3　109 年第 4 季公務機關資安事件原因比例圖

政府機關雖經常於內部律定密碼的重要性，但弱密碼仍占 13.82%之高，人員慣性使用弱密碼或同組萬用密碼情況仍屢見不鮮，尤其若出現在擁有特權帳號之使用者時，則相關衝擊與損害更不可小覷。因此不論是使用弱密碼或是不慎將機敏資訊外寄，應定期進行風險評估，找出可能脆弱點，就管理與技術等整體防護規劃改善措施。

1.3 資安防護重點

分析本季全球資安威脅現況，因機關常需要委外辦理資通系統之建置、維運或相關資通服務，在開始與供應商密切合作同時，如何選任適切之受託者，實屬挑戰性議題。供應商因防護強度或設計概念之不足，往往會影響其服務之組織安全，相關案例亦時有可聞，各國政府皆積極宣導應對供應商加強監督與管理之責，包含美國國防部亦開始要求承包商必須具備網路安全認證，可見其主動防禦管理之積極作法。

另一個值得注意之資通安全議題為支援之公用服務設施與資通訊設備，本

季發生之電信通訊設備故障與資通訊設備因容量規劃致服務緩慢，皆屬日常維運應重視之議題。對於資通系統維運，發現部分機關因接獲入侵事件警訊而進行通報，但調閱防火牆或 DNS Server 紀錄卻查無連線紀錄，而無法確認受害設備與入侵根因。稽核事件應先訂定與規劃日誌留存政策，不只記錄錯誤與失效日誌，藉著日誌留存政策定期檢視，亦能精進事件之偵測與回應。

個人資料外洩事件仍持續發生，分析風險發生來源包含系統管理者系統設定錯誤、人員疏失等原因，除運用資通訊科技自動偵測與防堵資料外洩外，資通安全教育訓練與認知應持續針對不同角色與面向，設計短、中及長期之規劃與實施方案。

綜整以上資安威脅現況，提供資安防護建議如下：

- 資通訊設備資安管理
  - 限制使用危害國家資通安全產品，避免潛在威脅之侵害。
  - 依資通系統防護需求分級原則，實施整體資通訊設備之盤點與安全性檢測。
  - 定期檢視與維護資通訊設備，確保其持續之可用性及完整性。
- 電子郵件資安管理
  - 使用電子郵件過濾與攻擊防護系統，防堵機密資訊外洩威脅。
  - 含個人資料或機敏資料之電子郵件，應要求遵循加密或其他保護原則。
  - 定期或不定期針對所有人員實施資安教育訓練，並測試訓練成效。

2. 資安專題分享_量子破密技術研究

近年來行動裝置普及、雲端服務發達及加密貨幣興起，為確保相關訊息傳遞、服務及交易資訊之機密、完整及不可否認性等目的，密碼學廣泛被運用於相關資通訊科技服務。現代密碼學旨在確保透過網際網路進行數據傳輸之安全性，將訊息轉換為無法被任何攔截者解釋之形式。不可否認地，隨著密碼學扮演的加密角色之重要性提升，亦間接促進破密技術之發展，對於當前廣泛使用之多種密碼演算法產生重大影響，已成為資安防護之一大威脅。

有鑑於此，為因應相關威脅，將探討先進破密技術之概況與相關資安議題，並以驅動後續重要密碼技術發展之量子破密技術，設計量子電路進行破密手法實作，並評估量子破密技術可能之威脅或應用範疇，以做為政府後續在前瞻資安防護技術研究之參考。

2.1 破密技術簡介現況

破密技術之目標在於降低破解密碼系統之金鑰或明文之時間複雜度，通常伴隨加密技術共同演進古典密碼破密技術，利用頻率分析找出明文之排列或置換現代密碼破密技術。量子電腦透過量子疊加與量子糾結特性，使得運算具有強大之量子平行性，進而提升速度來解決現今電腦所不能解決之問題，對於現行網際網路通訊所使用之密碼系統安全性產生巨大威脅。

量子破密技術運用量子平行運算之特性，設計出可降低破解密碼系統時間複雜度之演算法，由於量子破密係針對加密演算法進行破解，因此不受距離與設備種類之限制。目前量子破密仍受限於量子處理器之位元長度與抗雜訊能力，惟近期各國積極投入資源進行研發，隨著量子處理器技術逐漸成熟，現有許多密碼系統如 RSA 與 ECC(Elliptic Curve Cryptography)，已面臨被破解之威脅。

全球大廠包含 IBM、Google 及微軟，皆將量子電腦列為下階段重點開發技術。美國政府更研擬要求將量子技術與人工智慧等列為限制輸出技術，由此可窺見各國對量子技術之重視。針對量子資源發展預測，IBM 所提出專用預測量子處理器效能之「量子體積」，綜合評估量子處理器位元長度與抗雜訊能力。目前發表之量子體積如預期每年以倍數增長，IBM 也提出將於 2023 年發表高達 1,123 位元量子處理器之目標。目前許多國際大廠已著手發展量子運算環境，目前已公開之量子運算資源，詳見圖 4。

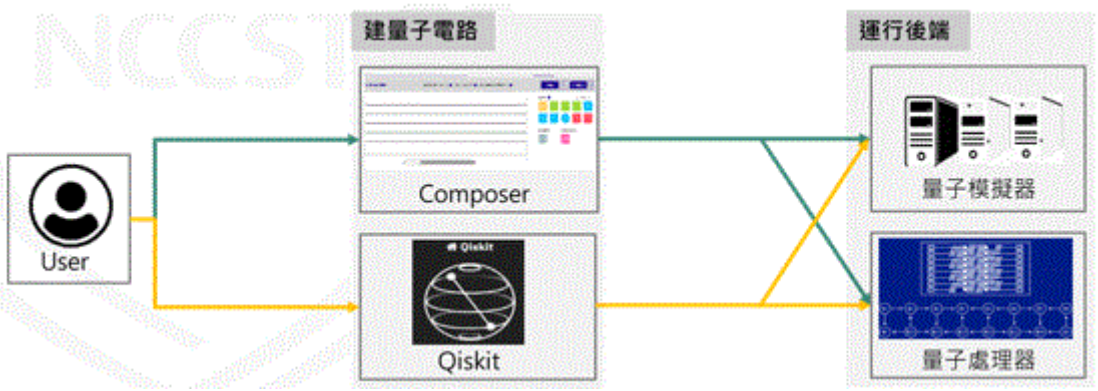
公司	IBM	D-wave	Intel	Google	Microsoft	AWS	Honeywell
硬體	• 量子模擬器 • 量子處理器	• 量子模擬器 • 量子處理器	量子處理器	量子處理器	• 量子模擬器 • 量子處理器	• 量子模擬器 • 量子處理器	量子處理器
硬體開放服務	√ 不限時免費使用	√ 免費使用1分鐘/月，付費使用1小時/月	X	X	X	X	X
程式語言相關資源	Qiskit軟體開發套件 為用於IBM Q平台之開發工具，可用於量子模擬器與量子處理器上遠端執行	Leap量子雲端服務 Leap量子雲算服務包含用於D-wave硬體之軟體開發套件	--	--	Q#量子程式設計語言 為微軟開發程式語言，用來開發量子程式與軟體	--	--
說明	2020提供65量子位元處理器	2019發表5,000量子位元處理器 • 主要為實現量子特定問題之處理器，而非採用通用量子閘技術，因此具有無法解決廣泛量子運算問題疑慮	2018發表49量子位元處理器	2018發表72量子位元處理器	尚未發表正式版服務，將推出使Q#量子語言可運行於合作量子設備之服務	2020發表量子運算服務，無開放免費使用	2020發表64量子位元處理器，將與Microsoft合作提供後端服務

資料來源：本報告整理

圖4　量子運算資源列表

2.2 量子破密技術研析與實作

IBM 與 D-wave 皆開放量子運算服務，惟 D-wave 使用上有時間限制且硬體實現方法仍有疑慮，因此將利用 IBM 提供之平台實作量子破密技術，自建量子電路並利用後端處理器執行運算。量子電路使用「Qiskit」撰寫程式碼(Python)來建構量子電路，運行後端則使用近似理論值之「量子模擬器」與真實之「量子處理器」比對以驗證實作結果，詳見圖 5。



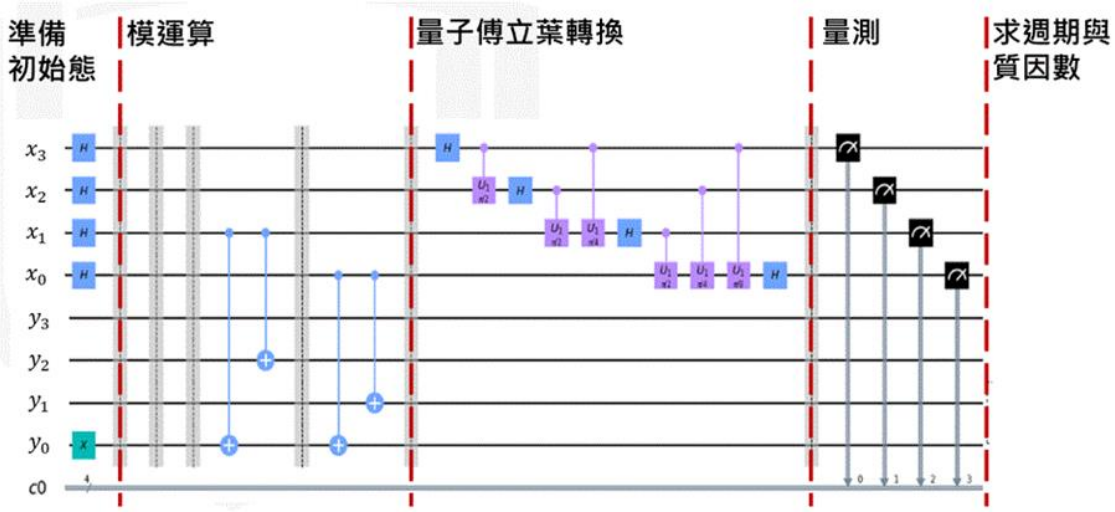
資料來源：本報告整理

圖5　IBM 平台實作環境

分別進行 RSA 破解實作、對稱式密碼系統破解實作(以 LFSR 為例)及雜湊函式破解實作。

RSA 破解實作以量子 Shor 演算法進行，量子 Shor 演算法是可對特定非對稱式密碼進行破解之演算法，其概念是將質因數分解問題轉換為週期找尋之問題。

Shor 演算法關鍵點在於量子平行運算，由於計算能力隨位元數增加呈指數級增長，使尋找週期時間加速。其中量子電路可分為準備初始態、模運算、量子傅立葉轉換、量測及求週期與質因數等 5 大部分，詳見圖 6。



資料來源：本報告整理

圖6　RSA 破解實作

實作結果顯示所建構之量子電路可正確完成質因數分解，比對量子模擬器與處理器之結果，目前處理器之誤差問題仍會影響量測結果，且導致破解時間增加。隨著未來量子位元之增長與雜訊抑制技術之成熟，參考 IBM 所提出的量子體積預測，RSA-1024 將可能於 2026 年遭破解，詳見圖 7。

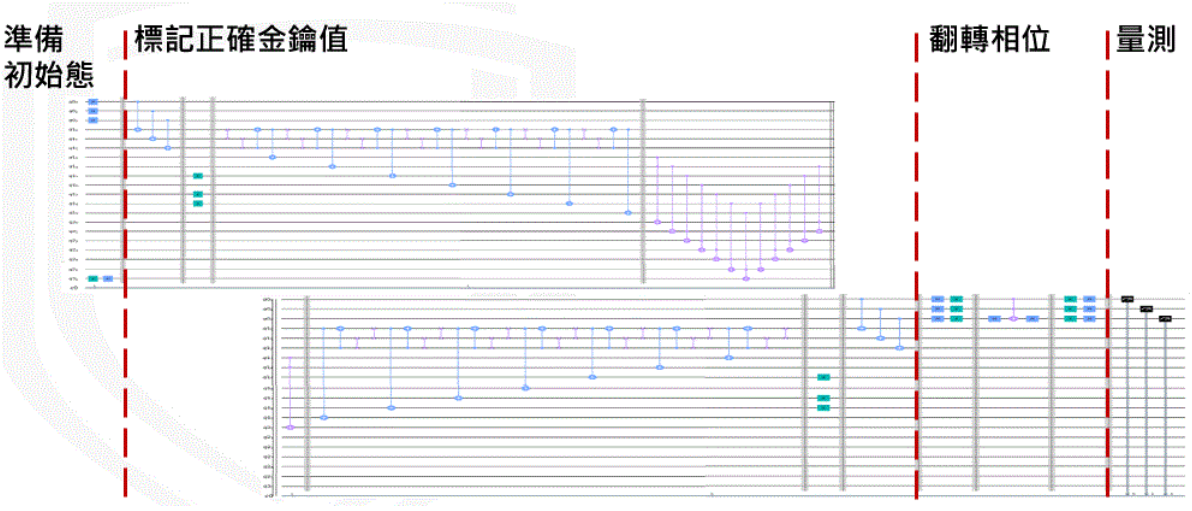
演算法	所需量子位元	安全等級(bits)		傳統運算破解時間	量子運算破解時間	
		傳統運算	量子運算		無考量糾錯	考量糾錯
RSA-1024	2,050	80	0[1]	約$3.8 * 10^7$年	約不到1秒	約3.58小時[2]
RSA-2048	4,098	112	0[1]	約$1.6 * 10^{17}$年	約不到1秒	約28.63小時[2] (約1天)
RSA-4096	8,194	128	0[1]	約$1.1 * 10^{22}$年	約不到1秒	約229小時[2] (約10天)

資料來源：本報告整理

圖7　RSA 破解預估期程

另一種對稱式密碼系統破解實作，則實作 Grover 演算法。量子 Grover 演算法為搜尋特定值/解之演算法，可用於搜尋對稱式加密演算法之金鑰(或雜湊函式之輸入值)。透過疊加態表示所有可能之金鑰值(或所有可能輸入值)，同時對所有可能性進行搜尋，藉由反覆「標記正確值」與「翻轉相位」過程，逐次提升正確解量測機率。

實作破解以 LFSR 所構成之對稱式加密法，其中量子電路可分為準備初始態、標記正確金鑰值、翻轉相位及量測 4 大部分，詳見圖 8。



資料來源：本報告整理

圖8　對稱式密碼系統破解實作

實作結果顯示所建構之量子電路，其正確金鑰之量測機率逼近 1，與理論值接近，惟須於量子電路中完整實現欲破解之加密演算法，所需量子位元數隨演算法之複雜度提升，且不易建構。針對金鑰總數為N之金鑰空間，Grover 演算法約運行$N1/2$ 運算即可找出正確金鑰，形同將現有加密演算法之安全等級減半。假設使用每秒執行 10^9 運算 CPU，若要破解 128 bits AES 量子運算需耗費約 600 年，詳見圖 9。

演算法	所需量子位元	安全等級(bits)		傳統運算破解時間	量子運算破解時間	
		傳統運算	量子運算		無考量糾錯	考量糾錯
AES-128	2,953	128	64	約10^{22}年	約585年	約$2.61 * 10^{12}$年[2]
AES-192	4,449	192	96	約$1.99 * 10^{41}$年	約$2.5 * 10^{12}$年	約$1.97 * 10^{22}$年[2]
AES-256	6,681	256	128	約$3.67 * 10^{60}$年	約10^{22}年	約$2.29 * 10^{32}$年[2]

資料來源：本報告整理

圖9　對稱式密碼系統破解預估期程

雜湊函式破解實作以 Grover 演算法，實作破解以 LFSR 所構成之雜湊函式，其中量子電路可分為準備初始態、標記正確輸入值、翻轉相位及量測

4 大部分。實作結果與破解對稱式密碼之情形相似，可成功搜尋雜湊函式之正確輸入值與理論量測機率相近。假設使用每秒執行 10^9 運算 CPU，若要找出 SHA2/3 固定 256-bit 長度之輸入則需 1022 年，詳見圖 10。

演算法	所需量子位元	安全等級(bits)		傳統運算破解時間	量子運算破解時間	
		傳統運算	量子運算		無考量糾錯	考量糾錯
AES-128	2,953	128	64	約10^{22}年	約585年	約$2.61 * 10^{12}$年[2]
AES-192	4,449	192	96	約$1.99 * 10^{41}$年	約$2.5 * 10^{12}$年	約$1.97 * 10^{22}$年[2]
AES-256	6,681	256	128	約$3.67 * 10^{60}$年	約10^{22}年	約$2.29 * 10^{32}$年[2]

資料來源：本報告整理

圖10 雜湊函式破解實作

以上破解實作仍需視實際情況，量子運算仍有誤差需大量資源糾正錯誤狀況發生，將可能導致攻擊時間增加。實作結果顯示，當量子處理器之位元長度足夠且能有效抑制雜訊時，量子 Shor 演算法已可直接在有效時限內破解 RSA 或 ECC 等非對稱式密碼系統，而量子 Grover 演算法亦可將現有密碼系統之安全強度減半。

因量子破密目前仍受限於量子處理器之量子位元與雜訊干擾，其破密能力仍有其侷限性，若量子運算之進程如「量子體積」發展之預測，或許將於 5 至 10 年內影響至現有密碼系統。因此，未來研究方向將持續關注量子運算之基礎環境與破密技術發展，以掌握可能之威脅並提前部署。

3.資安技術研析_ Zerologon 漏洞研析

本季所探討之資安技術研析為 Zerologon 漏洞研析，首先由資安廠商 Secura 於 9 月揭露之 Netlogon 遠端協定，存在 Zerologon 漏洞(CVE-2020-1472)。因此漏洞高達 CVSS(Common Vulnerability Scoring System) 10 分，各國政府與企業皆視為影響重大之漏洞，應儘速安裝修補程式。尤其是美國國土安全部於獲知漏洞訊息後一週內即發出緊急指令，要求聯邦政府所有機關必須在 3 天內完成相關修補措施。

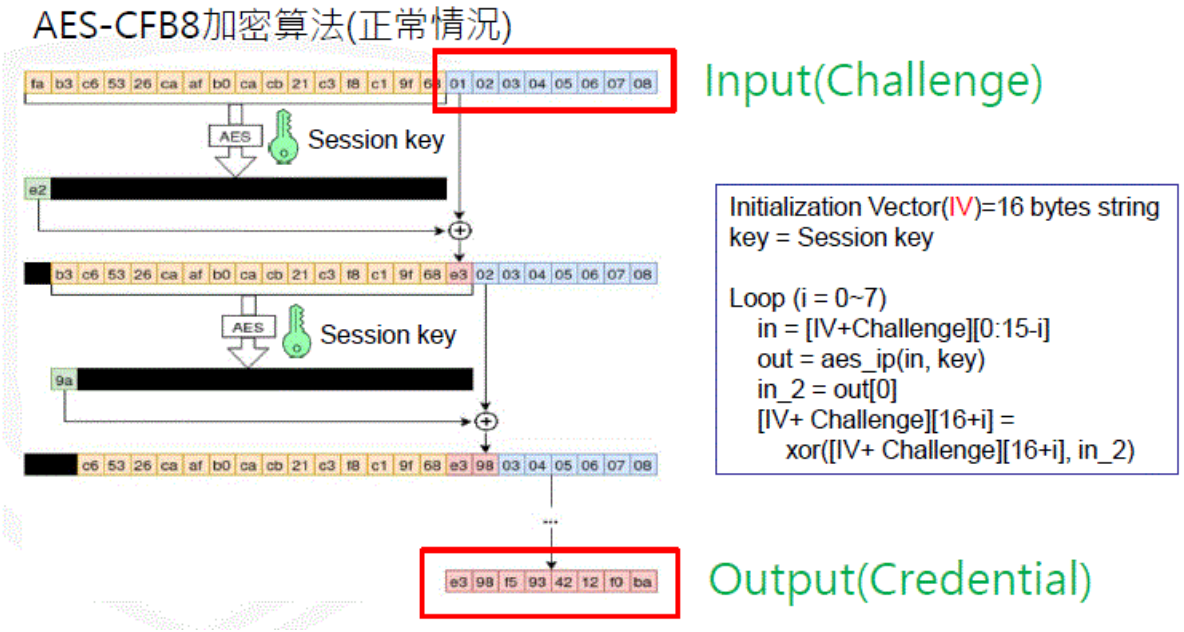
若成功利用此漏洞入侵後，未經驗證之攻擊者則可利用偽冒憑證繞過身分驗證，以任意身分與 DC(Domain controller)建立安全通道，進而取得 AD(Active Directory)資料庫內容，毋需多時就可控管整個網域。

3.1 攻擊漏洞解析

微軟 Defender ATP 成員於官方技術社群網站發文指出，漏洞被揭露數日後就發現 Zerologon 攻擊數量激增，其中已有少數案例屬於正式攻擊行動，受影響產品包含從 Windows Server 2008、2012、2019 及 Windows Server, version 1903、1909、2004 等若干版本。

Netlogon(MS-NRPC)主要運作於網域電腦與網域控制站間之遠端程序呼叫 RPC(Remote Procedure Call)介面，負責設備間之安全溝通，主要功能包含建立安全通道、更換電腦帳號之密碼、傳遞使用者身分驗證、傳輸資料加密簽章及 AD 資料庫(NTDS.dit)備份等。

此次漏洞攻擊主要發生在 Netlogon 安全通道建立流程，使用 AES-CFB8 加密演算法計算登入用憑證(Credential)。正常運作情況，詳見圖 11。

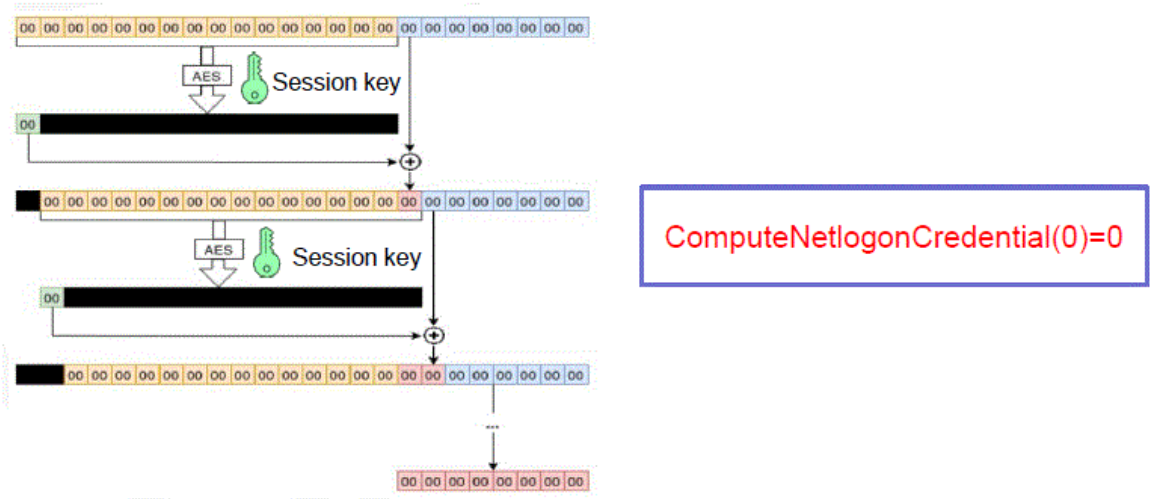


資料來源：本報告整理

圖11 Netlogon 使用 AES-CFB8 加密演算

正常運作情況由於攻擊者不知道帳號密碼(secret)，無法得出 Session key，也無法成功算出 Client credential，致無法通過 Server 端登入驗證。但因 Netlogon 登入驗證僅需比對 Credential，若攻擊者能在不知道 Session key，計算出 Credential，則可成功繞過身分驗證。

由於計算登入用 Credential 之 ComputeNetlogonCredential 函式沒有正確實做 AES-CFB8 加密演算法，將原本應為隨機數值之 IV 參數固定為全 0 字串，造成當攻擊者將 Client challenge 同樣設成一連串 0 時，有很高機率(1/256)得到輸出結果也為 0，詳見圖 12。



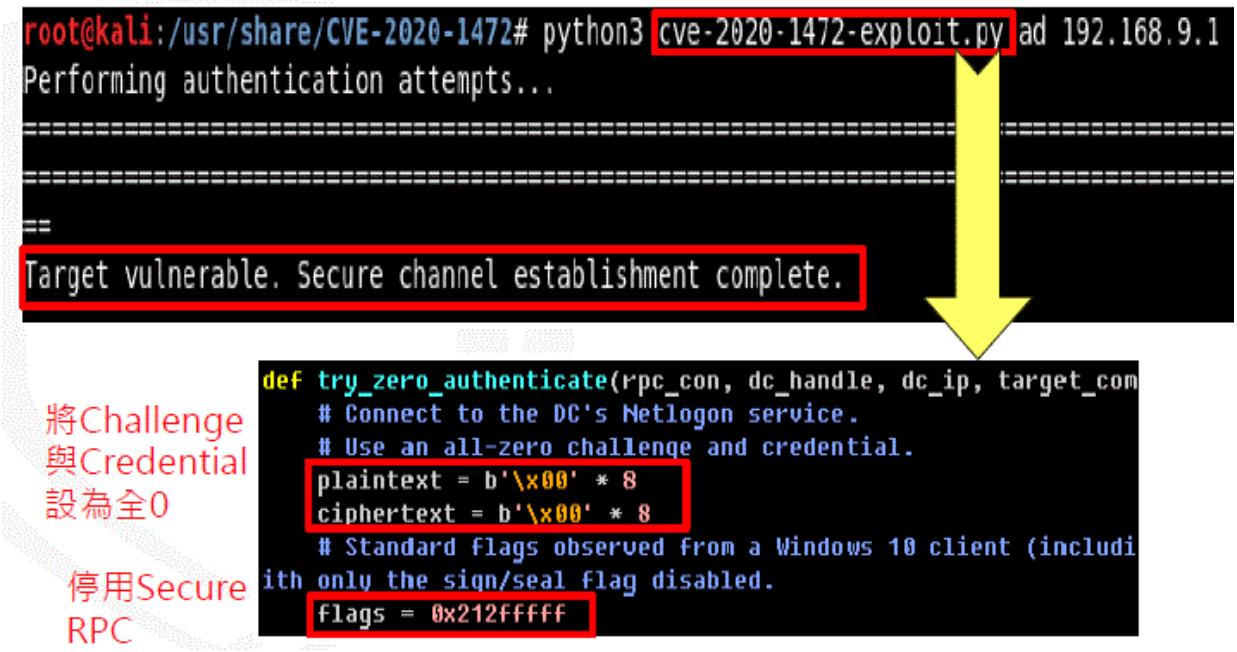
資料來源：本報告整理

圖12 IV 參數固定為全 0 字串

因為 Server Challenge 會變動，使 Session key 一直隨著更換，而又因登入失敗後不會被封鎖，故可在短時間內多次嘗試以 Credential=0 登入。當出現一把 Session key，使 Server 端算出之 Credential 亦為 0，即可通過登入驗證。

3.2 攻擊流程實作與因應措施

利用 Zerologon 攻擊，駭客會先駭進某內網使用者電腦後，再經連線發現此電腦若可連至內網主網域控制站 DC，即可成功發動 Zerologon 攻擊，再企圖控制整個網域。首先執行 CVE-2020-1472-exploit.py，藉由將 Challenge 與 Credential 設為全 0，並經多次登入嘗試後通過身分驗證，偽冒 DC 身分與 DC 建立安全通道，同時停用 Secure RPC，詳見圖 13。



資料來源：本報告整理

圖13 偽冒 DC 身分與 DC 建立安全通道

接續惡意程式 CVE-2020-1472-exploit.py 將 DC 自身電腦帳號(ad$)之密碼設為空字串(empty string)，再利用 DC 電腦帳號新密碼，透過 secretsdump.py 工具，以 DCSYNC 方式，取得全網域帳號密碼。最後利用已取得之網域管理員 hash 密碼，透過 evil-winrm 工具執行 PTH 攻擊，取得 shell 獲得網域控制權。整個攻擊流程，詳見圖 14。

資料來源：本報告整理

圖14 實作攻擊流程

面對 Zerologon 攻擊，CVE-2020-1472 漏洞修補方式首先應更新網域控制站，安裝 109 年 8 月 11 日或之後發行之安全性更新。此安全性更新會藉由檢查 Client Challenge 前 5 個 bytes 是否相同，成功將嘗試取得可通過登入驗證 Session key 之機率，由 1/250 下降至約 1/40 億。再者，應檢視事件紀錄檔，找出可能存在漏洞之內網裝置，並安裝更新及強制啟用 Secure RPC 模式，啟用強制模式後，不支援 Secure RPC 之第三方軟體將被拒絕連線。

原廠雖已針對 CVE-2020-1472 漏洞提供安全性更新，若能強制啟用 secure RPC 功能，則可減緩被攻擊成功機率。同時，在 110 年第一季釋出更新後，所有 Windows 與非 Windows 電腦在 Netlogon 安全通道中，皆強制使用 Secure RPC，則相關設備亦需更新為支援 secure RPC，或是透過群組原則，設定例外原則來允許連線。在此之前，機關內部仍應先辨識是否存在無法強制啟用安全連線之設備，並規劃相關配套控制措施，並持續監控內網認證活動，追蹤在此安全議題下是否發展其他風險。

4. 結論

本季具指標性案例為駭侵組織 Lazarus 以軟體供應鏈手法攻擊南韓用戶，駭客透過南韓資安監控驗證軟體，再利用竊取得來之合法數位憑證，將惡意程式植入受駭者電腦，造成使用者無法在第一時間查覺受害；第 2 起案例為駭客藉著入侵 MySQL 資料庫，再藉以勒索金錢。駭客會先將內容封裝為壓縮檔，傳至駭客伺服器，並刪除原資料庫內容，駭客最初目的為贖金，若勒索不成則轉至暗網拍賣。相關案例提醒除須檢視內部資安防護韌性外，亦應善盡監督與管理之責，以提升供應鏈安全整備度。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」類型為主，綜合類型「其他」次之，接續分別為「設備問題」與「網頁攻擊」為通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「資通訊設備資安管理」與「電子郵件資安管理」，提出資安防護建議。

資安專題分享主題為量子破密技術研究，隨著密碼學扮演的加密角色之重要性提升，亦間接促進破密技術之發展。為因應相關威脅，探討先進破密技術之概況與相關資安議題，並以量子破密技術，設計量子電路進行破密手法實作，並評估量子破密技術可能之威脅或應用範疇，以做為政府後續在前瞻資安防護技術研究之參考。

另外，資安技術研析主題為 Zerologon 漏洞研析，該漏洞高達 CVSS 10 分，各國政府與企業皆視為影響重大之漏洞，要求應儘速安裝修補程式。若成功利用此漏洞入侵後，未經驗證之攻擊者則可利用偽冒憑證繞過身分驗證，以任意身分與 DC 建立安全通道，進而取得 AD 資料庫內容，控管整個網域。

資安相關活動

本季行政院資通安全處辦理之資安相關活動，說明如下：

◆ 109 年第 2 次政府資通安全防護巡迴研討會

109 年第 2 次政府資通安全防護巡迴研討會恢復以實體方式，於台北、台中、高雄及台東等地辦理。本次課程主題，分別為資安威脅趨勢與案例分享、國家資通安全發展方案(110 年至 113 年)草案及 109 年網路攻防演練暨資安檢測重要發現事項說明。

本次資安威脅趨勢與案例分享，除分析全球資安威脅案例外，國內資安事統計發現資料外洩狀況仍時有所聞，事件主因包含 Google 表單權限設定錯誤與存取權限設置不當等。觀測到政府機關核心業務中斷，如因防火牆設備異常，致多台伺服器無法對外連線或維護廠商維運使用之帳號密碼遭外部暴力破解，再橫向擴散至其他設備。第二個主題說明第六期國家資通安全發展方案之願景、目標、策略、具體措施，具體說明推動策略包含「吸納全球高階人才，培植自主創研能量」、「推動公私協同治理，提升關鍵設施韌性」、「善用智慧前瞻科技，主動抵禦潛在威脅」及「建構安全智慧聯網，提升民間防護能量」。

最後主題為 109 年網路攻防演練暨資安檢測重要發現事項說明，綜整 109 年網路攻防演練攻擊紀錄，發現其中不安全的組態設定與無效的身分認證筆數比例最高。而弱點存在原因則可分為 4 大類型，分別為資料庫未限縮存取來源、上線前未落實安全設定檢查、公開預設帳號與通行碼原則及未落實權限檢查。除針對網路攻防演練暨資安檢測分析風險來源外，亦提供相對建議，包含完備資料保護機制、加強存取控制措施、建立內部驗證機制及確實落實資安防護政策等防護策略。

◆ N-ISAC 年會

109 年第 4 季辦理之 N-ISAC 年會，以「防範勒索軟體攻擊，強化 CI 資安防護能量」主題，分別辦理 WORKSHOP 與研討會活動。

N-ISAC 年會首次以 WORKSHOP 方式，針對 CI 領域辦理「勒索軟體防護與情資分享」活動，內容以事前之防護部署與情資蒐集、事中之即時處置與損害控管、事後之事件分析與情資分享等 3 個階段，分別採「防護講習」與「實作練習」進行練習活動，期增進彼此交流與深化應變處理能量。

研討會議則針對「資安威脅之挑戰與因應」與「強化 CI 領域勒索軟體防範與聯防」等議題進行交流討論，除就國內外資安威脅趨勢進行回顧與展望外，亦邀請產業界代表針對產業之威脅挑戰進行座談交流。另特別針對 CI 領域受到勒索軟體攻擊事件進行經驗分享，期透過不同領域之防護經驗，強化跨域資安聯防與合作。