113年第3季資通安全技術報告

Quarterly Technical Report

國家資通安全研究院

National Institute of Cyber Security


TECHNOLOGY.

目　次

圖 目 次

表 目 次

摘要

「第 3 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，提供政府機關需關注之資安風險重點。

「第 3 季資通安全技術報告」分為以下 4 個章節。

●資安威脅現況與防護重點

從分析全球資安威脅現況開始，以 CrowdStrike Falcon EDR 感測器更新錯誤造成微軟當機事件，引言概敘供應鏈帶來之衝擊與後果，同時以 2 件案例說明供應鏈之發生緣由、風險及防範事項，第一起案例為雙重認證應用程式 Authy 電話號碼遭外洩，業者於官網提醒使用者更新應用程式，並防範後續網路釣魚與簡訊攻擊；另一案例為防毒軟體卡巴斯基於美國被禁用後，逕行以新防毒軟體安裝於用戶電腦，引起使用者對資料安全與惡意程式潛藏之疑慮。

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」(占 38.94%)類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」(占 26.46%)與「阻斷入侵」(占 4.65%)為主要通報類型。

●資安專題分享

資安專題分享主題為在「自動化與協作」支柱中推進零信任成熟度介紹，藉由此網路安全資訊表說明具體之成熟度模型，協助組織逐步提升其安全防護能力，從而於不斷變化之威脅環境中維持網路安全韌性。

●資安技術研析

資安技術研析主題為 Polyfill 套件威脅案例分析，資安廠商揭露 Polyfill 套件威脅事件，發現有多個網域遭同一攻擊者注入惡意程式，網站遭植入惡

意網域 cdn.polyfill.io 之 JavaScript 後，將會被自動連結至惡意網站。

●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。資安專題分享在「自動化與協作」支柱中推進零信任成熟度介紹，說明於自動化與協作不同等級之成熟度要求，以因應自動化需求與 AI 科技浪潮，提升防護與回應韌性。此外，資安技術研析分析為 Polyfill 套件威脅案例分析，提醒機關應避免使用相關 Polyfill 套件，若已使用此套件應儘速進行風險與衝擊評估，分析可能影響範圍，再決定適切之處置方式，同時檢視使用第三方套件，並導入完整性驗證其套件之安全機制。

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及可能之衝擊與影響。113 年第 3 季(以下簡稱本季) 根據本季國際資安重大事件歸納探討議題，討論相關事件所造成之衝擊並提供建議之防護作為，以利政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

本季國際間最大資安事件應為 7 月 CrowdStrike Falcon EDR 感測器更新錯誤造成微軟當機事件，數以百萬計資通系統遭受影響，且使相關業務服務因此停頓，CrowdStrike 亦面臨客戶與投資者之賠償請求。CrowdStrike 於 8 月發布根因分析報告[1]，說明導致全球 Windows 作業系統癱瘓之軟體更新錯誤之資安事件，並將該事件歸咎於安全漏洞與流程缺陷之交互作用。事後 CrowdStrike 提出階段部署與層層驗證其流程正確性之作法，亦提出聘請獨立第三方軟體安全供應商對 Falcon 感測器程式碼執行進階審查，以確保其安全與品質。該事件發生當下，網路立即出現很多偽造訊息，如出現指證為該事件始作俑者 CrowdStrike 之員工照片、錯誤受害者之系統畫面及由駭客藉此事件進行之社交工程攻擊活動等，處處考驗管理者在事件發生時之應處態度與方案及如何完備委外供應鏈之安全，事件發生時，微軟即針對當機狀況提出修復方式，而 CrowdStrike 隨後亦發布修補程式與解決方案，建議使用者在更新端點或重要防護系統時，應在安全之測試環境內進行測試後再正式部署至作業區。

本季另外具指標性案例為雙重認證應用程式 Authy 電話號碼遭外洩，引發

[1] https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf

後續驗證安全與資料外洩危機；另一起案例為防毒軟體卡巴斯基於美國被禁用後，未經同意逕行以新防毒軟體取代並安裝於用戶電腦。

第 1 起案例為案例為 Authy 電話號碼遭外洩事件分析，雲端通訊平台公司 Twilio 所擁有 Authy 應用程式相關之數千萬個電話號碼因遭駭客外洩，導致後續其他資料外洩。駭客組織 ShinyHunters 於 BreachForums 網站公告洩露 Twilio 雙重認證應用程式 Authy 相關之 3 千萬個以上隨機電話號碼。Twilio 初始業務主要雲端通訊服務業者，提供電話、簡訊及使用其 Web 服務應用程式介面(Application Programming Interface, API)執行其他通訊功能之可程式化通訊工具，後續併購 Authy 做為兩階段驗證碼產生器，可跨平台同步使用者需產生驗證碼之服務帳號。

該事件攻擊是藉由不安全之 API 端點展開，因未設置嚴謹之身分驗證，攻擊者利用此弱點成功竊取 Authy 雙重認證用戶之電話號碼，駭客所揭露之 CSV 檔案欄位包含，包含帳戶 ID、電話號碼、帳戶狀態及設備數，所衍生後果使入侵者得以取得用戶於網路服務在使用時所輸入之兩階段驗證碼。Twilio 於官網針對該事件[2]請 Authy 使用者更新應用程式，表示因端點未經身分驗證致 Authy 帳戶相關資料，外洩之電話號碼後續恐遭利用，將引發網路釣魚與簡訊攻擊事件。

Twilio 於 111 年時亦傳出因駭客成功對其員工展開社交工程攻擊[3]，致員工員工憑證外洩後，殃及部分客戶帳號亦遭受未經授權存取。當時經 Twilio 內部分析，駭客已具備將員工姓名與其電話號碼進行匹配之能力，故能成功破解雙重驗證之方式。事後雖然 Twilio 展開一系列加強防範措施，此次事件發生再次驗證安全機制因詭譎多變因素，如攻擊、系統、科

[2] https://www.twilio.com/en-us/changelog/Security_Alert_Authy_App_Android_iOS?ref=escape.tech

[3] https://www.twilio.com/en-us/blog/august-2022-social-engineering-attack

技複雜化與人性弱點等，仍可能出現百密一疏之處。

第 2 起案例為防毒軟體卡巴斯基被禁用後引起之一連串安全疑慮，該公司於美國被禁用後，未經同意逕行以新防毒軟體取代並安裝於用戶電腦。美國政府於 6 月公告基於潛在之國家安全風險為由宣布自 9 月 29 日起禁止卡巴斯基防毒軟體在美國銷售，且包含所有軟體更新動作。卡巴斯基於 9 月初對客戶寄送電子郵件告知終止產品銷售與更新後，將由其信賴夥伴另一家廠商 Pango Group 之防毒軟體 UltraAV 提供可靠之網路安全保護，奠基於卡巴斯基已付費之用戶，可提供之產品功能包含 VPN、密碼管理及身分竊盜保護等，信件中提及將會收到來自於 UltraAV 訊息，以啓動相關帳號。

隨即社群媒體 Reddit 開始有用戶在平台反映[4]，電子郵件並未告知用戶卡巴斯基產品將自動從他們電腦中卸載，並自行安裝 UltraAV，且用戶購買卡巴斯基產品時，若有訂閱 VPN，同樣會一起安裝。有些用戶則表示從未收到郵件通知轉換訊息，其他安全疑慮包含啓用 Ultra AV 後，該防毒軟體刪除一個誤判為惡意軟體之應用程式，且除刪除前並未提供選項讓使用者選擇；最讓人詬病為使用者利用其他卸戴程式移除 UltraAV 時，發現在電腦重新啓動後會再次安裝該程式，這些狀況也引發卡巴斯基用戶對資料安全與惡意程式潛藏之風險疑慮。

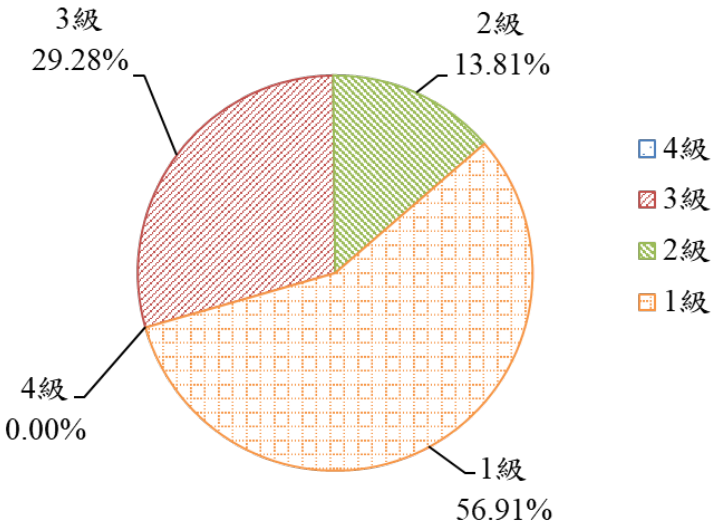
綜覽本季全球資安威脅與資安事件，雙重認證應用程式 Authy 資料外洩事件，警惕使用者不能完全信靠安全機制，且需提防偽冒驗證之網路風險。美國政府禁用卡巴斯基軟體，並未預料該公司會有替代產品，致其影響與衝擊餘波盪漾，對於有安全疑慮之使用者，建議應視既存電腦之資料敏感程式，先行做好保護動作。若僅想卸載 UltraAV，可先使用內建之卸載程

[4] ttps://www.reddit.com/r/antivirus/comments/1f9ps3e/kaspersky_beginning_transition_of_us_users_to/?rdt=56659

式或使用第三方卸載軟體確認卸載結果，並可藉由登錄編輯程式檢視相關程式是否已刪除乾淨。若採取格式化電腦處理，則可使用第三方低階格式化或資料清除與硬碟檢測之工具軟體，確認未有任何殘存程式。

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 56.91%為大宗，2 級事件占 13.81%次之，3 級事件占 29.28%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。



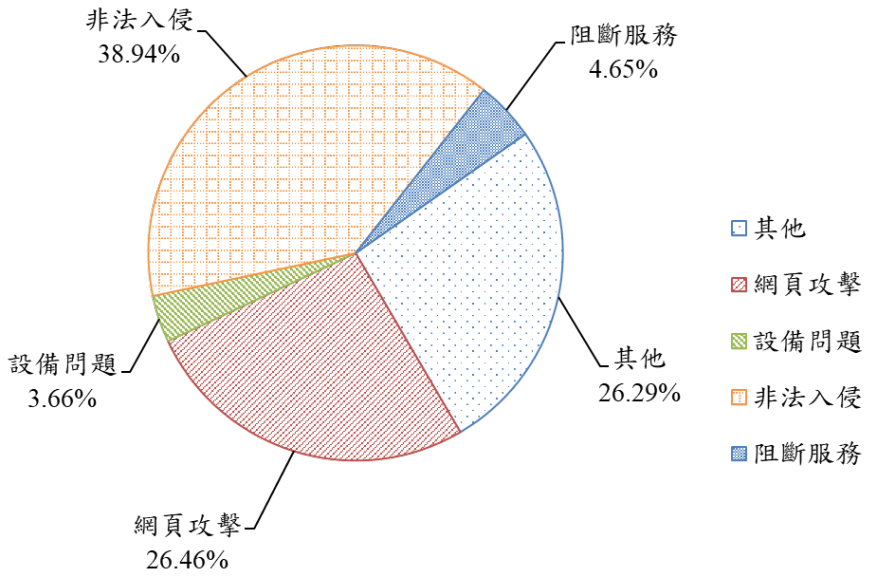
資料來源：本報告整理

圖1　113 年第 3 季通報事件影響等級比率圖

本季之重要通報事件統計，3 級事件相較於上季(13.72%)或去年同期占比(10.75%)明顯提升，乃因遭受國際受害者眾之供應鏈資安事件 CrowdStrike EDR 更新異常影響，導致涉及關鍵基礎設施維運之核心業務與核心資通系統之運作受影響，業務服務之可用性中斷。

3 級之個資外洩事件，發生案例有因承辦人員作業疏失，未考量資料索引與資料遮蔽不完整，致資料於處理時因資訊互相關聯後意外洩漏個人資料。而網站系統遭攻擊者偵測入侵現象仍然值得注意，特別是對外公開服務網站，因系統存在漏洞，致透過修改網址參數，即可取得敏感資訊。

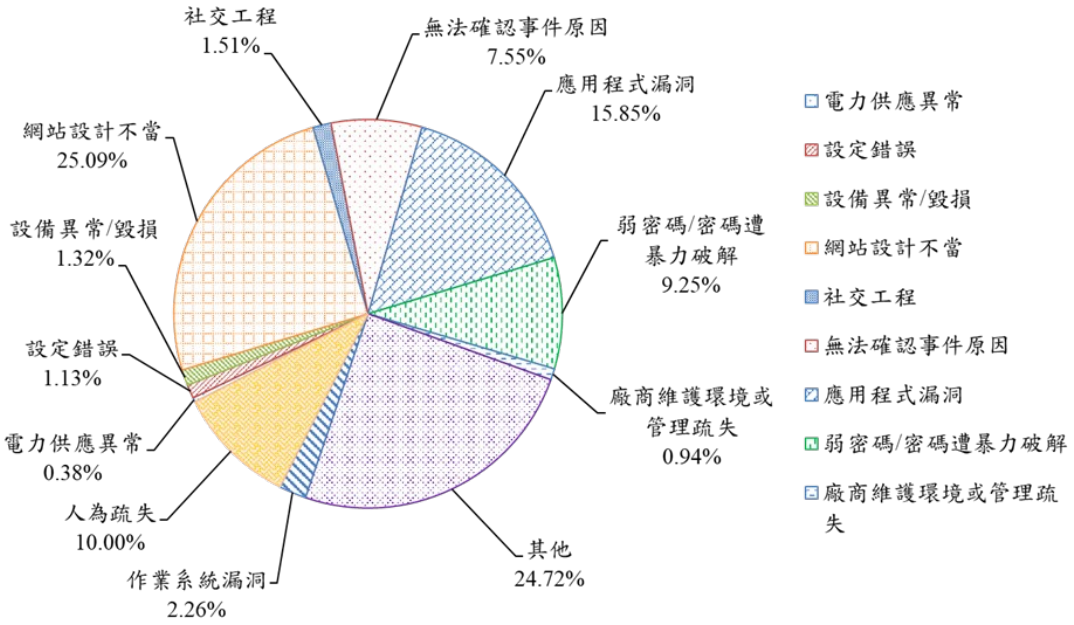
整體通報事件類型，以「非法入侵」(占 38.94%)類型為主，排除綜合類型「其他」外，「網頁攻擊」與「阻斷服務」類型次之，阻斷服務相較於去年同期(3.22%)占比呈現上升趨勢，提醒機關應加強應對措施，以防範此類攻擊行為，詳見圖 2。



資料來源：本報告整理

圖2　113 年第 3 季通報類型比率圖

分析通報事件發生原因，先排除其他類別後，以網站設計不當(25.09%)與應用程式漏洞(15.85%)為主，其次分別為人為疏失(10%)、弱密碼/密碼遭暴力破解(9.25%)、無法確認事件原因(7.55%)、作業系統漏洞(2.26%)、社交工程(1.51%)、設備異常/毀損(1.32%)、設定錯誤(1.13%)、廠商維護環境或管理疏失(0.94%)及電力供應異常(0.38%)，詳見圖 3。



資料來源：本報告整理

圖3　113 年第 3 季資安事件發生原因比例圖

分析第 3 季通報類型與通報事件發生原因，「網站設計不當」主要為實兵演練通報揭露為主，部分機關因對外網站存在注入攻擊或無效之存取控管，若未及時修補，恐遭惡意人士利用。「應用程式漏洞」大部分為使用第三方應用程式或套件，卻疏忽即時更新安全性漏洞。第三方應用程式包含使用開源軟體，因其舊版本可讓遠端攻擊者不需經經身分鑑別，即可執行任意程式碼，且漏洞之概念性驗證(Proof of Concept, PoC)已被公開，極具風險性。另發現有加密機制失效之案例，肇因為使用者運用 Adobe Reader 遮蔽敏感資訊未確實致敏感資訊可再被復原。

本季「其他」類別高居第 2 位，乃因通報系統中設定與系統預設事件發生原因項目無法符合實際狀況，則歸類為「其他」，因此機關遭遇 CrowdStrike EDR 更新異常之資安事件時，大部分通報為其他類別。

1.3 資安防護重點

分析本季全球資安威脅現況，不論是 CrowdStrike Falcon EDR 感測器更新

錯誤造成微軟當機、抑或雙重認證應用程式 Authy 電話號碼外洩及卡巴斯基自行安裝替代防毒軟體事件，皆為供應鏈之資安事件，Authy 案例提醒管理者雖運用安全機制，仍需注意供應鏈中可能出現之安全議題。面對不同來源之攻擊面，如何定義與盤點所有資產、服務及辨識關聯分析，應為首要課題，而最終能以強化供應鏈之韌性與資安服務水準能達到一致性之管理為目標。

國內部分藉由實兵演練揭露有加密機制失效之案例，肇因為使用者運用 Adobe Reader 遮蔽敏感資訊，因其加工原始文件時，以「插入圖片」遮蔽敏感資訊後再轉成 pdf 檔案格式，惟此方式若利用複製再貼上，則可見其所遮蔽之資訊。為避免此狀況發生，則需使用進階或專業版本，本身就支援遮蔽功能，而或是應於原始文件將遮蔽文字以圖片方式貼在原始文件，則可避免文字遭破解揭露。

綜整以上資安威脅現況，提供資安防護建議如下：

●多重驗證之資安管理

– 盤點與評估第三方身分驗證器應用程式，使用完整性驗證工具，確認其健康狀態後方能利用，且應納入弱點偵測範圍。

– 定義系統安全之組態管理準則且文件化，建議關閉預設雙重驗證允許多項設備關聯，滾動式檢視組態設定之安全性。

– 教育使用者檢查與其身分驗證關聯之所有設備，並刪除無法識別之設備，且自我檢視關聯帳戶是否有可疑活動。

●加密機制之資安管理

– 定義與區分資訊等級，視機敏等級訂定不同加密機制，規範資料生命週期之加解密標準作業準則與程序。

– 關注已遭公開揭露或破解之加密方式或演算法，公告或教育避免使用。

– 提供加解密機制之使用範例，並持續強化使用者資安意識，如加密後仍需配搭其他管理作為，以確保資料安全性。

2. 資安專題分享_在自動化與協作支柱中推進零信任成熟度介紹

網路攻擊與威脅無所不在，伴隨著資料存放與系統應用不再拘泥於地端，傳統網路類似護城河之概念已不足以回應相關風險，再加上有部分攻擊案例或趨勢因內部網路與外部攻擊者之界限逐漸模糊，來源可能來自於供應鏈或內部人員，因此不論是國際或台灣，皆積極推動零信任架構，透過動態信任策略逐步完備存取控管與資料保護。

推動零信任架構需訂定一系列持續推動與精進之網路安全策略與方案，絕非一蹴可幾之事，美國政府為推動零信任架構與其安全模型之發展、部署及維運，其中國防部(Department of Defense, DoD)發展零信任策略[5]，將零信任架構之功能再區分為七大功能支柱，以協同提供全面且有效之安全模型。國家安全局(National Security Agency, NSA)陸續針對美國國防部提出之零信任七大支柱，發布一系列網路安全資訊表(Cybersecurity Information Sheet, CSI)[6]，說明各個支柱功能與如何提升成熟度等級之建議。

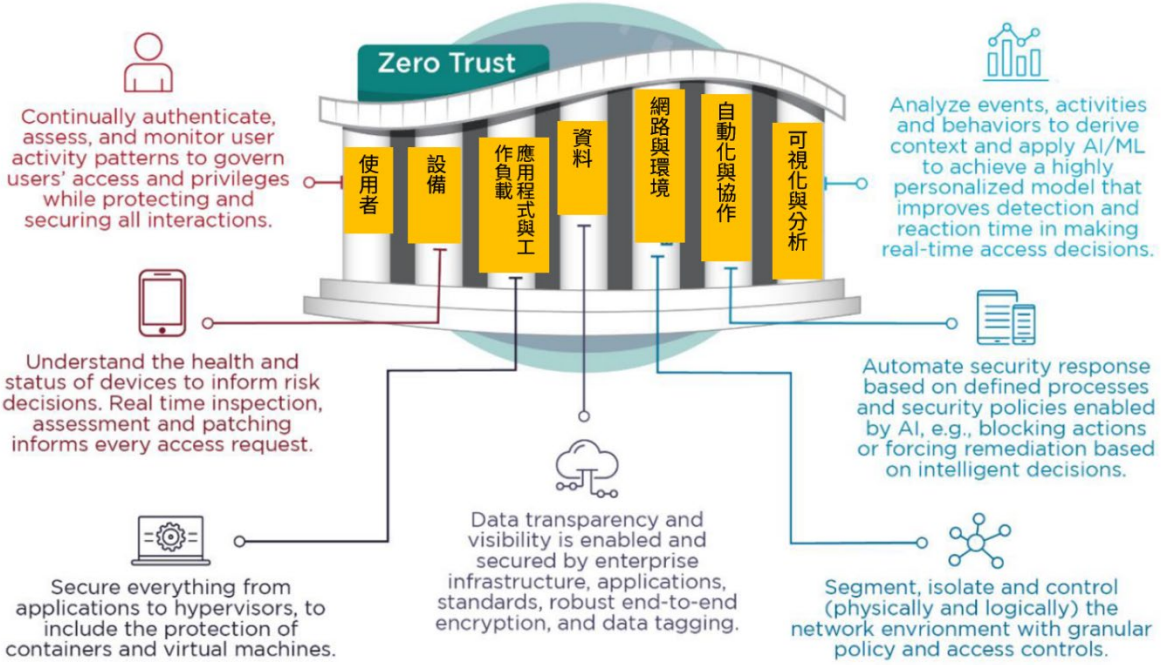
我國目前所推動之零信任架構，主要參考 NIST SP 800-207 零信任架構，採取資源門戶之部署方式(Resource Portal-Based Deployment)，涵括 3 大核心機制，分別為身分鑑別、設備鑑別及信任推斷。後續持續精進機制，規劃參考 NSA 推進零信任成熟度之網路安全資訊表，做為功能驗證與導入指引之參考。以下將概述零信任七大支柱之推進成熟度重點，並針對在自動化與協作支柱中推進零信任之不同成熟度進行說明。

[5] https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[6] https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF

2.1 零信任七大功能支柱概述

DoD 所發布之零信任架構七大支柱分別為使用者(User)、設備(Device)、應用程式與工作負載(Application and Workload)、資料(Data)、網路與環境(Network and Environment)、自動化與協作(Automation and Orchestration)及可視化與分析(Visibility and Analytics)，詳見圖 4。



資料來源：DoD

圖4　零信任架構七大支柱

零信任架構七大支柱相關支柱需互相輔助協作，且要求其個別能力得維持一致性，因此若要導入零信任架構，需先了解每一個功能支柱之重點與能力(Capabilities)要求，接續再從其功能柱間之關係發展基準與精進方案。以下依序說明功能柱之重點要求，「使用者」支柱，主要針對使用者持續驗證、存取及監控其活動模式，以管理相關存取權限與特權，並保護所有存取資源之互動行為；「設備」支柱，了解設備之健康與狀態，為風險決策提供資訊，且可即時檢查、評估及修補，以回應每個存取請求；「應用

程式與工作負載」支柱，保護從應用程式至管理程式，包含虛擬機與容器；「資料」支柱，透過組織基礎設施、應用程式、標準程序、健全之端對端加密及資料標記，以強化與保護資料透明度及可見性；「網路與環境」支柱，針對區域、隔離及控制(實體與邏輯)之網路環境，訂定細微分區政策與存取控制；「自動化與協作」，能依據預先定義流程與人工智慧(Artificial Intelligence, AI)安全策略，提供自動回應機制，如根據智慧決策停止操作或強制修復；「可視化與分析」，能分析事件、活動及行為，得出前後關聯並應用 AI/ML(Machine Learning)以實現高度客製化之模型，從而優化檢測收容日誌之準確率與更即時回應存取決策。

NSA 於 112 年 4 月率先推出針對在「使用者」與「資料」支柱推進零信任成熟度之網路安全資訊表，說明各個支柱功能與如何提升成熟度等級之建議。以「使用者」支柱為例，主要依據其他支柱重點關注之應用功能，聚焦在動態風險環境中，訂定管理使用者之存取原則，並關聯其他支柱之資料以提升決策效率，如可關聯「自動化與協作」支柱，運用 AI/ML 工具進行加速自動化與分析，提升相關成熟度，當關聯至「可視化與分析」支柱，則可基於使用者存取相關之資料，分析特定請求之風險。其他支柱，包含「網路與環境」、「資料」及「應用程式與工作負載」，皆會影響與使用者存取相關之憑證授予，同時以風險為基礎之存取控制原則，也取決於所使用之不同設備。

NSA 於同年推出「設備」支柱中推進零信任成熟度之網路安全資訊表，113 年則陸續發表「網路與環境」、「應用程式與工作負載」及「可視化與分析」等推進零信任成熟度之網路安全資訊表，在「自動化與協作」支柱中推進零信任成熟度為最後發表之資訊表。七個功能支柱中雖互為關聯，惟因應監管資訊之複雜且快速擴增與 AI 科技快速應用，「自動化與協作」支柱之成熟度提升將更為迫切，以下將以此表為案例，說明零信任成熟度之能力要求。

2.2 自動化與協作支柱中推進零信任成熟度

「自動化與協作」支柱中推進零信任成熟度之網路安全資訊表，主要在協助組織利用自動化流程，更為精確地偵測網路威脅，且可更即時主動回應常見威脅。除於日常維運提供自動化任務之一致性安全策略，亦可優先將資源集中於制定進階策略、技術及程序等，並調查任何異常情況，同時藉由提供具體之成熟度模型，協助組織逐步提升其安全防護能力，從而於不斷變化之威脅環境中維持網路安全韌性。

自動化與協作支柱包含七個關鍵能力，分別為運用政策決策點(Policy Decision Points)之政策協作、關鍵流程自動化、人工智慧、機器學習、安全協作、自動化與回應、資料交換標準化及安全營運協調與事件應變，關鍵能力，從準備階段開始後，分為基本、中級及進階等 3 級，詳見圖 5。

資料來源：NSA、本報告整理

圖5　零信任自動化與協作成熟度

自動化與協作支柱關鍵能力之不同成熟度要求，詳見表 1。

表1　自動化與協作成熟度要求

等級 / 構面	準備	基本	中級	進階
運用政策決策點之政策協作	使用威脅模型分析方法，盤點既有的存取控制點，包含了解資料流，以及相關控制點所牽涉到的零信任支柱	● 組織建立政策盤點與範圍內之存取與安全政策集 ● 組織開始蒐集並記錄所有現有基於規則之政策，以便在安全堆疊(Security stack)中進行有效之自動化協作	● 組織建立獨立於 PEPs[7]之 PIPs 與 PDPs，以根據既有政策做出資料與服務存取決定後由 PEPs 執行，從 PIPs 納入額外之上下文(Contextual)資訊 ● 將存取政策轉換為 PDP 可使用之標準格式	PDPs、PIPs 與 PEPs 確保對任何身分之所有資源存取請求正確實施動態與細部之資料存取政策
關鍵流程自動化	● 組織識別關鍵流程 ● 使用映射技術(Mapping Techniques)創建流程圖，以更佳了解自動化功能 ● 開始自動化低風險、重複性任務	針對最重要關鍵流程，以簡單明確的規則進行小範圍工作流程自動化	● 組織擴大自動化，採用諸如機器人流程自動化等工具與方法，處理更多關鍵功能中重複性與可預測任務 ● 持續優化已自動化之關鍵流程，包含改善	● 透過協作之工作流程與風險管理流程改善回應時間與能力 ● 自動化提出新流程與改善作為，以確保持續且更有效之結果

[7] PEP: 政策執行點；PIP: 政策資訊點；PDP: 政策決策點

構面 \ 等級	準備	基本	中級	進階
			回應時間與準確度等	
人工智慧	● 組織為網路中之 AI 定義明確目標與使用案例 ● 評估現有 AI 模型資料之準確性、完整性、一致性及相關性	● 根據預先定義之使用案例獲取或開發 AI 工具 ● 測試與評估 AI 模型之性能與準確性 ● 於小範圍內部署 AI 工具，以影響關鍵功能，如風險評估決策與環境分析	● 組織部署分析導向之 AI/ML 工具，並建議自動化與協作調整作為 ● 根據風險容忍度與 AI 風險原則，於整個網路中擴展 AI 工具	● 回應時間與能力透過 AI 協調之工作流程與更大程度之風險管理流程自動化獲得改善 ● 進階 AI 模型自動化實施更多跨 ZT 支柱之 ZT 能力，特別是用於預測、異常偵測，以及建議或在某些情況下協作適切之回應行動
機器學習	組織識別資料來源，並確保資料標記(Data Tags)適當標準化以便機器讀取	● 組織布建資料標記與分類 ML 工具 ● 組織採用 ML 工具執行與強化關鍵功能之執行，如事件應變、異常偵測、用戶基準建立與資料標記	● ML 工具擴展到在整個網路中運作 ● 隨著資料集增加，評估模型性能，以確保準確性、精確度及撤回率 ● 進行超參數(Hyperparameter)調整，以優化模型性能	使用非用於訓練模型的資料進行效能評估，以持續改善模型

等級 構面	準備	基本	中級	進階
		● 組織在擴大部署模型的同時，也設法處理模型偏差的議題		
安全協作、自動化與回應	● 制定日誌記錄與稽核政策，以允許 SOAR[8] 做出決策，並驗證決策與行動已執行 ● 組織獲取 SOAR 工具以滿足其使用案例之需求	● 實施政策與 SOAR 工具 ● 使用從蒐集到事件回應與分類之預定義腳本(Playbook)，以實現初始流程自動化 ● 組織實施安全技術之初始營運能力，協作與自動化政策(例如透過 PEPs 與 PDPs)與規則集以改善安全營運	● 強化 SOAR 工具以改善安全營運、威脅與漏洞管理，以及安全回應，並使用接收之警報資料與閾值警報觸發自動回應與緩解之劇本 ● SOAR 工具從 UEBA[9]解決方案接收資料以創建額外基準值並強化威脅獵捕之腳本	● 測試與改進流程自動化，並加速效能以滿足組織需求 ● 根據所需要實施複雜之決策邏輯，以確定回應行動 ● 將 AI/ML 整合至 SOAR 機制
資料交換標準化	● 組織盤點流程、應用程式、工作負載與系統，特別是當前與預期	● 組織選擇要使用之標準，並將所有 API 建	● 強化文件與格式指引 ● 徵求開發人員對先前所實施與未來方向之回饋	● 組織實施自動監控解決方案，以追蹤 API、協定與格式之效能、錯

[8] SOAR: Security Orchestration, Automation and Response 安全協作、自動化與回應

[9] UEBA: User and Entity Behavior Analytics 使用者與主體行為分析

構面 \ 等級	準備	基本	中級	進階
	之整合點，以更佳地了解標準化之環境 ● 組織研究了解產業所採用之 APIs 與其他標準	立完整目錄與統一格式 ● 根據採用之標準修改或替換不合規之 APIs、資料格式及協定 ● 產品採購包含遵守所選定標準之要求 ● 其他所使用之 API 先於小型專案或資料集中進行標準化測試，檢視是否存在意外衝突	● 擴大標準化實踐到整個資料環境 ● 進行額外功能測試，以確定產品與服務使用 APIs 與其他標準是否按預期運作	誤及使用模式，並偵測異常
安全營運協調與事件應變	● 組織定義安全維運中心(SOC 與/或事件回應團隊之明確範圍與目標 ● 制定初步事件應變計畫 ● 識別適用之政策、資料來源與其他要求 ● 採購解決方案以滿足要求	● 組織定義並建立 SOC，以部署、營運及維護安全監控 ● SIEM 解決方案開始整合資料來源(即端點保護、偵測與回應資料)，並開始初步監控與通報警訊 ● 開始針對回應動作依照需求	● 事件應變計畫已充分制定、測試並定期更新 ● 已識別之資料來源與 SIEM 解決方案完全整合 ● 整合 SOAR 解決方案，以提供基本腳本自動化需要	● SOAR 解決方案提供進階事件應變工作流程自動化，利用威脅情報資料、使用者活動監控、基於 AI 之異常偵測與 UEBA 來確定潛在問題 ● 自動化回應(腳本與工具)利用 ML 與 AI

等級 / 構面	準備	基本	中級	進階
		執行與整合腳本與工作流程	● 識別手動腳本，以進行自動化或停用	● 腳本完全自動化 ● 在決策中利用歷史資料

資料來源：NSA、本報告整理

針對自動化與協作支柱之七個關鍵能力不同成熟度，於該網路安全資訊表提及導入之指導網要重點，首先應關注自動化方法，處理重複性、勞動密集型及所有可預測的任務，針對關鍵功能，如資料豐富化、安全控制與事件應變工作流程，實現跨不同功能柱之能力進行協作，提高效率並減少手動負擔；其次為採用人工智慧與機器學習之進階演算法與分析，執行並強化關鍵功能，如風險與存取決策、環境分析、事件應變、異常偵測、用戶基準建立及資料標記等；最後則為透過安全維運中心協調安全營運與事件應變，利用 AI、ML 及其他自動化工具，以更快速、有效地偵測、回應及緩解威脅。

現行於政府機關推動零信任網路架構以身分鑑別、設備鑑別、信任推斷為 3 大核心，組織導入零信任架構後，針對持續精進架構部分，可先依據 NSA 成熟度等級檢視初始導入時之成熟度等級，設計符合性檢核表，俾了解持續改善方向。同時此 3 大核心架構，身分、設備鑑別及信任推斷，因需蒐集與監控來自於使用者、設備、應用程式及網路環境等大量資訊，將極需 AI、ML 及自動化工具等協作進行分析，以產生可信任與即時回應之存取決策。建議可參考 NSA 在自動化與協作支柱中推進零信任成熟度，因應自動化需求與 AI 科技浪潮，宜先檢視準備與基本階段之功能性符合要求，逐步設定與評估達成中級或進階成熟度之目標。

3.資安技術研析_Polyfill 套件威脅案例分析

本季探討之 Polyfill 套件威脅案例分析，Polyfill.js 為廣受歡迎之開放原始碼程式庫，其自動提供前端 polyfill 服務之平台網域「Polyfill.io」與相關之 GitHub 帳戶，於本(113)年 2 月由中國業者收購後，開始爆發供應鏈攻擊事件。

資安廠商 Sansec 於 6 月下旬率先揭露 Polyfill 套件威脅事件[10]，發現有越來越多網域遭同一攻擊者注入惡意程式，至少已逾十萬個網站受害。而網站遭植入惡意網域 cdn.polyfill.io 之 JavaScript 後，將會被自動連結至運動賽事賭博網站或其他惡意網站。為提升其可信賴度，Polyfill.io 該平台更刻意誤導使用者認為 Polyfill.io 獲得資訊服務供應商 Cloudflare 之認可。Cloudflare 發表迥然不同於 Polyfill.io 之聲明[11]，宣稱，Cloudflare 從未授權其使用相關之名稱或標章，澄清該網站未獲得 Cloudflare 許可，同時要求刪除虛假說明。

Sansec 揭露此事件後，刊載相關報導之 BeepingComputer 新聞平台接連遭不明駭客展開 DDoS 攻擊。資安院觀測到此事件，同時發現有部分政府機關網頁恐已引入可疑域名，因此著手研析此案技術手法並萃取相關 IOC 威脅指標，以下將概述此事件之緣由與威脅手法，以及後續應處方式。

3.1 威脅手法技術研析

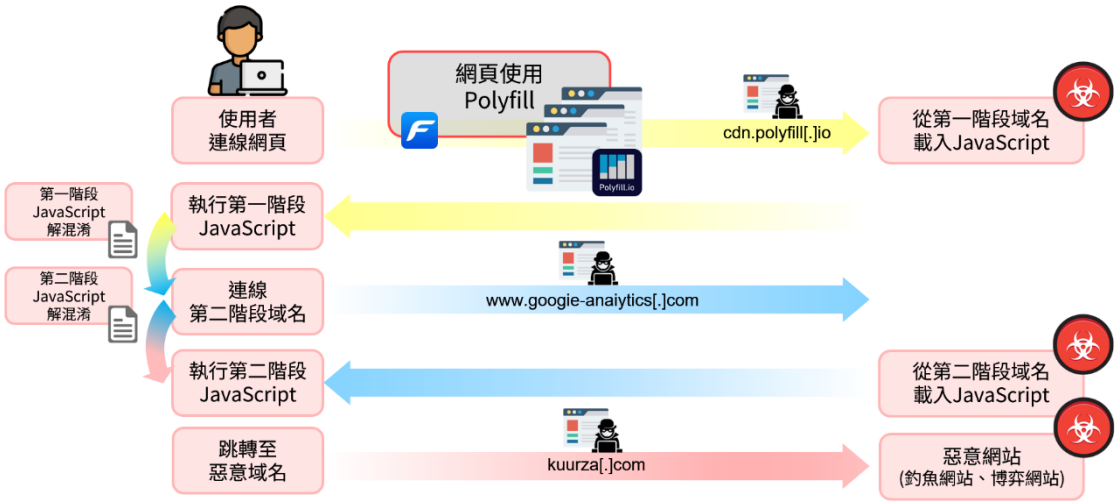
Polyfill 初始由金融時報之網頁團隊所開發，Polyfill.js 使用於舊版之 Web 瀏覽器，若網站採用較新網頁技術，將導致使用者瀏覽過程出現問題，導入 Polyfill JS 套件則可解決相關問題，惟於本年 2 月該網域與帳號出售予

[10] https://sansec.io/research/polyfill-supply-chain-attack

[11] https://blog.cloudflare.com/automatically-replacing-polyfill-io-links-with-cloudflares-mirror-for-a-safer-internet/

給中國內容傳遞網路(Content Delivery Network, CDN)業者方能(Funnull)後，Sansec 於 6 月即提出警訊，其網站功能相容性程式庫 Polyfill.io 傳出被植入惡意程式碼，導致使用該程式庫之網站遭到感染。當受害事件傳出後，網路服務廠商防護，亦紛紛提出緩解措施，如 Google 阻擋相關 Polyfill 域名，並向其廣告商通報此供應鏈攻擊，提及所使用之登入頁面包含惡意程式碼，可能會在網站擁有者不知情或未經允許情況下將使用者重新導向至惡意網站，Cloudflare 改寫相關 Polyfill 域名及網域提供商 Namecheap 則暫停解析 Polyfill 域名。

資安院針對其威脅手法技術進行研析，發現其兩階段入侵手法，第一階段當使用者連線至使用 Polyfill 套件網頁，會連線至第一階段域名下載 JavaScript，接續再連線至第二階段域名，從第二階段域名載入 JavaScript 後，隨即執行第二階段 JavaScript，並跳轉至惡意域名。研析中發現駭客為規避分析偵測機制，會將 JavaScript 程式混淆(Obfuscations)，以降低程式可分析性，因此使用分析工具解混淆(De-obfuscation)，俾分析人員分析程式內容。第一階段 JavaScript 解混淆後，解析出第二階段惡意域名 www.googie-anaiytics[.]com/ga.js，該域名偽裝 Google Analytic 網站分析服務。第二階段 JavaScript 解混淆結果，解析出轉導域名，會將使用者轉導至惡意網站 kuurza[.]com/redirect?from=bitget，經分析惡意網站為釣魚網站與博弈網站，威脅手法分析流程，詳見圖 6。



資料來源：本報告整理

圖6　Polyfill 套件威脅手法分析流程

資安院參考外部情資，彙整方能 CDN 公司所管理之其他可疑域名，整理域名關聯與 Polyfill 域名屬同一管理者，詳見表 2。

表2　惡意域名列表

編號	連線階段	惡意域名	說明
1	第一階段惡意域名	bootcdn[.]net	提供整合多個前端資源庫(Bootstrap、jQuery、Font Awesome)服務
2	第一階段惡意域名	bootcss[.]com	提供 Bootstrap 前端框架服務
3	第一階段惡意域名	staticfile[.]net	提供整合多個前端 Javascript 函式庫(React、Vue、AngularJS 、JQUERY)服務
4	第一階段惡意域名	staticfile[.]org	staticfile[.]net 別名
5	第二階段惡意域名	unionadjs[.]com	使用 bootcss[.]com 服務，連線惡意域名(www[.]unionadjs[.]com)

6	第二階段惡意域名	xhsbpza[.]com	無
7	第二階段惡意域名	macoms[.]la	使用 bootcss[.]com 服務，連線惡意域名(union[.]macoms[.]la)
8	第二階段惡意域名	newcrbpc[.]com	使用 bootcss[.]com 服務， 連線惡意域名(newcrbpc[.]com)

資料來源：本報告整理

3.2 影響範圍與處置方式

整理此事件受害者，其中不乏知名與美國上市公司等網站，如世界經濟論壇、JSTOR 及 Intuit 等平台，且因此複雜之惡意程式採用規避技術，使其檢測與防範具高度挑戰。而彙整國內政府機關受害案例，相關受駭偵測指標包含網站惡意域名、惡意 JavaScript 及惡意程式轉導域名至線上博弈網站等樣態，已即時於 7 月初發布機關警訊，且呼籲應避免使用相關 Polyfill 套件，後續並提供防護建議。建議系統開發或管理者能針對系統之程式碼使用能檢測 Polyfill 套件之原始碼檢測工具，先確認是否存在相關風險。若偵測發現惡意程式已內嵌於 Web 應用程式中，應立即將其移除。

針對此供應鏈攻擊，導致程式開發者已無法再信任 Polyfill.js 檔案，因為惡意程式碼可能已重新部署至 CDN 或是複製至多種外掛程式中。以漏洞編號 CVE-2024-38526 為例，為有關於 Python Package Index (PyPI)註冊表(Registry)上 PDOC 程式庫(Library)之安全性報告，該程式庫主要為 Python 專案提供應用程式介面(Application Programming Interface, API)文件，所提揭露之弱點為如果使用命令(Commend)產生之文件 PDOC-Math，將包含來自 Polyfill.io 之 JavaScript 惡意檔案，對於此項漏洞，建議應儘速更近至 PDOC 版本 14.5.1。

此事件根本解決之道在避免使用相關 Polyfill 套件，若於專案已使用，則

應進行風險與衝擊評估，分析是否仍要 Polyfill 與可能影響範圍，再決定適切之處置方式。同時亦應檢視於系統設計時，若使用第三方套件，則應導入完整性驗證其套件之安全，防止直接引入 CDN 線上服務。

供應鏈攻擊對開源專案之威脅日益增長，特別是在 Web 開發生態系統中，應用程式依賴開源套件之多樣化技術以實現互動式功能。系統開發專案更需評估複雜環境下之供應鏈風險。Sansec 將此案例定調為供應鏈攻擊之典型範例，因此當分析事件根源時，管理者需再次思考供應鏈之定義。供應鏈若只納入有簽約之供應商，則範圍偏狹隘，應先定義供應商之服務種類，如類別為服務、人員、軟體、硬體、韌體及元件類，區分授權與開源等不同來源方式。確實盤點後，接續定期盤點供應商之服務狀況與風險，及早偵測可能之威脅。特別是開源工具或軟體之使用日漸增長，針對網站開發系統需要仰賴開源工具或技術，除導入初期評估其安全性外，更應定期進行檢測，且隨時關注可能之風險來源或訊息。

4. 結論

本季具指標性案例為雙重認證應用程式 Authy 電話號碼遭外洩，引發後續驗證安全與資料外洩危機，藉由寬鬆身分驗證入侵不安全之 API 端點展開，並成功竊取 Authy 雙重認證用戶之個人資料，後續恐遭利用，將引發網路釣魚與簡訊攻擊事件。另一起案例為防毒軟體卡巴斯基於美國被禁用後，未經同意逕行以新防毒軟體取代並安裝於用戶電腦，引起卡巴斯基用戶對資料安全與惡意程式潛藏之風險疑慮。

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，排除綜合類型「其他」外，其次分別為「網頁攻擊」與「阻斷服務」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「多重驗證之資安管理」與「加密機制之資安管理」提出資安防護建議。

資安專題分享主題為在「自動化與協作」支柱中推進零信任成熟度介紹。NSA 針對美國國防部提出之零信任七大支柱，發布此網路安全資訊表說明如何協助組織利用自動化流程，更為精確地偵測網路威脅，且可更即時主動回應常見威脅。

另外，資安技術研析主題為 Polyfill 套件威脅案例分析，此受歡迎之開放原始碼程式庫爆發供應鏈攻擊事件，源自中國業者收購 polyfill 服務之平台網域「Polyfill.io」與相關之 GitHub 帳戶，使用 Polyfill 套件者發現有越來越多網域遭同一攻擊者注入惡意程式，本報告藉由案例提醒管理者評估所有供應鏈之風險。