110年第2季資通安全技術報告

Quarterly Technical Report

目　次

圖 目 次

摘要

「第 2 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 2 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 Python 專案遭挖礦程式滲透；第 2 起案例為俄羅斯駭客集團 Nobelium 透過郵件行銷平台 Constant Contact，發送惡意郵件。

分析政府資安威脅現況，發現政府機關通報事件，以「非法入侵」(占 72.01%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 7%)」與「網頁攻擊(占 2.88%)」為主要通報類型。

●2.資安專題分享

資安專題分享主題為 MITRE 資安攻防知識庫框架介紹 ATT&CK and Shield，Shield 目前涵蓋 8 類戰略與 36 個主動式防禦技術，前 5 大戰略適合所有企業組織進行資安防禦，若欲掌握攻擊者入侵後之 TTP 資訊，則可使用後續 3 大戰略，執行進階主動式防禦。

●3.資安技術研析

資安技術研析主題為 MyKings 殭屍網路中繼站調查，MyKings 為多重型殭屍網路，結合挖礦、木馬後門、漏洞攻擊等模組，做為駭客多種不同用途。MyKings 最早出現於 106 年，利用美國國家安全局被外洩之攻擊程式 EternalBlue 當做跳板工具，成功擴散其攻擊之目標對象。

●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 MITRE 資安攻防知識庫框架，介紹 ATT&CK and Shield，說明所涵蓋之 8 類戰略與 36 個主動式防禦技術。此外，資安技術研析主題為 MyKings 殭屍網路中繼站調查， MyKings 殭屍網路以挖礦為主要用途，駭客透過感染多台裝置非法獲取利益。

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。110 年第 2 季(以下簡稱本季)探討供應鏈安全與如何加強資通系統防護，以避免遭受攻擊致資料外洩。

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

資訊人員在面對資源短缺或是部分在商用軟體獲取功能時，皆有可能使用開源軟體。開源軟體若在原始開發者開放原始碼後，再加上後續使用者集思廣益改寫精進後，功能將會更加完整，因此造就開源軟體應用更為廣泛。反之，若缺乏審視、維護及更新相關管理機制，則將帶來風險加劇之可能性，如使用不明來源之函式庫與缺乏專責維護，系統發生缺陷或資安問題時將出現求助無門窘況。

另一值得探討之議題為近年來社交工程攻擊事件，透過釣魚郵件而來之威脅與日俱增。搭配使用合法平台之相關內容，看似正常之電子郵件，讓受駭者無法在第一時間察覺發現攻擊行為，以即時識別與攔截這類電子郵件之入侵。這類攻擊事件，往往需等待駭客發動橫向攻擊或受駭者資料遭竊，損害已造成時方暴露。

本季具指標性案例為Python 專案遭挖礦程式滲透；另一起案例為俄羅斯駭客集團 Nobelium 透過郵件行銷平台 Constant Contact 發送惡意郵件。

首先，探討案例為資安業者 Sonatype 指出，Python 官方認證之第三方程式庫 Python Package Index(PyPI)，存在多個含有挖礦程式碼之惡意套件，已知 6 個惡意套件皆由同一帳號上傳，名稱分別為「maratlib」、「maratlib1」、「matplatlib-plus」、「mllearnlib」、「mplatlib」及「learninglib」，部分惡

意套件名稱，如「matplatlib-plus」更近似知名合法繪圖軟體 matplotlib，容易讓人混淆，且總下載量已逼近 5,000 次。開發者若執行惡意套件內之程式碼，便會下載並執行挖礦程式 Ubqminer，利用開發者電腦之計算資源挖掘 Ubiq 加密貨幣，並轉帳予攻擊者。此外，亦發現另一變種程式使用相似之攻擊原理與手法，惟改用開源挖礦程式 T-Rex，透過開發者電腦之圖形處理器(Graphics Processing Unit, GPU)提升挖礦運算速度。資安業者 Sonatype 認為，針對開源開發工具之攻擊行動，近年有逐漸增加之趨勢，除此次受駭之 PyPI 外，尚有套件管理工具 NPM(Node Package Manager)，顯示開發者已逐漸成為駭客入侵之目標，而受駭者除開發者本身，亦包含透過惡意程式碼開發之產品，有危害軟體供應鏈安全之風險。

第 2 起案例為俄羅斯駭客集團 Nobelium 透過郵件行銷平台 Constant Contact，發送惡意郵件。微軟於 110 年 5 月 27 日表示，主導 SolarWinds 供應鏈攻擊行動之俄羅斯駭客組織 Nobelium(又名 APT29、UNC2452 或 Cozy Bear)，鎖定政府機關、研究機構、非政府組織及國際組織，發起新一波攻擊行動。

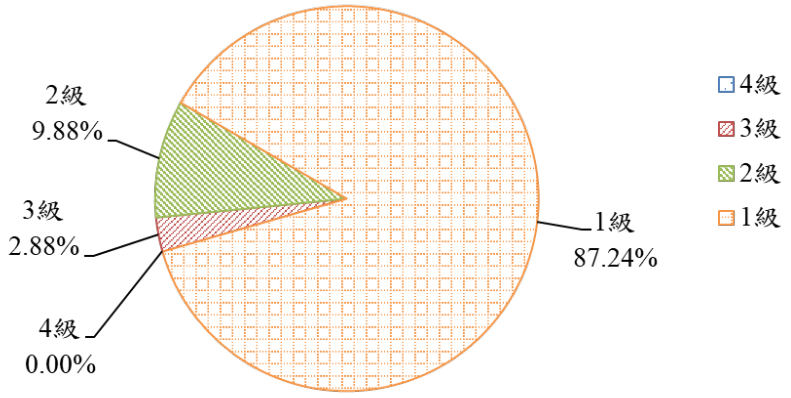
Constant Contact 為美國線上行銷業者，主要服務為寄送行銷電子郵件。該駭客組織藉由獲取美國國際開發總署(United States Agency for International Development, USAID)所使用之 Constant Contact 帳號，再寄送惡意釣魚郵件予全球 24 個國家，逾 150 個組織之 3,000 個電子郵件帳號。郵件內容嵌入惡意連結，受駭者先被引導致合法 Constant Contact 服務網頁，再跳至駭客掌握之網頁，接續將惡意程式植入受駭系統，使駭客可常駐於受駭系統中，以利後續進行橫向移動或竊取資訊等惡意行為。微軟指出，依據該駭客組織過往行動模式，其一貫之攻擊策略為入侵供應商，再進一步攻擊供應商之客戶。

綜覽本季重大資安事件，系統開發人員無論是使用商用軟體或開源軟體，在專案初始時，就應建立預設安全(security by default)機制，檢視所採用開發軟體之安全。另外，社交工程攻擊手法不斷推陳出新，如何就防守位置，明

確辨識可能風險，讓資安意識成為內部文化，謹慎應對創新且複雜之資通應用環境。

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」等 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 87.24%為大宗，2 級事件占 9.88%次之，3 級事件僅占 2.88%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

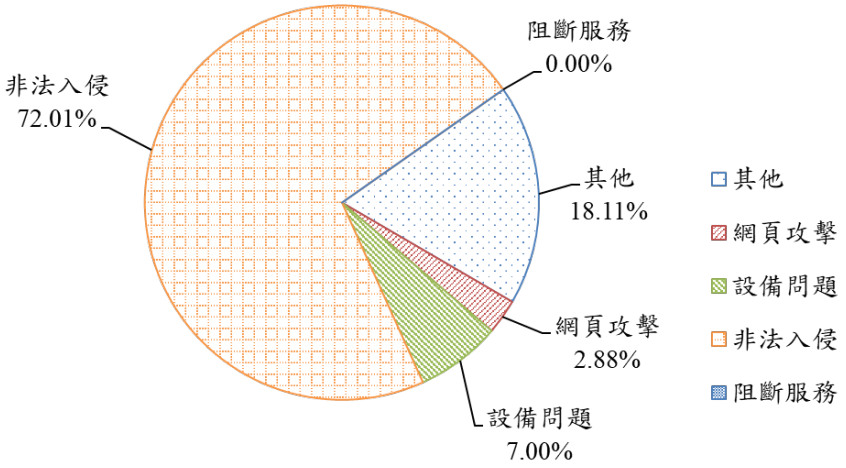


資料來源：本報告整理

圖1　110 年第 2 季通報事件影響等級比率圖

本季接獲之 3 級重要通報事件，以個人資料外洩事件居多，包含因活動系統報名設計不當，報名系統存在邏輯疏失問題，未限制登入後僅能查詢該個人資料，導致其他人員部分個資外洩。無獨有偶，另一起個資外洩事件亦因報名系統設計不當，有心人士可透過「忘記密碼」功能，自行輸入外部信箱，系統未經檢查自動將重新設置之帳號密碼發送至該信箱，致有心人士可利用新帳號密碼存取使用者資料。二起事件經調查，皆有資料遭存取狀況，顯示部分個資已有遭外洩之可能性。

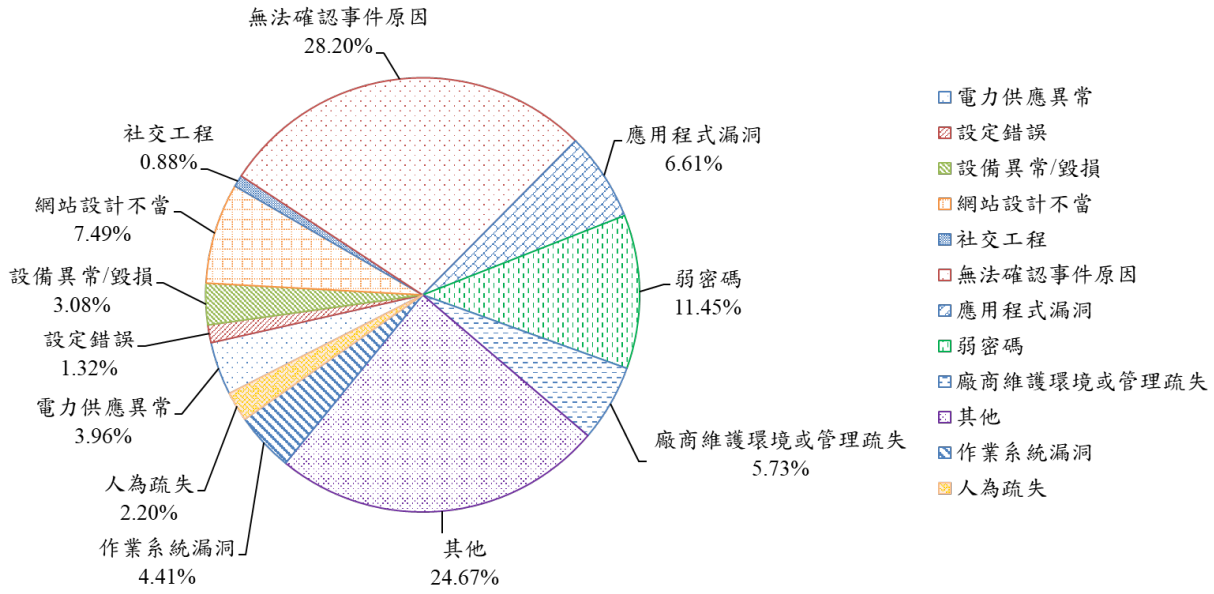
除上述資安事件外，尚接獲通報有網路儲存設備因系統漏洞遭利用，可允許遠端攻擊者對目標設備建立任意檔案至特定路徑下，進而執行任意程式碼後，植入勒索軟體。統計本季通報事件類型，以「非法入侵」(占 72.01%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　110 年第 2 季通報類型比率圖

進一步分析通報事件發生之原因(詳見圖 3)，可確認之事件原因分別為弱密碼(11.45%)、網站設計不當(7.49%)、應用程式漏洞(6.61%)、廠商維護環境或管理疏失(5.73%)、作業系統漏洞(4.41%)、電力供應異常(3.96%)、設備異常/毀損(3.08%)、人為疏失(2.2%)、設定錯誤(1.32%)及社交工程(0.88%)。統計本季事件發生原因，發現「弱密碼」致事件發生率，再度攀升。此外，由本季事件亦可見網站設計不當或應用程式漏洞造成事件發生，都顯示政府機關在系統開發時，不論是自行設計或委外開發，應逐步規劃與加入安全系統發展生命週期之機制。



資料來源：本計畫整理

圖3　110 年第 2 季公務機關資安事件原因比率圖

1.3 資安防護重點

分析本季全球資安威脅現況，開源軟體使用已成為普世價值，隨之而來之風險雖時有所聞，如系統漏洞、維護等議題卻尚未通盤討論。使用開源軟體前應先進行風險評估，規劃應用於非涉及機敏性系統上，隨時關注開源軟體之評價與脆弱點。近來不論是資安事件中常見目標式之釣魚攻擊活動，針對特定產業，以相關標題與內容誘使收件人下載並開啟惡意檔案(如偽冒成 PDF 檔案之圖檔等)，而更見利用合法業者之平台之行銷帳號，再寄送惡意釣魚郵件，更難讓使用者判斷是正常或社交工程郵件。

國內因網站設計不當與應用程式漏洞，如邏輯疏失設計問題或未採取適切之身分驗證，致發生個人資料外洩事件。如何讓系統開發人員在專案初始，安全程式設計概念成為預設之議題，同時在系統開發不同階段規劃源碼檢測、弱點掃描等活動，使系統安全從程式開發延展至整體防護。

綜整以上資安威脅現況，提供資安防護建議如下：

●開源軟體之資安管理

– 檢視開源軟體之評價，了解相關授權模式、軟體更新狀況、漏洞出現及修補更新率等資訊。

– 建立開源軟體資產清冊，包含第三方應用程式，並定期檢視程式安全與漏洞警訊公告。

– 建置內部網路環境之事件警示機制，提升預警與復原管理能量。

●系統開發與資料存取之資安管理

– 系統上線前應執行源碼檢測與弱點掃描，確認未存在邏輯錯誤或系統漏洞。

– 密碼失效或忘記密碼時，應採取雙驗證機制，確認使用者身分。

– 系統資料若涉及敏感性，特別是個人資料，應採部分遮罩或加密機制。

2. 資安專題分享_MITRE 資安攻防知識庫框架介紹 ATT&CK and Shield

MITRE 於 105 年提出 ATT&CK(Adversarial Tactics, Techniques and Common Knowledge)描述攻擊者行為之知識庫框架，讓企業組織與資安產業對於攻擊者能有共同之行為樣態描述，該框架彙整眾多駭侵組織攻擊行為，並建立共通描述語言，涵蓋攻擊前、中、後之入侵戰略、技術及流程(Tactics, Techniques, and Procedures, TTP)，讓企業組織與資安產業都受益，進而知己知彼，以強化資安防護。

MITRE 更於 109 年提出 Shield 用以描述主動式防禦之知識庫框架，使企業組織與資安產業能進一步防護攻擊者行為。該框架參考 ATT&CK 知識庫，提供防護、欺敵及交戰行動之參考準則，讓企業組織與資安產業可依據攻擊者行為，進行偵測、擾亂及阻擋等防護措施，進而制敵機先以完備資安防護方案。

108 年第 2 季內容已針對 ATT&CK 與相關應用案例進行簡介，本章節將說明 ATT&CK 新舊版之差異，並介紹 Shield 主動式防禦知識庫。

2.1 ATT&CK 攻擊者行為知識庫

109 年 10 月發布 ATT&CK Version 8 最新版，主要為完整呈現網際攻擊狙殺鍊(Cyber Kill Chain)，整合原先 PRE-ATT&CK，增加偵查(資訊蒐集)與資源開發(工具開發)，並汰除不夠精確與重複之技術項目。相較於原版本之技術(Technique)涵蓋範圍與執行細節不一致，新增子技術(Sub-technique)項目，可更細緻化描述各式攻擊技術之實行方式，並提供防護建議。更新版本亦公布適用於工控系統之攻擊者行為知識庫(ICS-ATT&CK)，詳見圖 4。

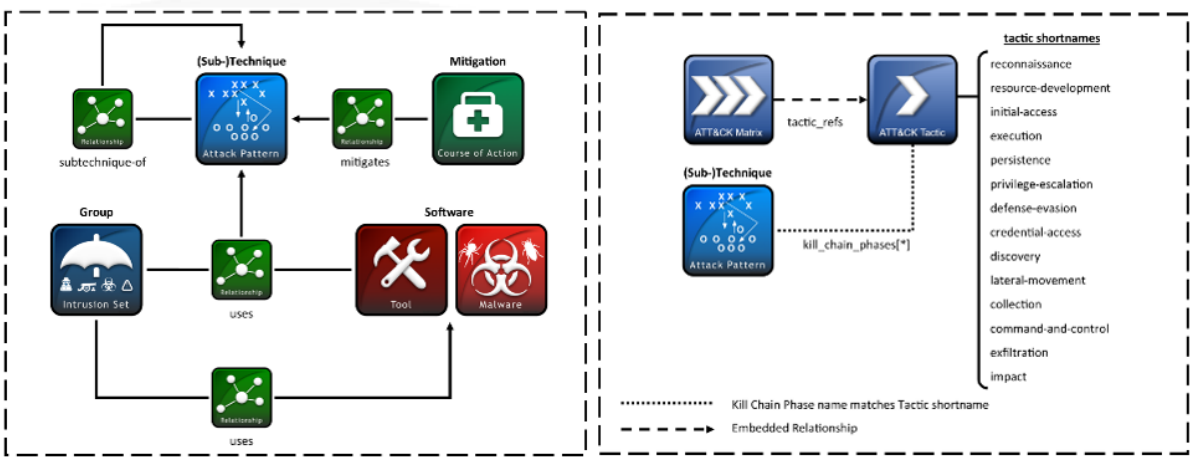
原有ATT&CK Matrix	現有ATT&CK Matrix
Enterprise-ATT&CK	Enterprise-ATT&CK
PRE-ATT&CK	ICS-ATT&CK
Mobile-ATT&CK	Mobile-ATT&CK

資料來源：本報告整理

圖4　ATT&CK 更新比較圖

Enterprise-ATT&CK，主要為對應狙殺鍊之攻擊者行為知識庫，包含 13 類戰略與 1 類影響(Impact)；ICS-ATT&CK 為適用於工控系統之攻擊者行為知識庫，包含 10 類戰略與 1 類影響；Mobile-ATT&CK 則適用於行動裝置之攻擊者行為知識庫，包含 11 類戰略與 3 類影響。

V8 版本引入子技術(Sub-techniques)，針對日新月異之攻擊技術，加入具體執行方式，如入侵初期(Initial Access)戰略中釣魚郵件(Phishing)技術，即包含惡意連結、惡意附檔及第三方郵件服務等 3 種執行子技術，3 種不同子技術所建議之緩解措施(Mitigation)亦有所不同。緩解措施相較先前版本亦有所新增，目前每項技術與子技術皆有相關緩解措施。以釣魚郵件為例，可透過防毒軟體與入侵防禦系統發現惡意程式；限制網頁郵件內容避免惡意連結觸發；實施員工教育訓練，以及早發現惡意郵件等方案。另外，ATT&CK 關聯模型相容於 STIX Attack Pattern，並可透過 kill_chain_phase 對應相關攻擊情資，詳見圖 5。



資料來源：https://github.com/mitre/cti

圖5　ATT&CK 關聯模型對應 Kill Chain Phase

2.2 主動式防禦知識庫

面對詭譎多變之駭客攻擊，以往被動式之資安防護策略已明顯捉襟見肘，因此主動式防禦防護策略逐漸成為顯學。美國國防部曾定義主動式防禦(Active Defense)為「採取受限之進攻性行動與反擊以拒止敵對入侵」。Shield 框架由 MITRE 交戰小組(Engagement Team)於 108 年建立，並於 109 年 8 月發布，目的為改善作戰計畫，協助防禦方於資安攻擊事件中，主動取得攻擊者 TTP 資訊，框架分為基本之網路防護能力(General Cyber Defense)、網路欺敵(Cyber Deception)及與攻擊對手之交戰行動(Adversary Engagement)等 3 大構面。Shield 目前涵蓋 8 類戰略與 36 個主動式防禦技術，前 5 大戰略適合所有企業組織進行資安防禦，若欲掌握攻擊者入侵後之 TTP 資訊，則可使用後續 3 大戰略，執行進階主動式防禦，詳見圖 6。

戰略		說明
引導	Channel	將攻擊者引導至特定路徑，增加成功攻擊所需之時間成本有助防禦者取得攻擊者資訊
蒐集	Collect	蒐集攻擊者TTP情資，可供其他防禦機制參考
限制	Contain	限制攻擊者進入不可控環境，如阻止攻擊者橫向移動
偵測	Detect	針對攻擊者行為，透過偵測機制進行警示通知
破壞	Disrupt	破壞攻擊者行為，使其無法成功攻擊
促進	Facilitate	促進攻擊者執行其部分或全部攻擊行為，有助防禦者取得攻擊者TTP情資
擬真	Legitimize	增加欺敵技術之真實性，如於假環境中，創建真實帳號使攻擊者認為此環境為真實使用環境
測試	Test	釋出假訊息或系統，測試是否引起攻擊者興趣，並透過取得系統控制權之難易度，測試攻擊者能力

資料來源：本報告整理

圖6　Shield 8 大類戰略

為達有效之主動式防禦，Shield 於攻擊行動中提供執行策略之運用機會(Opportunity)，並以使用場景(Use Case)展示具體執行方式。以使用者訓練(User Training)為例，透過訓練使用者識別異常行為與反釣魚郵件技術等方式，提升使用者資安意識，將有助於發現資安威脅。

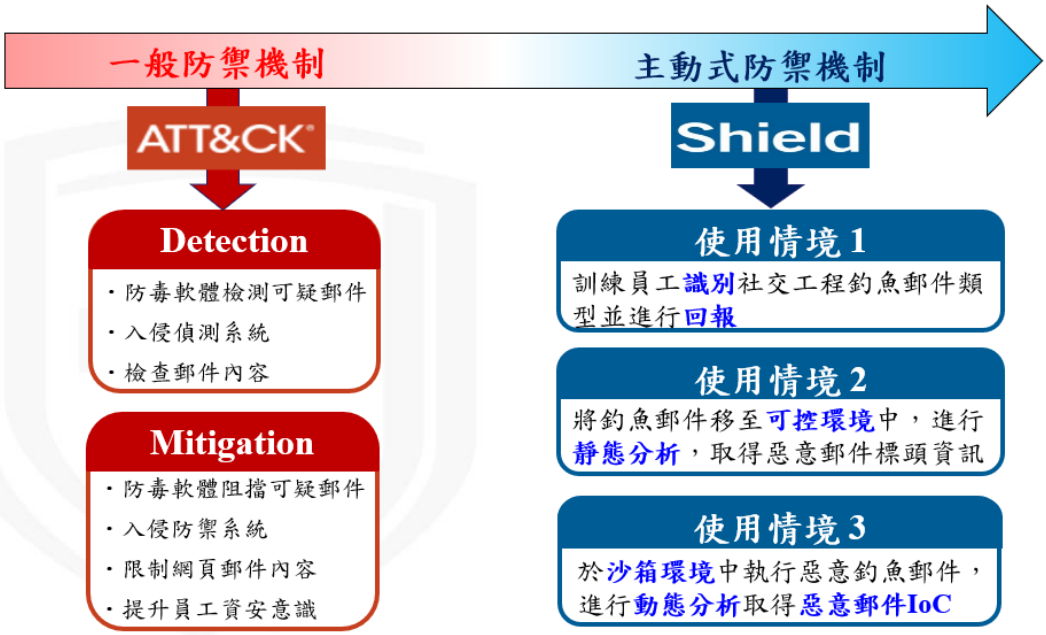
MITRE 提供 ATT&CK 攻擊技術與 Shield 防禦技術對照，防護端可針對所關注之攻擊技術，制定主動式防禦策略。以釣魚郵件為例，分析威脅情境中之機會，為避免惡意電子郵件直接寄送至使用者信箱，可運用防禦策略或技術，如電子郵件管理、過濾郵件等，成功攔截或提醒惡意郵件，詳見圖 7。

ATT&CK Tech.	Opportunity	Shield Tech.	Use Case
T1534 – Internal Spearphishing	透過識別異常行為，有助於發現資安威脅	DTE0035 – User Training	教育訓練使用者判別寄件夾中是否存在未知之寄送郵件
T1566 – Phishing	檢測郵件，避免其直接寄達目標收件者	DTE0019 – Email Manipulation	防護端可攔截遭偵測機制判別為惡意之郵件，避免成功寄達目標收件者
	將可疑郵件移置可控環境或欺敵帳號中，進行讀取與執行	DTE0023 – Migrate Attack Vector	將可疑郵件於確實執行前移至可控環境中讀取檢視
	透過提升使用者資安意識與回報機制，有助於發現防禦機制未能偵測之郵件	DTE0035 – User Training	提升使用者反釣魚郵件技術，以偵測釣魚郵件攻擊
	藉由釣魚郵件，掌握企業組織主要攻擊目標	DTE0015 – Decoy Persona	防禦者提供假資訊，測試攻擊者是否於攻擊行動中使用

資料來源：本報告整理

圖7　以釣魚郵件為例之 ATT&CK 使用場景

若再進階整合 ATT&CK 與 Shield 主動式防禦策略，藉由 ATT&CK 攻擊者行為知識庫，提供一般防禦機制，包含偵測與緩減技術方案，再加上 Shield 主動式防禦機制，分別從不同使用情境辨識相關風險、機會及設計防護方案，詳見圖 8。



資料來源：本報告整理

圖8　ATT&CK 與 Shield 防禦整合運作機制

MITRE 繼提出 ATT&CK 攻擊者行為知識庫，再提出 Shield 主動式防禦知識庫，系統性歸納主動式防禦之各種戰略技術。對於過往單純防守之局面，主動式防禦將可提供「欺敵、觀察及互動」之策略與執行方式。機關可參考其內容加強主動式防禦能量，改變攻防不對等之問題，提升欺敵技術，進而觀察並預測駭客之攻擊行動，設計適切之防護方案。

3.資安技術研析_ MyKings 殭屍網路中繼站調查

本季探討之資安技術研析為 MyKings 殭屍網路中繼站調查，MyKings 為多重型殭屍網路，結合挖礦、木馬後門、漏洞攻擊等模組，做為駭客多種不同用途。MyKings 最早出現於 106 年，利用美國國家安全局被外洩之攻擊程式 EternalBlue 當作跳板工具，成功擴散其攻擊之目標對象。

近期 MyKings 殭屍網路以挖礦為主要用途，駭客透過感染多台裝置非法獲取利益。根據資安公司 SophosLabs 研究報告發現，MyKings 所進行之一系列攻擊包含 MySQL、MSSQL、telnet、ssh、遠端桌面協定，甚至是 CCTV 監視設備等，入侵路徑主要是利用這些系統設定之脆弱使用者名稱與密碼，接續尚會利用 EternalBlue，展開擴散攻擊。報告指出，此殭屍網路背後之操控者偏好運用開源或共享軟體並進行客製化，以加強攻擊力道。

3.1 情蒐分析與研究調查流程

技服中心接獲資安情資，台灣境內出現惡意下載站樣本活動，隨即與調查機關合作前往受駭單位進行現地調研，藉由架設側錄設備，蒐集主機資料，進而分析該資料與網路流量。

調查之受駭主機主要提供下游廠商下訂單使用，同時做為 FTP 與 Email 伺服器用途，初步發現所使用之作業系統，原廠已停止更新支援，所幸該主機直連 ISP 業者之數據機，未與內部網路相連。經分析該主機資料後，發現確有符合受駭情資之後門連線域名。

為進一步了解主機感染情況，透過硬碟 MFT(Master File Table)紀錄之檔案時間，嘗試尋找存在之可疑檔案，經分析發現，該主機早於 106 年已陸續被植入多個惡意程式。分析後確認與情資連線特徵相符之惡意程式共 3 個，1 個常駐服務執行，其餘 2 個目前已無明顯活動軌跡，無明顯活動之其中 1 個樣本已遭防毒軟體移置隔離區。

仍有執行活動之惡意程式為/WINDOWS/system32/inetsrv/dllhost.exe，該惡意程式建立系統服務"WmiApSrus"常駐執行。嘗試連線目標主機已無回應，無法得知回應之連線行為細節，詳見圖 9。

資料來源：本報告整理

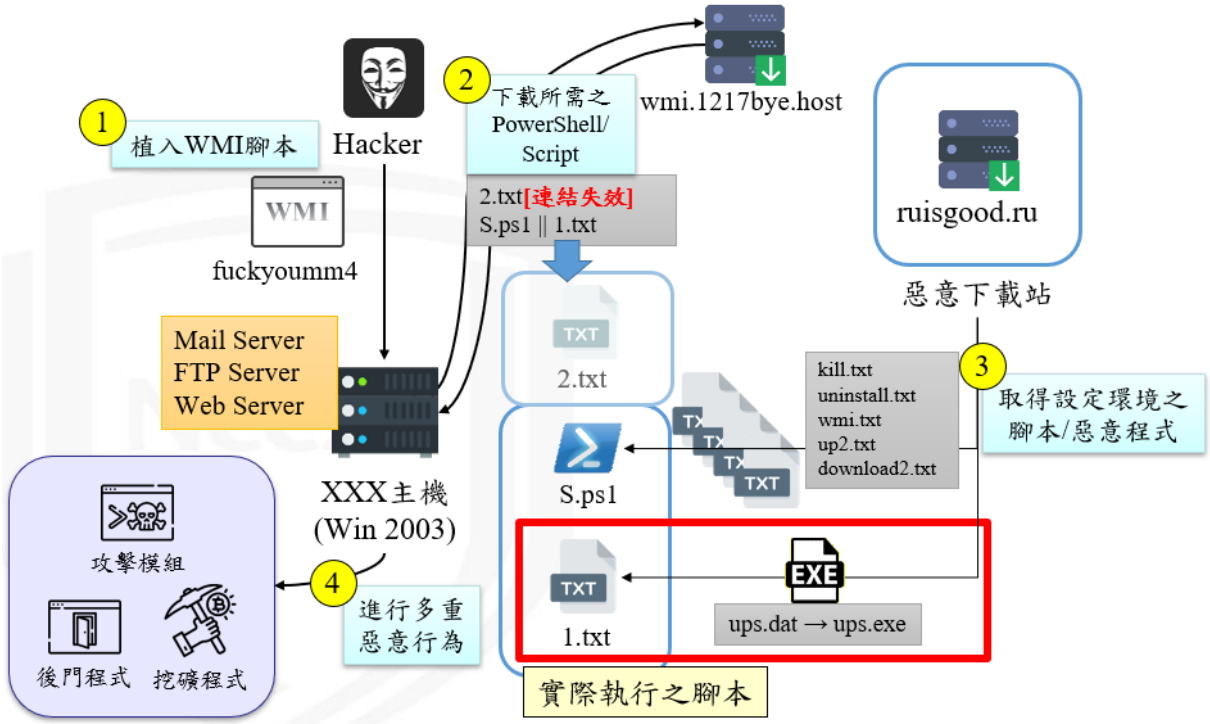
圖9　與情資符合且仍有執行活動之惡意程式

分析主機攻擊活動時間軸，遭 MyKings 殭屍網路入侵成功後，殭屍網路持續活躍至今，共計有 9 波惡意程式相關活動。第 1 波攻擊成功植入 MyKings 程式工作排程，接續第 2 波活動下載後門程式，第 3 波活動更新程式模組，第 4 波活動植入 EternalBlue 攻擊模組與門羅幣挖礦程式，第 5 波活動植入 Bootkit，第 6 波活動更新與植入門羅幣挖礦程式，第 7 波活動則更新 MyKings 程式工作排程，包含持續潛伏工具、EternalBlue 攻擊程式及 PCShare 後門程式，第 8 波活動為更新惡意程式 EternalBlue 攻擊程式與 Bootkit，第 9 波活動為植入後門程式 dllhost.exe，並至惡意中斷站報到。

3.2 MyKings 感染流程與活動軌跡

MyKings 殭屍網路利用 WMI(Windows Management Instrumentation)腳本做為入侵起點，WMI 為 Windows 管理規範，提供系統管理員使用 Script 進行本機或遠端管理主機，由於 WMI 之強大功能，經常被做為駭客攻擊手法之一，並可搭配 PowerShell 執行惡意指令與系統操控。此外，惡意程式碼可

在無需儲存到檔案系統情況下進行安裝與執行，屬於無檔案攻擊型，若應用程式被限制執行環境，仍可於作業系統進行互動。因其無檔案攻擊型特性，將成功降低被防毒軟體與資安機制偵測機會，提升資安人員鑑識分析之難度，MyKings 感染流程，詳見圖 10。

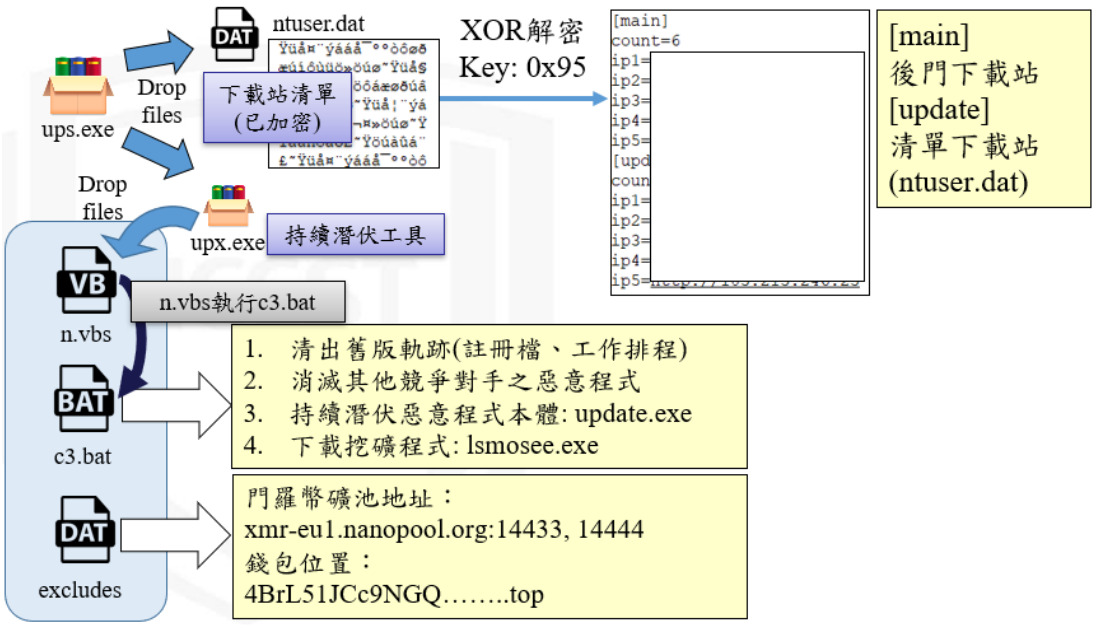


資料來源：本報告整理

圖10 MyKings 感染流程

主機開機啟動配置遭植入惡意 WMI 腳本，並以此腳本連結至 MyKings 殭屍網路之惡意腳本下載站，目標域名為 wmi.1217bye.host。受駭主機每 3 小時檢查下載站腳本更新，實際存取下載站僅有 regsvr32 註冊登錄之 URL(http://wmi.1217bye.host:8888/1.txt)，其中 1.txt 目的為植入持續潛伏工具 ups.exe。

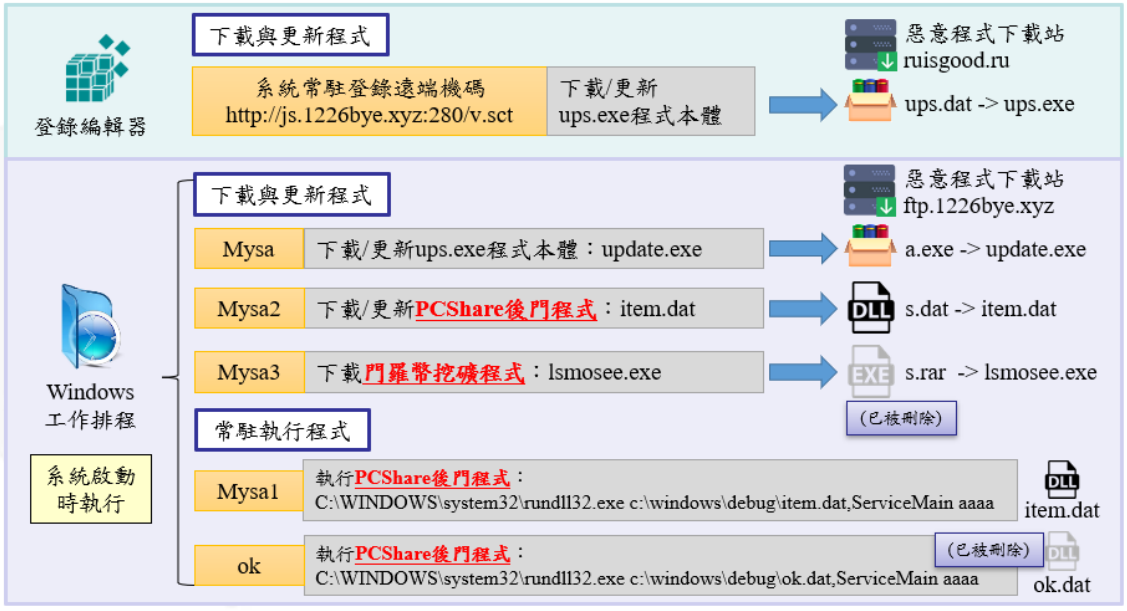
ups.exe 為自解壓縮檔案，包含 ntuser.dat 與 upx.exe，主要功能為進行持續潛伏與惡意程式環境設定，其中 upx.exe 包含 n.vbs、c3.bat 及 excludes 檔案，詳見圖 11。



資料來源：本報告整理

圖11 惡意程式 ups.exe 檔案分析

攻擊者利用 c3.bat 惡意腳本，登錄系統機碼與建立工作排程，以達到持續性潛伏目標主機之目的，詳見圖 12。



資料來源：本報告整理

圖12 執行惡意程式

MyKings 透過持續潛伏工具所建立之工作排程，取得 PCShare 後門程式 item.dat。PCShare 為開源後門程式，可對電腦做監控與控制，其功能包含檔案管理、資料傳輸、系統控制、硬體控制及硬體資訊擷取，並可於 Github 獲取原始碼。透過鑑識 MFT 紀錄與配合沙箱動態分析，確認 PCShare 後門程式 item.dat 亦可由下載後門模組 upsupx.exe 取得，以維持其持續性。下載後門模組主要依據 down.txt 之下載清單，下載所需惡意程式，包含 PCShare 後門程式 item.dat、權限提升工具 down.exe 及持續潛伏工具 msiefsaa.exe。

分析惡意 WMI 攻擊腳本，曾利用 PowerShell 下載開機型病毒(bootkit) max.rar。max.rar 為開機時執行之惡意程式碼，程式執行後會產生之 Binary 檔，內容包含防毒軟體執行檔名稱列表，用於終止防毒軟體執行程序，並會被複製到主開機紀錄(Master Boot Record, MBR)磁區。此外，調研另發現攻擊套件下載程式 msinfo.exe，其功能除為下載與更新 EternalBlue 攻擊套件，進行擴散感染外，亦具有掃描網路功能。除已知之 MyKings 惡意程式外，發現主機上感染其他多個非典型 MyKings 惡意程式，依據 MFT 時間線推測，其餘非典型 MyKings 惡意程式可能透過 PCShare 後門程式植入。

此次調研發現受駭主機使用已停止支援之 Windows 2003 作業系統，本身漏洞無法修補且易遭受入侵。後續改善方案除應儘速更新作業系統外，並再次檢視 WMI 使用需求，若無需求則應停用，或依實際需求限制授權之管理者使用 WMI，降低 WMI 攻擊風險。同時，美國國安局遭外洩之攻擊程式 EternalBlue，目前仍被駭客廣泛使用，EternalBlue 已於 106 年發布修補程式，亦應定期檢視是否已更新。鑒於部分 MyKings 下載站仍處於存活狀態，本案之入侵指標(Indicator of Compromise, IoC)已分享至資安情資，提供相關單位進行阻擋與清除，所蒐集之惡意程式 IoC 亦已納入技服中心主動防禦偵測，以持續關注國內 GSN 殭屍網路活動情形。

4. 結論

本季具指標性案例為探討Python 專案遭挖礦程式滲透，Python 官方認證之第三方程式庫 Python Package Index(PyPI)，存在多個含有挖礦程式碼之惡意套件。部分惡意套件名稱，使用近似知名合法繪圖軟體之名稱，讓人混淆且下載。開發者一旦執行惡意套件內之程式碼，便會下載並執行挖礦程式 Ubqminer，利用開發者電腦之計算資源挖掘 Ubiq 加密貨幣，並轉帳予攻擊者。第 2 起案例為美國線上行銷業者 Constant Contact，遭利用寄送惡意釣魚郵件，受駭範圍包含全球 24 個國家，逾 150 個組織之 3,000 個電子郵件帳號。分析該駭客組織過往行動模式，其一貫之攻擊策略為入侵供應商，再進一步攻擊供應商之客戶。

國內部分，分析政府資安威脅現況，發現政府機關通報事件類型，以「非法入侵」為主，綜合類型「其他」次之，接續分別為「設備問題」與「網頁攻擊」。針對本季全球與政府所面臨之主要資安威脅，本報告就「開源軟體之資安管理」與「系統開發與資料存取之資安管理」，提出資安防護建議。

資安專題分享主題為 MITRE 於 109 年所提出之知識庫框架 Shield，用以描述主動式防禦，使企業組織與資安產業能進一步防護攻擊者行為。該框架參考 ATT&CK 知識庫，提供防護、欺敵及交戰行動之參考準則，讓企業組織與資安產業可依據攻擊者行為，進行偵測、擾亂及阻擋等防護措施，進而制敵機先以完備資安防護方案。

另外，資安技術研析主題為 MyKings 殭屍網路，主要以挖礦為主，駭客透過感染多台裝置非法獲取利益。MyKings 利用這些系統設定之脆弱使用者名稱與密碼，接續利用 EternalBlue，展開擴散攻擊。此殭屍網路背後之操控者偏好運用開源或共享軟體並進行客製化，以加強攻擊力道。

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：

◆ 中央及地方政府資通安全長暨行政院國家資通安全會報委員會議

110 年度中央及地方政府資通安全長暨行政院國家資通安全會報第 37 次委員會議(擴大會議)於 5 月 5 日假南港展覽館 2 館辦理，會議除對參與資安會報網路攻防演練及資安稽核表現績優之機關頒發獎座及表達肯定之意外，另針對「政府機關資安強化執行情形」進行主題報告與討論，透過各機關於資安強化之實務經驗分享，使與會人員對資安防護有更進階之認識與技術交流。

會議亦安排「國內外資安現況與政府機關資安防護強化重點」等議題討論，以產業界觀點與各界代表就如何提升政府機關資安防護等議題進行意見交流，議題包含部分未完成重大弱點修補、資安事件通報逾時等討論修補、通報及改善方案。對於 110 年重點資安工作檢查表，亦於會議中請各機關落實及推動重點資安防護項目，並確實發揮機關與所屬機關之聯防效果。