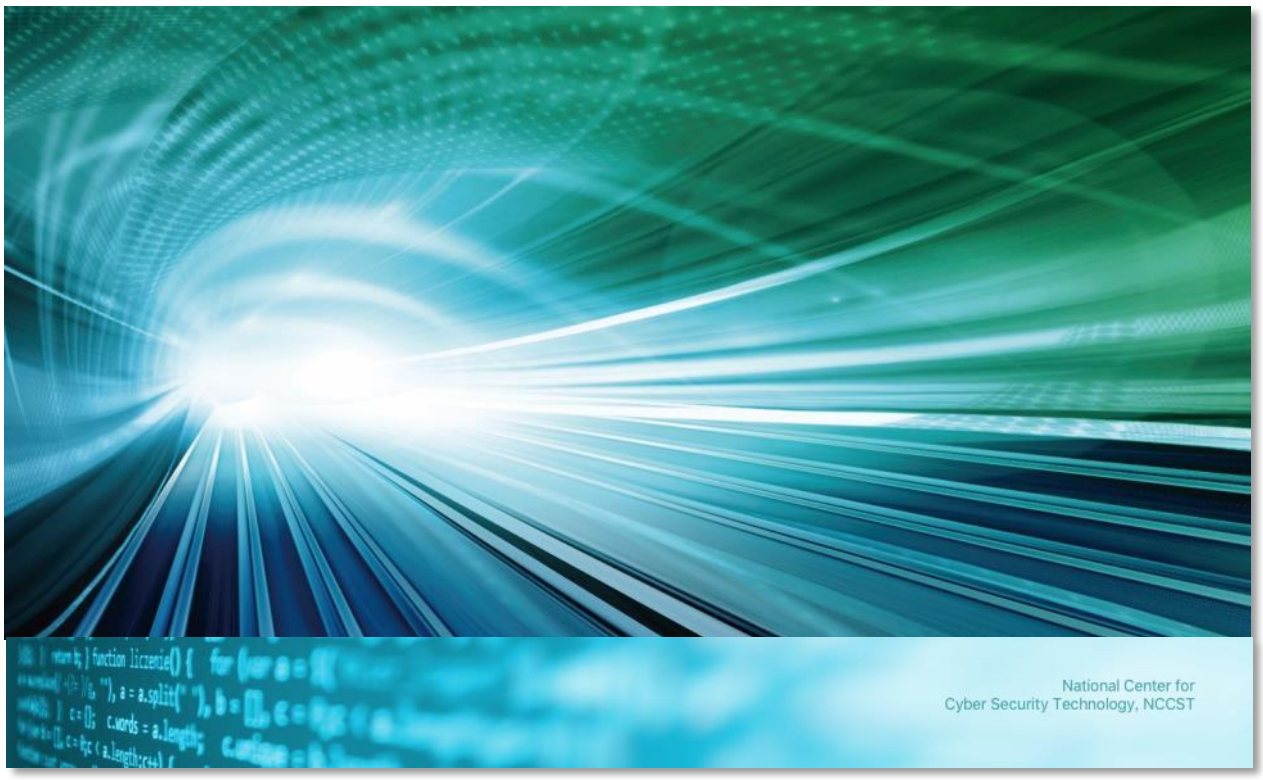
108年第1季資通安全技術報告

Quarterly Technical Report



目　次

圖 目 次

摘要

「第 1 季資通安全技術報告」除分析本季全球資安威脅、政府通報之資安事件外，並提供相對應之防護建議。同時，藉由資安專題之分享與資安技術之研析，提供政府機關(構)於資安風險的關注重點。

「第 1 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 起案例探討多個美國聯邦政府網站的網域名稱服務(Domain Name Services, DNS)系統遭到駭客挾持。第 2 起案例為新的 Mirai 變種，針對商務型物聯網設備展開新一波攻擊。第 3 起案例為國內科技大廠更新主機遭駭事件。

分析政府資安威脅現況，發現政府機關(構)通報事件原因以「非法入侵」(占 50.75%)類型為主，「網頁攻擊」(占 22.39%)次之。

●2.資安專題分享

物聯網的應用廣泛，不管是在日常生活應用，包括在辦公室環境的各種物聯網應用，都已進入百家爭鳴的時代。物聯網相關資訊設備為何更輕易被駭客鎖定的原因之一，也是因為大家所關注的焦點仍在伺服器、作業平台的防護上，殊不知隨著物聯網便利的連網特性與廣泛使用，已成為駭客首選的入侵路徑。因此因應駭客利用物聯網多面向的攻擊，必須正視跟隨著物聯網便利而來的資安危機。

●3.資安技術研析

由資安研究人員整理之資安技術研析，本季主題為基於網頁漏洞之攻擊技術研析。技服中心發現網頁攻擊利用 JuicyPotato 做為提權工具，此為新型態的攻擊手法，主要是利用系統 Kernel 層 COM 元件進行資料傳遞時的缺

陷，以中間人攻擊方式取得高權限 Token 進行提權。

●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，了解最新資安威脅現況與因應之防護重點。同時，資安專題分享物聯網的應用與威脅。此外，透過資安技術的研析，深入探討基於網頁漏洞之攻擊技術。在掌握本季之資安威脅現況時，亦說明下一季之資安專題重點，將探討與說明 5G 與新興網路資安議題。

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。目前駭客運用多種攻擊手法，包括利用社交工程、資通系統漏洞挖掘等，多方刺探資通系統防護上之弱點，同時隨著進階持續威脅(Advanced Persistent Threat，以下簡稱 APT)攻擊的盛行，受駭組織發現遭入侵時，通常已有一定之災情，因此如何能通盤了解內部防禦之完備或洞窺新興攻擊手法，將是組織一大挑戰。本章節的事件與議題皆配合整理相關之防護重點，提供組織就相關資安風險或議題進行評估，並依循防護重點進行強化。

1.1 全球資安威脅現況

研析全球網路攻擊事件可歸納出 6 大面向之全球資安威脅趨勢，分別為「進階持續威脅攻擊竊取機密資料」、「分散式阻斷服務攻擊癱瘓網路運作」、「物聯網設備資安弱點威脅升高」、「關鍵資訊基礎設施資安風險倍增」、「網路與經濟罪犯影響電子商務與金融運作」及「資安(訊)供應商持續遭駭破壞供應鏈安全」。除上述這些廣為人知的資安威脅外，包括駭客利用社群網站、雲端儲存點的資料外洩、憑證外洩及網站伺服器漏洞等問題，都是今年在相關資安威脅預測榜上有名且已真實發生的案例。面對這些不同面向的攻擊議題，如何確保防禦策略的完備度，且能從橫向縱深角度提升資安防護能量，是持續觀注全球威脅現況主要用意。

第 1 季(以下簡稱本季)具指標性的案例為多個美國聯邦政府網站的網域名稱服務(Domain Name Services，以下簡稱 DNS)系統遭到駭客挾持；另一起案例為新的 Mirai 變種，針對商務型物聯網設備展開新一波攻擊。

首先，探討案例為美國國土安全部(Department of Homeland Security，以下簡稱 DHS)在 1 月 22 日發出緊急指令(Emergency Directive)，表示有多個美國聯邦政府網站的 DNS 系統遭到駭客挾持，要求所有.gov 的美國聯邦政府

網站在 10 個工作天內採取防禦行動。DHS 表示，所屬的網路安全及基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)正在追蹤一系列有關 DNS 基礎設施遭到竄改的事件，駭客利用破壞使用者憑證，或是藉由其它方法取得憑證後，再竄改 DNS 的各種紀錄，包括地址、郵件交換器或名稱伺服器紀錄等，將他們置換成駭客所掌控的位址。因此駭客得以先將使用者流量變更至其所控制的架構，再轉回合法服務，由於駭客可設定 DNS 紀錄，因此能獲得聯邦政府網站網域名稱的加密憑證，也能解密流量，取得使用者所提交的任何資料，而且難以被追蹤發現。

第 2 起案例為 Palo Alto Networks 的研究單位 Unit 42 於 108 年初發現 11 隻新的 Mirai 變種，與先前版本不同之處，這些變種並非於消費型物聯網裝置上發現，其中一隻攻擊 WePresent WiPG-1000 無線投影系統的 WePresent WiPG-1000 Command Injection 漏洞，另一隻則攻擊 LG Supersign TV 智慧電視的 CVE-2018-17173。這 2 款都是商務型聯網設備，顯示駭客可能將目標轉向企業網路，藉以取得更大頻寬建立殭屍網路，方便日後發動分散式阻斷服務(Distributed denial-of-service，以下簡稱 DDoS)攻擊。

這已不是 Mirai 首度攻擊企業網路，107 年 9 月 Mirai 也攻擊 Apache Struts 及 SonicaWall 網路設備漏洞，前者導致美國第三大消費者信用管理公司 Equifax 伺服器重大資料外洩。Unit 42 發現這批 Mirai 變種從代管在哥倫比亞的一個受駭網站下載惡意程式，他們也在其中發現用於暴力破解連網裝置的預設帳密檔案。

第 3 起為國內科技大廠發生之更新主機遭駭案例，資安業者卡巴斯基發現國內科技大廠因更新主機遭駭，讓更新主機在協助用戶電腦更新系統軟體時，卻也無意中安裝包含惡意後門的更新程式，卡巴斯基將此複雜的供應鏈攻擊命名為「ShadowHammer」。

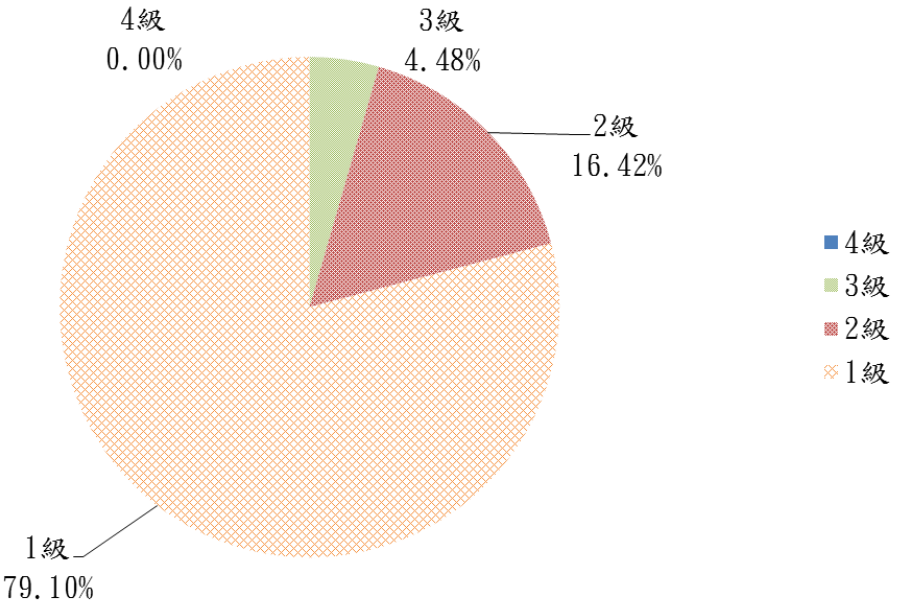
依據卡巴斯基的觀察發現，散布惡意更新的時間推測發生於 107 年 6 月到

11 月間。至於為何這麼長期間仍未被發現的原因，據分析由於更新程式使用的是合法的數位簽章，以及惡意更新程式是存放在合法的更新伺服器，隱藏於正常的軟體更新動作中。根據卡巴斯基公布的統計數據，有超過 5 萬 7 千名卡巴斯基用戶，下載並安裝含後門版本的 Live Update，雖然無法依據他們公布的數據來計算所有受影響的用戶數，但估計全球超過 1 百萬用戶受此影響。

綜覽本季重大資安事件，駭客鎖定政府機關的 DNS 基礎設施，竄改各種伺服器紀錄，以取得使用者所提交的資料。也因這起事件所影響及衝擊範圍重大，所以美國國土安全部發出緊急指令，要求所有.gov 的美國聯邦政府網站在 10 個工作天內採取防禦行動。另一方面，原本以為 Mirai 殭屍網路病毒已經消失匿跡，但在 108 年卻又捲土重來，因此組織更應記取相關事件之經驗，學習如何面對進階式的威脅與風險。供應鏈的資安威脅因為國內這起更新主機遭駭事件，組織應重新審思並規劃將供應鏈廠商之資安要求與檢測納入資安管理範圍內。在面臨新科技的應用時，所應著手準備面對的是可能來到的灰犀牛效應，既已知道有其風險與衝擊存在，就應即早作為。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關(構)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(構)之資安威脅現況。通報事件依資安事件對「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級資安事件。彙整事件影響等級，本季以 1 級事件占 79.1%為大宗，2 級事件占 16.42%次之，3 級事件僅占 4.48%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

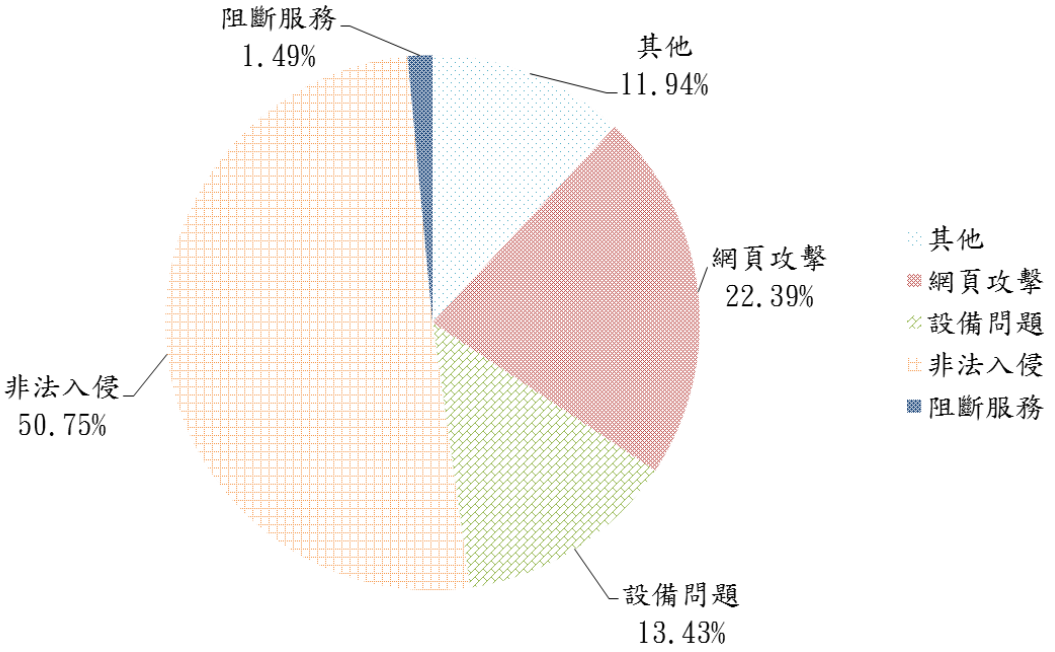


資料來源：本報告整理

圖1　108 年第 1 季資安事件影響等級比率圖

本季 3 級重要資安事件主要有機房作業量過大不堪負荷造成系統緩慢，導致部分服務中斷，因涉及關鍵基礎設施之資通系統，故通報為 3 級重要資安事件。另有因資通系統遭植入惡意程式或管理不當，致少數個人資料外洩問題，皆列為 3 級重要資安事件。

此外，資安事件通報類型依其所發現之異常情形，包括非法入侵、網頁攻擊、設備問題、阻斷服務及其他，其中，以「非法入侵」(占 50.75%)類型為主，詳見圖 2。「網頁攻擊」類型長久以來為駭客感興趣之目標對象，藉由網頁攻擊不但可以干擾網頁之正常服務，亦可透過網頁設計之漏洞，達到入侵內部資通系統的目的，因此亦有超過 2 成的攻擊是針對網頁。

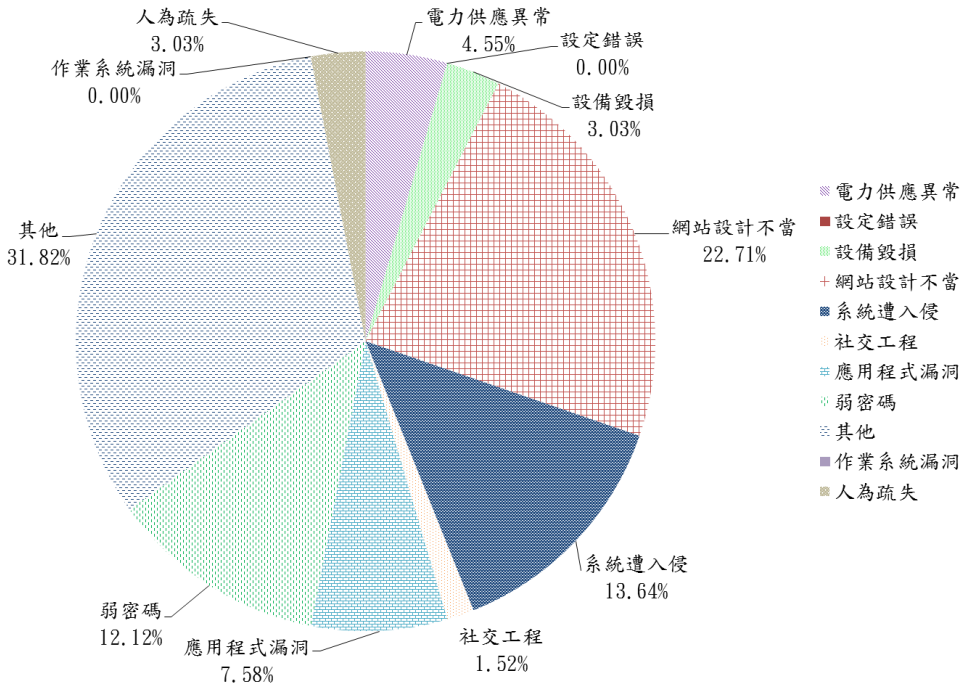


資料來源：本報告整理

圖2　108 年第 1 季資安事件通報類型比率圖

最後，分析通報事件發生原因，以其他(占 31.82%)為主，其次分別為網站設計不當(占 22.71%)、弱密碼(占 12.12%)、應用程式漏洞(占 7.58%)、系統遭入侵(占 13.64%)、電力供應異常(占 4.55%)、人為疏失(占 3.03%)、設備毀損(占 3.03%)、社交工程(占 1.52%)、作業系統漏洞及設定錯誤(皆為 0%)，詳見圖 3。本季事件之其他(占 31.82%)高的原因為部分機關因人力、資源不足或紀錄遭駭客刪除，無相關日誌紀錄可進行事件調查，或無直接證據說明遭入侵管道，而以事件原因不明進行結報。

本季並未有作業系統漏洞與設定錯誤之事件，顯示政府機關(構)在長期推動政府組態基準管理與配合資安稽核、技術檢測等資安活動，已收一定資安防護成效。



資料來源：本報告整理

圖3　108 年第 1 季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，發生多個美國聯邦政府網站的 DNS 系統遭到駭客挾持，駭客利用 APT 攻擊，達到竊取機密資料之目的，又因目標對象為政府網站的網域名稱服務，同時是危及關鍵資訊基礎設施的資安風險。可見現在駭客之攻擊對象更具目標性，且變換不同手法進行攻擊，達到入侵與竊取機敏資料之目的。Mirai 變種再度捲土重來，象徵組織對過去之攻擊型態亦應保持高度警覺，同時委外廠商的資安防護亦不應有片刻懈怠。

分析政府機關(構)通報的 3 級資安事件可看出，個人資料或機敏性資料依然是駭客的首選目標。另外，機關因因備援機房進行不斷電系統汰換暫停服務，致主機房作業量過大不堪負荷造成系統緩慢或無法連線，在資安管理上仍有待加強之處。

綜整以上資安威脅現況，提供資安防護建議如下：

●安全認證與存取管控

– 強化安全認證或設定安全啟動(Secure boot)機制，確保憑證或簽章的安全，以防止被植入惡意程式。

– 定期檢視與稽核重要系統日誌，以即時發現異常行為。

– 定期變更管理者帳號之密碼，加強特權帳號之管理原則。

●資通系統之營運持續管理

– 定期測試容量管理，確保資通系統整體可用度。

– 檢視設定之復原時間目標(RTO)或復原點目標(RPO)，並定期測試目標之達成可行性。

– 記錄事件發生之根因，並將事件做成資安訓練教材，避免再次發生。

●供應鏈之委外安全

– 訂定委外廠商之資安準則與要求，遴選具資安防護能量之廠商。

– 開放存取權限予委外廠商時，應先經安全檢測與規劃活動日誌之留存。

– 定期檢視與稽核委外廠商之服務水準協議符合性與安全規範。

2. 資安專題分享

物聯網的應用廣泛，不管是在日常生活應用，包括在辦公室環境的各種物聯網應用，都已進入百家爭鳴的時代。以往大家所關注的焦點在伺服器、作業平台的防護上，殊不知隨著物聯網便利的連網特性與廣泛使用，物聯網相關資訊設備成為駭客首選的入侵路徑。因此因應駭客利用物聯網多面向的攻擊，必須正視跟隨著物聯網便利而來的資安危機。以下將藉由幾個物聯網設備的資安問題進行研析，並提供相關防護建議。

2.1 物聯網的應用與威脅

2.1.1 MikroTik 路由器弱點

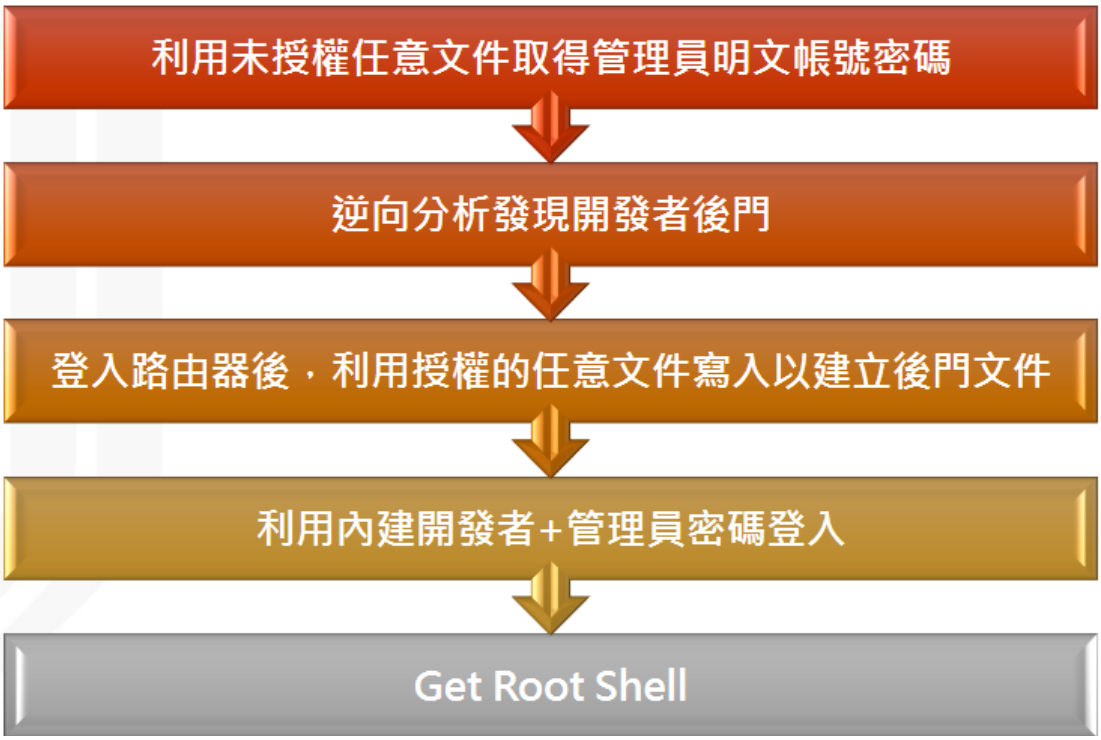
MikroTik 是位於歐洲拉脫維亞的知名網路公司，其商品包括路由器與相關網通設備，目前全球已知的使用數量約 1,879,520 台，市占率為 2.8%。MikroTik 傳出遭駭客利用安全漏洞，透過 MikroTik 路由器的漏洞 (CVE-2018-14847 與 CVE-2018-1156)，攻擊者可入侵受害設備取得 Root Shell 權限，並竊取受害設備相關資訊，CVSS 分數為 7.5 分與 9 分，皆為高風險。

主要產品 RouterOS 係基於 Linux 作業系統，可安裝於一般電腦使其變成路由器設備，且無需高規格的硬體要求，又因 RouterOS 擁有許多功能，包括 Firewall, VPN, QoS & Band Management 等，具備相當多的管理權限。

107 年 4 月 MikroTik 路由器被揭露 1 個目錄瀏覽的弱點，CVE 編號為 CVE-2018-14847，屬於中風險弱點。遠端攻擊者能通過修改請求來繞過身分驗證，並可讀取任意檔案。依據這個弱點延伸出其他弱點，其中較為嚴重的為 CVE-2018-1156 之身分驗證的遠端程式碼執行(RCE)弱點，可允許攻擊者取得完整的系統存取權。

隨著 107 年 10 月釋出一段新的概念驗證(PoC)程式碼，又使風險程度提高，

遠端攻擊者能在受漏洞影響的 MikroTik 路由器上執行遠端程式碼，攻擊手法詳見圖 4。



資料來源：本報告整理

圖4　駭客利用 MikroTik 路由器漏洞之攻擊手法

依據 108 年 1 月 14 日 Shodan 統計數，MikroTik 在全球的使用量共 1,879,520 台，排名前 5 之使用國家分別為巴西(250,129 台)、中國(190,830 台)、印尼(142,513 台)、俄羅斯(134,837 台)及伊朗(91,722 台)，MikroTik 在台灣的使用量則有 13,156 台，故全球所傳出之災情，受害者遍及全球。

此次弱點之肇因為目錄瀏覽的弱點，導致駭客可取得管理員的登入憑證與進行解密，再搭配既存之開發者「後門」機制，從遠端即可取得 root shell 訪問許可權。

政府機關(構)因為在 GSN 亦有 MikroTik 做為連網資通訊設備，因此除持續掌握相關路由器之弱點，並透過資安稽核技術檢測與資安宣導案例機制，

以降低政府機關(構)可能發生之風險。在一般民眾使用此路由器，也應關注相關議題與弱點威脅發展，同時注意漏洞更新釋出，以即時更新相關系統。

2.1.2 網路印表機弱點

網路印表機在辦公室或民眾家中環境隨處可見，但所衍生之資安議題也常被視而不見，隨著網路印表機遭駭客攻擊的事件陸續發生，也使管理者與大眾開始重視網路印表機此項物聯網設備之資安問題。

網路印表機安全防護機制，主要的問題發生在使用者設定不當、印表機程式/韌體設計漏洞及列印語言先天的不足 3 個層面。

常見的印表機弱點，又可區分以下幾點：

- 資訊洩漏：如洩漏印表機的影印內容或系統狀態等。
- 竄改列印的內容或印表機設定：針對列印的內容進行竄改。
- DoS 攻擊：針對印表機執行 DoS 攻擊使其無法執行任務。
- 權限控制不當：存在權限控制不當，導致可以寫入語法，進而控制設備。
- RCE 遠端代碼注入：存在遠端代碼弱點，可使印表機執行任何命令。
- 網頁管理介面未限制權限：網頁版的管理介面未限制存取權限。

以 CVE-2017-2741 所揭露之權限控制不當為例，駭客可以藉由連線至印表機，利用系統所存在之 path traversal 問題，令其列出重要的系統資訊。藉由發現 etc/profile.d 內可以寫入資料，使用 edit 指令，建立一個 tt.sh 檔案，並使用 mkfifo 來呼叫 nc 程式，並 listen port 1444，詳見圖 5。當確定檔案建立完成情況下，便可重新開啟機器。之後連線至主機，在確定成功取得管理者權限下，便可檢視任意檔案，詳見圖 6。

資料來源：本報告整理

圖5　使用 mkfifo 呼叫 nc 程式

資料來源：本報告整理

圖6　駭客取得管理者權限

因應以上網路印表機之連網威脅，整理以下管理重點：

●定期更新印表機的韌體，降低因為韌體漏洞可能產生的風險。

●印表機應變更預設密碼，包括本機密碼與 Webadmin 密碼。

●關閉不必要的服務，如 SNMP，Webadmin 等服務，並限制可存取的位置。

2.2 物聯網的管理與防護重點

物聯網已是現今資訊科技發展的趨勢，惟相關資安防護尚未普及。物聯網資安事件的發生也預告著風險發生的可能性逐步升高，以下綜整物聯網的管理與防護重點提供政府機關(構)參考。

●避免採購具資安疑慮之物聯網資訊設備：部分國家的物聯網資訊設備頻傳資安外洩危機，應以白名單或黑名單方式管制相關採購。

●盤點物聯網資訊設備：政府機關(構)所使用之物聯網設備眾多，應定期盤點相關設備，並視需要更新。

●修改預設密碼：物聯網資訊設備通常具備連網功能，於正式上線前，刪除預設帳號或更新密碼是基本防範之道。

●建立存取控制機制：限制物聯網資訊設備相關應用程式與元件之權限，只提供該設備之必須或最小權限。

●進行安全更新或程式升級：相關物聯網資訊設備應如同其他資訊設備定期執行安全性更新，並時時關注漏洞之發現，提供防範機制。

●定期檢測物聯網資訊設備：發展物聯網資訊設備之檢測機制，如路由器、網路攝影機、網路印表機及門禁系統等辦公室連網設備，都應包括在檢測範圍內。

3. 資安技術研析

本季所探討的資安技術研析，主要是技服中心在近期觀察到 APT 相關類型攻擊，有轉向透過網頁漏洞進行入侵的趨勢。主要攻擊手法是藉由搜尋與利用網頁漏洞，再運用網頁操作(webshell)提權方式，藉以取得並提升當前帳號權限，達到擴散的目的，並利於後續攻擊的部署。

相較於社交工程郵件可由政府骨幹網路(GSN)中蒐集並偵測阻擋，網頁攻擊較難偵測與防範。且現今政府機關(構)提供的線上服務越多，網頁連結或功能就越趨複雜，再加上資通系統常委由不同廠商進行開發，在未有一致性資安要求廠商的情況下，容易造成不同的漏洞與後門存在的可能性。

3.1 基於網頁漏洞之攻擊技術研析

以 Windows 網頁伺服器為例，駭客透過網頁漏洞進行攻擊，僅能取得 IIS_IUSRS(iis apppool\defaultapppool)權限，此帳戶權限較低，無法執行高權限指令。以往駭客的提權工具均是透過系統漏洞提升權限，如 MS11-080、MS14-058、MS16-035 等漏洞，都可將 IIS_IUSRS 提權至 Administrator 或 System 權限。因此，若系統管理者發現漏洞即同時進行系統更新修補後，駭客便無法進行提權的動作。

技服中心發現網頁攻擊的新型態攻擊手法，是利用 JuicyPotato 做為提權工具，原理主要是利用系統 Kernel 層 COM(Component Object Model)元件進行資料傳遞時的缺陷，以中間人(Man in the middle，以下簡稱 MITM)方式取得高權限 Token 進行提權。COM 是 Windows 作業系統的物件導向實作方式，將系統中複雜的功能全部模組化並包成 COM 元件，往後使用者僅須透過 API 呼叫即可使用。

Windows 從 1988 年開始使用 COM 架構，一直到 2015 年才被發現可透過此技術提權，該提權所使用的技術十分複雜，使用條件包括欲利用的 COM 權限為 SYSTEM，且欲提權帳號本身需具有 SeImpersonate 或

SeAssignPrimaryToken 特殊權限。以下將概述利用 JuicyPotato 工具進行提權的技術細節與相關因應之減緩作法。

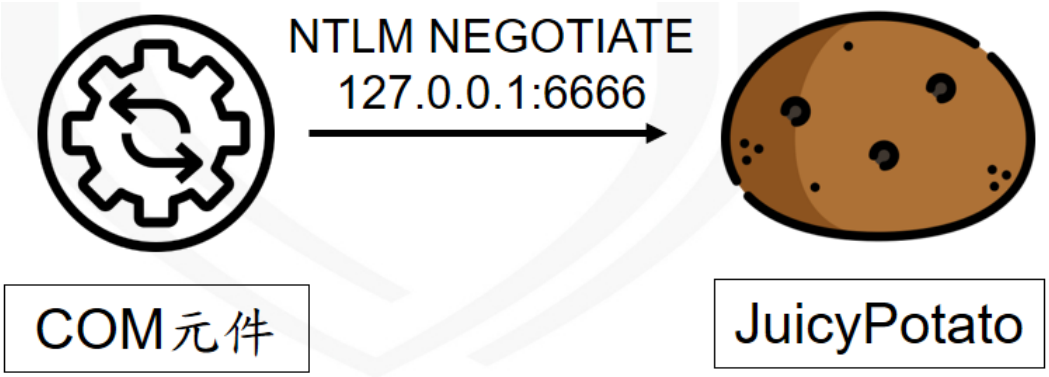
3.2 JuicyPotato 提權技術細節

首先，利用 API CoGetInstanceFromIStorage 新建一個 Object，負責與 COM 元件溝通，詳見圖 7。

資料來源：本報告整理

圖7　建立 Object 與 COM 元件溝通

接續，當 COM 元件收到 CoGetInstanceFromIStorage 後，會主動向 Object 發出 NTLM 身分驗證請求，驗證成功才可繼續執行，身分驗證需進行 3 次溝通，類似 TCP 協定的 3 向交握，此階段會送出 NEGOTIATE 封包，以做為身分驗證的第 1 次溝通，詳見圖 8。

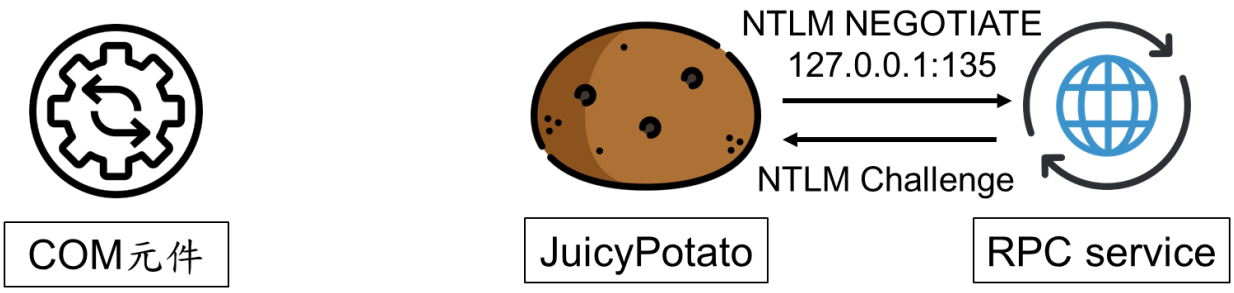


資料來源：本報告整理

圖8　COM 元件向 Object 發出 NTLM 驗證請求

COM 為支援遠端呼叫，因此採用 RPC 協定(Remote Procedure Call Protocol)進行通訊，由於系統底層實作的問題，不同版本作業系統的 RPC 傳遞的封包格式均不相同。為確保不會因格式錯誤導致驗證失敗，因此 Object 不回應此 NEGOTIATE，取而代之是將此封包轉送至 RPC Service，每台 Windows 都一定會啟動 RPC Service，預設 port 為 135。

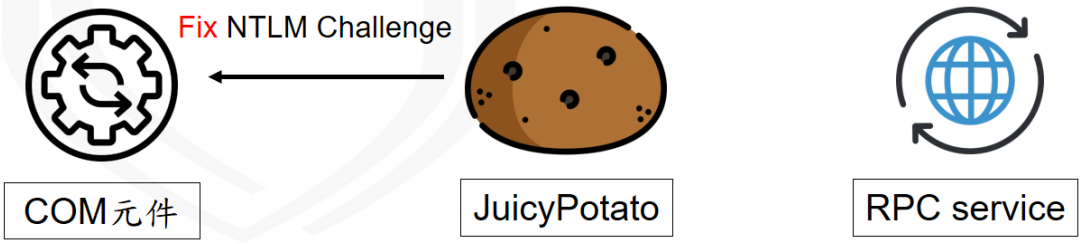
由於 RPC Server 與 COM 元件都在同一台電腦上，故不致產生 RPC 格式不同的問題，因此 RPC Server 可順利回應 NTLM Challenge，詳見圖 9。



資料來源：本報告整理

圖9　封包轉送至 RPC Service

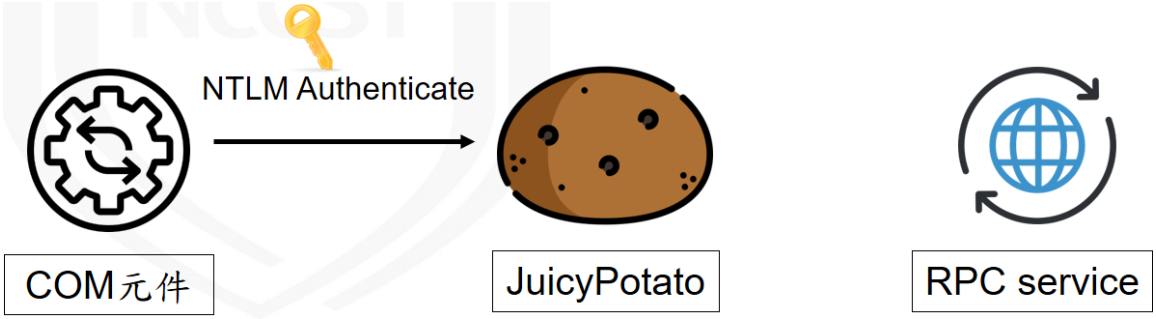
接續，向 COM 元件發送修改過的 NTLM Challenge，由於要進行 MITM 攻擊，因此需要將 NTLM Challenge 中 RPC service 的 KEY 換成自己的 KEY，若單純只是轉送封包，後續便無法進行 COM 與 RPC service 間之密文破解，詳見圖 10。



資料來源：本報告整理

圖10 向 COM 元件發送改過的 NTLM Challenge

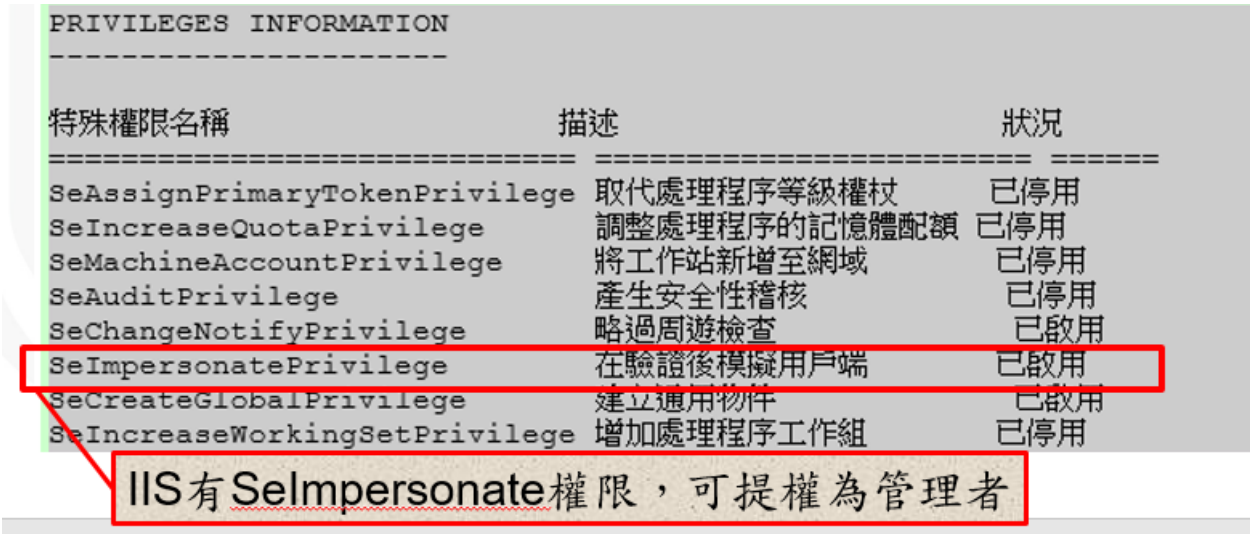
接續，COM 元件會發送 NTLM Authenticate 給 Object，進一步解密 NTLM Authenticate，則可解出 COM 元件的 Token。若 COM 元件是利用 System 身分啟動，如此便可取得 System 的 Token，詳見圖 11。



資料來源：本報告整理

圖11 COM 元件發送 NTLM Authenticate

最後階段，示範利用 Token 進行提權。若帳號擁有 SeImpersonate 或 SeAssignPrimaryToken 等特殊權限，就可利用 Token 進行提權。以 Windows 2016 的 IIS 帳號為例，預設有 SeImpersonate 特殊權限，可用 Token 提權為管理者，詳見圖 12。



資料來源：本報告整理

圖12 利用 Token 進行提權

3.3 JuicyPotato 緩解方案說明

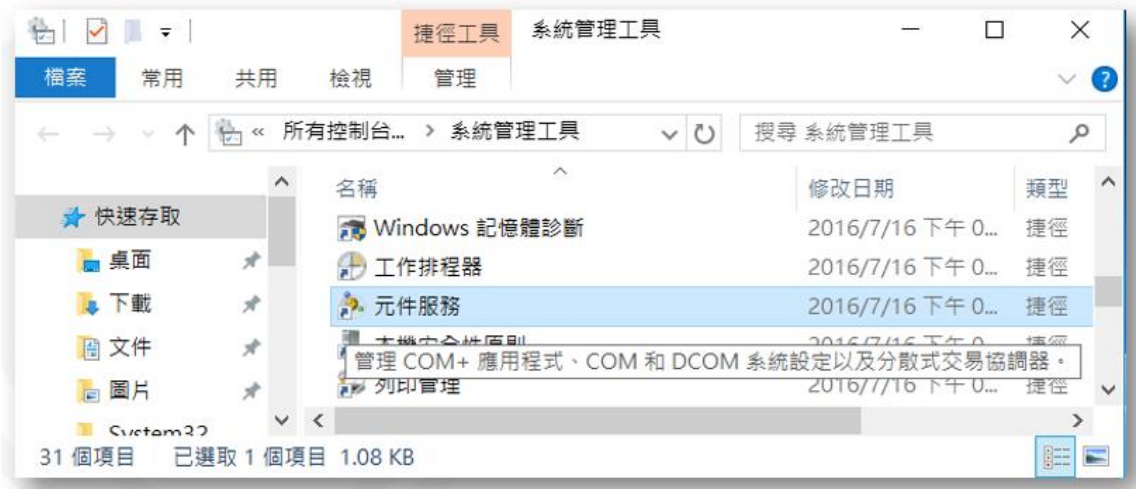
即便此 JuicyPotato 提權技術細節已經公開於眾，微軟公司至今仍未針對此攻擊釋出任何修補。原因在於其係利用 Windows Kernel 層的通訊缺陷進行提權，若要修正勢必要調整體架構，影響甚鉅。

最直接的解決方式則是將作業系統升級至 Windows Server 2019，微軟公司已針對底層架構進行調整，該工具已無法成功提權。而其他可能的緩解方式包含把特定的 COM 元件(如 BITS 等)關掉，但不推薦此作法的原因是，以 Windows 2016 為例，預設有 255 個 COM 元件在運行，其中 61 個具有 SYSTEM 權限，全關閉則會造成系統會有許多服務無法運作，如無法進行

Windows 更新。當然也有另一項作法是移除 IIS_IUSRS 的 SeImpersonate 權限，但也有極大可能造成 IIS 無法順利運作，因此也不建議使用此方案。

以下介紹的適宜作法為禁止 IIS_IUSRS 呼叫 COM 元件，經實證評估此做法影響相對較小。

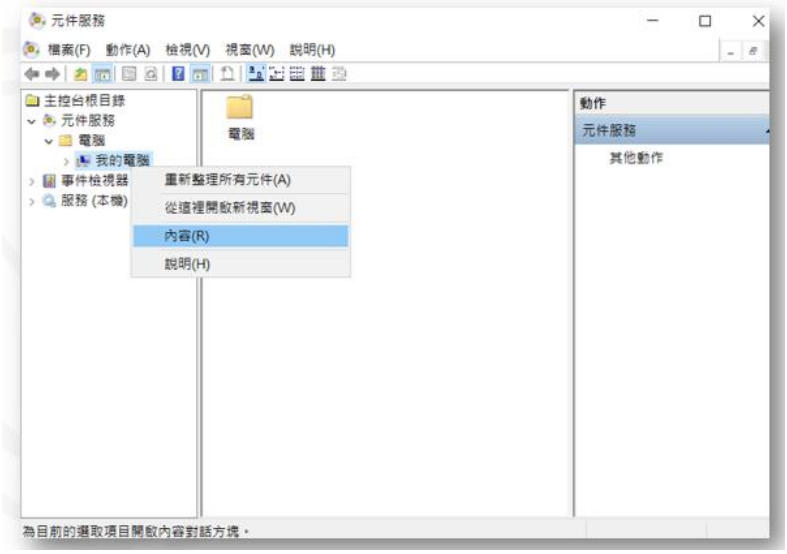
首先，進入控制台→所有控制台項目→系統管理工具→元件服務，詳見圖 13。



資料來源：本報告整理

圖13 進入系統管理工具之元件服務台介面

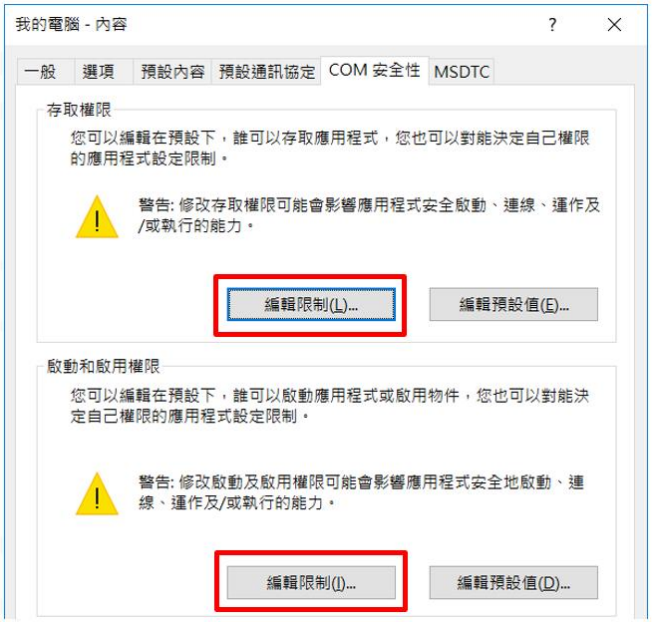
之後，進入主控台根目錄→元件服務→電腦→我的電腦→滑鼠右鍵點內容，詳見圖 14。



資料來源：本報告整理

圖14 進入元作服務介面

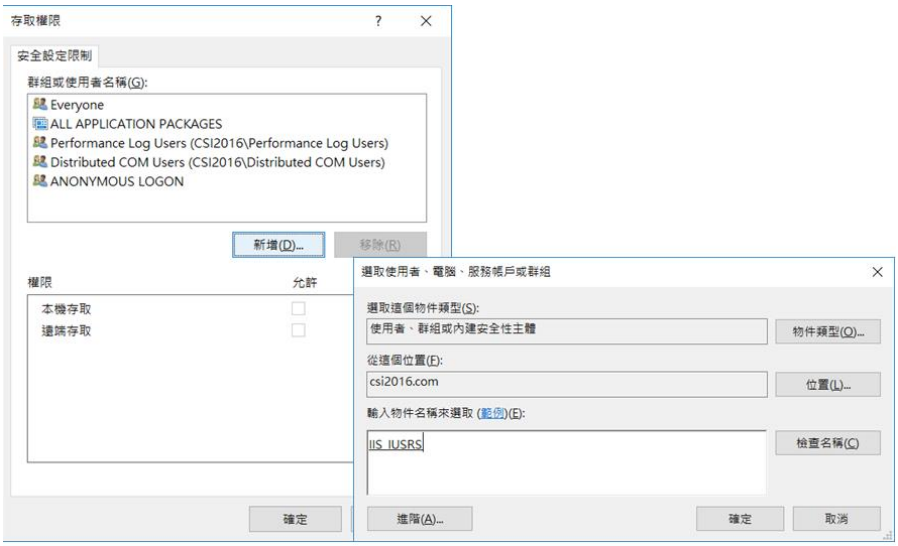
接續，進入 COM 安全性→存取權限\啟動和啟用權限→編輯限制，詳見圖15。



資料來源：本報告整理

圖15 進入編輯限制介面

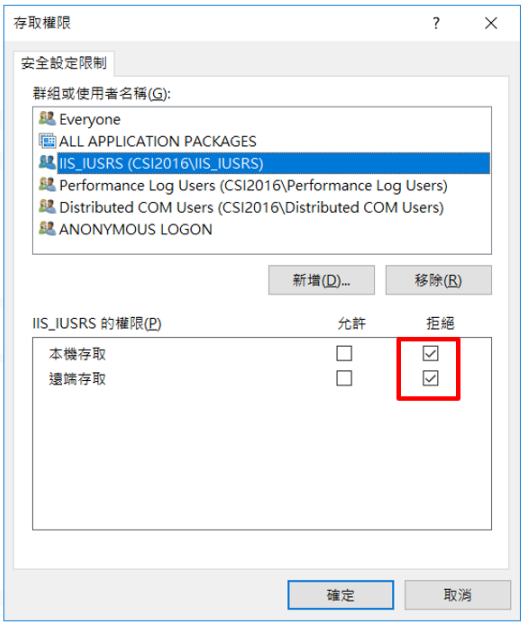
之後，新增→輸入 IIS_IUSRS，詳見圖 16。



資料來源：本報告整理

圖16 新增 IIS_IUSRS

再將 IIS_IUSRS 的存取權限全部勾選拒絕，詳見圖 17。



資料來源：本報告整理

圖17 權限設為拒絕

當修改完成後，再利用 JuicyPotato 測試時，發現已無法和 COM 元件溝通，因此將無法再執行提權動作，詳見圖 18。

資料來源：本報告整理

圖18 與 COM 元件溝通失敗

觀察目前 APT 攻擊，網頁攻擊所占的比例在近年有日漸提高的趨勢。當駭客透過網頁入侵後，會嘗試利用各式工具(如提權、掃描等)進行攻擊與擴散，對於組織而言，駭客鎖定網頁入侵顯然有逐漸攀升之勢，後續應積極規劃針對網頁入侵縱深防禦的資安防範計畫。

4. 結論

本報告針對美國發生大規模之 DNS 系統遭到駭客挾持、新型態 Mirai 變種針對商務型物聯網設備展開新一波攻擊及國內科技大廠更新主機遭駭事件等 3 大事件進行分析，同時以本季發生的重大資安事件與探討議題來概述駭客如何利用系統憑證外洩與新興物聯網設備達到入侵之目的。在國內部分，分析政府資安威脅現況，發現事件原因以「非法入侵」類型為主，其次為「網頁攻擊」。針對本季全球與政府所面臨的主要資安威脅，本報告就「安全認證與存取管控」、「資通系統之營運持續管理」及「供應鏈之委外安全」方面，提出資安防護建議。

資安專題分享物聯網資安威脅，隨著物聯網便利的連網特性與廣泛使用，成為駭客首選的入侵路徑。因此因應駭客利用物聯網多面向的攻擊，必須正視跟隨著物聯網便利而來的資安危機。

本季資安技術研析探討主題為「基於網頁漏洞之攻擊技術研析」，以往駭客透過網頁漏洞進行攻擊，僅能取得 IIS_IUSRS(iis apppool\defaultapppool) 權限。而技服中心發現網頁攻擊使用 JuicyPotato，做為新型態的提權工具，可利用 MITM 方式取得高權限 Token 進行提權，威脅度頗高。

下一季「資通安全技術報告」，除持續分析全球與國內政府機關之資安威脅現況，以及蒐集新興資安議題，從國內外情資與相關研究人員角度提供防護重點。另外，隨著 5G 網路時代的即將來臨，代表資訊科技又將進入另一個新興網路運用的階段，運算裝置的擴大與連網速度的增加，將涉及資料防護、個人隱私及防禦安全等議題，故下期資安專題分享主題規劃為 5G 與新興網路資安議題。

資安相關活動

本季行政院資通安全處辦理多項資安相關活動，活動細節說明如下：

◆ 資訊安全長及資訊主管會議

本年資訊安全長及資訊主管會議於 3 月時辦理，由行政院資安長陳副院長其邁主持。開始先就 107 年網路攻防演練及資安稽核表現績優的機關頒發獎座表達肯定之意，期達到建立資安防護標竿之展現。

會議中就當前資安情勢與未來推動策略、現階段資通安全重點工作、資通安全管理法推動作為、新型態資安攻擊手法、資安聯防及辦公場所資安防護強化措施等議題，交換意見與心得。同時，報告現今資安威脅現況與趨勢，提醒機關注意相關威脅，並提早因應準備。最後，特別就關鍵資訊基礎設施防護執行成果與地方區域聯防中心執行成果，協請機關進行報告與經驗交流。綜合討論部分，主題為辦公場所資安防護強化措施，聚焦在辦公場所可能面臨之資安風險。

此次，共有 78 個機關參與，其中有 40 位資安長親自出席，顯現政府在高階管理者的承諾與支持下，展現由上至下的全方位資安整備。

◆ N-ISAC 會員研討會議

為因應關鍵資訊基礎設施成為駭客攻擊趨勢，行政院資通安全處規劃每季定期召開國家資安資訊分享與分析中心(以下簡稱 N-ISAC)技術交流會議，期透過相關議題的交流與討論，提升我國關鍵資訊基礎設施之資安防護能力。

N-ISAC 現有一般會員 22 名，技術會員 7 名。本季於 3 月辦理一般會員研討會議，首先就 N-ISAC 執行情形報告及資安情勢分析，說明會員情資分享項目及相關運作配合事項等。

本次會議重點在攻防演練經驗分享，包括網路攻防演練經驗分享與領域資安攻防演練經驗分享主題，演練項目包括內外網滲透測試、DDoS 演練及社交工程演練等。希望透過演練過程與結果，檢測政府機關(構)及所轄、領域資安機構對外系統之資安防護能力，並強化在資安事件發生時之緊急應變、系統復原及協調管控等能力。