臺灣臺北地方檢察署新聞稿

Taipei District Prosecutors Office Press Release

發稿日期:115 年 9 月 18 日
聯絡人：襄閱主任檢察官郭進昌
電　話：(02)23146881

臺北地檢署偵辦國家資通安全研究院內部電腦系統遭人入侵案件，於今(18)日偵查終結，對被告許○璋等 4 人提起公訴，茲簡要說明如下：

壹、 本案係本署檢察官廖彥鈞指揮法務部調查局新北市調查處偵辦。

貳、 偵查結果

一、 提起公訴

被告許○彰、彭○君、丁○楓、李○勳等 4 人，均係犯個人資料保護法第 41 條之非法蒐集、處理、利用個人資料、刑法第 358 條之利用電腦系統漏洞而入侵他人之電腦相關設備、刑法第 359 條之無故取得他人電腦相關設備電磁紀錄、刑法第 362 條之製作專供妨害電腦使用之電腦程式等罪嫌，**均提起公訴**。

二、不起訴處分

被告蕭○方、吳○芝、趙○鼎、張○瑜、歐○茹等 5 人，涉犯個人資料保護法第 41 條之非法蒐集、處理、利用個人資料、刑法第 358 條之利用電腦系統漏洞而入侵他人之電腦相關設備、刑法第 359 條之無故取得他人電腦相關設備電磁紀錄、刑法第 362 條之製作專

供妨害電腦使用之電腦程式等罪嫌；**被告黃○睿**，涉犯刑法第 132 條第 3 項之洩漏國防以外秘密罪嫌，因犯罪嫌疑不足，**均為不起訴處分**。

參、 起訴犯罪事實摘要

一、人物關係：

（一）許○璋於民國 112 年 2 月 9 日起，擔任行政法人國家資通安全研究院（下稱資安院）前瞻研究及籌獲中心（位於臺南市歸仁區之資安院沙崙院區，下稱前瞻中心）研究發展組（下稱研發組）總監，於 114 年 3 月升任前瞻中心副主任，負責督導及推動前瞻中心資安防護技術開發、前瞻性資安政策及數位訊息分析與架構設計研究等業務。

（二）彭○君於 112 年 2 月 9 日起，擔任研發組經理，於 114 年 10 月升任前瞻中心總監，負責督導研發組有關新興資安應用技術發展研析、技術研究方向與技術研發規格要求之擬定等。

（三）丁○楓於 112 年 9 月起至 115 年 3 月 20 日止，擔任研發組副研究員，負責資安智評系統、資安週報系統、自定義流程設計系統及暗網爬蟲程式等軟體開發科技專案。

（四）李○勳於 112 年 2 月 9 日起至 115 年 3 月 20 日止，擔任研發組副研究員，負責分散式通訊、防火牆日誌檔分析及資安預警等科技專案。

二、資安院之設立宗旨與業務敏感性

資安院係政府為提升國家資通安全科技能力、推動

資通安全科技研發級應用，而於 112 年 1 月 1 日設立之行政法人，監督機關為數位發展部（下稱數發部），經費來源則以政府核撥、資助及受託科技研究計畫收入為主。因資安院承接國家核心科技研究計畫，並支援具有特殊敏感之政府機關資通安全防護工作，該院人員依「國家資通安全研究院人員安全查核辦法」規定應接受一般安全查核，前瞻中心總監以上職務之主管人員則應接受特殊安全查核；且前瞻中心人員除於任職時簽署「國家資通安全研究院員工服務契約書」（下稱資安院服務契約書）外，因工作需要分別加入多個不同科技研究計畫而涉及核心科技，須依「國家資通安全研究院承接政府資助國家核心科技研究計畫安全管制作業要點」（下稱安全管制作業要點）規定，簽署「政府資助國家核心科技研究計畫保密切結書」（下稱保密切結書）。資安院需定期將上述安全查核、特殊安全查核人員資料函送數發部辦理查核，或將管制人員資料函送數發部資通安全署備查，是資安院公文系統除含有記載資安院人員姓名、出生年月日、國民身分證統一編號、健保級距等個人基本資料外，公文內容暨相關附件尚包含安全查核及核心科技研究計畫等密等以上資料，均屬個人資料保護法適用範圍，應於蒐集目的必要範圍內為之，不得無故蒐集、處理及利用。

三、許○彰、彭○君、丁○楓、李○勳以爬蟲程式撈取資安院之公文、人事、流程表單系統資料

許○彰、彭○君、丁○楓、李○勳於前瞻中心任職後，均有簽署資安院服務契約書、保密切結書，均明知依

該契約書第 9 條約定「對於非因執行職務應知之業務秘密，不得刺探或取得」、第 11 條第 3 項約定「於任職期間因執行職務而有蒐集、處理及利用個人資料時，僅能於執行業務及授權範圍之範圍內使用」，依保密切結書第 4 條約定「僅得於執行專案之必要範圍且專案有效期間內蒐集或取得資安院公務資訊與業務資訊，且不得刺探與本專案無關之公務資訊與業務資訊」。而渠等身為資訊安全人員，亦均明知不得利用電腦系統之漏洞，製作專供入侵電腦之程式而入侵他人之電腦或其相關設備，進而無故取得他人電腦或其相關設備之電磁紀錄，更不得無故蒐集、處理、利用他人之個人資料。詎渠等未經資安院之同意或授權，竟意圖為自己及他人不法之利益，共同基於妨害電腦使用、非法蒐集、處理及利用個人資料之接續犯意，由時任前瞻中心總監許○璋於 114 年 1 月間，指示時任研發組經理彭○君，以改善經費結報系統為由，交辦研發組副研究員丁○楓利用資安院網站系統 API 權限控管之漏洞，製作爬蟲系統入侵該院之公文、人事、流程表單系統，並蒐集取得上開系統之全部資料，據以建構「中心預算系統」(下稱 XMAS 系統)，足生損害於資安院相關資料之機密性與管理安全性。

（一）彭○君於 113 年 1 月 4 日，無意間從資安院人事系統漏洞取得全院人員之個人資料，遂以通訊軟體 LINE 傳送「nics_emp.xlsx」向許○璋告知，彭○君、許○璋因而知悉可從系統漏洞撈取資料之方法。嗣許○璋於 114 年 1 月初，見資安院各項專案計畫之經費管理效能不彰，向時任資安院院長林○達表達希由前瞻中

心開發新型財務管理系統，惟未獲林○達同意。詎許○璋明知資安院並未同意或授權建構新經費結報系統，竟與彭○君謀議利用資安院網站系統之 API 權限控管漏洞，以自動化方式每日擷取資安院之流程表單系統資料，以掌握前瞻中心在採購不同階段之經費動支狀況，遂指示研發組研究員丁○楓著手開發自動化擷取院內流程表單系統資料之程式，許○璋同時提供其製作之 python 程式邏輯管理機制及帳號密碼供丁○楓參考運用，彭○君則向丁○楓告知以非 API 方式改用 JavaScript 抓取流程表單內容以繞過權限限制之方法。

（二）丁○楓接獲指示後，旋即參照許○璋、彭○君提供之意見，研究資安院編碼邏輯、系統設計機制、如何規避資訊安全管制程序，因而發現資安院內部之 EIP 系統（Enterprise Information Portal，即企業資訊入口平臺，用以整合企業內部資訊、工作流程與應用程式）有權限控管不足之漏洞，可透過傳送任意表單編號得到該編號申請經費之表單內容， 遂基於製作專供入侵他人電腦系統程式之犯意，製作專供入侵資安院流程表單系統、人事系統之「爬蟲程式」（Crawler，即自動上網抓取網頁資料之機器人程式），而以排程方式自流程表單、人事系統定時爬取並下載資料。嗣因流程表單系統僅能取得資安院內部差旅費申請及小額採購等資料，大額採購資料因以公文方式申請，無法藉由入侵流程表單系統取得，丁○楓復依許○璋、彭○君指示，續行製作入侵公文系統之爬蟲程式，而接續大量撈取資安院公文、人事、流程表單系統之資料。丁○楓並將入侵人事系統下載之資料，存放於丁

○楓個人之雲端硬碟（該硬碟同時存放資安院人員加班差勤及個人基本資料）；入侵流程表單系統下載之資料，存放於前瞻中心共享資料夾；入侵公文系統下載之資料，則存放於丁○楓個人電腦主機，丁○楓復將下載之公文以微軟 Azure 之「大型語言模型應用程式介面」（LLM API）進行語意分析，判讀解析有關公文內容、大額採購金額及預計請款期數等相關資訊，再將解析完成之公文資料存放至前瞻中心共享資料夾。許○璋、彭○君、丁○楓即以上開利用電腦系統漏洞之入侵方式，逾越渠等權限範圍，無故蒐集、處理及利用渠等從公文、人事、流程表單系統撈取之個人資料及電磁紀錄。

（三）許○璋、彭○君指示丁○楓製作爬蟲程式抓取資安院之公文、人事、流程表單系統資料後，復指示研發組之李○勳、歐○茹、趙○鼎及時任專管技轉組經理吳○芝（除李○勳外，無證據顯示其餘人員參與前述爬蟲程式之開發及運作），協助丁○楓架構 XMAS 系統。由歐○茹主要負責 XMAS 系統使用者介面功能設計補強，趙○鼎協助 XMAS 系統介面設計與開發，吳○芝則提供自身預算管控及大小額採購背景知識，以協助丁○楓完善系統之業務邏輯，並確認使用者需求。嗣因資安院於 114 年 5 月 16 日停止內外網連通之 VPN 管道，導致爬蟲程式無法正常運作，彭○君復指示李○勳建置能串接資安院內、外網路之跳板機。而李○勳明知丁○楓係以前述利用電腦系統漏洞之入侵方式撈取相關資料，仍將資安院配發予渠之內網筆記型電腦作為跳板機，安裝具內外網串接功能之「Cloudflare Tunnel」應用程式， 並負責管理登入

及存取權限，此後爬蟲程式即可從丁○楓之公務外網桌機正常連線至資安院內網之公文、人事、流程表單系統爬取資料，撈取之資料檔案存放於丁○楓公務外網桌機路徑「D:\Projects\selenium\flowSelenium」下資料夾。嗣 XMAS 系統於 114 年 6 月底完成後，即上線供前瞻中心員工使用，迄至 115 年 3 月 13 日止，上開爬蟲程式共計爬取次數達 20 萬 7,938 次，每次間隔時間約 2.6 秒，佔全體職員讀取比例達 85%，致生損害於資安院對於人事、流程表單、公文系統之資料管理。

肆、 量刑意見

資安院係我國政府為提升國家資通安全科技能力、推動資通安全科技研發及應用而特別設立，承接國家核心科技研究計畫，並支援具有特殊敏感之政府機關資通安全防護工作，**被告許○彰、彭○君、丁○楓、李○勳卻未經資安院之同意或授權，擅自利用資安院網站系統之授權漏洞，開發爬蟲程式以逾越授權範圍，撈取資安院內部大量之公文、人事、流程表單系統資料，嚴重破壞資安院之資通安全，所為實屬不該，惟考量其等素行良好，因一時失慮，為處理經費結報而逾越權限實施本案犯行，且尚無證據顯示有內部資料外洩至資安院現任或前任員工以外之對象**，倘其等於審判中坦承犯罪，建請法院審酌資安院之意見及被告 4 人犯後態度而量處適當之刑，以啟自新。