香港文匯報訊（記者 趙一存 北京報道）27日發布的西北工業大學遭美國國家安全局（NSA）網絡攻擊第二份調查報告披露，特定入侵行動辦公室（TAO）在對西工大發起網絡攻擊過程中，實現了對中國基礎設施的滲透控制。報告進一步揭露，美國真實目的即滲透控制中國基礎設施核心設備，竊取中國用戶隱私數據，查詢中國境內身份敏感人員，並將用戶信息傳回NSA總部。報告稱，中國技術團隊成功鎖定美攻擊實施者身份線索，並查明了13名攻擊者的真實身份。

美網攻內地高校 13攻擊者身份查實

第二份調查報告披露：美意在滲透控制中國基礎核心設備

今年6月，西工大發布聲明稱，有來自境外的黑客組織對其服務器實施網絡攻擊。隨後西安警方對此正式立案調查，中國國家計算機病毒應急處理中心和360公司聯合組成技術團隊全程參與此案的技術分析工作。9月，相關部門調查顯示針對西工大的網絡攻擊來自TAO，並於9月5日發布第一份調查報告。

最新的調查報告披露，TAO在網絡攻擊西工大過程中，暴露出多項技術漏洞，多次出現操作失誤，相關證據進一步證明對西北工業大學實施網絡攻擊竊密行動的幕後黑手即為NSA。

報告表明，TAO長期隱蔽控制西工大的運維管理服務器，同時採取替換原系統文件和擦除系統日誌的方式消痕隱身，規避溯源。網絡安全技術人員根據TAO攻擊西工大的隱蔽鏈路、滲透工具、木馬樣本等特徵關聯發現，TAO對中國基礎設施運營商核心數據網絡實施了滲透控制。

不僅如此，TAO通過掌握的中國基礎設施運營商的思科PIX防火牆、天融信防火牆等設備的賬號口令，以「合法」身份進入運營商網絡，然後實施內網滲透拓展，分別控制相關運營商的服務質量監控系統和短信網關服務器，利用「魔法學校」等專門針對運營商設備的武器工具，查詢了一批中國境內敏感身份人員，並將用戶信息打包加密後，經多級跳板回傳至美國國家安全局總部。

報告揭何時何種方式竊用戶隱私

報告還披露了入侵的細節，進一步證明TAO實施網絡攻擊行為，其中包括在具體的時間通過何種方式竊取中國用戶隱私數據，相當於「人贓俱獲」。細節顯示，北京時間20××年3月7日22時53分，TAO通過位於墨西哥的攻擊代理148.208.××.××，攻擊控制中國某基礎設施運營商的業務服務器211.136.××.××，通過兩次內網橫向移動（10.223.140.××、10.223.14.××）後，攻擊控制了用戶數據庫服務器，非法查詢多名身份敏感人員的用戶信息。同日15時02分，TAO將查詢到的用戶數據保存在被攻擊服務器「/var/tmp/.2e434fd8aeae73e1/erf/out/f/」目錄下，被打包回傳至攻擊跳板，隨後竊密過程中上傳的滲透工具、用戶數據等攻擊痕跡被專用工具快速清除。

報告稱，TAO運用同樣的手法，分別於北京時間20××年1月10日23時22分、1月29日8時41分、3月28日22時00分、6月6日23時58分，攻擊控制另外一家中國基礎設施業務服務器，非法多批次查詢、導出、竊取多名身份敏感人員的用戶信息。

至少80國電信基建被相同手法控制

報告還顯示，TAO長期攻擊入侵西工大網絡運維管理服務器，秘密竊取網絡設備運維配置文件和日誌文件。針對西工大遭TAO網絡攻擊的技術分析行動中，中國打破了一直以來美國的「單向透明」優勢，掌握了美國實施網絡攻擊的充分證據。值得一提的是，TAO在實施網絡攻擊中因操作失誤暴露了工作路徑。此外，技術分析還發現，美國仰仗自己強大的技術優勢，針對西工大的攻擊竊密者都是按照美國國內工作日的時間安排進行活動，肆無忌憚，毫不掩飾。

據了解，技術團隊經過持續攻堅，成功鎖定了TAO對西工大實施網絡攻擊的目標節點、多級跳板、主控平台、加密隧道、攻擊武器和發起攻擊的原始終端，發現了攻擊實施者的身份線索，並成功查明了13名攻擊者的真實身份。

另據技術團隊分析，TAO用上述手法，利用相同的武器工具組合，「合法」控制了全球至少有80個國家的電信基礎設施網絡。技術團隊與歐洲和東南亞國家的合作夥伴通力協作，成功提取並固定了上述武器工具樣本，並成功完成了技術分析，擬適時對外公布，協助全球共同抵禦和防範美國國家安全局（NSA）的網絡滲透攻擊。

如何鎖定是美國幹的？

◆攻擊時間

TAO使用tipoff激活指令和遠程控制NOPEN木馬時，必須通過手動操作，從這兩類工具的攻擊時間可以分析出網絡攻擊者的實際工作時間。而大數據顯示，攻擊時間完全吻合美國工作作息時間規律，且在美國節假日和下班時間從未發動過類似攻擊。

◆語言習慣

攻擊者有使用美式英語的習慣，與攻擊者相關聯的上網設備均安裝英文操作系統及各類英文版應用程序，同時攻擊者使用美式鍵盤進行輸入。

◆失誤暴露工作路徑

在對西北工業大學內網實施第三級滲透後試圖入侵控制一台網絡設備時，在運行上傳PY腳本工具時出現人為失誤，未修改指定參數。腳本執行後返回出錯信息，信息中暴露出攻擊者上網終端的工作目錄和相應的文件名，從中可知木馬控制端的系統環境為Linux系統，且相應目錄名「/etc/autoutils」係TAO網絡攻擊武器工具目錄的專用名稱（autoutils）。

◆武器基因高度同源

此次被捕獲的、對西工大攻擊竊密中所用的41款不同的網絡攻擊武器工具明顯具有同源性，都歸屬於TAO。

◆部分網絡攻擊在「影子經紀人」曝光之前

技術團隊綜合分析發現，在對中國目標實施的上萬次網絡攻擊，特別是對西北工業大學發起的上千次網絡攻擊中，部分攻擊過程中使用的武器攻擊，在黑客組織「影子經紀人」曝光NSA武器裝備前便完成了木馬植入。按照NSA的行為習慣，上述武器工具大概率由TAO僱員自己使用。

整理：香港文匯報記者 趙一存

美採半自動化流程長期竊密

香港文匯報訊 據央視報道，此次調查報告顯示，美國國家安全局（NSA）下屬的特定入侵行動辦公室（TAO）對他國發起的網絡攻擊技戰術針對性強，採取半自動化攻擊流程，單點突破、逐步滲透、長期竊密。

360公司網絡安全專家邊亮說，美國對網絡當中的設備或者一段IP進行批量地投漏洞、投病毒，從而獲取相關的權限，且可做到自動化。後續再進行潛伏和長期控制，且有針對性地去竊取相關文件。在過程中需要有人來操作，來指令竊取什麼，及最後撤退時銷毀證據。此外，當攻擊者控制了西工大（相關設備）之後，會利用西工大將自己偽裝成正常用戶，再去對其他單位進行攻擊，但實際上西工大的相關服務器是被美國（TAO）所控制的，去進一步對其他單位產生攻擊。

國家計算機病毒應急處理中心高級工程師杜振華說，網絡攻擊者進入到服務器後，會對網絡流量進行劫持，採用中間人攻擊方式，把其他武器投送到西北工業大學內網的主機或服務器上，以獲取西北工業大學內網的訪問權。在此基礎上，對內網進行探測，尋找高價值的服務器、高價值的主機，然後再向這些服務器和主機進行橫向移動，成功進入之後，便部署嗅探竊密類武器。

內地電騙立案數連15個月下降

香港文匯報訊（記者 趙一存 北京報道）公安部刑事偵查局副局長、一級巡視員姜國利27日在公安部新聞發布會上介紹，夏季治安打擊整治「百日行動」開展以來，國家反詐中心攔截詐騙電話2.8億次、短信4億條，封堵涉詐域名網址81.9萬個，實現立案數連續15個月同比下降，電信網絡詐騙犯罪持續上升的勢頭得到有效遏制。

姜國利介紹，2021年以來，公安部會同工信部、人民銀行聯合推出了反詐五大利器——國家反詐中心App、96110預警勸阻專線、12381涉詐預警勸阻短信系統、全國移動電話卡「一證通查」服務、雲閃付App「一鍵查卡」，不斷加強預警防範工作，構築防詐反詐「防火牆」，成效顯著。

今年6月以來，公安部又會同工信部相繼推出了反詐名片和「一證通查2.0」。他表示，反詐名片功能是指手機用戶在接聽國家反詐部門的預警勸阻電話時，同步彈顯國家反詐中心、工信部反詐中心溫馨提示信息，讓手機用戶快速甄別來電號碼，安心接聽反詐預警電話。「一證通查2.0」服務是指用戶輸入本人手機號和身份證號，一鍵查詢本人名下關聯的互聯網賬號數量，了解本人賬號是否被他人冒用，從而有效防範互聯網賬號被冒用而帶來的涉詐風險。

◇ 早前民警在廣西柳州「雷鋒街市」給市民講解反電信詐騙知識。 資料圖片

攔截詐騙電話2.8億次短信4億條

姜國利介紹，「百日行動」開展以來，全國公安機關先後組織開展「斷卡」「斷流」「拔釘」等專項行動，着力斬斷電詐犯罪鏈條、摧毀電詐犯罪網絡、擠壓電詐犯罪空間，公安部組織華南、華東和京津冀片區的區域會戰，發起集群戰役78次，國家反詐中心推送預警指令6,546萬條，預警準確率達79.9%，會同有關部門攔截詐騙電話2.8億次、短信4億條，封堵涉詐域名網址81.9萬個，實現立案數連續15個月同比下降，電信網絡詐騙犯罪持續上升的勢頭得到有效遏制。

公安部「百日行動」辦公室副主任、治安管理局二級巡視員尹春吉亦在發布會上表示，近年來內地發展夜間經濟、有力促進消費增長，不過夏季夜間人流、車流、物流大量增多，也導致各類違法犯罪活動時有發生。他介紹，「百日行動」期間，全國公安機關開展了3個輪次的夏夜治安巡查宣防集中統一行動。其間，累計抓獲現行違法犯罪嫌疑人16.2萬人，實現了震懾犯罪、安定人心的預期效果。尹春吉表示，下一步，公安機關將把夜間治安臨查臨檢向平時、向防範薄弱的地方延伸，為民眾「守好夜」、為平安「站好崗」。

湖南破虛擬幣洗錢案 涉案400億 93人被捕

香港文匯報訊 據證券時報報道，湖南衡陽縣公安日前發布消息稱，破獲一起涉嫌利用虛擬幣交易，為網絡賭博和電信詐騙集團洗錢的犯罪集團，涉案金額高達400億元（人民幣，下同）。警方在海南、廣東、福建、江西等地收網，抓獲犯罪嫌疑人93人，搗毀洗錢、跑分窩點10餘個，繳獲涉案手機、電腦100餘台，查封凍結涉案資金3億元，為受害人挽回經濟損失780萬元。目前，已串並涉電信詐騙案件300餘起。

經查，自2018年開始，以犯罪嫌疑人洪某某為首的犯罪團夥先後在國內多個城市聯繫代收代付點，將涉詐涉賭等犯罪資金轉換為虛擬幣再變現為美元進行洗白，最後利用國內多家公司採用非法回匯的手段將資金交付給其他金主，從中攫取非法利益。該犯罪集團利用虛擬幣交易的方式洗錢金額高達400億元。

目前，犯罪嫌疑人洪某某等93人已被刑拘。

9月26日晚，人民銀行發文稱，持續打擊境內虛擬貨幣交易炒作，中國境內比特幣交易量在全球佔比大幅下降。公安部早前發布消息稱，2021年，針對虛擬貨幣洗錢新通道，全國公安機關共破獲相關案件259起，收繳虛擬貨幣價值110億餘元。