查實美竊取中國高校核心技術數據

攻擊竊密西北工業大學逾千次 完整證據鏈已還原

香港文匯報訊（記者 李陽波 西安報道）9月5日，國家計算機病毒應急處理中心發布「西北工業大學遭美國NSA網絡攻擊事件調查報告」，揭露了美國國家安全局（NSA）長期以來針對包括西北工業大學（簡稱「西工大」）在內的中國信息網絡用戶和重要單位開展網絡間諜活動的真相。報告指出，在今年「西北工業大學遭受境外網絡攻擊事件」調查中，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，全程參與了此案的技術分析工作。初步判明相關攻擊活動源自美國國家安全局（NSA）「特定入侵行動辦公室」（Office of Tailored Access Operation，簡稱TAO）。報告顯示，美方對西北工業大學發起攻擊竊密行動上千次，竊取了一批核心技術數據。近年裏，TAO已對中國國內的網絡目標實施了上萬次的惡意網絡攻擊。

坐落於陝西西安的西北工業大學，是一所以發展航空、航天、航海等領域人才培養和科學研究為特色的多科性、研究型、開放式國家「一流大學」，先後研發出全國第一架小型無人機、第一台地效飛行器、第一型50公斤級水下無人智能航行器和第一台航空機載計算機，現建有8個國家級重點實驗室、2個國家工程研究中心、4個國家級國際科技合作基地、1個國防科技創新中心、5個國家地方聯合創新平台、140個省部級科研平台，重點參與了大飛機、載人航天與探月等10個國家重大專項的論證及科研攻關，深度參與了兩機專項論證、神舟系列飛船研製。

以釣魚郵件非法獲取權限

然而，這些巨大成就也讓該校成為境外別有用心者覬覦的對象。今年6月22日，西北工業大學發布《公開聲明》稱，近期該校電子郵件系統遭受網絡攻擊。「系統發現木馬程序，企圖非法獲取權限，這給學校的正常工作和生活秩序造成了重大的風險隱患。」西北工業大學信息化建設與管理處副處長兼信息中心主任宋強在接受央視採訪時表示，該校高度重視網絡安全工作，當時便報了警。

接警後，西安市公安機關立即組織警力與網絡安全技術專家對此案進行立案偵查。經調查，在西北工業大學電子郵件系統發現一批以科研評審、答辯邀請和出國通知等為主題的釣魚郵件，內含木馬程序，引誘部分師生點擊鏈接，同時部分教職工個人上網電腦中也發現遭受網絡攻擊的痕跡。6月23日，西安警方發布《警情通報》指出，經初步判定，此事件為境外黑客組織和不法分子發起的網絡攻擊行為。

調查中，由國家計算機病毒應急處理中心和360公司聯合組成的技術團隊，先後從西北工業大學的多個信息系統和上網終端中提取到了多款木馬樣本，綜合使用國內現有數據資源和分析手段，並得到了歐洲、南亞部分國家合作夥伴的通力支持，全面還原了相關攻擊事件的總體概貌、技術特徵、攻擊武器、攻擊路徑和攻擊源頭，相關攻擊活動也指向美國國家安全局所屬TAO。

◆西北工業大學早前在工博會展示的新型垂直起降高速無人機。 資料圖片

TAO採40餘種專屬網絡攻擊武器

經香港文匯報記者梳理調查報告發現，在針對西北工業大學的網絡攻擊中，TAO使用了40餘種不同的NSA專屬網絡攻擊武器，持續對西北工業大學開展攻擊竊密，竊取該校關鍵網絡設備配置、網管數據、運維數據等核心技術數據。

經溯源分析，技術團隊現已全部還原了NSA的攻擊竊密過程，澄清其在西北工業大學內部滲透的攻擊鏈路1,100餘條、操作的指令序列90餘個、多份遭竊取的網絡設備配置文件、遭嗅探的網絡通信數據及口令、其它類型的日誌和密鑰文件，基本還原了每一次攻擊的主要細節。掌握並固定了多條相關證據鏈，涉及在美國國內對中國直接發起網絡攻擊的人員13名，以及NSA通過掩護公司為構建網絡攻擊環境而與美國電信運營商簽訂的合同60餘份，電子文件170餘份。

西安市公安局碑林分局副局長靳琪表示，目前，聯合專案組已將相關調查結果上報國家有關部門。後續，技術團隊還將陸續公布相關事件調查的更多技術細節。

西工大：反對任何形式網絡攻擊

9月5日，西北工業大學再次發布《公開聲明》表示，2022年4月12日，我校就郵件系統遭受釣魚郵件攻擊的情況向公安機關報案。近期，公安機關向我校通報了案件偵辦的相關情況。在此，我校公開聲明：我們堅決反對以任何形式實施網絡攻擊。學校高度重視網絡安全工作，為師生營造安全的網絡環境。學校號召廣大師生進一步提高網絡安全意識，共同維護學校網絡安全。

◆研究人員在西北工業大學無人機試驗測試中心工作。受訪者供圖

高校政府企業聯手「挖」出境外黑手

香港文匯報訊（記者 李陽波 西安報道）美國國家安全局（NSA）下屬TAO成立於1998年，是目前美國政府專門從事對他國實施大規模網絡攻擊竊密活動的戰術實施單位，由2,000多名軍人和文職人員組成，下設10個單位。其力量部署主要依託NSA在美國和歐洲的各密碼中心，目前已被公布的共有六個密碼中心。

根據調查報告顯示，在針對西北工業大學的網絡攻擊中，TAO使用了41種不同的NSA專屬網絡攻擊武器。並且在攻擊過程中，TAO會根據目標環境對同一款網絡武器進行靈活配置。同時，為掩護其攻擊行動，TAO在開始行動前會進行較長時間的準備工作，主要進行匿名化攻擊基礎設施的建設。據介紹，TAO在攻擊中使用了位於17個國家的54台跳板機和5台代理服務器，其中70%位於中國周邊國家，用以掩蓋發起網絡攻擊的真實IP。

目前，技術團隊已經至少掌握TAO從其接入環境（美國國內電信運營商）控制跳板機的四個IP地址。

為各國抵禦NSA網絡攻擊提供借鑒

一直以來，NSA針對中國各行業龍頭企業、政府、大學、醫療機構、科研機構甚至關乎國計民生的重要信息基礎設施運維單位等機構長期進行秘密黑客攻擊活動，其行為或對我國的國防安全、關鍵基礎設施安全、金融安全、社會安全、生產安全以及公民個人信息造成嚴重危害，值得深思與警惕。

此次西北工業大學聯合中國國家計算機病毒應急處理中心與360公司三方聯手「挖」出境外黑手，積極採取防禦措施的行動不僅值得遍布全球的NSA網絡攻擊活動受害者學習，同時也將成為世界各國有效防範抵禦美國NSA後續網絡攻擊行為的有力借鑒。

外交部強烈譴責 促美立即停止不法行為

香港文匯報訊 據中新社報道，對於西北工業大學遭到美國國家安全局網絡攻擊一事，在9月5日舉行的中國外交部例行記者會上，發言人毛寧表示，中方對此強烈譴責。美國應立即停止對他國進行竊密和攻擊，為維護網絡安全作出建設性作用。

有記者提問，日前，國家計算機病毒應急處理中心和360公司分別發布了關於西北工業大學遭受美國國家安全局網絡攻擊的調查報告，顯示美國國家安全局下屬的特定入侵行動辦公室針對中國的網絡目標實施了上萬次惡意網絡攻擊。中方對此有何評論？

美長期對中國手機用戶語音監聽

毛寧指出，調查報告揭露了美國政府對中國進行網絡攻擊的又一實例。根據國家計算機病毒應急處理中心和360公司聯合技術團隊的技術分析與追蹤溯源，美國國家安全局對中國實施網絡攻擊和數據竊密的證據鏈清晰完整，涉及在美國國內對中國直接發起網絡攻擊的人員13名，以及為構建網絡攻擊環境而與美國電信運營商簽訂的合同60餘份，電子文件170餘份。報告顯示，美方先後使用41種專用網絡攻擊武器裝備，對西北工業大學發起攻擊竊密行動上千次，竊取了一批核心技術數據。美方還長期對中國的手機用戶進行無差別語音監聽，非法竊取手機用戶的短信內容，並對其進行無線定位。

「美方行徑嚴重危害中國國家安全和公民個人信息安全。中方強烈譴責，要求美方作出解釋並立即停止不法行為。」毛寧說。

她強調，網絡空間安全是世界各國面臨的共同問題。作為擁有最強大網絡技術實力的國家，美國應立即停止對他國進行竊密和攻擊，以負責任的態度參與全球網絡空間治理，為維護網絡安全發揮建設性作用。

美國才是當今最大網絡竊密者

微觀點

近年來，美國一直聲稱自己是捍衛信息安全領域的「衛士」，並接連糾集其所謂的盟友向中國發難，發表聲明指責對其進行系統性網絡攻擊。而通過此次「西北工業大學遭網絡攻擊事件」以及技術團隊的報告不難看出，美國才是當今世界上最大的網絡竊密者，也是中國網絡的頭號攻擊國。

根據調查報告顯示，近年裏，美國NSA下屬TAO對中國國內的網絡目標實施了上萬次的惡意網絡攻擊，控制了數以萬計的網絡設備（網絡服務器、上網終端、路由器、防火牆等），竊取了超過140GB的高價值數據。與此同時，TAO還長期對中國的手機用戶進行無差別的語音監聽，非法竊取手機用戶的短信內容，並對其進行無線定位。這些在全球範圍都屬於違反法律、侵犯個人隱私的行為，被美國成系統地用來危害他國。

面對這樣一個國家級背景的強大對手，西北工業大學聯合中國國家計算機病毒應急處理中心與360公司，全面還原了數年間美國NSA利用網絡武器發起的一系列攻擊行為，打破了一直以來美國對中國的單向透明優勢，不僅幫助國家真正感知風險、看見威脅、抵禦攻擊，將境外黑客攻擊暴露在陽光下，同時也用事實告訴美國，中國是網絡安全的堅定維護者，也有能力捍衛本國網絡安全。

◆香港文匯報記者 李陽波