香港文匯報訊（記者 趙一存 北京報道）27日發布的中國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。

美網攻中國高校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。

前8月中國規上工業企業營收增8.4%

工業盈利喜憂參半 內生動力待增強

香港文匯報訊（記者 海巖 北京報道） 中國國家統計局27日公布數據顯示，今年前8個月，全國規模以上工業企業營業收入同比增長8.4%，延續較快增長態勢，利潤總額同比下降2.1%，為2020年10月以來最低。不過，隨着工業生產企穩帶動盈利邊際改善，8月當月工業企業利潤降幅收窄，上下游利潤結構繼續改善，外資企業利潤由降轉增。國家統計局對此表示，工業企業效益呈現恢復態勢，但工業企業利潤總體仍在下降，生產經營成本仍然較高，下階段要加大助企紓困力度，推動工業經濟持續穩定恢復。

數據顯示，8月，在41個工業大類行業中，有27個行業利潤增速較上月加快或降幅收窄、由降轉增，佔比超六成，其中多數為中下游行業。國家統計局工業司高級統計師朱虹表示，隨着部分大宗商品價格漲幅回落，工業企業利潤上下游結構明顯改善，裝備製造業利潤降幅連續4個月收窄，電力行業利潤持續回升。

裝備製造業效益顯著好轉

8月，隨着產業鏈供應鏈持續恢復，重點地區企業復工復產加快，加之減免車輛購置稅等政策推動消費，裝備製造業效益狀況顯著好轉。數據顯示，汽車製造業利潤延續高增速，8月同比增長1.02倍。增速較7月擴大24.2個百分點，是拉動工業企業利潤回升貢獻最大的行業。在鋰離子電池、光伏設備、空調製造等行業帶動下，電氣機械行業利潤增長36.7%，增速較7月加快11.1個百分點；電子、儀器儀表行業利潤分別增長22.9%、21.3%，增速均由負轉正。

工業生產持續恢復疊加高溫天氣，用電需求旺盛，發電量增速升至近年高位，帶動電力行業利潤快速恢復，8月電力行業利潤同比增長1.58倍，增速較7月加快111.8個百分點。

處於下游的消費品製造業盈利也出現好轉，隨着促消費政策逐步顯效，市場需求有所回升，多數消費品行業利潤改善，酒飲料茶、煙草、文教工美行業利潤分別增長59.8%、33.8%、29.1%。

建築行業景氣度疲軟

地產、建築相關產業鏈利潤則繼續承壓，房地產市場下行，建築行業景氣度疲軟，導致上游的鋼鐵、水泥行業需求和利潤降幅繼續擴大，1-8月鋼鐵行業利潤同比下降87.7%。

此外，1-8月規模以上工業企業中，不同類型企業利潤繼續分化，國有企業利潤同比增長5.4%，股份制企業利潤同比增長0.8%，但私營企業利潤同比下降8.3%，外商及港澳台商投資企業利潤大幅下降12.0%。


◆今年前8個月，全國規模以上工業企業營業收入同比增長8.4%，延續較快增長態勢，利潤總額同比下降2.1%。圖為山西晉中工人在生產重載汽車車間工作。 中新社

下階段加大助企紓困力度

不過，從8月單月看國企與民企利潤同比差距或開始縮小。國家統計局數據稱，8月外商及港澳台商投資企業營收增長加快，利潤由7月同比下降轉為增長6%；小微企業利潤同比下降4.1%，降幅較7月有所收窄，利潤恢復程度好於全部工業，表明大型企業與小微企業利潤差距有所收窄。

「工業企業效益呈現恢復態勢，當月利潤降幅較上月收窄，行業結構有所改善，中下游行業利潤繼續恢復。但也要看到，工業企業利潤仍在下降，企業生產經營成本仍然較高，加之外部環境不穩定不確定因素較多，工業企業利潤恢復的基礎不牢。」國家統計局工業司高級統計師朱虹表示，下階段，要加力推進穩經濟一攬子政策和接續政策效能釋放，着力擴大有效需求，加大助企紓困力度，推動工業經濟持續穩定恢復。

專家解讀

專家普遍認為，8月經濟數據、工業企業利潤及高頻數據顯示，經濟活動有所恢復，可能預示迎來新一輪小復甦，但同時面臨工業盈利內生動力不足、增收不增利等困難，需要政策有針對性給予支持。

招商證券首席宏觀分析師張靜靜指出，從1-8月看，工業企業營業收入保持較快增長但利潤持續走弱，說明當前工業企業運營延續恢復態勢，但「增收不增利」的問題依然突出，工業企業利潤將在四季度逐步呈現改善趨勢，上下游行業利潤都有望呈現恢復上行。

浙商證券首席經濟學家李超指出，當前工業盈利喜憂參半，兩大偏離現象需關注，一是工業企業盈利增速下降幅度大於營收增速下降幅度；二是上游原材料價格持續回落，但工業企業，尤其是製造業企業的營收成本卻持續大幅上行。「背後主要原因是工業盈利內在動力不足。疫情以來持續的減稅降費政策對企業利潤改善的貢獻已十分有限，而在經濟弱復甦背景下，工業企業產能利用率沒有起色，使得單位產品成本抬升，企業盈利承壓。」

仲量聯行大中華區首席經濟學家兼研究部總監龐溟則指出，大宗商品價格漲幅回落一定程度改善了工業企業利潤上下游結構，但對原來以低成本作為競爭優勢佔領市場的企業尤其是部分外貿企業和規模以下的中小微企業而言，利潤空間被此前上游大宗商品的價格上漲擠佔，市場主體依然存在困難，亟需採取有力措施來紓困扶持。未來政策應重視擴大和支持社會有效需求，增強市場主體的內生動力，有效彌補需求不足問題。

◆香港文匯報記者 海巖 北京報道