責任編輯：林子奇 王 旭
美術編輯：葉錦秋

黑客侵西工大竊密 中方揭美騎劫17國服務器施襲

中國網絡遭美國安局攻擊逾萬次

真相大白

【大公報訊】綜合央視新聞、中新社報道：9月5日，中國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境外網絡攻擊的調查報告。報告顯示網絡攻擊源頭為美國國家安全局（下稱NSA），過程動用分布17國的跳板機和代理服務器。報告並指出NSA近年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，竊取高價值中國網絡數據超140GB。

拆解美國網絡攻擊手法

▶美國國家安全局位於馬里蘭州米德堡的總部。

攻擊來源

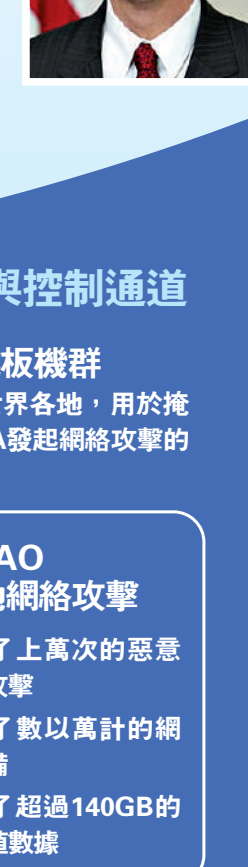
美國國家安全局（NSA）

行動代號：「阻擊XXXX」(shotXXXX)

行動單位：特定入侵行動辦公室

- 簡稱TAO，NSA資訊情報部數據偵察局的下屬部門，代號S32
- 是目前美國政府專門對他國實施大規模網絡攻擊竊密活動的戰術實施單位
- 由2000多名軍人和文職人員組成，主要依託NSA在美國和歐洲的各密碼中心部署力量

行動指揮：羅伯特·喬伊斯（Robert Edward Joyce）



- 1989年進入NSA工作，2013年至2017年擔任TAO主任
- 2017年10月開始擔任代理美國國土安全顧問，2018年4月至5月，擔任美國白宮國務安全顧問
- 後回NSA擔任局長網絡安全戰略高級顧問，現任NSA網絡安全主管

漏洞攻擊利用通道

5台代理服務器

- 屬於美國Terremark公司，主要部署FOXACID
- 通過NSA的掩護公司購買

▲美國民眾在華盛頓反對NSA的活動。

TAO對西工大網絡攻擊

- 使用了41種NSA專屬網絡攻擊武器
- 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
- 滲透攻擊鏈路最少1100餘條、操作的指令序列最少90餘個

此次調查發現，針對西北工業大學的網絡攻擊中，NSA下屬的「特定入侵行動辦公室」（下稱TAO）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。TAO針對西工大網絡攻擊，動用分布17國的54台跳板機和代理服務器。

西安市公安局碑林分局副局長靳琪表示，西工大是目前內地從事航空、航天、航海工程教育和科學研究領域的重點大學，擁有大量國家頂級科研團隊和高端人才，承擔國家多個重點科研項目，地位十分特殊，網絡安全十分關鍵。由於其所具有的特殊地位和從事的敏感科學研究，所以才成為此次網絡攻擊的目標。

據了解，西工大今年4月12日就郵件系統遭受釣魚郵件攻擊的情況向公安機關報案。該校6月22日並發布聲明，稱有來自境外的黑客組織和不法分子向學校師生發送包含木馬程序的釣魚郵件，企圖竊取相關師生郵件數據和公民個人信息。

41種網攻武器盜取逾140GB數據

調查報告顯示，NSA在對西工大的網絡攻擊行動中，先後使用了41種專用網絡攻擊武器裝備，僅後門工具「狡詐異端犯」（NSA命名）就有14款不同版本。通過取證分析，技術團隊累計發現攻擊者在西工大內部滲透的攻擊鏈路多達1100餘條、操作的指令序列90餘個，並從被入侵的網絡設備中定位了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、其他類型的日誌和密鑰文件以及其他與攻擊活動相關的主要細節。技術團隊將此次攻擊活動中所使用的武器類別分為四大類，具體包括：1、漏洞攻擊突破類武器；2、持久化控制類武器；3、嗅探竊密類武器；4、隱蔽消痕類武器。

此次調查報告披露，NSA利用大量網絡攻擊武器，針對內地各行業龍頭企業、政府、大學、醫療、科研等機構長期進行秘密黑客攻擊活動，竊取超140GB數據。360公司創始人周鴻禕表示，美國就是瞄準中國的科研機構、政府部門、軍工單位、高校這些地方來竊取情報或者竊取數據，「對於我們國家而言這十分危險，因為未來整個國家都在發展數字化，很多重要的這種業務都是由數據來驅動，數據一旦被偷竊或一旦被破壞，肯定會帶來嚴重的風險。」

外交部強烈譴責 反對網絡霸權

外交部新聞發言人毛寧在5日的記者會上表示，美方行徑嚴重危害中國國家安全和公民個人信息安全。中方對此強烈譴責，要求美方作出解釋並立即停止不法行為。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，美國應立即停止利用自身優勢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。

命令與控制通道

49台跳板機群

- 分布世界各地，用於掩蓋NSA發起網絡攻擊的眞實IP

近年TAO對內地網絡攻擊

- 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
- 竊取了超過140GB的高價值數據

資料來源：國家計算機病毒應急處理中心《西北工業大學遭美國NSA網絡攻擊事件調查報告（之一）》

話你知

西工大總師輩出「20家族」搖籃

位於西安的西北工業大學早在1961年被確定為內地七所國防工業院校之一，現直屬工信部，設有材料科學與工程、航空宇航科學與技術兩個國家重點一級學科。作為國防軍工重鎮，西工大的航空航天類各專業在全國首屈一指，為航空軍工界提供了大量人才，包括多位國防裝備的總設計師，如直–20總設計師鄧景輝、運–20總設計師唐長紅和殲–20總設計師楊偉，堪稱「20家族」搖籃。

隱匿真實IP 借刀殺人

【大公報訊】據央視新聞報道：此次調查報告披露，NSA為了隱匿其對西北工業大學等中國信息網絡實施網絡攻擊的行為，做了長時間準備工作，並且進行了精心偽裝。

技術團隊分析發現，特定入侵行動辦公室（下稱TAO）利用其掌握的針對SunOS操作系統的兩個「零日漏洞」利用工具，選擇了中國周邊國家的教育機構、商業公司等網絡應用流量較多的服務器為攻擊目標；攻擊成功後，即安裝NOPEN木馬程序，控制了大批跳板機。

向非「五眼聯盟」國家設備下手

TAO在針對西北工業大學的網絡攻擊行動中先後使用了54台跳板機和代理服務器，主要分布在日本、韓國、瑞典、波蘭、烏克蘭等17個國家，其中70%位於中國周邊國家，如日本、韓國等。其中，用以掩蓋真實IP的跳板機都是精心挑選，所有IP均歸屬於非「五眼聯盟」國家。針對西北工業大學攻擊平台所使用的網絡資源涉及代理服務器，NSA通過秘密成立的兩家掩護公司購買了埃及、荷蘭和哥倫比亞等地的IP，並租用一批服務器。

國家計算機病毒應急處理中心高級工程師杜振華表示，使用這種虛擬身份，或者是代理人的身份去租用和購買互聯網上的這種服務器、IP地址、域名，可以在對方不知情的情況下接管第三方用戶的這種服務器資源，實施網絡攻擊，如同借刀殺人。

NSA為了保護其身份安全，使用了美國隱私保護公司的匿名保護服務，相關域名和證書均指向無關聯人員，以便掩蓋真實攻擊平台對西北工業大學等中國信息網絡展開的多輪持續性攻擊、竊密行動。

入侵目標

中國 西北工業大學

美網企開後門 助紂爲虐

【大公報訊】綜合央視新聞、中國青年報報道：調查報告指出，「NSA利用其控制的網絡攻擊武器平台、『零日漏洞』（Oday）和網絡設備，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訊內容，並對其進行無線定位。」

長期監聽中國手機用戶

相關網絡攻擊活動開始前，NSA在美國多家大型知名互聯網企業配合下，將掌握的中國大量通信網絡設備的管理權限，提供給美國國家安全局等情報機構，為持續侵入中國國內的重要資訊網絡大開方便之門。

資訊安全新媒體「安在」今年6月曾發布報告指出，美方多管道竊取全球各類網絡數據。「安在」報告列舉了美方威脅全球網路安全的多種方式，比如TAO持續對全球互聯網用戶實施無差別數據竊密。美方利用潛艇對全球海底光纜和電纜進行網絡竊密，美國國安局接入技術行動處還將網絡攻擊武器交由美國等「五眼聯盟」國家使用。英國政府曾利用歐盟電信運營商對歐盟總部進行網絡竊密。此外，美國政府要求美互聯網公司配合網絡武器研發製造，並研發針對中國電信設備的攻擊武器。

360公司網絡安全專家邊亮表示，目前據我們了解是TAO代表了全球網絡攻擊的最高水準。他們所掌握的大量的攻擊武器，相當於有了互聯網當中的萬能鑰匙一樣，它可以任意地去進出它想要的目標設備，從而去進行比如情報的竊取，或者說進行破壞等動作。

專家：速堵漏洞 定位攻擊源頭

【大公報訊】據央視新聞報道：調查報告顯示，一直以來，NSA針對我國各行業龍頭企業、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，值得我們深思與警惕。

全面還原真相 見招拆招

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，全面還原了數年間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我國的單向透明優勢。360公司創始人周鴻禕表示，只要能迅速發現這種威脅，感知到這種攻擊，那麼就能夠定位溯源，就知道它從哪進來的，知道他們用什麼漏洞進來的，然後就能把它給處置掉，把它清理掉，同時把該修補的漏洞都修補上。

報告認為，西北工業大學此次公開發布遭受境外網絡攻擊的聲明，本着實事求是、絕不姑息的決心，堅決一查到底，積極採取防禦措施的行動值得遍布全球的NSA網絡攻擊活動受害者學習，這將成為世界各國有效防範抵禦NSA後續網絡攻擊行為的有力借鑒。