2022.9.6 星期二
责编:王娟 美编:江佳锲 组版:郝莎莎
现代快报+

西北工业大学遭网络攻击事件调查报告发布

查清了！攻击源头是美国国家安全局

9月5日，国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告，调查发现，美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）多年来对我国国内的网络目标实施了上万次的恶意网络攻击，控制了相关网络设备，疑似窃取了高价值数据。

今年4月，西安市公安机关接到一起网络攻击的报警，西北工业大学的信息系统发现遭受网络攻击的痕迹。校方表示该校系统发现木马程序，企图非法获取权限，给学校的正常工作和生活秩序造成了重大的风险隐患。

西安市公安机关立即组织警力与网络安全技术专家成立联合专案组对此案进行立案侦查。国家计算机病毒应急处理中心和360公司联合组成技术团队，全程参与了此案的技术分析工作。技术团队先后从西北工业大学的多个信息系统和上网终端中提取到了多款木马样本，综合使用国内现有数据资源和分析手段，并得到了欧洲、南亚部分国家合作伙伴的通力支持，全面还原了相关攻击事件的总体概貌、技术特征、攻击武器、攻击路径和攻击源头，初步判明相关攻击活动源自美国国家安全局（NSA）“特定入侵行动办公室”（Office of Tailored Access Operation，简称TAO）。

本次调查还发现，在近年里，美国国家安全局（NSA）下属特定入侵行动办公室（TAO）对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备，包括：网络服务器、上网终端、网络交换机、电话交换机、路由器、防火墙等，窃取了超过140GB的高价值数据。

联合技术团队经过复杂的技术分析与溯源，还原了西北工业大学遭受网络攻击的过程和被窃取的文件，掌握了美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）对中国信息网络实施网络攻击和数据窃密的相关证据，涉及在美国国内对中国直接发起网络攻击的人员13名，以及美国国家安全局（NSA）通过掩护公司为构建网络攻击环境而与美国电信运营商签订的合同60余份、电子文件170余份。

美长期对中国手机用户进行无差别监听

调查报告显示，“特定入侵行动办公室”（TAO）长期对中国的手机用户进行无差别的语音监听，非法窃取手机用户的短信内容，并对其进行无线定位。

外交部：强烈谴责！要求美方立即停止不法行为

5日，外交部发言人毛宁主持例行记者会称，美方先后使用41种专用网络攻击武器装备，对西北工业大学发起攻击窃密行动上千次，窃取了一批核心技术数据。美方还长期对中国的手机用户进行无差别语音监听，非法窃取手机用户的短信内容，并对其进行无线定位。美方的行径严重危害中国国家安全和公民个人信息安全。中方对此强烈谴责，我们要求美方作出解释，并立即停止不法行为。

毛宁强调，网络空间安全是世界各国面临的共同问题，作为拥有最强大网络技术实力的国家，美国应该立即停止利用自身优势对他国进行窃密和攻击，以负责任的态度参与全球网络空间治理，为维护网络安全发挥建设性作用。

综合 央视新闻

视觉中国供图

揭秘

美国安局用了41种网络攻击武器

5日，国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告。报告显示网络攻击源头系美国国家安全局（NSA）。

NSA使用41种网络攻击武器窃取数据

此次调查发现，针对西北工业大学的网络攻击中，美国国家安全局（NSA）下属的特定入侵行动办公室（TAO）使用了40余种不同的专属网络攻击武器，持续对西北工业大学开展攻击窃密，窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。

此次遭受攻击的西北工业大学位于陕西西安，隶属于工业和信息化部，是一所多科性、研究型、开放式大学。是目前我国从事航空、航天、航海工程教育和科学研究领域的重点大学，拥有大量国家顶级科研团队和高端人才，承担国家多个重点科研项目，地位十分特殊，网络安全十分关键。由于其所具有的特殊地位和从事的敏感科学研究，所以才成为此次网络攻击的针对性目标。

调查报告显示，美国国家安全局（NSA）在对西北工业大学的网络攻击行动中，先后使用了41种专用网络攻击武器装备，仅后门工具“狡诈异端犯”（NSA命名）就有14款不同版本。

通过取证分析，技术团队累计发现攻击者在西北工业大学内部渗透的攻击链路多达1100余条、操作的指令序列90余个，并从被入侵的网络设备中定位了多份遭窃取的网络设备配置文件、遭嗅探的网络通信数据及口令、其他类型的日志和密钥文件以及其他与攻击活动相关的主要细节。

技术团队将此次攻击活动中所使用的武器类别分为四大类，具体包括：1.漏洞攻击突破类武器；2. 持久化控制类武器；3. 嗅探窃密类武器；4. 隐蔽消痕类武器。此次调查报告披露，美国国家安全局（NSA）利用大量网络攻击武器，针对我国各行业龙头企业、政府、大学、医疗、科研等机构长期进行秘密黑客攻击活动。

360公司创始人周鸿祎表示，美国国家安全局（NSA）就是瞄准国家的科研机构、政府部门、军工单位、高校这些地方来窃取情报或者窃取数据，它从攻击从策划到部署，到通过很长的跳板，一直到攻到核心岗位里面，持续的时间有的要长达数年。危害非常大，因为我们整个国家都在搞数字化，很多重要的业务都是由数据来驱动，数据一旦被偷窃或破坏，会带来严重风险。

调查同时发现，美国国家安全局（NSA）还利用其控制的网络攻击武器平台、“零日漏洞”（Oday）和网络设备，长期对中国的手机用户进行无差别语音监听，非法窃取手机用户的短信内容，并对其进行无线定位。

NSA掩盖真实IP，先后使用54台跳板机和代理服务器

调查报告披露，美国国家安全局（NSA）做了长时间准备，并且进行了精心伪装。

技术团队分析发现，特定入侵行动办公室（TAO）利用其掌握的针对SunOS操作系统的两个“零日漏洞”利用工具，选择了中国周边国家的教育机构、商业公司等网络应用流量较多的服务器为攻击目标；攻击成功后，即安装NOPEN木马程序，控制了大批跳板机。

特定入侵行动办公室（TAO）在针对西北工业大学的网络攻击行动中先后使用了54台跳板机和代理服务器，主要分布在日本、韩国、瑞典、波兰、乌克兰等17个国家，其中70%位于中国周边国家，如日本、韩国等。其中，用以掩盖真实IP的跳板机都是精心挑选，所有IP均归属于非“五眼联盟”国家。

针对西北工业大学攻击平台所使用的网络资源涉及代理服务器，美国国家安全局（NSA）通过秘密成立的两家掩护公司购买了埃及、荷兰和哥伦比亚等地的IP，并租用一批服务器。相关域名和证书均指向无关联人员，以便掩盖真实攻击平台对西北工业大学等中国信息网络展开的多轮持续性攻击、窃密行动。

技术团队还发现，相关网络攻击活动开始前，美国多家大型知名互联网企业配合将掌握的中国大量通信网络设备的管理权限，提供给美国国家安全局等情报机构，为持续侵入中国国内的重要信息网络大开方便之门。

TAO是什么？是网络攻击窃密活动的战术实施单位

调查报告显示，美国国家安全局（NSA）下属的“特定入侵行动办公室”（TAO）不仅对中国国内的各重点企业和机构实施恶意网络攻击，而且还长期对中国的手机用户进行无差别的语音监听，非法窃取手机用户的短信内容，并对其进行无线定位。那么这个简称TAO的特定入侵行动办公室到底是一个什么机构呢？

经技术分析和网上溯源调查发现，实施此次网络攻击行动的美国国家安全局（NSA）下属特定入侵行动办公室（TAO）部门，成立于1998年，其力量部署主要依托美国国家安全局（NSA）在美国和欧洲的各密码中心。目前已被公布的六个密码中心分别是：

1.国安局马里兰州的米德堡总部

2. 瓦湖岛的国安局夏威夷密码中心（NSAH）

3. 戈登堡的国安局乔治亚密码中心（NSAG）

4. 圣安东尼奥的国安局得克萨斯密码中心（NSAT）

5. 丹佛马克利空军基地的国安局科罗拉罗密码中心（NSAC）

6. 德国达姆施塔特美军基地的国安局欧洲密码中心（NSAE）

特定入侵行动办公室TAO是目前美国政府专门从事对他国实施大规模网络攻击窃密活动的战术实施单位，由2000多名军人和文职人员组成。下设10个单位：

1.远程操作中心，主要负责操作武器平台和工具进入并控制目标系统或网络

2.先进/接入网络技术处，负责研究相关硬件技术，为TAO网络攻击行动提供硬件相关技术和武器装备支持

3.数据网络技术处，负责研发复杂的计算机软件工具，为TAO操作人员执行网络攻击任务提供支撑

4.电信网络技术处，负责研究电信相关技术，为TAO操作人员隐蔽渗透电信网络提供支撑

5.任务基础设施技术处，负责开发与建立网络基础设施和安全监控平台，用于构建攻击行动网络环境与匿名网络

6.接入行动处，负责通过供应链，对拟送达目标的产品进行后门安装

7.需求与定位处，接收各相关单位的任务，确定侦察目标，分析评估情报价值

8.接入技术行动处，负责研发接触式窃密装置，并与美国中央情报局和联邦调查局人员合作，通过人力接触方式将窃密软件或装置安装在目标的计算机和电信系统中

9.S32P：项目计划整合处，负责总体规划与项目管理

10.NWT：网络战小组，负责与133个网络作战小队联络

美国国家安全局NSA针对西北工业大学的攻击窃密行动负责人是罗伯特·乔伊斯。此人于1967年9月13日出生，1989年进入美国国家安全局工作。曾经担任过“特定入侵行动办公室TAO”副主任、主任，现担任美国国家安全局NSA网络安全主管。

360公司网络安全专家边亮表示，目前（TAO）代表了全球网络攻击的最高水平，他们掌握大量攻击武器，相当于有互联网的万能钥匙，可以任意进出目标设备，进行情报窃取或进行破坏等。

你的信息可能被泄露！专家呼吁提高网络安全防范

调查报告显示，一直以来，美国国家安全局（NSA）针对我国各行业龙头企业、政府、大学、医疗机构、科研机构甚至关乎国计民生的重要信息基础设施运维单位等机构长期进行秘密黑客攻击活动。其行为或对我国的国防安全、关键基础设施安全、金融安全、社会安全、生产安全以及公民个人信息造成严重危害，值得我们深思与警惕。

此次西北工业大学联合中国国家计算机病毒应急处理中心与360公司，全面还原了数年间美国国家安全局（NSA）利用网络武器发起的一系列攻击行为，打破了一直以来美国对我国的单向透明优势。360公司创始人周鸿祎表示，只要能迅速发现威胁，就能够定位溯源，知道它从哪来，知道他们用什么漏洞来的，然后就能把它处置掉，清理掉，同时把漏洞都修补上。

调查报告认为，西北工业大学此次公开发布遭受境外网络攻击的声明，本着实事求是、绝不姑息的决心，坚决一查到底，积极采取防御措施的行动值得遍布全球的美国国家安全局（NSA）网络攻击活动受害者学习，这将成为世界各国有效防范抵御美国国家安全局（NSA）后续网络攻击行为的有力借鉴。

据央视新闻