西北工业大学遭美国NSA网络攻击事件调查报告（之一）

2022年6月22日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布《警情通报》，证实在西北工业大学的信息网络中发现了多款源于境外的木马样本，西安警方已对此正式立案调查。

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（以下简称“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，后文简称TAO）。

一、攻击事件概貌

本次调查发现，在近年里，美国NSA下属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（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。TAO利用其网络攻击武器平台、“零日漏洞”（0day）及其控制的网络设备等，持续扩大网络攻击和范围。经技术分析与溯源，技术团队现已澄清TAO攻击活动中使用的网络攻击基础设施、专用武器装备及技战术，还原了攻击过程和被窃取的文件，掌握了美国NSA及其下属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。

二、攻击事件分析

在针对西北工业大学的网络攻击中，TAO使用了40余种不同的NSA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。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、其它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。具体分析情况如下：

（一）相关网络攻击基础设施

为掩护其攻击行动，TAO在开始行动前会进行较长时间的准备工作，主要进行匿名化攻击基础设施的建设。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，安装NOPEN木马程序（详见有关研究报告），控制了大批跳板机。

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。

这些跳板机的功能仅限于指令中转，即：将上一级的跳板指令转发到目标系统，从而掩盖美国国家安全局发起网络攻击的真实IP。目前已经至少掌握TAO从其接入环境（美国国内电信运营商）控制跳板机的四个IP地址，分别为209.59.36.*、69.165.54.*、207.195.240.*和209.118.143.*。同时，为了进一步掩盖跳板机

和代理服务器与NSA之间的关联关系，NSA使用了美国Register公司的匿名保护服务，对相关域名、证书以及注册人等可溯源信息进行匿名化处理，无法通过公开渠道进行查询。

技术团队通过威胁情报数据关联分析，发现针对西北工业大学攻击平台所使用的网络资源共涉及5台代理服务器，NSA通过秘密成立的两家掩护公司向美国泰瑞马克（Terremark）公司购买了埃及、荷兰和哥伦比亚等地的IP地址，并租用一批服务器。这两家公司分别为杰克•史密斯咨询公司（Jackson Smith Consultants）、穆勒多元系统公司（Mueller Diversified Systems）。同时，技术团队还发现，TAO基础设施技术处（MIT）工作人员使用“阿曼达•拉米雷斯（Amanda Ramirez）”的名字匿名购买域名和一份通用的SSL证书（ID：e42d3bea0a16111e67ef79f9cc2*****）。随后，上述域名和证书被部署在位于美国本土的中间人攻击平台“酸狐狸”（Foxacid）上，对中国的大量网络目标开展攻击。特别是，TAO对西北工业大学等中国信息网络目标展开了多轮持续性的攻击、窃密行动。

（二）相关网络攻击武器

TAO在对西北工业大学的网络攻击行动中，先后使用了41种NSA的专用网络攻击武器装备。并且在攻击过程中，TAO会根据目标环境对同一款网络武器进行灵活配置。例如，对西北工业大学实施网络攻击中使用的网络武器中，仅后门工具“狡诈异端犯”（NSA命名）就有14个不同版本。技术团队将此次攻击活动中TAO所使用工具类别分为四大类，具体包括：

1、漏洞攻击突破类武器

TAO依托此类武器对西北工业大学的边界网络设备、网关服务器、办公内网主机等实施攻击突破，同时也用来攻击控制境外跳板机以构建匿名化网络作为行动掩护。此类武器共有3种：

①“剃须刀”

此武器可针对开放了指定RPC服务的X86和SPARC架构的Solarise系统实施远程漏洞攻击，攻击时可自动探知目标系统服务开放情况并智能化选择合适版本的漏洞利用代码，直接获取对目标主机的完整控制权。此武器用于对日本、韩国等国家跳板机的攻击，所控制跳板机被用于对西北工业大学的网络攻击。

②“孤岛”

此武器同样可针对开放了指定RPC服务的Solaris系统实施远程溢出攻击，直接获取对目标主机的完整控制权。与“剃须刀”的不同之处在于此工具不具备自主探测目标服务开放情况的能力，需由使用者手动配置目标及相关参数。NSA使用此武器攻击控制了西北工业大学的边界服务器。

③“酸狐狸”武器平台

此武器平台部署在哥伦比亚，可结合“二次约会”中间人攻击武器使用，可智能化配置漏洞载荷针对IE、FireFox、Safari、Android Webkit等多平台上的主流浏览器开展远程溢出攻击，获取目标系统的控制权（详见：国家计算机病毒应急处理中心《美国国家安全局（NSA）“酸狐狸”漏洞攻击武器平台技术分析报告》）。TAO主要使用该武器平台对西北工业大学办公内网主机进行入侵。

2、持久化控制类武器

TAO依托此类武器对西北工业大学网络进行隐蔽持久控制，TAO行动队可通过加密通道发送控制指令操作此类武器实施对西北工业大学网络的渗透、控制、窃密等行为。此类武器共有6种：

①“二次约会”

此武器长期驻留在网关服务器、边界路由器等网络边界设备及服务器上，可针对海量数据流量进行精准过滤与自动化劫持，实现中间人攻击功能。TAO在西北工业大学边界设备上安置该武器，劫持流经该设备的流量引导至“酸狐狸”平台实施漏洞攻击。

②“NOPEN”

此武器是一种支持多种操作系统和不同体系架构的远控木马，可通过加密隧道接收指令执行文件管理、进程管理、系统命令执行等多种操作，并且本身具备权限提升和持久化能力（详见：国家计算机病毒应急处理中心《“NOPEN”远控木马分析报告》）。TAO主要使用该武器对西北工业大学网络内部的核心业务服务器和关键网络设备实施持久化控制。

③“怒火喷射”

此武器是一款基于Windows系统的支持多种操作系统和不同体系架构的远控木马，可根据目标系统环境定制化生成不同类型的木马服务端，服务端本身具备极强的抗分析、反调试能力。TAO主要使用该武器配合“酸狐狸”平台对西北工业大学办公网内部的个人主机实施持久化控制。

④“狡诈异端犯”

此武器是一款轻量级的后门植入工具，运行后即自删除，具备权限提升能力，持久驻留于目标设备上并可随系统启动。TAO主要使用该武器实现持久驻留，以便在合适时机建立加密管道上传NOPEN木马，保障对西北工业大学信息网络的长期控制。

⑤“坚忍外科医生”

此武器是一款针对Linux、Solaris、JunOS、FreeBSD等4种类型操作系统的后门，该武器可持久化运行于目标设备上，根据指令对目标设备上的指定文件、目录、进程等进行隐藏。TAO主要使用该武器隐藏NOPEN木马的文件和进程，避免其被监控发现。技术分析发现，TAO在对西北工业大学的网络攻击中，累计使用了该武器的12个不同版本。

3、嗅探窃密类武器

TAO依托此类武器嗅探西北工业大学工作人员运维网络时使用的账号口令、命令行操作记录，窃取西北工业大学网络内部的敏感信息和运维数据等。此类武器共有两种：

①“饮茶”

此武器可长期驻留在32位或64位的Solaris系统中，通过嗅探进程间通信的方式获取ssh、telnet、rlogin等多种远程登录方式下暴露的账号口令。TAO主要使用该武器嗅探西北工业大学业务人员实施运维工作时产生的账号口令、命令行操作记录、日志文件等，压缩加密存储后供NOPEN木马下载。

②“敌后行动”系列武器

此系列武器是专门针对电信运营商特定业务系统使用的工具，根据被控业务设备的不同类型，“敌后行动”会与不同的解析工具配合使用。TAO在对西北工业大学的网络攻击中使用了“魔法学校”、“小丑食物”和“诅咒之火”等3类针对电信运营商的攻击窃密工具。

4、隐蔽消痕类武器

TAO依托此类武器消除其在西北工业大学网络内部的行为痕迹，隐藏、掩饰其恶意操作和窃密行为，同时为上述三类武器提供保护。现已发现1种此类武器：

“吐司面包”，此武器可用于查看、修改utmp、wtmp、lastlog等日志文件以清除操作痕迹。TAO主要使用该武器清除、替换被控西北工业大学上网设备上的各类日志文件，隐藏其恶意行为。TAO对西北工业大学的网络攻击中共使用了3款不同版本的“吐司面包”。

三、攻击溯源

技术团队结合上述技术分析结果和溯源调查情况，初步判断对西北工业大学实施网络攻击行动的是美国国家安全局（NSA）信息情报部（代号S）数据侦察局（代号S3）下属TAO（代号S32）部门。该部门成立于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、美国马里兰州米德堡的NSA总部；

2、美国夏威夷瓦胡岛的NSA夏威夷密码中心（NSAH）；

3、美国佐治亚州戈登堡的NSA佐治亚密码中心（NSAG）；

4、美国德克萨斯州圣安东尼奥的NSA德克萨斯密码中心（NSAT）；

5、美国科罗拉罗州丹佛马克利空军基地的NSA科罗拉罗密码中心（NSAC）；

6、德国达姆施塔特美军基地的NSA欧洲密码中心（NSAE）。

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，其内设机构包括：

第一处：远程操作中心（ROC，代号S321），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。

第二处：先进/接入网络技术处（ANT，代号S322），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。

第三处：数据网络技术处（DNT，代号S323），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。

第四处：电信网络技术处（TNT，代号S324），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。

第五处：任务基础设施技术处（MIT，代号S325），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。

第六处：接入行动处（ATO，代号S326），负责通过供应链，对拟送达目标的产品进行后门安装。

第七处：需求与定位处（R&T，代号S327），接收各相关单位的任务，确定侦察目标，分析评估情报价值。

S32P：项目计划整合处（PPI，代号S32P），负责总体规划与项目管理。

NWT：网络战小组（NWT），负责与网络作战小队联络。

美国国家安全局（NSA）针对西北工业大学的攻击行动代号为“阻击XXXX”（shotXXXX）。该行动由TAO负责人直接指挥，由MIT（S325）负责构建侦察环境、租用攻击资源；由R&T（S327）负责确定攻击行动战略和情报评估；由ANT（S322）、DNT（S323）、TNT（S324）负责提供技术支撑；由ROC（S321）负责组织开展攻击侦察行动。由此可见，直接参与指挥与行动的主要包括TAO负责人，S321和S325单位。

NSA对西北工业大学攻击窃密期间的TAO负责人是罗伯特•乔伊斯（Robert Edward Joyce）。此人于1967年9月13日出生，曾就读于汉尼拔高中，1989年毕业于克拉克森大学，获学士学位，1993年毕业于约翰斯•霍普金斯大学，获硕士学位。1989年进入美国国家安全局工作。曾经担任过TAO副主任，2013年至2017年担任TAO主任。2017年10月开始担任代理美国国土安全顾问。2018年4月至5月，担任美国白宫国务安全顾问，后回到NSA担任美国国家安全局局长网络安全战略高级顾问，现担任NSA网络安全主管。

四、总结

本次报告基于国家计算机病毒应急处理中心与360公司联合技术团队的分析成果，揭露了美国NSA长期以来针对包括西北工业大学在内的中国信息网络用户和重要单位开展网络间谍活动的真相。后续技术团队还将陆续公布相关事件调查的更多技术细节。