关于西北军工高校发现美丽国 NSA 网络攻击--调查报告篇

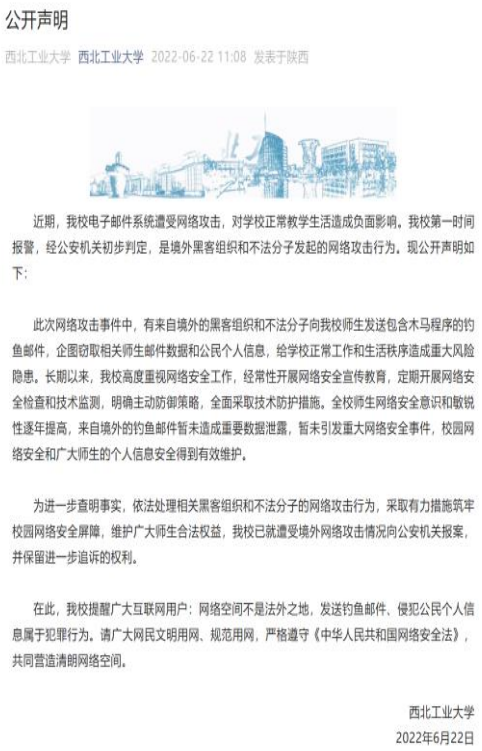
---本报告来自于《百度百科》

关于西北军工高校发现美丽国 NSA 网络攻击调查报告，是某互联网安全大厂于 2022 年 9 月 5 日发布的报告。

2022 年 6 月 22-日，西北军工高校发布《公开声明》称，该校遭受境外网络攻击。

2022 年 9 月 5 日，关于西北军工高校发现美丽国 NSA 网络攻击调查报告（之一）发布。

2022 年 9 月 27 日，《西北军工高校遭美丽国 NSA 网络攻击事件调查报告（之二）》发布，进一步揭露了美丽国对西北军工高校组织网络攻击的目的：渗透控制中国基础设施核心设备，窃取中国用户隐私数据。



公开声明

西北工业大学 西北工业大学 2022-06-22 11:08 发表于陕西

近期，我校电子邮件系统遭受网络攻击，对学校正常教学生活造成负面影响。我校第一时间报警，经公安机关初步判定，是境外黑客组织和不法分子发起的网络攻击行为。现公开声明如下：

此次网络攻击事件中，有来自境外的黑客组织和不法分子向我校师生发送包含木马程序的钓鱼邮件，企图窃取相关师生邮件数据和公民个人信息，给学校正常工作和生活秩序造成重大风险隐患。长期以来，我校高度重视网络安全工作，经常性开展网络安全宣传教育，定期开展网络安全检查和技术监测，明确主动防御策略，全面采取技术防护措施。全校师生网络安全意识和敏锐性逐年提高，来自境外的钓鱼邮件暂未造成重要数据泄露，暂未引发重大网络安全事件，校园网络安全和广大师生的个人信息安全得到有效维护。

为进一步查明事实，依法处理相关黑客组织和不法分子的网络攻击行为，采取有力措施筑牢校园网络安全屏障，维护广大师生合法权益，我校已就遭受境外网络攻击情况向公安机关报案，并保留进一步追诉的权利。

在此，我校提醒广大互联网用户：网络空间不是法外之地，发送钓鱼邮件、侵犯公民个人信息属于犯罪行为。请广大网民文明用网、规范用网，严格遵守《中华人民共和国网络安全法》，共同营造清朗网络空间。

西北工业大学

2022年6月22日

事件历程

2022 年 6 月 22 日，西北军工高校发布《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》，证实在西北军工高校的信息网络中发现了多款源于境外的**木马程序样本**，西安警方已对此正式立案调查。

中国国家计算机病毒应急处理中心和某互联网安全大厂第一时间成立技术团队开展调查工作，全程参与此案技术分析。技术团队先后从多个信息系统和上网终端中捕获到了木马程序样本，综合使用国内现有数据资源和分析手段，并得到欧洲、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丽国国家安全局（NSA）的“特定入侵行动办公室”（Office of Tailored Access Operation，后文简称 TAO）。**

该系列研究报告将公布美丽国国家安全局（NSA）“**信号特定入侵行动办公室”（TAO）**对西北军工高校发起的**上千次**网络攻击活动中，某些特定攻击活动的重要细节，为全球各国有效防范和发现 TAO 的后续网络攻击行为提供可以借鉴的案例。

2022 年 9 月 5 日，关于西北军工高校发现美丽国 NSA 网络攻击调查报告（之一）发布。

2022 年 9 月，《环球时报》记者从有关部门独家获悉，美丽国国家安全局（NSA）“特定入侵行动办公室”（TAO）在对西北军工高校发起网络攻击的过程中构建了对**中国电信运营商核心数据网络远程访问的“合法”通道**，对**我电信基础设施渗透控制**。技术人员根据 TAO 攻击方式、渗透工具、木马样本等特征深入分析，发现 TAO 非法攻击渗透中国境内某电信运营商，构建了对核心数据网络远程访问的“合法”通道，对我电信基础设施渗透控制。

2023 年 9 月，国家计算机病毒应急处理中心和某互联网安全大厂对**一款名为“二次约会”的间谍软件**进行了技术分析，分析报告显示，该软件是美丽国国家安全局（NSA）开发的网络间谍武器。据了解，在国家计算机病毒应急处理中心会同某互联网安全大厂配合侦办西北军工高校被美丽国国家安全局（NSA）网络攻击案过程中，**成功提取了这款间谍软件的多个样本**，并锁定了

这起网络间谍行动背后美丽国国家安全局（NSA）工作人员的真实身份。在多国业内伙伴的通力配合下，国家计算机病毒应急处理中心的联合调查工作取得了突破性进展。已经成功锁定了针对西北军工高校发动网络攻击的美丽国国家安全局（NSA）相关工作人员的真实身份。

报告全文

报告一

一、攻击事件概貌

分析发现，美丽国 NSA 的“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**，控制了相关网络设备（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），疑似**窃取了高价值数据**。与此同时，美丽国 NSA 还利用其控制的**网络攻击武器平台、“零日漏洞”（0day）和网络设备**，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。经过复杂的技术分析与溯源，技术团队现已澄清 NSA 攻击活动中使用的**网络资源、专用武器装备及具体手法，还原了攻击过程和被窃取的文件**，掌握了美丽国 NSA“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**证据链**。

二、攻击组织基本情况

经技术分析和网上溯源调查发现，此次网络攻击行动是美丽国国家安全局（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丽国国家安全局（NSA）在美丽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德克萨斯密码中心（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）。

TAO 是目前美丽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：

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（AO，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。

第八处：接入技术行动处（ATO，编号 S328）

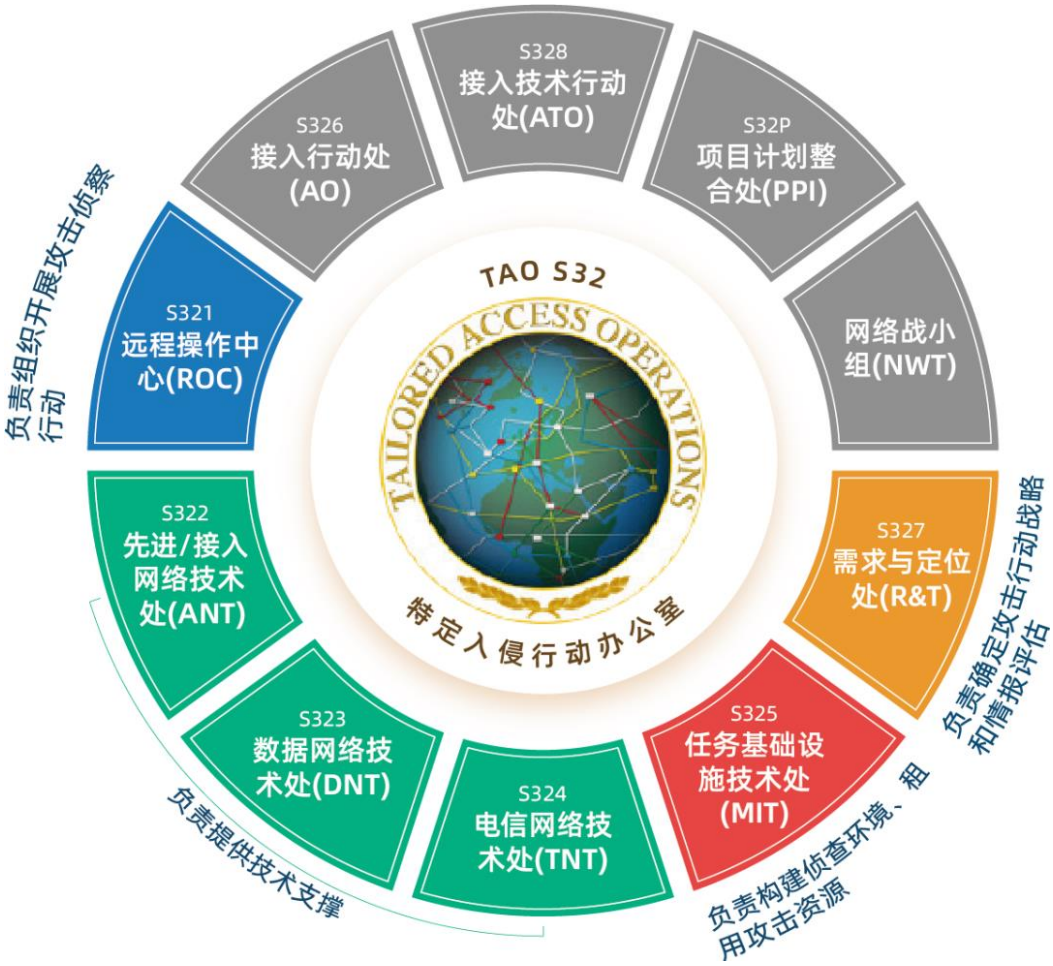
负责研发接触式窃密装置，并与美丽国中央情报局和联邦调查局人员合作，通过人力接触方式将窃密软件或装置安装在目标的计算机和电信系统中。

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 133 个网络作战小队联络。



图一 TAO 组织架构及参与“阻击 XXXX”行动的 TAO 子部门

此案在美丽国国家安全局（NSA）内部攻击行动代号为“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 窃密期间的 TAO 负责人是罗伯特·乔伊斯（Robert Edward Joyce）。此人 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·霍普金斯大学，获硕士学位。1989 年进入美丽国国家安全局工作。曾经担任过 TAO 副主任，2013 年至 2017 年担任 TAO 主任。2017 年 10 月开始担任代理美丽国国土安全顾问。2018 年 4 月至 5 月，担任美丽国白宫国务安全顾问，后回到 NSA 担任美丽国国家安全局局长网络安全战略高级顾问，现担任 NSA 网络安全局主管。

图二 罗伯特•乔伊斯（Robert E. Joyce）原 TA

三、TAO 网络攻击实际情况

美丽国国家安全局 TAO 部门的 S325 单位，通过层层掩护，构建了由 **49 台跳板机和 5 台代理服务器组成的匿名网络**，**购买专用网络资源**，**架设攻击平台**。S321 单位运用 40 余种不同的 NSA 专属网络攻击武器，持续对我国开展攻击窃密，窃取了关键网络设备配置、网管数据、运维数据等核心技术数据，窃密活动持续时间长，覆盖范围广。技术分析中还发现，TAO 已于此次攻击活动开始前，在美丽国多家大型知名互联网企业的配合下，**掌握了中国大量通信网络设备的管理权限**，为 NSA 持续侵入中国国内的重要信息网络大开方便之门。

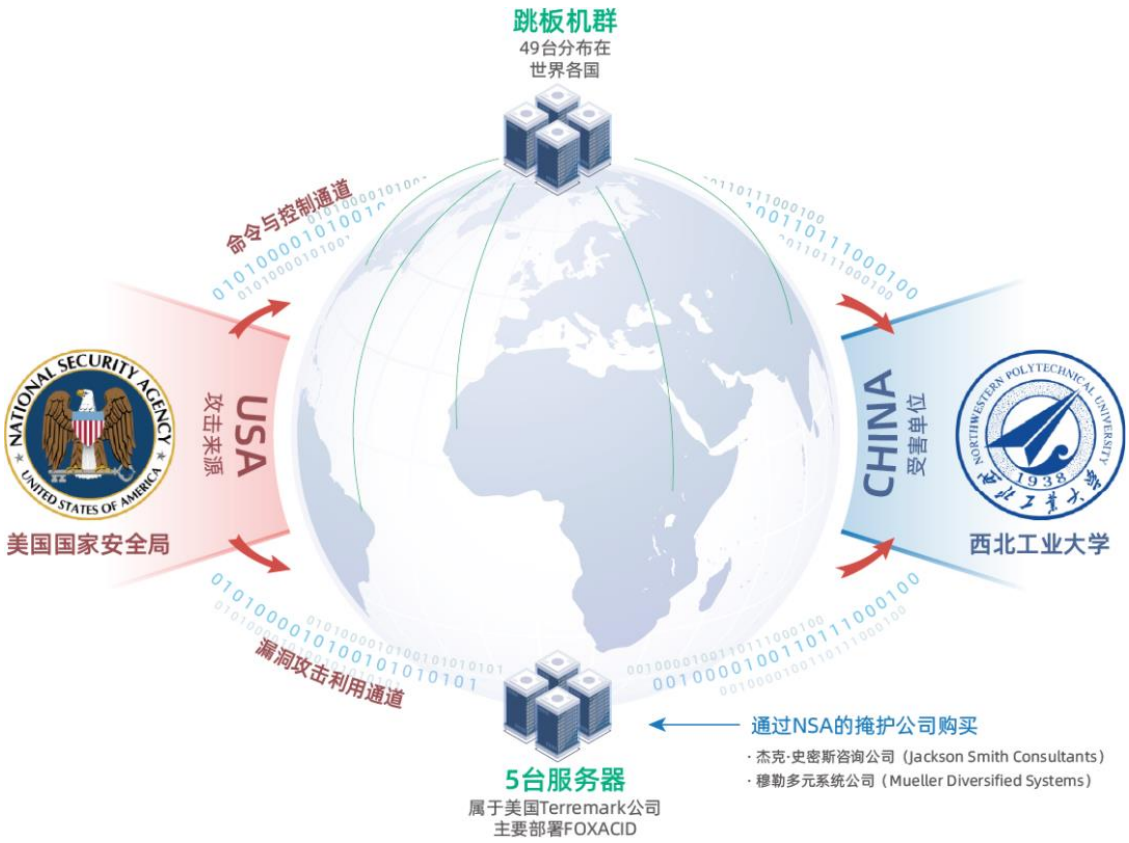
经**溯源分析**，技术团队现已全部还原了 NSA 的**攻击窃密过程**，澄清其在西北军工高校内部渗透的**攻击链路 1100 余条**、**操作的指令序列 90 余个**，**多份遭窃取的网络设备配置文件**，**嗅探的网络通信数据及口令、其它类型的日志和密**

钥文件，基本还原了每一次攻击的主要细节。掌握并固定了多条相关证据链，涉及在美丽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丽国电信运营商签订的合同 60 余份，电子文件 170 余份。

四、NSA 攻击网络的构建

经技术团队溯源分析发现，美丽国国家安全局 TAO 部门对西北军工高校的网络攻击行动先后使用了 **49 台跳板机**，这些跳板机均经过精心挑选，所有 IP 均归属于**非“五眼联盟”国家**，而且大部分选择了**中国周边国家（如日本、韩国等）的 IP**，约占 70%。

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（已提取样本）**，工具名称分别为 **EXTREMEPARR（NSA 命名）**和 **EBBISLAND（NSA 命名）**，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（NSA 命名，已提取样本）后门，控制了大批跳板机**。



图三 美丽国国家安全局（NSA）对西北军工高校实施网络攻击

根据溯源分析，本次窃密行动共选用了其中的 49 台跳板机，这些跳板机仅**使用了中转指令，将上一级的跳板指令转发到目标系统，从而掩盖美丽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 攻击实施者从其接入环境（美丽国国内电信运营商）控制跳板机的四个 IP：

209.59.36.*

69.165.54.*

207.195.240.*

209.118.143.*

TAO 基础设施技术处（MIT）人员通过将匿名购买的域名和 SSL 证书部署在位于美丽国本土的**中间人攻击平台“酸狐狸”（FOXACID，NSA 命名）**上，对中国境内的大量网络目标开展攻击。特别值得关注的是，NSA 利用上述域名和证书部署的平台，对西北军工高校等中国信息网络展开了多轮持续性的攻击、窃密行动。

美丽国国家安全局 NSA 为了保护其身份安全，使用了美丽国 Register 公司的匿名保护服务，相关域名和证书无明确指向，无关联人员。

TAO 为了掩盖其攻击来源，并保护工具的安全，对需要长期驻留互联网的攻击平台，通过掩护公司向服务商购买服务。

针对西北军工高校攻击平台所使用的网络资源共涉及 5 台代理服务器，NSA 通过两家掩护公司向美丽国泰瑞马克（Terremark）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。

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）。

五、TAO 的武器装备分析

技术分析发现，TAO 先后使用了 **41 种 NSA 的专用网络攻击武器装备**，通过分布于**日本、韩国、瑞典、波兰、乌克兰等 17 个国家的 49 台跳板机**和 **5 台代理服务器**，对西北军工高校发起了攻击窃密行动上千次，窃取了一批网络数据。

美丽国国家安全局 TAO 的网络攻击武器装备针对性强，得到了美丽国互联网巨头的鼎力支持。同一款装备会根据目标环境进行灵活配置，在这中使用的**41 款装备**中，仅**后门工具“狡诈异端犯”（NSA 命名）**在对西北军工高校的网络攻击中就有 **14 款不同版本**。

NSA 所使用工具类别主要分为四大类，分别是：

（一）漏洞攻击突破类武器

TAO 依托此类武器对西北军工高校的边界网络设备、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网络。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 Solaris 系统实施远程溢出攻击，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军工高校的网络攻击。

2.“孤岛”

此武器同样可针对开放了制定 **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”工具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，需由使用者手动选择欲打击的目标服务。

NSA 使用此武器攻击控制了西北军工高校的边界服务器。

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。

TAO 主要使用该武器平台对西北军工高校**办公内网主机**开展突破攻击。

（二）持久化控制类武器

TAO 依托此类武器对西北军工高校网络进行**隐蔽持久控制**，TAO 工作人员可通过**加密通道发送控制指令操作**此类武器实施对西北军工高校网络的**渗透、控制、窃密**等行为。此类武器共有 5 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 在西北军工高校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”木马

此武器是一种支持**多种操作系统和不同体系架构**的**控守型木马**，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。

TAO 主要使用该武器对西北军工高校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控守型木马，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”平台对西北军工高校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，具备提权功能，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，保障对西北军工高校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。

TAO 在对西北军工高校的网络攻击中共使用该武器的 **12 个不同版本**。

（三）嗅探窃密类武器

TAO 依托此类武器嗅探西北军工高校工作人员运维网络时使用的账号口令、生成的操作记录，窃取西北军工高校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军工高校业务人员实施运维工作时产生的账号口令、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。

在对西北军工高校运维管道的攻击中共使用了“魔法学校”、“小丑食物”和“诅咒之火”等 3 类针对运营商的攻击窃密工具。

（四）隐蔽消痕类武器

TAO 依托此类武器消除其在西北军工高校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。

现已发现的此类武器共有 1 种：

1.“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、替换被控西北军工高校上网设备上的各类日志文件，隐藏其恶意行为**。

TAO 对西北军工高校的网络攻击中共使用了 3 款不同版本的“吐司面包”。

小结

一直以来，美丽国国家安全局（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。

此次西北军工高校联合中国国家计算机病毒应急处理中心与某互联网安全大厂，全面还原了数年间美丽国 NSA 利用网络武器发起的一系列攻击行为，打破了一直以来美丽国对我国的单向透明优势。面对国家级背景的强大对手，首先要知道风险在哪，是什么样的风险，什么时候的风险，从此次美丽国 NSA 攻击事件也可证明，看不见就要挨打。这是一次三方集中精力联手攻克“看见”难题的成功实践，帮助国家真正感知风险、看见威胁、抵御攻击，一举将境外黑客攻击暴露在阳光下。

西北军工高校公开发布遭受境外网络攻击的声明，体现了其对国家负责、对学校负责、对社会负责的精神，本着实事求是、绝不姑息的决心，坚决一查到底。其积极采取防御措施的行动更是值得遍布全球的 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丽国 NSA 后续网络攻击行为的有力借鉴。

报告二

技术团队先后从西北军工高校的多个信息系统和上网终端中提取到了木马程序样本，综合使用国内现有数据资源和分析手段，并得到欧洲、东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于美丽国国家安全局（NSA）的“特定入侵行动办公室”（即：Office of Tailored Access Operation，后文简称“TAO”）。

本系列研究报告将公布 TAO 对西北军工高校发起的上千次网络攻击活动中，某些特定攻击活动的重要细节，为全球各国有效发现和防范 TAO 的后续网络攻击行为提供可以借鉴的案例。

一、TAO 攻击渗透西北军工高校的流程

TAO 对他国发起的网络攻击技战术针对性强，采取**半自动化攻击流程**，**单点突破**、**逐步渗透**、**长期窃密**。

（一）单点突破、级联渗透，控制西北军工高校网络

经过长期的精心准备，TAO 使用**“酸狐狸”平台**对西北军工高校内部主机和服务器实施**中间人劫持攻击**，部署**“怒火喷射”远程控制武器**，控制多台关键服务器。利用**木马级联控制渗透的方式**，向西北军工高校内部网络深度渗透，先后控制运维网、办公网的核心网络设备、服务器及终端，并获取了部分西北军工高校内部**路由器、交换机等重要网络节点设备的控制权**，窃取身份验证数据，并进一步实施渗透拓展，最终达成了对西北军工高校内部网络的隐蔽控制。

（二）隐蔽驻留、“合法”监控，窃取核心运维数据

TAO 将作战行动掩护武器**“精准外科医生”**与**远程控制木马 NOPEN** 配合使用，实现进程、文件和操作行为的全面“隐身”，长期隐蔽控制西北军工高校的**运维管理服务器**，同时采取**替换 3 个原系统文件和 3 类系统日志的方式**，**消痕隐身，规避溯源**。TAO 先后从该服务器中窃取了**多份网络设备配置文件**。利用窃取到的配置文件，TAO 远程“合法”监控了一批网络设备和互联网用户，为后续对这些目标实施拓展渗透提供数据支持。

（三）搜集身份验证数据、构建通道，渗透基础设施

TAO 通过窃取西北军工高校**运维和技术人员远程业务管理的账号口令、操作记录以及系统日志**等关键敏感数据，掌握了一批**网络边界设备账号口令**、业务设备访问权限、路由器等设备配置信息、FTP 服务器文档资料信息。根据 TAO 攻击链路、渗透方式、木马样本等特征，关联发现 TAO 非法攻击渗透中国境内的基础设施运营商，构建了对基础设施运营商核心数据网络远程访问的**“合法”通道**，实现了对中国基础设施的渗透控制。

（四）控制重要业务系统，实施用户数据窃取

TAO 通过掌握的中国基础设施运营商的思科 PIX 防火墙、TRX 防火墙等设备的账号口令，以**“合法”身份进入运营商网络**，随后实施内网渗透拓展，分别控制相关运营商的服务质量监控系统和短信网关服务器，利用“魔法学校”等专门针对运营商设备的武器工具，查询了一批**中国境内敏感身份人员**，并将**用户信息打包加密后经多级跳板回传至美丽国国家安全局总部**。

二、窃取西北军工高校和中国运营商敏感信息

（一）窃取西北军工高校远程业务管理账号口令、操作记录等关键敏感数据

TAO 通过在西北军工高校运维管理服务器安装**嗅探工具“饮茶”**，长期隐蔽嗅探窃取西北军工高校**运维管理人员远程维护管理信息**，包含网络边界设备账号口令、业务设备访问权限、路由器等设备配置信息等。

遭到嗅探的网络设备类型包括固定互联网的接入网设备（路由器、认证服务器等）、核心网设备（核心路由器、交换机、防火墙等），也包括通信基础设施运营企业的重要设备（数据服务平台等），内容包括账号、口令、设备配置、网络配置等信息。

1、窃取西工大核心网络设备账号口令及配置信息

北京时间 20××年 12 月 11 日 6 时 52 分，TAO 以位于**日本京都大学的代理服务器**（IP：130.54.××.××）为**攻击跳板**，非法入侵了西北军工高校运维网络的“telnet”管理服务器，**上传并安装 NOPEN 木马**，然后**级联控制其内网监控管理**

服务器，上述 2 台服务器事先均已被安装“饮茶”嗅探工具。TAO 远程操控木马检索并下载被压缩加密的监听记录文件，然后清痕退出。窃取数据包括路由器、核心网设备（核心路由器、交换机、防火墙）管理账号、口令、设备配置、网络配置等信息。

2、多次窃取接入网认证设备账号口令及配置信息

（1）北京时间 20××年 5 月 30 日 0 时 28 分，TAO 以位于日本的代理服务器（IP：210.135.××.××）为攻击跳板，非法入侵了西北军工高校运维网络“telnet”管理服务器，上传并安装 NOPEN 木马，然后级联控制其内网监控管理服务器，这 2 台服务器事先均已被安装“饮茶”嗅探工具，TAO 远程操控木马检索并下载窃密记录文件后清痕退出。窃取数据包括接入网认证设备的账号、口令及配置信息。

（2）北京时间 20××年 7 月 4 日 1 时 12 分，TAO 利用位于德国莱比锡技术经济和文化学院的代理服务器（IP：141.57.××.××）作为攻击跳板，非法入侵西北军工高校运维网络“telnet”管理服务器，上传并安装 NOPEN 木马工具，级联控制其内网监控管理服务器等其他 3 台服务器，这 4 台服务器事先均已被安装“饮茶”嗅探工具，TAO 远程操控木马检索并下载窃密文件后清痕退出。

（3）北京时间 20××年 10 月 11 日 10 时 35 分，TAO 利用位于韩国首尔国立江原大学的代理服务器（IP：210.115.××.××）作为攻击跳板，非法入侵西北军工高校运维网络监控管理服务器，上传并安装 NOPEN 木马工具，然后级联控制其内网备份服务器、认证服务器等其他 4 台服务器，这 5 台服务器事先均已被安装“饮茶”嗅探工具，TAO 远程操控木马分别检索并下载窃取记录文件后清痕退出。

（4）北京时间 20××年 10 月 19 日 2 时 46 分，TAO 以位于韩国大田的高等科学技术研究学院的代理服务器（IP：143.248.××.××）为攻击跳板，非法入侵西北军工高校运维网络“telnet”管理服务器，级联控制其内网监管服务器等其他 2 台服务器，这 3 台服务器事先均已被安装“饮茶”嗅探工具，TAO 通过远程操控木马检索并下载窃密文件，然后清痕退出。

（二）窃取西北军工高校网络设备运维配置文件和日志文件

美丽国国家安全局“特定入侵行动办公室”（TAO）长期攻击入侵西北军工高校网络运维管理服务器，秘密窃取网络设备运维配置文件和日志文件。

1、窃取西北军工高校网络运行日志文件

北京时间 20××年 3 月 2 日 3 时 41 分，TAO 通过位于日本的代理服务器（IP：210.135.××.××）非法入侵控制西北军工高校 1 台网络运维管理服务器。3 时 49 分，TAO 从该运维管理服务器横向移动到另一台运维监控服务器，以特定字符串为关键词检索日志文件并进行窃取了一批系统运行日志文件和系统日常自检报告备份文件。

2、窃取西北军工高校服务器定期任务配置脚本

北京时间 20××年 10 月 11 日 10 时 41 分，TAO 通过位于韩国的代理服务器（IP：210.115.××.××）入侵控制了西北军工高校一台内网服务器。10 时 48 分，TAO 经过两次横向移动，入侵了另一台内网服务器，访问了特定目录下的定期任务配置脚本，共检索到 14 个用于定期执行任务的配置文件。随后，一次性窃取了这 14 个文件，这些文件可用于执行定期清理、备份、检查电源等操作。

3、窃取西北军工高校公司服务器系统信息文件

北京时间 20××年 6 月 6 日 1 时 27 分，TAO 通过位于韩国的代理服务器（IP：222.122.××.××）入侵控制了西北军工高校一台内网服务器。2 时 4 分，TAO 经过两次横向移动，入侵了另一台内网服务器，访问了目录/var/下的系统文件，窃取了 60 个常用的系统信息文件，被窃取的系统信息文件内容包含系统发行版本、用户密码哈希、用户权限、本地域名解析配置等。

（三）渗透控制中国基础设施核心设备

美丽国国家安全局“特定入侵行动办公室”（TAO）利用窃取到的网络设备账号口令，以“合法”身份进入中国某基础设施运营商服务网络，控制相关服务质量监控系统，窃取用户隐私数据。

1、窃取中国用户隐私数据

北京时间 20××年 3 月 7 日 22 时 53 分，美丽国国家安全局“特定入侵行动办公室”（TAO）通过位于墨西哥的攻击代理 148.208.××.××，攻击控制中国某基础设施运营商的业务服务器 211.136.××.××，通过两次内网横向移动（10.223.140.××、10.223.14.××）后，攻击控制了**用户数据库服务器，非法查询多名身份敏感人员**的用户信息。

同日 15 时 02 分，TAO 将查询到的用户数据保存在被攻击服务器 /var/tmp/.2e434fd8aeae73e1/erf/out/f/目录下，被打包回传至攻击跳板，随后窃密过程中上传的渗透工具、用户数据等攻击痕迹被专用工具快速清除。

美丽国国家安全局“特定入侵行动办公室”（TAO）运用同样的手法，分别于北京时间 20××年 1 月 10 日 23 时 22 分、1 月 29 日 8 时 41 分、3 月 28 日 22 时 00 分、6 月 6 日 23 时 58 分，攻击控制**另外 1 家中国基础设施业务服务器，非法多批次查询、导出、窃取多名身份敏感人员的用户信息**。

2、渗透控制全球电信基础设施

据分析，美丽国国家安全局“特定入侵行动办公室”（TAO）以上述手法，利用相同的武器工具组合，**“合法”控制了全球不少于 80 个国家的电信基础设施网络**。技术团队与欧洲和东南亚国家的合作伙伴通力协作，成功提取并固定了上述武器工具样本，并成功完成了技术分析，拟适时对外公布，协助全球共同抵御和防范美丽国国家安全局 NSA 的网络渗透攻击。

三、TAO 在攻击过程中暴露身份的相关情况

美丽国国家安全局“特定入侵行动办公室”（TAO）在网络攻击西北军工高校过程中，暴露出多项技术漏洞，**多次出现操作失误**，相关证据进一步证明对西北军工高校实施网络攻击窃密行动的幕后黑手即为美丽国国家安全局 NSA。兹摘要举例如下：

（一）攻击时间完全吻合美丽国工作作息时间规律

美丽国国家安全局“特定入侵行动办公室”（TAO）在使用 tipoff 激活指令和远程控制 NOPEN 木马时，必须通过手动操作，从这两类工具的攻击时间可以分析出**网络攻击者的实际工作时间**。

首先，根据对相关网络攻击行为的大数据分析，对西北军工高校的网络攻击行动 98%集中在北京时间 21 时至凌晨 4 时之间，该时段对应着美丽国东部时间 9 时至 16 时，属于美丽国国内的工作时间段。其次，美丽国时间的全部周六、周日中，均未发生对西北军工高校的网络攻击行动。第三，分析美丽国特有的节假日，发现美丽国的“阵亡将士纪念日”放假 3 天，美丽国“独立日”放假 1 天，在这四天中攻击方没有实施任何攻击窃密行动。第四，长时间对攻击行为密切跟踪发现，在历年圣诞节期间，所有网络攻击活动都处于静默状态。依据上述工作时间和节假日安排进行判断，针对西北军工高校的攻击窃密者都是按照美丽国国内工作日的时间安排进行活动的，肆无忌惮，毫不掩饰。

（二）语言行为习惯与美丽国密切关联

技术团队在对网络攻击者长时间追踪和反渗透过程中（略）发现，攻击者具有以下语言特征：一是攻击者有使用**美式英语**的习惯；二是与攻击者相关联的上网设备均**安装英文操作系统及各类英文版应用程序**；三是**攻击者使用美式键盘进行输入**。

（三）武器操作失误暴露工作路径

20××年 5 月 16 日 5 时 36 分（北京时间），对西北军工高校实施网络攻击人员利用位于**韩国的跳板机**（IP:222.122.××.××），并使用 NOPEN 木马再次攻击西北军工高校。在对西北军工高校内网实施第三级渗透后试图入侵控制一台网络设备时，在运行**上传 PY 脚本工具时出现人为失误**，未修改指定参数。脚本执行后返回出错信息，信息中**暴露出攻击者上网终端的工作目录和相应的文件名**，从中可知木马控制端的系统环境为 Linux 系统，且相应目录名“/etc/autoutils”系 **TAO 网络攻击武器工具目录的专用名称（autoutils）**。

出错信息如下：

Quantifier follows nothing in regex; marked by -- HERE in m/* - HERE .log/ at ../etc/autoutils line 4569

（四）大量武器与遭曝光的 NSA 武器基因高度同源

此次被捕获的、对西北军工高校攻击窃密中所用的 **41 款不同的网络攻击武器工具**中，有 **16 款工具与“影子经纪人”曝光的 TAO 武器完全一致**；有 **23 款**

工具虽然与“影子经纪人”曝光的工具不完全相同，但其基因相似度高达 97%，属于同一类武器，只是相关配置不相同；另有 2 款工具无法与“影子经纪人”曝光工具进行对应，但这 2 款工具需要与 TAO 的其它网络攻击武器工具配合使用，因此**这批武器工具明显具有同源性，都归属于 TAO**。

（五）部分网络攻击行为发生在“影子经纪人”曝光之前

技术团队综合分析发现，在对中国目标实施的上万次网络攻击，特别是对西北军工高校发起的上千次网络攻击中，部分攻击过程中使用的武器攻击，在“影子经纪人”曝光 NSA 武器装备前便完成了木马植入。**按照 NSA 的行为习惯，上述武器工具大概率由 TAO 雇员自己使用**。

四、TAO 网络攻击西北军工高校武器平台 IP 列表

技术分析与溯源调查中，技术团队发现了一批 TAO 在网络入侵西北军工高校的行动中托管所用相关武器装备的服务器 IP 地址，举例如下：

五、TAO 网络攻击西北军工高校所用跳板 IP 列表

研究团队经过持续攻坚，成功锁定了 TAO 对西北军工高校实施网络攻击的**目标节点、多级跳板、主控平台、加密隧道、攻击武器**和**发起攻击的原始终端**，发现了**攻击实施者的身份线索**，并成功查明了 13 名攻击者的真实身份。