西工大遭美国NSA网络攻击事件分析

姓名：任宇 学号：33920212204567

2022年6月，位于中国西安的西北工业大学遭受了一系列网络攻击。据报告，这次网络攻击事件被判定为是由美国国家安全局（NSA）下属的“特定入侵行动办公室”（TAO）发起的。在这起事件中，TAO使用40余种网络攻击武器长时间隐秘地控制了目标网络并窃取了大量敏感数据。

根据中国国家计算机病毒应急处理中心和360公司的调查，此次攻击主要利用了以下攻击策略：

1. 零日漏洞利用：零日漏洞是指攻击者在软件厂商修补漏洞之前发现并利用的漏洞。在这次攻击中，TAO使用了至少两个针对SunOS Unix-based操作系统的零日漏洞，这种策略允许攻击者未经授权地访问或控制受影响的系统。零日漏洞的利用显示了攻击者拥有高级技术能力，能够发现并利用尚未公开的安全漏洞。在​攻击目标服务器成功后，TAO通过安装NOPEN木马程序控制了大批跳板机以供后续攻击使用。
2. 使用网络代理服务器：通过在多个国家（如日本、韩国、瑞典、波兰和乌克兰）托管的网络代理服务器中继指令，攻击者能够掩盖自己的真实位置和IP地址，使追踪变得极其困难。这种方法不仅增加了攻击的匿名性，还增加了追踪和防御的复杂度。此策略的有效运用显示了攻击者对于网络基础设施的深入理解，以及在全球范围内操控网络流量的能力​。
3. 跨国网络基础设施的渗透策略：这次攻击不仅局限于对西北工业大学的攻击，而是通过控制基础设施的监控系统和消息服务器，攻击者能够在至少80个国家的电信基础设施网络中获取并窃取具有敏感身份人员的个人信息。这种广泛的网络基础设施渗透显示了攻击者具有全球网络侦察和攻击能力，能够对全球多个关键基础设施实施精准的网络攻击​。
4. 高级持久性威胁（APT）的运用：APT攻击通常由国家支持的黑客团队或高度专业的犯罪集团实施，旨在长期、隐秘地监控和窃取目标网络中的信息。此次事件中，APT攻击的显著特征包括利用零日漏洞和定制的恶意软件（如“怒火喷射”、“狡诈异端犯”、 “坚忍外科医生”、和“酸狐狸”）对西北工业大学进行定向攻击。这些恶意软件不仅针对特定的系统漏洞，还能够隐蔽地植入目标网络，建立后门以便未来的访问和控制​​。通过长时间的监控和数据收集，攻击者能够深入了解目标网络的运作机制，为将来的攻击活动或情报收集奠定基础。

同时，网络攻击武器的多样性也是本次网络攻击事件的显著特征，其主要可以分为四类：

1. 漏洞攻击突破类武器：包括"剃须刀"、"孤岛"和"酸狐狸"武器平台，这些工具主要针对特定的系统漏洞实施远程攻击，以获取目标主机的完整控制权。通过这些工具，TAO能够突破西北工业大学的网络边界防御，控制跳板机，并构建用于行动掩护的匿名化网络。
2. 持久化控制类武器：如"二次约会"、"NOPEN"、"怒火喷射"、"狡诈异端犯"和"坚忍外科医生"，这类工具使TAO能够隐蔽地控制被攻击的网络系统，实施长期监视和数据窃取。这些武器支持多种操作系统，具有高度的隐蔽性和持久性，能够在目标网络中长期驻留。
3. 嗅探窃密类武器：包括"饮茶"和"敌后行动"系列工具，专门用于嗅探和窃取西北工业大学网络内的敏感信息，如账号口令、操作记录和运维数据等。通过这些工具，TAO能够细致地收集目标网络的内部信息。
4. 隐蔽消痕类武器："吐司面包"，用于消除网络攻击留下的痕迹，以避免攻击活动被发现。这类武器确保了TAO行动的隐蔽性，帮助攻击者隐藏其在网络内部的恶意操作和窃密行为。

这次针对西北工业大学的网络攻击揭示了网络战的新境界，其中不仅展示了技术上的先进性，还暴露了国际间网络空间的紧张关系。通过利用高级持久性威胁技术、零日漏洞、多层代理网络等多种复杂手段，攻击者能够长时间隐秘地控制目标网络，窃取大量敏感数据。

这一事件不仅对西北工业大学造成了直接的网络安全威胁，也对国际社会的网络安全治理提出了新的挑战。面对如此复杂多变的网络攻击手段，国家安全部门应该更加重视网络空间安全，提升网络防御能力，保护关键信息基础设施不受此类高级持久性威胁的侵害。