【看点】

网袭西工大，美国安局网络武器曝光！

《环球时报》记者13日从相关部门获悉，在西北工业大学遭受美国国家安全局（NSA）网络攻击事件中，名为“饮茶”的嗅探窃密类网络武器是导致大量敏感数据遭窃的最直接“罪魁祸首”之一。对此，网络安全专家建议，在信息化建设过程中，建议选用国产化产品和“零信任”安全解决方案。

9月5日，中国相关部门对外界宣布，此前西北工业大学声明遭受境外网络攻击，攻击方是美国国家安全局（NSA）特定入侵行动办公室（TAO）。此后国家计算机病毒应急处理中心与北京奇安盘古实验室对此次入侵事件进一步深入分析，在最新的调查报告中，美国实施攻击的技术细节被公开：即在41种网络武器中名为“饮茶”的嗅探窃密类网络武器就是导致大量敏感数据遭窃的最直接“罪魁祸首”之一。

相关网络安全专家介绍，TAO使用“饮茶”作为嗅探窃密工具，将其植入西北工业大学内部网络服务器，窃取了SSH等远程管理和远程文件传输服务的登录密码，从而获得内网中其他服务器的访问权限，实现内网横向移动，并向其他高价值服务器投送其他嗅探窃密类、持久化控制类和隐蔽消痕类网络武器，造成大规模、持续性敏感数据失窃。

经技术分析与研判，“饮茶”不仅能够窃取所在服务器上的多种远程管理和远程文件传输服务的账号密码，并且具有很强的隐蔽性和环境适应性。上文中的网络安全专家称，“饮茶”被植入目标服务器和网络设备后，会将自身伪装成正常的后台服务进程，并且采用模块化方式，分阶段投送恶意负载，具有很强的隐蔽性，发现难度很大。“饮茶”可以在服务器上隐蔽运行，实时监视用户在操作系统控制台终端程序上的输入，并从中截取各类用户名密码，如同站在用户背后的“偷窥者”。网络安全专家介绍：“一旦这些用户名密码被TAO获取，就可以被用于进行下一阶段的攻击，即使用这些用户名密码访问其他服务器和网络设备，进而窃取服务器上的文件或投送其他网络武器。”


美国国家安全局（NSA）总部，马里兰州米德堡。

技术分析表明，“饮茶”可以与NSA其他网络武器有效进行集成和联动，实现“无缝对接”。今年2月份，北京奇安盘古实验室公开披露了隶属于美国国家安全局（NSA）黑客组织——“方程式”专属的顶级武器“电幕行动”（Bvp47）的技术分析，其被用于奇安盘古命名为“电幕行动”的攻击活动中。在TAO此次对西北工业大学实施网络攻击的事件中，“饮茶”嗅探窃密工具与Bvp47木马程序其他组件配合实施联合攻击。根据介绍，Bvp47木马具有极高的技术复杂度、架构灵活性以及超高强度的分析取证对抗特性，与“饮茶”组件配合用于窥视并控制受害组织信息网络，秘密窃取重要数据。其中，“饮茶”嗅探木马秘密潜伏在受害机构的信息系统中，专门负责侦听、记录、回送“战果”——受害者使用的账号和密码，不论其是在内网还是外网中。

报告还指出，随着调查的逐步深入，技术团队还在西北工业大学之外的其他机构网络中发现了“饮茶”的攻击痕迹，很可能是TAO利用“饮茶”对中国发动大规模的网络攻击活动。

值得注意的是，在美国对他国实施的多次网络攻击活动中，反复出现美国IT产业巨头的身影。例如在“棱镜”计划中，美国情治部门掌握高级管理员权限，能够随时进入微软、雅虎、谷歌、苹果等公司的服务器中，长期秘密进行数据挖掘。在“影子经纪人”公布的“方程式”组织所使用的黑客工具中，也多次出现了微软、思科甚至中国部分互联网服务商旗下产品的“零日漏洞”（0Day）或者后门。“美国正在利用其在网络信息系统软硬件领域的技术主导地位，在美国IT产业巨头的全面配合下，利用多种尖端网络武器，在全球范围发动无差别的网络攻击，持续窃取世界各地互联网设备的账号密码，以备后续随时‘合法’登录受害者信息系统，实施更大规模的窃密甚至破坏活动，其网络霸权行径显露无遗。”因此，网络安全专家建议用户对关键服务器尤其是网络运维服务器进行加固，定期更改服务器和网络设备的管理员口令，并加强对内网网络流量的审计，及时发现异常的远程访问请求。同时，在信息化建设过程中，建议选用国产化产品和“零信任”安全解决方案。（“零信任”是新一代的网络安全防护理念，默认不信任企业网络内外的任何人、设备和系统。）

这位专家进一步指出，无论是数据窃取还是系统毁灭瘫痪，网络攻击行为都会给网络空间甚至现实世界造成巨大破坏，尤其是针对重要关键信息基础设施的攻击行为，“网络空间很大程度是物理空间的映射，网络活动轻易跨越国境的特性使之成为持续性斗争的先导。没有网络安全就没有国家安全，只有发展我们在科技领域的非对称竞争优势，才能建立起属于中国的、独立自主的网络防护和对抗能力。” 据新华社

【要闻】

最高人民检察院依法对王滨决定逮捕

新华社北京9月13日电 中国人寿保险（集团）公司原党委书记、董事长王滨涉嫌受贿、隐瞒境外存款一案，由国家监察委员会调查终结，移送检察机关审查起诉。日前，最高人民检察院依法以涉嫌受贿罪、隐瞒境外存款罪对王滨作出逮捕决定。该案正在进一步办理中。

【科技】

美“新谢泼德”飞行器不载人试飞时火箭坠毁

新华社洛杉矶9月12日电 美国蓝色起源公司的“新谢泼德”飞行器12日进行不载人太空试飞，火箭在发射后出现故障并坠毁，没有造成人员伤亡。

这次试飞在蓝色起源公司位于美国得克萨斯州西部的一处发射场进行。该公司在网站上介绍说，火箭在发射后不久出现故障，太空舱逃生系统成功启动，将没有载人的太空舱与火箭分离。随后火箭坠毁于地面，太空舱打开降落伞落回地面，没有人员伤亡。

据介绍，蓝色起源公司自2012年起对“新谢泼德”飞行器及其安全系统进行飞行测试，这是“新谢泼德”飞行器第23次太空试飞。“新谢泼德”飞行器的设计目标是将宇航员和科研载荷送入太空，其飞行高度可达约107千米，超过距地表约100千米的“卡门线”，这是国际航天界定义的地球大气层与太空的边界。

蓝色起源公司表示，在此次试飞前，“新谢泼德”飞行器已连续成功完成22次飞行测试，其中包括3次逃生测试，表明飞船的逃生系统能够在飞行任何阶段安全启动。

【国际】

意大利林场大量砍树满足燃木取暖需求

随着取暖季临近，如何削减“天价”燃气账单是欧洲民众逃不开的话题。在意大利，不少家庭选择“回归”燃木取暖方式，购买木材需求因此高涨，一些地区的树木砍伐量激增。

意大利农林能源协会发布的最新数据显示，今年前8个月，意大利林业企业承包林场的成交价较去年同期涨幅高达50%，用于燃烧木材的炉灶购买量增加约20%。同时，碎木块和木材销量分别增长37.3%和60.8%。据意大利媒体统计，今年意大利普通家庭的天然气账单金额将较往年增长70%至80%，如果欧洲不改善与俄罗斯的关系，今年冬季前这笔花费还会进一步增加。 据新华社

■全国统一邮发代号：23-343
■本地统一零售价1元
■本报编辑部地址：青岛市崂山区株洲路190号
■发行热线：82880022
■新闻热线：82860085
■广告咨询：82933112
■差错举报：82860085
■青岛报业传媒集团法律顾问：[illegible]