小心“饮茶”！西北工大遭网袭事件又一细节曝光

美国NSA专用网络武器浮出水面

9月13日，国家计算机病毒应急中心发布《美国NSA网络武器“饮茶”分析报告》。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。

“饮茶”是网络攻击事件“罪魁祸首”之一

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、TELNET、FTP、SCP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”主要针对Unix/Linux平台。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。”

“饮茶”包含“验证模块（authenticate）”“解密模块（decrypt）”“解码模块（decode）”“配置模块”“间谍模块（agent）”等多个组成部分。

基于相关分析结果，技术分析团队认为，“饮茶”编码复杂，高度模块化，支持多线程，适配操作系统环境广泛，包括FreeBSD、Sun Solaris系统以及 Debian、RedHat、Centos、Ubuntu等多种Linux发行版，反映出开发者先进的软件工程化能力。

可以与其他网络武器有效进行集成和联动

技术分析表明，“饮茶”还具有较好的开放性，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”。其采用加密和校验等方式加强了自身安全性和隐蔽性，并且其通过灵活的配置功能，理论上可以提取所有攻击者想获取的信息，是功能先进、隐蔽性强的网络武器。今年2月份，北京奇安盘古实验室公开披露了隶属于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。

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。

美国网络攻击活动中反复出现IT产业巨头身影

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疑。”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。”

本报综合

莫尔古洛夫被任命为俄罗斯驻华大使

本报综合消息　俄罗斯总统普京当地时间9月13日签署命令，任命莫尔古洛夫为俄罗斯驻华大使。

据央视新闻客户端报道，莫尔古洛夫出生于1961年，曾于2006年至2009年在俄罗斯驻华使馆担任公使，2011年12月被任命为俄外交部副部长。

据北京青年报报道，此前担任俄罗斯驻华大使的是杰尼索夫，他于2013年5月上任，至今已有9年。

半个月第三次调整发射日期

美国航天局无人绕月之旅再推迟

据新华社电　美国国家航空航天局12日通报，“阿耳忒弥斯1号”无人绕月飞行任务将再次推迟，最早发射日期拟为9月27日。这是这项任务半个月来连遭故障后，第三次调整发射日期。

按照“阿耳忒弥斯”登月计划，执行无人绕月任务的新一代登月火箭“太空发射系统”原定8月29日第一次发射，把“猎户座”无人飞船送入绕月轨道，但当天因故障推迟；9月3日又因燃料泄漏故障取消发射。美国航天局原本期望9月23日再次尝试发射，如今推迟4天至9月27日。下一个备选日期为10月2日。

按照美国航天局的通报，9月27日，“70分钟的发射窗口将在美国东部时间11时37分开启”，飞行任务将以“猎户座”飞船11月5日在海上溅落结束。

飞行任务能否如期执行，仍将取决于工程团队是否成功完成“太空发射系统”火箭液态氢燃料填充测试，以及东部发射试验场是否允许工程团队不对火箭自毁装置电池系统重新做调试。如果东部发射场要求必须再做电池调试，火箭就需要从发射台拉回总装大楼，那么发射日期还得往后推迟几周。

美国航天局希望借这次任务测试“太空发射系统”及其搭载的“猎户座”飞船性能，尤其是飞船配备的巨大防热罩是否顶用，为今后载人登月任务做好准备。美方下一步计划执行“阿耳忒弥斯2号”任务，用飞船搭载航天员作绕月飞行，但不登陆月球表面；载人登月任务预定本世纪20年代中期执行。美国航天局还计划建造一座月球空间站，为实现长时间航天任务以及登陆火星目标“探路”。

风雨钱江潮

这是9月13日拍摄的钱塘江潮水。

当日是农历八月十八，每年农历八月十八是观赏钱塘江潮水的最佳时机。今年，受台风“梅花”影响，钱塘江在风雨之中迎来大潮。

新华社发

国家发展改革委：

本周将投放今年第二批中央储备肉

新华社北京9月13日电　记者13日从国家发展改革委了解到，根据当前生猪市场形势，为切实做好生猪市场保供稳价工作，本周国家将投放今年第二批中央猪肉储备。下一步，国家发展改革委将会同有关部门继续密切关注生猪市场供需和价格形势，积极组织开展猪肉储备调节，必要时进一步加大投放力度。建议养殖场（户）合理安排生产经营决策，保持正常出栏节奏、顺势出栏育肥猪。