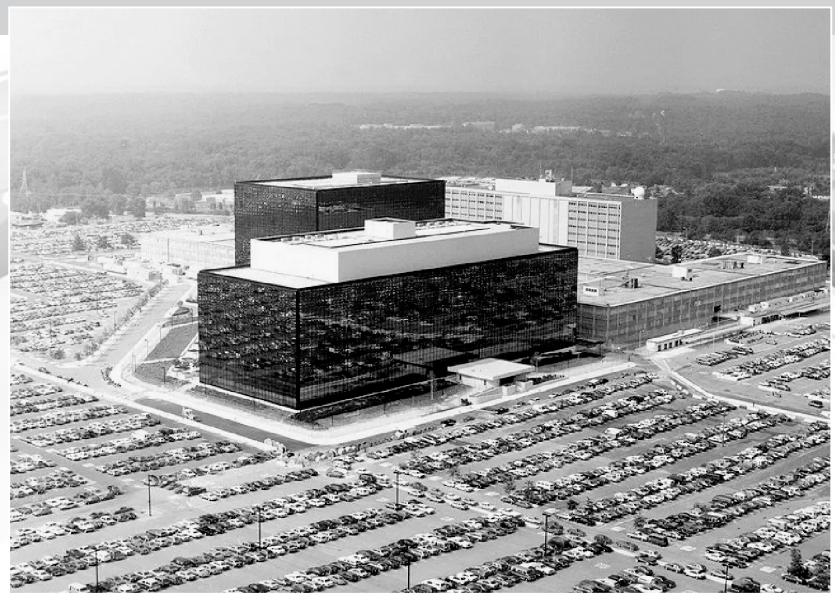
小心“饮茶”!

西工大被美网络攻击重要细节曝光



美国国家安全局(NSA)总部,马里兰州米德堡。

《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。”

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,只有要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。”

据环球时报

外交部:美方尚未就网络攻击西北工业大学作出实质性回应

在9月13日举行的中国外交部例行记者会上,有记者提问说:在360公司发布关于西北工业大学遭受美国国家安全局网络攻击的调查报告后,中方有关机构今天再次发布了对美国国家安全局网络武器“饮茶”的技术分析报告,引起了媒体的高度关注。中方对此有何评论?

发言人毛宁对此表示,确实今天中方有关机构发布了美国国家安全局攻击西北工业大学、使用网络武器的技术分析报告,报告中披露了更多的细节和证据,中方已经通过多个渠道要求美方对恶意网络攻击作出解释,并立即停止不法行为,但是迄今,我们还没有得到美方实质性的回应。

毛宁强调,美方行径严重侵犯中国有关机构的技术秘密,严重危害中国关键基础设施安全机构和个人信息安全。美方有关行为必须立即停止,并作出负责任的解释。 据中新网

新闻速览

“唐山打人案”昨日公开审理 预计会持续数日

网传一份盖有廊坊市广阳区人民法院公章的公告显示“唐山打人案”于9月13日9时在河北省廊坊市广阳区人民法院第一审判庭公开审理。9月13日下午4时左右,该院信访科工作人员对记者表示,该案件确于13日上午开庭,目前审理尚未结束,预计将持续数日。 据红星新闻

去世老人核酸报告还在不断更新? 上海辟谣平台:因福利院混淆!

9月12日,网民“Micheael_小鱼”发帖称家中老人于2022年8月3日去世,却发现老人的核酸报告还在不断更新。上海辟谣平台注意到,当天下午该网民已删除原帖,并更新状态表示“感谢各位的关注,此事得到了迅速解决,经相关部门核实,为同名同姓弄错了,老人的核酸不会再更新”。

据澎湃新闻

台风“梅花”预计14日登陆浙江

今年第12号台风“梅花”已于13日凌晨移入东海南部海面,并加强为强台风级。中央气象台预计“梅花”将于14日下午至夜间在浙江温岭到舟山一带沿海登陆,预计登陆时强度为台风级或强台风级。中央气象台昨日将台风预警提升至橙色预警。 据新华社

国家发改委: 本周将投放今年第二批猪肉储备

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。 据新华社

2.8亿农村群众饮水安全问题解决

中国水利部部长李国英13日表示,十年来,中国共解决了2.8亿农村居民饮水安全问题,困扰亿万农民祖祖辈辈的“吃水难”问题历史性地得到解决。 据新华社

中秋假期全国共揽投快递包裹 超17亿件

国家邮政局监测数据显示,2022年中秋假期全国邮政快递业运行平稳有序,共揽收快递包裹8.52亿件,与2021年中秋假期相比增长0.24%;投递快递包裹9.31亿件,与2021年中秋假期相比增长0.11%。

据新华社

全自动核酸检测平台获批上市

近日,由上海之江生物研发的“小青耕”全自动核酸检测平台获国家药监局批准上市,成为目前国内体积最小、自动化程度更高的一体化磁珠法+荧光PCR核酸检测系统,这一台设备仅重45Kg,可放置桌面,能自动化完成样本管开关盖、移液前处理、纳米磁珠法核酸提取、PCR体系构建、荧光PCR扩增等核酸检测全流程,从而实现无人值守,以此来缓解目前核酸检测专业人员数量不足的问题。 据澎湃新闻