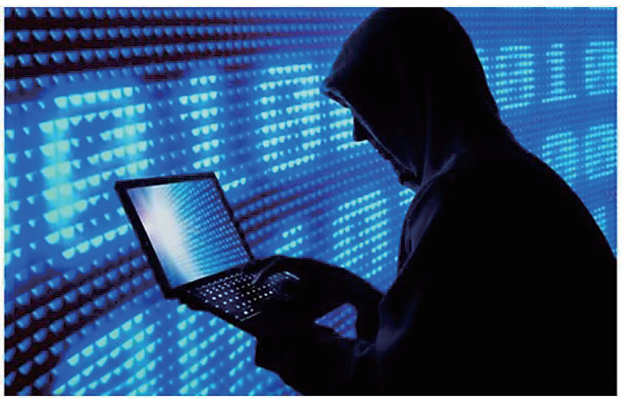
报眉广告 139 307 58 496
沧州佳航汽车服务有限公司为汽车一站式服务
经营:车险投保,定损查勘,道路救援,钣金喷漆,维护保养等一切车辆服务。
精湛的工艺,亲民的价格,让您省心省力更省钱!
地址:沧州市新华区海河东路(沧州荣复军人疗养院对面) 联系人:黄经理17888777771

西北工业大学被美国网络攻击“罪魁祸首”曝光

小心“饮茶”

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。



揪出“罪魁祸首”

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。

作为网络武器的“饮茶”

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”可以与美国国家安全局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。

其他机构也有被网络攻击痕迹

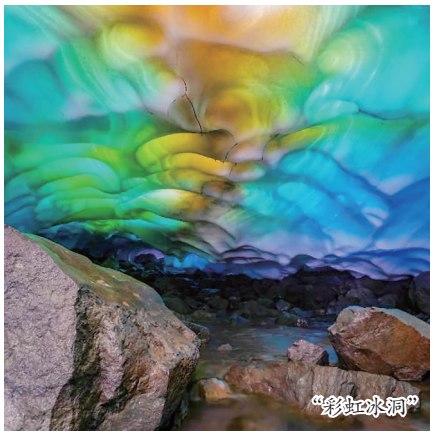
报告还指出,随着调查的逐步深入,技术团队还在西北工业大学之外的其他机构网络中发现了“饮茶”的攻击痕迹,很可能是TAO利用“饮茶”对中国发动大规模的网络攻击活动。

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,“网络空间很大程度上是物理空间的映射,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《环球时报》

美国一公园现神秘“彩虹冰洞”

官方警告:探索冰洞或致命



据报道,美国雷尼尔山国家公园此前被拍到出现神秘“彩虹冰洞”的奇观,在社交媒体上引发热议。不过,美国国家公园管理局近日发布警告称,探索这些冰洞可能是致命的。

今年8月,自然摄影师马修·尼科尔斯在社交媒体上发布了一张令人惊奇的照片,照片显示,位于美国华盛顿州雷尼尔山国家公园的一个神秘冰洞内部闪耀着彩虹色。照片配文称“当太阳正好照射到雷尼尔山的这些冰洞外部时,它们就变成了彩虹冰洞。我专门去雷尼尔山探索冰洞,没想到它们会如此多彩。”

不过,美国国家公园管理局近日发布新闻稿警告,游客不应接近或进入冰洞或融水通道,因为它们很容易因融化而自发坍塌,非常不稳定。冰洞坍塌、碎冰和岩石的坠落都可能是致命的,可能对那些冒险进入冰洞或靠近入口的人造成严重伤害。 据海外网

蓝色不明生物现身

表面有凸起 形状不规则

近日,美国国家海洋和大气管理局科学家在加勒比海深水区发现一种奇怪的不明生物,其通体呈蓝色,表面有明显的凸起,形状不规则。

科学家推测,该生物可能是软珊瑚、海绵或者被囊动物。 据海外网

盐山县成立消防志愿者宣讲队 奏响消防宣传好声音

为深入推进社会化消防宣传机制创新,拓展壮大消防志愿者队伍,推动消防志愿服务活动制度化、常态化发展,盐山县消防救援大队在开学之际,走进校园和社会单位吸纳老师、学生、社会单位员工等成为消防志愿者,并成立了消防志愿者“宣讲队”。

消防志愿者“宣讲队”将从普及消防安全知识、提高消防安全意识、壮大消防宣传志愿者队伍等方面入手,助力建设“平安盐山”。

为了提高志愿者综合素质,盐山县消防救援大队先对消防志愿者们进行了消防知识培训,让其在了解到更多消防知识的基础上,进一步提升了开展消防宣传工作重要性和必要性的认识。

消防志愿者们化身为消防员的“好帮手”,跟随消防员走进校园、企业工厂、商场、社区等地进行广泛宣传,采取张贴挂图通告、发放消防安全宣传单、面对面培训等形式,大力普及消防安全常识,提高群众消防安全意识和逃生自救能力。

接下来,消防志愿者“宣讲队”还将以建立更加完善的志愿服务体系为目标,切实承担起消防宣传“五进”工作。“宣讲队”会策划一系列接地气、惠民生、有成效的消防志愿活动,将消防宣传工作做细做实,增强群众消防意识,促进全社会防火灭火、逃生自救能力的提高,打造共建、共治、共享的消防安全治理格局。 肖宣