2023年9月15日 星期五 齐鲁晚报

网攻西工大的神秘黑客身份被锁定

系美国国家安全局工作人员,“二次约会”间谍软件是关键

近日,国家计算机病毒应急处理中心和360公司对一款名为“二次约会”的间谍软件进行了技术分析,分析报告显示,该软件是美国国家安全局(NSA)开发的网络间谍武器。

据了解,在国家计算机病毒应急处理中心会同360公司配合侦办西北工业大学被美国国家安全局(NSA)网络攻击案过程中,成功提取了这款间谍软件的多个样本,并锁定了这起网络间谍行动背后美国国家安全局(NSA)工作人员的真实身份。

据技术分析报告显示,“二次约会”间谍软件是美国国家安全局(NSA)开发的网络间谍武器,该软件可实现网络流量窃听劫持、中间人攻击、插入恶意代码等恶意功能,它与其他恶意软件配合可以完成复杂的网络“间谍”活动。

国家计算机病毒应急处理中心高级工程师杜振华表示,该软件是具有高技术水平的网络间谍工具,使攻击者能够全面接管被攻击的(目标)网络设备以及流经这些网络设备的网络流量,从而实现对目标网络中主机和用户的长期窃密,同时还可以作为下一阶段攻击的“前进基地”,随时向目标网络中投送更多网络攻击武器。

据专家介绍,“二次约会”间谍软件长期驻留在网关、边界路由器、防火墙等网络边界设备上,其主要功能包括网络流量嗅探、网络会话追踪、流量重定向劫持、流量篡改等。另外,“二次约会”间谍软件支持在各类操作系统上运行,同时兼容多种体系架构,适用范围较广。

杜振华说:“该间谍软件通常是结合特定入侵行动办公室(TAO)的各类针对防火墙、网络路由器的网络设备漏洞攻击工具一并使用。一旦漏洞攻击成功,攻击者成功获得了目标网络设备的控制权限,就可以将这款网络间谍软件植入到目标的网络设备中。”

报告显示,国家计算机病毒应急处理中心和360公司与业内合作伙伴在全球范围开展技术调查,经层层溯源,发现了上千台遍布各国的网络设备中仍在隐蔽运行“二次约会”间谍软件及其衍生版本,并发现被美国国家安全局(NSA)远程控制的跳板服务器,其中多数分布在德国、日本、韩国、印度和中国台湾。

杜振华表示,在多国业内伙伴的通力配合下,我们的联合调查工作取得了突破性进展。目前已经成功锁定了针对西北工业大学发动网络攻击的美国国家安全局(NSA)相关工作人员的真实身份。

此次对间谍软件样本的成功提取,并展开溯源,进一步表明中国防范抵御美国政府网络攻击和维护全球网络安全的决心,这种将美国政府实施网络犯罪的细节昭告世界的做法也证明中国具备“看得见”的网络技术基础,可以更有力地帮助本国和他国感知风险、看见威胁、抵御攻击,将具有国家背景的黑客攻击暴露在阳光下。

相关人士向记者表示,适时将通过媒体公布NSA实施网络攻击人员真实身份信息。相信到时将会再次引发全球民众对美国政府肆意网攻他国的关注。

据央视新闻等

西工大遭美国NSA网络攻击案时间线

◎2022年6月22日 西北工业大学:学校电子邮件系统遭受境外黑客组织网络攻击

◎2022年6月23日 西安公安通报:已立案侦查

◎2022年9月5日 《西北工业大学遭美国NSA网络攻击事件调查报告(之一)》发布:攻击源头系美国国家安全局

◎2022年9月5日 警方通报:攻击系具有美国政府背景的机构及其雇员所为

◎2022年9月5日 外交部:要求美方立即停止不法行为

◎2022年9月5日 西北工业大学声明:坚决反对以任何形式实施网络攻击

◎2022年9月11日 外交部就美网络攻击西工大提出交涉

◎2022年9月13日 美对西工大网袭技术细节公开

◎2022年9月13日 外交部:美国尚未就网络攻击西北工业大学作出实质性回应

◎2022年9月27日 《西北工业大学遭美国NSA网络攻击事件调查报告(之二)》发布,进一步揭露了美国对西北工业大学组织网络攻击的目的:渗透控制中国基础设施核心设备,窃取中国用户隐私数据

本报综合

评论

抹黑中国洗不白『黑客帝国』

近一段时间,美国一些官员和机构频繁炒作“中国网络威胁论”,编造散播所谓“中国黑客”的谎言,企图将美国装扮成网络攻击“受害者”,转移国际社会视线并打压中国。然而,这招抹黑他人洗白自己的手段注定行不通。

美国才是名副其实的全球头号“黑客帝国”,其滥用技术优势在全球各地大搞监听、窃密的劣迹罄竹难书。从“棱镜”计划、“怒角”计划、“星风”计划,到“电幕行动”、“蜂巢”平台、“量子”攻击系统,这些被曝光的事实证据足以让美国坐实“黑客帝国”“监听帝国”“窃密帝国”的名号。美国情报机构的窃密手段五花八门,包括利用模拟手机基站信号接入手机盗取数据,操控手机应用程序、侵入云服务器,通过海底光缆进行窃密,利用美驻外使领馆对驻在国窃密等等。美国实施的是“无差别”监视监听,从竞争对手到盟友,甚至包括德国前总理默克尔、法国多任总统等盟国领导人以及联合国秘书长古特雷斯,无不在其监听范围。前段时间发生的美军方“泄密门”事件再次暴露了美国肆意对他国进行窃听、发动网络攻击等霸凌恶行。美国记者巴顿·格尔曼在《美国黑镜》一书中说:“没有可避难之地,没有可安息之所,美国政府不会接受任何地方处于其监控视野之外。”

美国长期把中国作为网络攻击的主要目标之一,攻击对象涉及航空航天、科研机构、石油行业、大型互联网公司以及政府机构等。中国国家互联网应急中心网站发布的一份报告显示,2020年中国捕获计算机恶意程序样本数量超过4200万个,其中境外恶意程序主要来自美国,占比达53.1%。2020年,控制中国境内主机的境外计算机恶意程序控制服务器数量达5.2万个,其中位于美国的控制服务器数量同样高居首位。去年9月,中国有关机构发布报告,详细披露了美国家安全局网络攻击中国西北工业大学情况。

美国诬陷栽赃的调门越高,世人越能看清“黑客帝国”的真面目。奉劝执迷于网络霸权的美国反躬自省,停止对中国的网络攻击和恶意抹黑,还世界一个和平、安全、开放、合作、有序的网络空间。

据新华社

延伸阅读

“数字”间谍来自何处?有何招式?

当前网络技术发展突飞猛进,5G、元宇宙、ChatGPT等崭新事物骈兴错出,令人惊呼“未来已来”。而与之一同到来的,还有隐藏其中的大量网络安全风险隐患。

国家安全机关作为维护国家安全的专门机构和反间谍工作主管部门,持续加强对有关活动追踪监测和防范打击,切实维护网络安全,让“数字”间谍原形毕露、无处藏身!

攻击来自何处?千里之外的重重谍影

当前,网络空间已经成为境外间谍情报机关对我国开展网络间谍工作的重要阵地,我国已成为高级别持续性威胁(APT)攻击的主要受害国。近年来,国家安全机关已发现不同国家、地区的数十个间谍情报机关对我境内开展网络攻击活动。他们或组建专门机构力量、成立“掩护公司”、研发专业手段对我直接实施网络攻击渗透行动,或通过“幕后操控”“服务外包”等方式指使专业公司机构、黑客组织实施,或通过“购买”数据、漏洞、工具等方式拉拢引诱境内机构、人员实施,也有国家打着“前出狩猎”等幌子拉拢他国共同实施。

谁是潜在目标?近在咫尺的刀光剑影

从攻击目标看,除了持续对我国家机关、涉密单位等“传统目标”开展网络攻击外,境外间谍情报机关还不断加强对我关键信息基础设施、重大基础设施网络系统的攻击渗透,并将黑手进一步伸向我高等院校、科研机构、大型企业、高科技公司等机构和企业高管、专家学者等群体。

从受攻击情况看,涉及电子邮件、办公自动化、用户管理、安全防护等各类软件系统,服务器、计算机、交换机、路由器等各种硬件设备,以及手机、WiFi、摄像头等民用家用设备,可谓“无孔不入”。

有何招式手段?极具威胁的“专业团队”

与一般社会黑客不同,境外间谍情报机关可调动资源多、技术能力强大,网络攻击活动经验丰富、手法更加隐蔽。

他们有的搜集窃取个人信息数据,运用社会工程学,针对目标对象精准伪造“钓鱼”邮件和网站进行诱骗攻击;有的通过挖掘、购买关键软件系统、硬件设备“零日漏洞”,直接对我开展攻击渗透;有的先侵入控制我供应链企业或运维服务机构网络,再以此为“跳板”攻击下游用户单位;有的大规模渗透控制我民用网络、家用网设备,建立“阵地”对我及其他国家开展网络攻击活动。极具专业性、隐蔽性的攻击手法背后,往往是更加危险的企图!

造成多少危害?不容小觑的安全问题

境外间谍情报机关网络攻击活动规模大、层次深、持续性强。我国家机关、涉密单位及其他重要企业机构网络系统一旦遭攻击、侵入,所存储、处理的国家秘密、重要数据、文件资料等就可能被“一网打尽”。我关键信息基础设施、重大基础设施网络系统一旦被侵入、控制,就会面临随时被干扰、破坏的“致命一击”风险。境外间谍情报机关网络攻击窃取我企业机构商业秘密、知识产权,长期监控我公民网络通信内容,也严重侵害我公民、组织合法权益。

据国家安全部微信公号

编辑:魏银科 组版:颜莉

报料电话:13869196706 欢迎下载齐鲁壹点 600多位在线记者等你报料

报纸发行:(0531)85196329 85196361 报纸广告:(0531)85196150 85196557 文字差错投诉:(0531)85193436 发行投诉:4001176556 (0531)85196527 邮政投递投诉:11185 全省统一零售价:1元

邮发:23-55 广告许可证:鲁工商广字01081号 地址:济南泺源大街2号 大众传媒大厦 邮编:250014 大众华泰印务公司(大众日报印刷厂)印刷(济南市长清区玉皇山路1678号)