营造安全清朗的网络环境

2023国家网络安全宣传周法治主题日系列活动在福州举行

N福建日报
海都记者 李嘉琪

14日，2023国家网络安全宣传周法治主题日系列活动在福州举行。本次法治日主题活动以“法治力量护航数字中国 共建一带一路网络文明”为主题，旨在增强广大网民网络安全意识，提升网络安全基本防护技能，推进网络安全相关法律及治理体系建设。

在14日上午举行的法治主题日主论坛上，公安部网安局、福建省公安厅、福州市公安局有关负责人介绍了网络空间执法举措和成效，来自中国工程院、中科院、中国计算机学会互联网专委会的专家学者聚焦论坛主题，分享各自研究成果，深入分析数字经济时代网络安全现状，为网络空间安全维护和网络强国建设出谋划策。

在当天下午举办的网络安全监管分论坛上，来自公安部网安局、北京理工大学的专家学者，详细解读了网络安全等级保护、关键信息基础设施安全保护以及我国个人信息保护和数据安全法要点等内容。同期举行的公安机关“净网专项”分论坛上，最高人民检察院、最高人民法院、公安部网安局等职能部门就严打网上突出违法犯罪分别作主题发言。

记者获悉，福州公安专门创建网络生态治理中心，2021年“净网”行动开展以来，累计侦破涉网案件1500余起，抓获犯罪嫌疑人2100余人。今年福州市打击的各类涉网案件中，侵犯公民个人信息罪、帮助信息网络犯罪活动罪等案件较多。侵犯公民个人信息罪多为上游犯罪，其危害不仅仅在于罪名本身给受害人带来的个人信息安全的损害、信息财产损失、人格权侵害，更会引发其他严重犯罪，严重损害被害人的人身财产安全。

嘉宾在2023年国家网络安全宣传周网络安全博览会上参观（新华社/图）

网攻西工大的神秘黑客身份已锁定

N央视新闻

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介绍，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。

杜振华表示，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。

杜振华介绍，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。

守护网络安全 打击“数字”间谍

国家安全部揭秘境外间谍情报机关网络攻击活动

N国家安全部微信号

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。

唐昊/制图

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。