近日,在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,
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,国家计算机病毒应急处理中心和360公司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。

新证据!起底美国国家安全局开发的间谍软件
网攻西工大的神秘黑客身份被锁定

幕后黑手 美国国家安全局下属特定入侵行动办公室

2022年6月,西北工业大学发布公开声明称,西北工业大学遭受网络攻击,有来自境外的黑客组织企图窃取相关数据。此后,我国成功侦破此次网攻的幕后凶手是美国国家安全局(NSA)信息情报部(代号S)数据侦察局(代号S3)下属特定入侵行动办公室(TAO)(代号S32)部门。

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,与其他恶意软件配合可以完成复杂的网络“间谍”活动。

最新消息显示,国家计算机病毒应急处理中心和360公司在侦办西北工业大学网络攻击案过程中,成功提取了该“间谍”软件的多个样本,并锁定了这起网络“间谍”行动背后NSA工作人员的真实身份。

间谍软件 植入目标设备实施长期窃密

随后的技术分析发现,“二次约会”间谍软件是一款高技术水平的网络间谍工具。开发者应该具有非常深厚的网络技术功底,尤其对网络防火墙技术非常熟悉,其几乎相当于在目标网络设备上加装了一套内容过滤防火墙和代理服务器,使攻击者可以完全接管目标网络设备以及流经该设备的网络流量,从而实现对目标网络中的其他主机和用户实施长期窃密,并作为攻击的“前进基地”,随时可以向目标网络投送更多网络进攻武器。

“二次约会”间谍软件通常结合TAO的各类针对防火墙、路由器的网络设备漏洞攻击工具使用,在漏洞攻击成功并获得相应权限后,植入至目标设备。该间谍软件使用控制方式分为服务端和控制端,服务端部署于目标网络边界设备上(网关、防火墙、边界路由器等),通过底层驱动实时监控、过滤所有流量;控制端通过发送特殊构造的数据包触发激活机制后,服务端从激活包中解析回连IP地址并主动回连。网络连接使用UDP协议,通信全程加密,通信端口随机。控制端可以对服务端的工作模式和劫持目标进行远程配置,根据实际需要选择网内任意目标实施中间人攻击。

坚决回击 “看得见”的网络技术将黑客攻击暴露在阳光下

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,在遍布多个国家和地区上千台网络设备中发现了仍在隐蔽运行“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。

此次我方对“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。

相关链接

国家安全部披露——“数字间谍”来自何处?

据国家安全部微信公众号消息,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,切实维护我网络安全,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。

■来源:央视新闻 ■图片:VCG