这是2021年5月17日在丹麦哥本哈根拍摄的美国国务卿布林肯(右)和丹麦外交大臣科弗德共同出席新闻发布会的资料照片。

窥探渗透无所不在 美国如何打造“黑客帝国”

美国对全世界的监听无孔不入。率先曝光“斯诺登事件”的前英国《卫报》记者格伦·格林沃尔德写过一本书,书名《无处可藏》正是美国这个“黑客帝国”窥探全球的最好写照。

在美国总统拜登即将访问欧洲之际,美国被曝曾在丹麦帮助下监听包括德国总理默克尔在内的欧洲政要,这是美国监听全世界的又一明证。

近些年,美国实施的各种网络情报项目陆续曝光。专家认为,美国在网络空间拥有强大的监听、攻击、威慑和防御能力,利用不对称优势对他国发动“降维打击”,而中国是网络攻击的主要受害国之一。

“弹道无痕”

2012年7月至2013年9月,就在美国国家安全局利用丹麦互联网设施监听欧洲人的同时,被认为与美国国安局密切关联的网络犯罪组织“方程式组织”悄悄攻破总部设在迪拜的EastNets公司网络。EastNets公司是中东地区最大的SWIFT(环球银行间金融通信协会)支付系统服务提供商。

得益于黑客组织“影子经纪人”2017年曝光的文件,中国网络安全厂商安天复盘发现,“方程式组织”首先利用日本、德国等地的6台被入侵服务器作为跳板,借助身份认证漏洞攻破EastNets网络外围4台VPN(虚拟专用网络)防火墙并植入后门,进而突破其后两台企业级的防火墙,进入内网的两台管理服务器,由此进一步攻陷至少9台业务服务器,成功窃取EastNets在比利时、约旦、埃及和阿联酋的上千个雇员账户等信息,从而获取其感兴趣的交易信息、资金流动轨迹等。

安天的报告写道,以“方程式组织”为代表的美国情报机构攻击团队“高度追求作业过程的隐蔽性、反溯源性,使其攻击看似‘弹道无痕’,其突破、存在、影响、持续直至安全撤出网络环境或系统的轨迹很难被察觉”。

近些年来,美国实施的各种监听项目陆续曝光。这类项目多由美国国安局负责具体实施,包括发起于20世纪60年代针对卫星等各种通信信号监听的“梯队”项目、监听目标涵盖美国公民的“星风”计划、针对全球网络安全厂商的“拱形”计划、针对电话监听的“神奇”项目、从网络骨干光缆和交换机上复制光信号的“上游”项目。

全世界这才知道,从电子邮件、语音通话到社交网络信息,从外国领导人、外国民众到美国民众,原来一切都可能处在美国监听窥视之下。2015年,美国国会迫于国内压力通过法案,决定结束只针对美国国内的监听项目。但美国《涉外情报监视法》702条款于2018年获准延长6年,允许美国情报机构继续在没有法庭授权的情况下,监控美国境外目标的电邮和短信等。

必须指出的是,网络入侵只是美国现代间谍情报战使用的手段之一,美国把人力、电磁等传统情报手段和网络攻击深度结合,在与互联网物理隔离的内部网络中植入病毒长期“潜伏”,在合适时间“引爆”。2010年曝光的“震网”蠕虫病毒,据报道就是由荷兰情报人员帮助美国和以色列招募的“内鬼”利用U盘植入伊朗核设施内部网络,最终摧毁大批离心机,破坏了伊朗核计划。

“降维打击”

除美国国安局,美国还有另一大情报机构——中央情报局。该机构一直被认为主要从事针对人的情报工作。然而,2017年“维基揭秘”曝光的近9000份中情局机密文件表明,中情局的网络攻击能力也极其强大,它致力于发现并利用现代科技产品的漏洞,已成功侵入手机、电脑乃至智能电视等众多智能设备。

这些机密文件显示,中情局“网络情报中心”拥有“注册用户”逾5000人,设计的攻击工具超过1000个,运行的代码数量比社交网站“脸书”还要多。此外,中情局还设立海外网络攻击基地,其中一个基地位于美国驻德国法兰克福领事馆,负责欧洲、中东和非洲地区的网络攻击活动。

中情局攻击团队至少干了这几件事:入侵智能电视让其“假关机”变成窃听器;入侵智能车辆控制系统以执行暗杀等活动;开发针对苹果手机与谷歌安卓系统的攻击工具;入侵包括微软视窗、苹果OSx以及Linux等在内的操作系统;入侵网络路由器等等。

文件还显示,中情局特别设立一个小组,专门负责收集、管理“偷自”俄罗斯等国家的攻击工具,因为这样做不仅能丰富中情局网络攻击的花样,还能留下“假指纹”,让调查人员误以为遭到其他国家的网络攻击。

美国还一直肆无忌惮地打造网军。2017年,美国政府宣布将美军网络司令部升级为美军第十个联合作战司令部,网络空间由此正式与海洋、陆地、天空和太空并列成为美军的第五战场。目前,美军共有133支网络部队,由13支国家任务部队、68支网络保护部队、27支作战部队与25支支持部队组成。

安天研究院专家对记者说,从机构和团队看,美国有庞大复杂的情报体系,其情报作业遍布网络空间和物理空间各个领域;从装备体系看,恶意代码等攻击武器完整覆盖服务器、云、移动智能设备等各类场景,适配各类操作系统,功能上涵盖侦察、物理隔离突破、内网横向移动、持久化潜伏驻留、供应链与物流链渗透、远程控制等网络攻击各个环节。这些装备还只是浮出水面的部分,其行动由美国花费数十年建设、监听和作业的数十个庞大的情报工程体系作为支撑。

专家认为,美国占据网络空间霸主地位,与其他国家在网络技术方面始终保持巨大的位势差,美国可在网络空间利用不对称优势对他国发动“降维打击”。

本版稿件文图均据新华社

“中国是主要受害国”

美国一直宣扬其面临所谓“数字9·11”和“网络珍珠港”威胁,所谓中俄黑客常被其当成假想敌。但事实上,中国才是网络攻击的主要受害者之一。

中国国家互联网应急中心网站5月26日发布的2020年中国互联网网络安全态势综述报告显示,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以约1.9万个位于首位。

中国360公司推出的360安全大脑去年3月发布的调查报告发现,美国中情局攻击团队对中国进行了长达11年的网络攻击和渗透,包括航空航天、科研机构、石油行业、大型互联网公司以及政府机构等多个单位受影响。360安全大脑还定位到负责从事研发和制作相关网络武器的中情局前雇员乔舒亚·亚当·舒尔特。舒尔特在中情局的秘密行动处担任科技情报主管职位,直接参与研发针对中国的网络武器。

360安全大脑在报告结尾写道:“我们发现境外针对中国境内目标的攻击……至少影响了中国境内超过万台电脑,攻击范围遍布国内31个省级行政区。……(这些攻击)都可以直接证明中国是APT(高级可持续威胁)攻击中的主要受害国。”

这张2008年8月14日的资料照片显示,在美国弗吉尼亚州兰利,一名男子走过中央情报局总部的大厅。