劣迹斑斑的“黑客帝国”

——起底美国破坏全球网络安全

中国国家计算机病毒应急处理中心最新通报，在会同360公司配合侦办西北工业大学遭受网络攻击案过程中，成功提取了名为“二次约会”的间谍软件多个样本。据介绍，该软件为美国国家安全局开发的网络“间谍”武器，调查团队发现它在上千台遍布全球多国的网络设备中隐蔽运行。

长期以来，美国在网络安全领域劣迹斑斑。从十年前的“棱镜门”到今年的“泄密门”，大量证据表明美国网络监听和攻击行为从未停息，包括联合国和美国盟友都是受害者。“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。”美国记者巴顿·格尔曼在《美国黑镜》一书中如此揭露。

作为全球最大“黑客帝国”和网络窃密者，美国的所作所为严重损害别国主权，严重侵犯全球互联网用户隐私。中国是全球网络攻击的最大受害者，其中大部分攻击来自美国。

中国是网络攻击最大受害者

今年7月，中国有关部门通报武汉市地震监测中心遭受网络攻击。据媒体跟踪报道，国家计算机病毒应急处理中心高级工程师杜振华表示，联合调查组在受害单位的网络中发现了技术非常复杂的后门恶意软件，符合美国情报机构特征。

中国外交部发言人汪文斌同月在例行记者会上指出，中国政府部门几乎每天都在遭受海量的网络攻击，其中大多数源头都来自美国。

今年5月4日，中国国家计算机病毒应急处理中心与360公司共同发布《“黑客帝国”调查报告——美国中央情报局》。这份报告显示，美国中央情报局开展了规模庞大的全球性网络攻击行动：使用一大批至今未被披露的后门和漏洞，在世界各地建立“僵尸”网络和攻击跳板网络，针对网络服务器、网络终端、交换机和路由器、以及数量众多的工业控制设备分阶段实施攻击入侵行动。在专门针对中国境内目标实施的网络攻击行动中，相关机构成功提取了多个“穹顶7”网络攻击武器样本，多个东南亚国家和欧洲的机构也提取到了几乎完全相同的样本。“穹顶7”正是2017年“维基揭秘”网站披露的美国中央情报局网络情报中心的秘密攻击手段。

去年4月，西安警方接到报警，中国西北工业大学信息系统发现遭受网络攻击痕迹。调查这一事件的技术团队先后从该大学的多个信息系统和上网终端中提取到木马程序样本，综合使用国内现有数据资源和分析手段，并得到欧洲、东南亚部分国家合作伙伴的通力支持，全面还原了相关攻击事件的总体概貌、技术特征、攻击武器、攻击路径和攻击源头，初步判明相关攻击活动源自美国国家安全局的“特定入侵行动办公室”。

中国国家计算机病毒应急处理中心最新发布的通报说，在配合侦办西北工业大学遭受网络攻击案过程中，成功提取了名为“二次约会”的间谍软件多个样本。根据黑客组织“影子经纪人”泄露的美国国家安全局内部文件，该恶意软件为美国国家安全局开发的网络“间谍”武器。它主要部署在目标网络边界设备（网关、防火墙、边界路由器等），隐蔽监控网络流量，并根据需要精准选择特定网络会话进行重定向、劫持、篡改。

上述案例是美国对中国开展网络攻击的冰山一角。中国国家互联网应急中心网站2021年发布的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约1.9万个，高居首位。

美国网络监听和攻击从未停息

“间谍行为是一项已经嵌入美国历史、根深蒂固的习惯。”美国《时代》周刊一篇文章曾这样评论。

中国国家计算机病毒应急处理中心的最新通报说，调查团队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。

今年4月，“泄密门”事件闹得沸沸扬扬。一批疑似美军秘密文件被泄露到社交媒体上，其内容显示，美国监听乌克兰总统泽连斯基与乌官员的内部对话，并获取了韩国和以色列等盟国内部沟通情况。美媒指出，有关信息是美方通过所谓“信号情报”获取，而“信号情报”是情报界专用术语，意味着美国政府持续监听这些国家。

美国的监听丑闻早已不是什么新鲜事。2013年，美国前防务承包商雇员爱德华·斯诺登向媒体曝光美方代号“棱镜”的大规模秘密监听项目，监听对象不仅覆盖美国公民，也包括法国、德国等欧洲国家政要和民众。2021年5月，欧洲媒体爆料，美国在丹麦情报部门帮助下，监听德国、法国、瑞典、挪威等欧洲国家领导人。

近年来，美国各种监听项目不断被曝光，包括发起于20世纪60年代针对卫星通信的“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。可以说，从电子邮件、语音通话到社交网络，从外国领导人、外国民众到美国民众，美国都要也都在监听。

除监听外，美国还频繁对他国发动网络攻击。据黑客组织“影子经纪人”爆料，美国国家安全局针对包括俄罗斯、日本、西班牙、德国、意大利在内的超过45个国家和地区的287个目标进行网络攻击，持续时间长达十几年。俄外交部国际信息安全司司长安德烈·克鲁茨基赫说，截至2022年5月，来自美国等国的6.5万多名黑客定期参与针对俄方关键信息基础设施的攻击。

美国还把网络攻击与传统情报手段相结合，作为“混合战争”的重要手段。2010年，美国通过间谍活动将“震网”病毒植入伊朗纳坦兹核设施内部网络，导致大批铀浓缩离心机瘫痪。

美国的网络军事力量近年来也在不断膨胀。2017年，美军网络司令部升级为美军第十个联合作战司令部，网络空间正式与海洋、陆地、天空和太空并列，成为美军“第五战场”。2018年美国国防部网络战略报告强调，要在网络空间“先发制人”。

美国为维护霸权始终我行我素

多年来美国网络监听和攻击等行为屡遭曝光，受到国际社会广泛批评。但美国为维护自身霸权依旧我行我素，持续肆意破坏网络安全，践踏国际准则和他国主权。

“棱镜门”曝光后，时任联合国秘书长发言人内西尔基2013年10月表示，联合国就遭美国情报部门监听的报道与美方接触，美国政府已保证不会对联合国进行监听。他强调，包括联合国在内的外交使团不可侵犯是早已被广泛接受的国际法原则，联合国所有会员国都应恪守这一原则。但今年“泄密门”曝光的情报显示，美国仍在监听联合国秘书长与其他联合国官员之间的私密对话。

美国对盟友也是如此。“棱镜门”曝光的文件显示，美国对包括韩国驻美大使馆在内的数十个外交机构实施监听。韩国政府当时要求美方作出解释，美方则以“将重新评估情报行动”的说法搪塞。然而，今年“泄密门”曝光的信息显示，美国情报部门还在继续监听韩国政府官员。2013年“棱镜门”事件几个月后，德国政府披露时任总理默克尔的移动电话可能遭美情报机构监听，默克尔后来直接致电当时的美国总统奥巴马，批评这是“严重背弃信任”之举。此事以美方承诺不再监听默克尔的通信设备告终。但2021年曝光的“监听门”表明，美国至少至2014年还在监听默克尔。

假意承诺但实际上毫无收敛，大搞网络攻击损害他国主权，种种行径印证芬兰《赫尔辛基时报》网站文章的评述：美国已被证明是世界上最大黑客帝国和全球网络安全最严重的威胁。

本版文图据新华社