

我国互联网新闻研究中心发表《美国全球监听行动纪录》

揭开美“监听帝国”的画皮

核心提示

我国互联网新闻研究中心26日发表《美国全球监听行动纪录》。纪录说,2013年6月,英国、美国和中国香港媒体相继根据美国国家安全局前雇员爱德华·斯诺登提供的文件,报道了美国国家安全局代号为“棱镜”的秘密项目,内容触目惊心。中国有关部门经过几个月的查证,发现针对中国的窃密行为的内容基本属实。

纪录指出,美国的监听行动,涉及中国政府和领导人、中资企业、科研机构、普通网民、广大手机用户等等。中国坚持走和平发展道路,没有任何理由成为美国打着“反恐”旗号进行秘密监听的目标。美国必须就其监听行动做出解释,必须停止这种严重侵犯人权的行为,停止在全球网络空间制造紧张和敌意。

美国对全球和中国

进行秘密监听的行径

■ 每天收集全球各地近50亿条移动电话纪录

■ 窥探德国现任总理默克尔手机10多年

■ 多年来一直监控手机应用程序,抓取个人数据

■ 针对中国进行大规模网络进攻,并把中国领导人和华为公司列为目标



■ 秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络,窃取了数以亿计的用户信息

延伸阅读

今天你被监听了吗

我国互联网新闻研究中心26日发布《美国全球监听行动纪录》,披露了美国国家安全局如何监听世界。记者梳理了11个“你不知道的秘密”,看看美国打着“反恐”旗号进行秘密监听的行为有多扭曲。

1.全球政要难逃魔爪。包括联合国秘书长潘基文、德国总理默克尔、乌克兰前总理尤利娅·季莫申科、马来西亚前总理阿卜杜拉·巴达维、巴西总统罗塞夫等122名外国领导人被监控,美国还专门搭建存放外国领导人信息的数据库用于保存相关信息。

2.使馆使团是监听“总部”。2009年20国集团峰会期间,美方设于英国北约克郡一处情报分支机构监听俄罗斯时任总统梅德韦杰夫与国内的卫星通话。实际上,美国国家安全局已经渗透的使馆与使团名单包括巴西、保加利亚、哥伦比亚、欧盟、法国、格鲁吉亚、希腊、印度、意大利、日本、墨西哥、斯洛文尼亚、南非、韩国、委内瑞拉和越南。

3.苹果和安卓操作系统是“数据金矿”。美国国家安全局将苹果和安卓手机操作系统视为是“数据资源的金矿”,早在2007年,美、英情报部门就已合作监控手机应用程序。当人们使用手机游戏“愤怒的小鸟”、应用程序“谷歌地图”以及“脸谱”、推特和网络相册Flickr等手机客户端时,个人用户的位置数据(基于GPS)、种族、年龄等个人数据以及其他个人资料都被抓取。

4.计算机不连接上网仍能被入侵。美国国家安全局至少从2008年起,向全球近10万台计算机植入专门软件,旨在时刻监控或攻击目标计算机,即使计算机没有连接上网,美国国家安全局仍可通过无线电波入侵。自2010年起,美国国家安全局用收集到的资料,分析部分美国公民的“社交连结,辨识他们来往对象、某个特定时间的所在地点、与谁出游等私人信息”。

5.全球主要公司安全架构被攻破。2013年12月29日,德国《明镜》周刊称,美国国家安全局多年前就已攻破了主要公司开发的几乎所有安全架构,其中包括来自思科、华为、瞻博和戴尔的产品。据媒体报道,美国还侵入了巴西国家石油公司的电脑网络。

6.金融交易“尽收眼底”。据德国

《明镜》周刊报道,美国国家安全局的监视项目包括国际金融交易,尤其是信用卡交易。一项名为“追踪金钱”的监视项目专门关注国际上银行金融交易往来。其为此专门建立一个名为Tracfin的金融数据库,用以存储从各个金融机构得到的信息。2011年,这一数据库的信息量达到1.8亿条,其中84%的数据是信用卡信息,涉及用户主要分布在欧洲、中东和非洲。

7.投入20亿美元建全球最大数据中心。由美国国家安全局兴建的犹他州大数据中心,是目前世界上最大的数据中心,投入20亿美元,主要用于通过秘密监控系统收集数据,获取有价值的情报。

8.网络行动预算43亿美元。2013年美国情报预算高达526亿美元,网络行动预算占43亿美元,约占8%,任务显著侧重。从微软到苹果,美国情报机构与私营机构尤其是主要互联网服务提供商的监控合作,从来没有中断过,迄今已持续6年多时间。

9.九大IT厂商提供核心技术支持。美国互联网主要的九大硬件供应商都提供了很核心的技术支持,特别是微软最早与美国国家安全局合作,开放outlook、hotmail内部接口。曾声称其加密技术和P2P架构无法被政府“搭线接听”的Skype,在被微软收购后,主动为“搭线窃听”打开“后门”。

10.无所不在的“棱镜”项目。“棱镜”项目相继与微软、雅虎、谷歌、脸谱、PalTalk、YouTube、Skype、AOL和苹果等9家互联网公司合作。情报人员可以直接进入上述公司的服务器和数据库获取数据,内容包括电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料等10类信息,甚至可以实时监控用户网络搜索内容。

11.用“大数据”提升监控水平。2012年3月,奥巴马政府将大数据战略上升为最高国策,认为大数据是“未来的新石油”,将对数据的占有和控制,作为陆权、海权、空权之外的另一种国家核心能力。美国国家安全局拥有一种名为“无边界情报员”系统,这套系统以30天为周期,可以从全球网络系统中接收到970亿条信息,再通过对比信用卡等方式,能几近真实地还原个人的实时状况。

(本版图文均据新华社)

1

窃听范围涵盖中国国家领导人

纪录称,斯诺登曝光的证据证明:中国是美国非法窃听的主要目标之一,窃听范围涵盖国家领导人、科研机构、大学、企业等等。

斯诺登向德国《明镜》周刊提供的文件表明:美国针对中国进行大规模网络进攻,并把中国领导人和华为公司列为目标。攻击的目标包括商务部、外交部、银行和电信公司等。《明镜》周刊称,美国的监控目标还包括数位中国前任国家领导人和多个政府部门及银行。

中国的政府机构是美国窃听的重点关照对象。白宫的一位外交政策助理也曾透露,美国曾在1990年8月落成的中国驻澳大利亚新使馆的每间办公室的混凝土墙里埋设了光纤窃听器,这种细细的玻璃丝在全面安全检查中没有被发现。直到这件事在前些时候被泄露给《悉尼先驱晨报》和其他新闻媒体后,才引起中国的警觉。

美国《外交政策》杂志报道,美国国家安全局旗下设有一个“获取特定情报行动办公室”,1997年以来通过网络攻击行动获得包括有关中国情报在内的多项重要情报。

据德国《明镜》周刊报道,已被曝光的一份美国2010年的“监听世界地图”包含了世界90个国家的监控点,中国作为美国在东亚的首要监听对象,北京、上海、成都、香港及台北等城市,均在美国国家安全局重点监控目录之下。从2009年开始,美国国家安全局就开始入侵中国大陆和香港的电脑和网络系统,中国大陆和香港已有数百个目标受到监视。在香港的目标中,多数是大学、政府官员、商人和学生。

2

渗入华为计算机网络复制文件

纪录称,据德国《明镜》周刊网站、《纽约时报》网站报道,美国国家安全局尤其花大力气监控全球第二大通信设备供应商华为公司。2009年初,该局启动了一项针对华为的大规模行动。华为被视为美国思科公司最大的竞争对手之一。美国国家安全局的一个特别小组成功渗透进华为公司的计算机网络,并复制了超过1400个客户的资料和工程师使用的内部培训文件。

报道称,该局人员不但窃取了华为的电子邮件存档,还获得了个别华为产品的源代码。美国国家安全局渗入华为的深圳总部,因为该公司通过总部处理每个员工的邮件往来,所以美国人从2009年1月起就读取了该公司很大一部分员工的电子邮件——包括公司高管的邮件。

美国情报部门说,如果了解了该公司如何运行,那么未来将会得到回报。迄今为止,网络结构由西方主宰,但中国人将努力使西方的公司变得“更不重要”。那样的话,迄今由美国公司主导的互联网技术标准将被打破,中国将逐步控制网络中的信息流。

美国《纽约时报》网站3月22日称,长期以来,美国官员一直将中国电信巨头华为公司视为安全威胁,竭力阻挠该公司在美国达成商业协议,担心它会在自己的设备中植入“后门”以便让中国军方或北京支持的黑客窃取企业和政府机密。不过,机密文件表明,美国国家安全局正直接向华为的网络植入自己的“后门”。

《纽约时报》报道指出,美国国家安全局对中国的情报活动并不仅仅局限于华为。根据2013年4月斯诺登曝光的文件,去年,美国国家安全局入侵了中国两家大型移动通信网络,从而得以追踪具有战略重要性的中国军方部门。

3

大规模入侵中国主要电信公司

纪录称,《南华早报》援引斯诺登的话说:“美国国家安全局无所不用其极,利用非法侵入中国主要电信公司等手段,窃取用户的手续数据。”

《南华早报》称斯诺登爆料:美国国家安全局还对中国顶尖高等学府清华大学的主干网络发起大规模的黑客攻击。其中2013年1月的一次攻击中,至少63部电脑和服务器被黑。报道指出,中国六大骨干网之一的“中国教育和科研计算机网”就设在清华大学,“清华的主干网络被黑,意味着数百万中国公民的网络数据可能失窃”。

《南华早报》公布的对斯诺登的采访说,美国政府正大规模入侵中国的主要电信公司,以获取数以百万计短信内容。斯诺登表示,美国监控远不止这些,“美国国家安全局做各种事情,诸如入侵中国移动电话公司,以窃取你们所有的短信数据”。

据路透社报道,美国国家安全局曾与加密技术公司美国安全服务商RSA达成了1000万美元的协议,联合在加密算法中加入漏洞后门,旨在削弱软件加密标准,辅助相关机构RSA开展大规模监控程序。RSA的中国客户包括三大电信运营商中国电信、中国移动、中国联通,中国银行、中国工商银行、中国建设银行以及电信设备商华为和家电制造商海尔等。

美国《华盛顿邮报》依据斯诺登提供的多份机密文件爆料说,在2012年5月之前的一年间,美国国家安全局未经授权收集、存储、获取或分发受法律保护的信息多达2776次。其中2012年第一季度的非法操作次数增加尤其明显。报告说,原因可能在于2012年农历春节期间美国国家安全局非法监听访美的中国公民大量通话信息。

4

网络游戏、聊天软件成获取情报渠道

纪录称,连网络游戏都成了美国获取情报的渠道,英国《卫报》和《纽约时报》公布了美国著名新闻调查机构“为了人民”的文件,名为“对恐怖分子利用游戏和虚拟环境的研究”。该文件显示,美英两国的情报人员假扮“玩家”,曾渗透进网络游戏《魔兽世界》、《第二生命》中,收集真正电脑游戏玩家的纪录,监视游戏玩家。而实际上,这两款游戏的中国玩家最多。

针对中国的监控无孔不入:据媒体报道,斯诺登披露了一批机密文件,这些文件显示,腾讯聊天软件QQ和中国移动的移动即时通信应用飞信竟然也在美国国家安全局的监视范围之内。

美国《外交杂志》说,美国一直就网络攻击问题施压中国之时,却从不提及美方大范围攻击中国网络的情况。而在中方指出美方动作时,面对媒体的求证,美国政府始终拒绝公开置评。