新民环球

本报国际新闻部主编 | 第510期 | 2013年7月11日 星期四 责编:张 颖

热点锁定

韩亚航空214航班6日在旧金山机场降落时机尾撞击地面,继而起火,在这架波音777客机上,有中国公民141人,其中两人遇难。

“监视帝国”布层层密网 “棱镜”背后有技术黑手

网络科技巨头沦为美政府“枪手”

文 / 本报驻美记者 **徐东海**

集结全球最顶尖的电脑黑客、密码破译员、语言学家、电子技术专家,进行着人类历史迄今为止规模最庞大的窃听活动,“棱镜”项目自从被曝光后,全球哗然。

人们在震惊之余,更多的是恐惧,一只由政府主导的技术黑手,竟然已经悄无声息地出现在每个人的生活当中。

今天你发送的任何一封邮件,搜索的任何一个信息,浏览的任何一张图片,都赤裸裸地在“棱镜”中呈现。个人,已无隐私可言。

■ 美国情报机构能轻易获取几大高科技公司服务器上的任何信息 本版图片 GJ

透视“棱镜”背后隐藏的可怕的“监视帝国”,一个事实越来越清晰。大多数人每天都要通过手机、电脑打交道的那些全球科技巨头,包括谷歌、苹果、微软等,已经成为美国政府扩大情报收集触角的“枪手”。

美国利用“先天优势”

“棱镜”项目主要由美国国家安全局负责实施,主要监控全球互联网通讯的邮件、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,甚至可以实时监控某个人的网上搜索。而参与这个计划的科技巨头,个个大名鼎鼎,在全球科技和通讯界呼风唤雨。

根据“棱镜”计划,美国情报人员可以通过“后门”进入9家主要网络科技公司的服务器,包括微软、雅虎、谷歌、Facebook、PalTalk、美国在线、Skype、YouTube、苹果。此外,思科、IBM、高通、英特尔、甲骨文等高科技公司也参与了“棱镜”计划。

据报道,一个苹果手机用户所拍摄的照片、用iOS操作系统发送的每一条信息、使用的软件、存储的信息,都可能被美国情报部门截获、读取。微软在发现电脑病毒和安全漏洞时,最先告知情报机关,然后再向外发布修复消息。

美国国家安全局宣称,由于全球互联网主干“基础设施”都在美国,所以美国在情报搜集领域具有“先天优势”。美国高科技公司的互联网基础服务成为美国国安局监视目标的渠道,这些公司也成为帮助美国政府收集情报的得力下属。

情报机构为所欲为

据统计,国家安全局近七分之一的情报包含来自“棱镜”计划的数据。因为“国家安全局可以直接接入各大公司的服务器,因此它能为所欲为,随时获取想要的任何数据。

斯诺登披露的信息显示,美国国家安全局的“元数据计划”主要通过威瑞森通讯公司实施。威瑞森是美国最大的电话公司之一,光美国客户就达1.21亿。按照安全局的要求,威瑞森每天都要提交元数据,即信息记录。这个计划监视的对象主要是美国人。

■ 美国民众示威抗议政府“棱镜”计划

■ 美国民众用国家安全局的缩写“NSA”制作标语,抗议政府监控计划

《纽约时报》撰文称,目前人们绝大多数的交流通讯是借助第三方服务提供商、云服务提供商完成的。虽然互联网是分布式的,它的基础物理结构却依赖一些关键的节点。这使得政府监控成为可能。

美国国安局只需要与一些可以发挥关键作用的大公司建立合作关系,便可以轻易对大多数互联网数据进行监控。而这种监控耗时短、耗资低。

“棱镜”拥有高端“武器”

科技,是第一生产力。但“棱镜”计划所展示出的,则是科技的另一面:暴力和恐怖。《赫芬顿邮报》称,一旦高科技被拥有无上权力的人所掌控,其产生的效力,犹如核爆般不可阻挡。

据美国媒体报道,“棱镜”项目之所以能产生如此巨大的效力,因为它同时具备了硬件基础、软件基础和通讯自动监控的最高端能力。

网络巨头公司提供了客户端操作系统、电子邮件功能、即时通讯、网络接入服务等功能。所有服务器上的数据都要通过路由器来传送,而思科的路由器拥有监控窃听这些数据的功能,国安局能够通过思科的路由器神不知鬼不觉地获得微软等服务器中心的数据。在硬件层面,“棱镜”拥有最高精尖的武器。

此外,一种新型的数据库软件系统NoSQL突破了传统数据库的弊端,极大地提升了数据存储和访问的需求,允许针对所有类型的数据创建信息要求,帮助国安局快速分析处理数据。

在掌握海量数据后,如何从数据中寻找有用的信息,这是最后一道环节。“棱镜”项目通过对通讯层面进行自动监控,这是最简单有效的方法。

目前,常见的网络传输协议只有几种(HTTP、FTP、SMTP、POP3、TELNET等),大部分网络传输协议都是明文传输数据,国安局只需在路由器的关键节点部署网络监听设备,就可以截取到所有明文传输的信息。如果遇到加密,如https,可以通过发假证书进行中间人攻击,从而破解https传输的内容。

因此,美国国安局只需与数家通讯服务商建立合作,便可以收集超过3亿美国人的电话记录,无需一对一跟踪、监控。

仅在2013年4月,美国国安局便在全球范围收集了超过970亿份情报,这是旧式情报采集方法绝对不可能做到的。

更新保护隐私法律

“棱镜门”使包括美国在内的全世界不得不重新思考隐私保护的边界并更新保护隐私的法律。

《华尔街日报》撰文称,各家科技公司都会收集大量广告数据。除了搜索关键词之外,这些企业还会收集用户的地理位置信息、IP地址、互联网提供商、使用的浏览器、电子邮件地址和手机号码,甚至有的时候他们还会收集用户的面部信息数据。他们通过不同的服务来获取资料,以及使用cookies来分析用户所点击过的广告。

然而,大多数情况下,用户很难决定是否向这些企业发送相关数据。而且这些企业的服务协议通常都很长,用户也没有耐心将其通读一遍。例如Facebook的隐私政策长达3112个单词,谷歌的隐私政策为2250个单词。有时候,这些协议中还夹杂着一些难以理解的专业词汇,谁会喜欢阅读这种东西?

“棱镜”曝光之后,包括谷歌、苹果等巨头都感受到了舆论的巨大压力。“脸谱”、谷歌和微软敦促美国政府允许他们公开更多信息,以驳斥媒体的一些说法。

《洛杉矶时报》称:“新的隐私保护法律也许永远追不上技术前进的脚步。”美国反恐专家雷纳德说,安全和隐私之间的界限或许永远都很难分清楚,但有一点非常明确,公众必须拥有知情权。

相关链接

美国家安全局情报系统庞大

美国国家安全局(NSA),是美国情报系统中,下属机构最多、雇佣人员最多、支出费用最多的一个。国安局表面上隶属于国防部,实际上是一个军政一体化联合情报机构,直接服务于国家安全委员会,向总统提供“最核心”的情报。

美国国安局现有军职和文职人员约16万,超过美国其他16个情报机构雇员的总和。其中43%是密码破译员、语言学家、电子技术专家,是全世界独立聘用数学博士和电脑专家最多的机构。美国国安局年耗资在120亿美元以上,每年的电费就高达2100万美元,门前的访客停车位高达1.8万个。

打开安全局网站主页,标题行赫然写着:“保卫我们的国家,保障我们的未来。”下方常年挂着安全局的招聘广告。计算机科学家、计算机工程师、电子工程师、网络专家四类专业人群成为招揽的对象。安全局在明确提出了工作人员的重要使命——收集国外情报,保卫美国政府信息系统。

美国国家安全局在全球设有4120个监听站和窃听哨所。其中许多设在国外的美国军事基地内,有的设在舰艇、潜艇和飞机上,在太空中运行的200多颗各种卫星也担负监听任务。

美国国家安全局总部大楼里的电子计算机储备器能同时监听100万台电话,利用先进的电子设备系统对通讯信号进行截收、分析、破译、处理。

“定制入口行动”专门针对中国

据美国媒体透露,美国国安局内一个专门针对中国的“定制入口行动”办公室,有超过1000名军事和民间黑客,以及电子工程师、情报分析师、目标定位专家、计算机软硬件专家等,是国家安全局最大、最重要、最神秘的部门,连办公区域都与其他部门隔离。

有一些外国情报机构与美国国安局“合作”,实际上成为美国情报机构的外围组织。

本刊主编 汪一新 卫 蔚

(本刊除“论坛”及本报记者署名文章外,均由新华社供稿)