美国大断网和杭州一家公司有关?

智能设备成了黑客野蛮攻击的“帮凶”
你家里的摄像头可能会泄露你的隐私
扎克伯格也会用胶带封住电脑摄像头

一场在大洋彼岸突如其来的网络瘫痪,让杭州一家科技公司陷入了舆论漩涡。

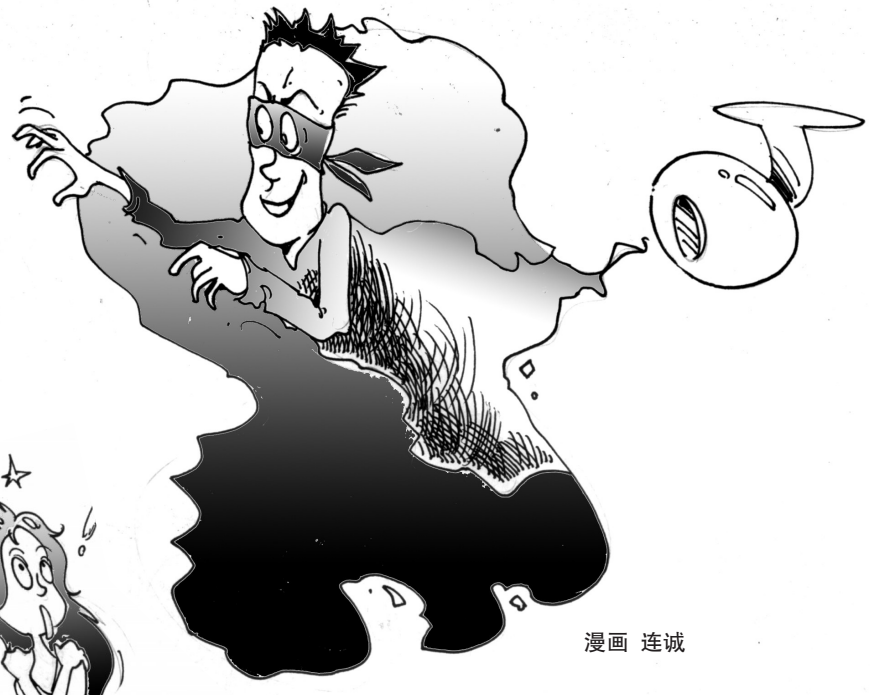
上周末,美国发生了一起规模极大的互联网瘫痪事故,多个城市的主要网站被攻击,包括推特、亚马逊、Paypal等在内的大量互联网知名网站数小时无法正常访问。

事情的蹊跷之处在于,一家名为“雄迈”的杭州公司被指要对此事负主要责任。

更让人不解的是,与这起事件有直接关联的漏洞不但低级,而且存在于眼下大量智能硬件设备中,意味着全球其他地区的网络也可能中招。

在物联网时代,智能设备一路飞快地向前奔跑,将安全远远甩在身后。物联网设备为我们提供了便捷,却也让我们丧失了安全感。

记者 梁应杰



漫画 连诚

智能设备成了野蛮攻击的“帮凶”

引发全美“断网”的罪魁祸首,其实是令互联网业界深恶痛绝的公敌:DDoS,翻译成中文是分布式拒绝服务攻击。

这是一种相当野蛮的攻击方式,黑客只要通过技术手段控制一些服务器或者个人电脑,植入相应程序即可向目标发动“流量攻击”,导致对方带宽被占用,系统瘫痪。就好像一个正常营业的超市突然涌进许多不买东西的人,让真正购物的人一时半会儿无法进入。

发动大规模DDoS的前提是黑客手里有大量的“肉鸡”,也就是那些可以被黑客远程控制的机器。在这起事件中,“肉鸡”不再是电脑,而是已经大规模普及的物联网设备,比如最为常见的摄像头。

而被卷入事件的杭州雄迈信息技术有限公司恰好是一家提供摄像模组的公司,而且规模不小。

资料显示,雄迈是杭州的一家安防视频产品方案和技术提供商,成立于2008年,目前总部位于杭州市富阳区银湖创新中心,公司员工总人数近2000人,研发人员300多人。公司产品主打安防监控模组、主板、配套软件以及产品解决方案,包括AHD同轴高清模组及主板、网络高清模组及主板、AHD/网络一体机芯、自动聚焦模组等。

杭州公司召回部分产品但不背黑锅

不过,在雄迈上下看来,公司对这次事件有一定责任,但远远没有达到如一些国外媒体所说,要对整个事件负责的程度。

“雄迈主要生产安防设备,安防本身在美国物联网设备中占比就很低,涉及到我们产品的就更低了。”雄迈公司负责人说,“而且,这次事件中多数物联网智能设备被黑客入侵,不只雄迈一家。”

本周一,雄迈宣布召回在美国销售的早期部分产品,其中主要是2015年4月之前在美国销售的消费类产品,包括100万(像素)卡片网络摄像机、100万云台网络摄像机(摇头机)、100万全景网络摄像机、130万全景网络摄像机。这些产品召回后会修补弱密码等部分漏洞,并在之后返回给消费者继续使用。

他们同时强调,对2015年4月之后的产品,黑客是根本没办法利用该端口进行攻击的,而针对2015年4月份之前生产的产品,雄迈也已经提供了固件升级程序,若真的担心有风险可以通过升级解决。

多数智能设备正在“裸奔”

据雄迈公司透露,本次事件中黑客入侵控制产品主要是利用用户未及时更改预设密码的操作习惯,如用户更改密码,这个问题就自然解决。这与美国媒体所称的“攻击者通过漏洞猜测设备的默认用户名和口令,控制了这些智能设备系统”基本一致。

因为预设密码过于简单受到黑客控制,这么低级的漏洞听上去有些匪夷所思,但这却是目前大多智能设备的通病。换句话说,这次攻击的技术含量并不高。

现在,多数物联网设备采用与路由器相同的密码体系。例如:用户名是admin,初始密码是12345,用户拿到这些设备连上网后通常没有意识修改,之前网上有种说法,“通过12345、1234、password等简单密码,可以控制10%以上的设备。”

而根据安天安全研究与应急处理中心发布的分析报告,包括Cisico、Sumsung、Dreambox、中兴通讯等多个知名公司的部分设备均存在单一默认密码的问题。

“目前物联网设备的安全状态就像2000年左右的Windows操作系统安全状态。”阿里云首席安全研究员吴翰清说,“很多物联网设备天生就存在缺陷,日常也缺少安全监控机制,无法及时发现自己设备被黑客利用。”

除了预设密码漏洞外,一些企业会忘记关闭一些客户端调试功能的权限,设备端跟云端的通信基本上都没加密,还有一些设备未做身份校验,容易被伪造命令所控制。

不仅是个人设备,政府采购的设备也存在同样的情况。去年,国内一家已上市的知名安防企业曾爆发黑天鹅事件,也是因为初始密码过于简单,客户使用时又没有修改,导致部分设备被境外IP控制。为此,江苏省公安厅发文,要求各级公安机关对涉事设备进行全面清查。

每个人都该把摄像头遮起来?

这不是物联网设备第一次因为黑客攻击走到聚光灯下。今年的3·15晚会上,央视就曾播放过一个“黑科技”视频,视频里正在执行任务的无人机突然不听指挥,家中的电灯和微波炉无故被开启……

问题不仅出在独立的智能硬件上,为了实现智能化以及数据抓取,眼下许多物联网设备都带有小型的硬件模块,比如扫地机器人配备了小型摄像头,空调里有麦克等,这些看上去不起眼的硬件同样可能被黑客攻破,成为对方窥探隐私的“眼睛”和“耳朵”。

不久前,美国联邦调查局局长科米在演讲中表示,出于安全考虑,他用胶带盖住了私人笔记本电脑的摄像头,并建议每个人都这样做。实际上不光是他,Facebook创始人扎克伯格平时在使用电脑时就会用胶带封住摄像头。

如果说小产品关乎的是隐私,那么大产品很可能关乎生命。今年9月,腾讯科恩实验室花了两个月的时间,以“远程无物理接触”的方式成功入侵了特斯拉汽车,他们只要坐在办公室就能控制车里的天窗、门锁,甚至还能紧急刹车。

在智能设备普及程度和安全性的赛跑中,后者已经落后太多。据调研公司Gartner统计,2015年,为解决物联网安全问题而产生的安全费用不足行业年度预算的1%,这一比例到2020年需要提高到20%。

阿里云物联网高级专家张宗锋建议,从事物联网硬件研发的团队多关注和使用较为成熟的物联网解决方案,保障设备端、云端及通信过程的全链路安全,“现在太多团队一味追求市场扩张,重视硬件迭代,忽视了软件的安全性。”

360攻防实验室负责人刘健皓给普通消费者支了个小招:“如果担心自己的设备被黑,也可以自己查查流量是否异常,目前市面上大部分的智能路由器支持终端流量统计。如果我们发现自己的设备被黑,尽量地先初始化这个设备的系统,然后把设备升级到最新版本。”