手机中毒变“肉鸡” 个人信息1元贱卖

黑客通过“手机肉鸡软件”控制他人手机;网上公开叫卖“手机攻击软件”及机主信息

手机中莫名多了几款App;即使换了新号码后,也会接到广告、推销电话;流量会时常无故流失……这些场景发生在众多手机用户身上。记者调查发现,在网络上大量黑客兜售“手机肉鸡软件”,客户只需1至10元钱,即可购买他人的手机信息,从而控制别人的手机。

甚至还有黑客专门在QQ群中收费传授“抓鸡和攻击手机的技术”,声称只需花300元钱,一台电脑一根网线,普通用户即可成为攻击他人手机的黑客。

对此,京润律师事务所律师韩骁表示,利用“手机肉鸡”远程控制他人手机,涉嫌“非法侵入计算机信息系统罪”“非法获取计算机信息系统数据、非法控制计算机信息系统罪”,情节特别严重的,最高可处七年以下有期徒刑,并处罚金。同时,发布病毒链接的网站平台及手机通信运营商也要承担相应的法律责任。

网站被攻击 “肉鸡”干的?

11月28日晚9时,一家网站的编辑孙玲(化名)像往常一样进行稿件的录入,忽然网站的后台不能正常打开。半小时后,网站瘫痪。

“一台电脑有问题影响一大片,我们也接到了异常的反馈。”该网站技术部门负责人周群回忆,刚开始,他怀疑是服务器硬件或者软件故障,就一步步去排查,最后发现网站的访问人数瞬间出现异常。

周群注意到,当时的网站瞬间点击量是两三万人次,往日即使是搞活动也没有那么多。“这一定是被攻击了”。

从11月28日晚9时30分到11月29日凌晨3时许,周群不得不三次切断投票服务站点,不再提供对外的访问,但效果并不明显。“再次打开网络服务后,攻击依然继续。”

第三次主动关闭网络服务的同时,该网站联络到青松智慧(北京)科技有限公司的第三方防护平台,经过商议,由青松协助网站对攻击进行识别和拦截。

凌晨两点多,还在睡梦中的青松智慧(北京)科技有限公司市场总监吴祖欣被公司CEO的电话吵醒,让他起来一起对这家网站受到的攻击进行拦截。“攻击高峰时,一分钟200万次访问请求,一小时就是1200万次,那天我们拦截了将近10亿次的攻击。”吴祖欣说。

一直到11月29日上午8时许,吴祖欣三人才将拦截工作移交给技术人员。他说:“真正攻击结束时间一直到当晚8时25分左右,整个攻击持续了近24小时。”

事后,周群在对服务器日志分析时发现,攻击IP有六七成来自手机“肉鸡”。

谁侵入了我们的手机?

何为“手机肉鸡”?吴祖欣介绍,“手机肉鸡”是被植入了病毒或有安全漏洞的个人手机。这种手机被黑客控制后,可任意被攻击或窃取信息。

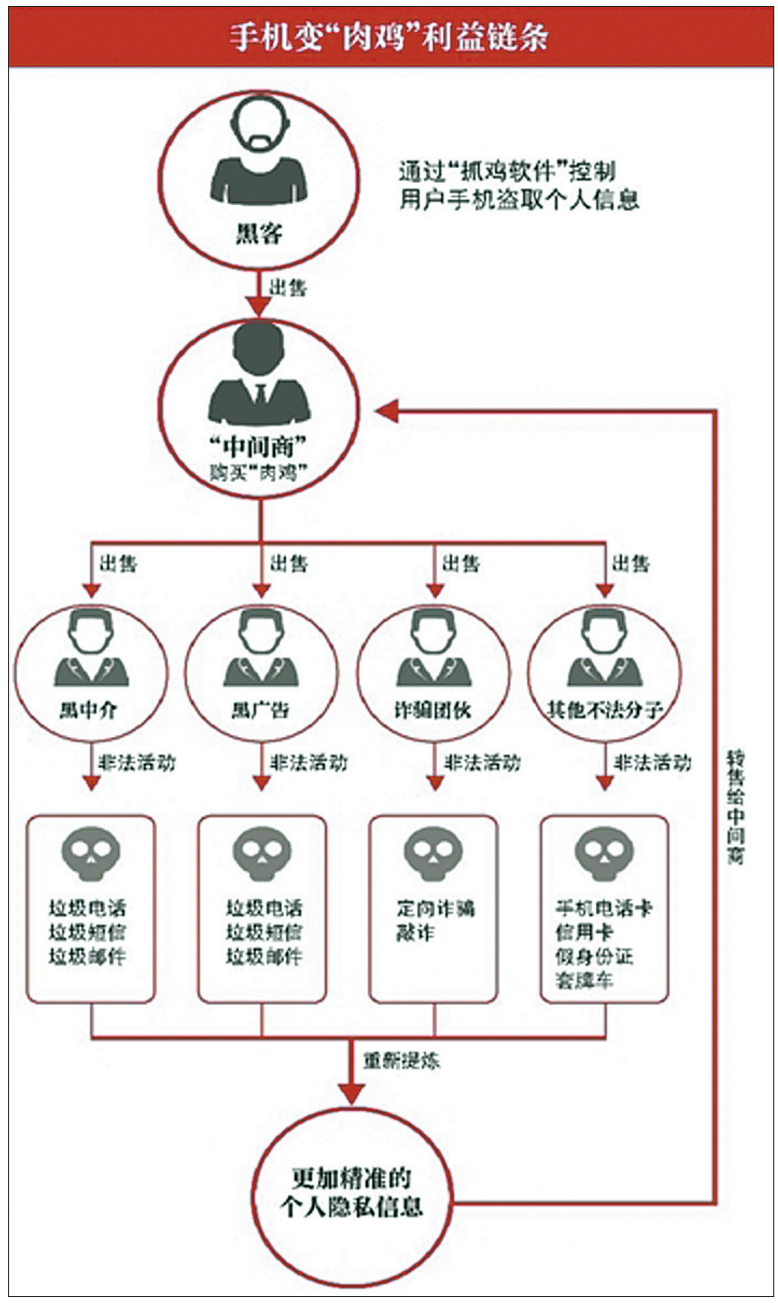
去年8月份,广东韶关市一名企业负责人,在手机没有离开身边的情况下,手机在他睡梦中离奇地向企业财务人员发送了要求转账的短信。财务人员根据上级的这条短信,向诈骗分子转账57万多元。

后经查实,原因竟是他点了一下短信发来的下载链接,中了木马病毒,遭到不法分子远程控制手机,盗取里面的信息。

一位互联网安全防御公司人员介绍,他们接触到移动互联网被攻击的客户是在2013年左右,而“手机肉鸡”的出现,则是伴随着智能手机的兴起便开始出现,“简单来说,手机就是一台小型电脑,在电脑上可以实现的东西,在手机上同样适用”。

今年2月28日,北京朝阳区法院审理的一起案件中,北京麦德联合信息技术有限公司、深圳市安丰易联信息技术有限公司、深圳万丰博通信息技术有限公司三家企业负责人,由于利用静默插件恶意推广App、获取用户隐私数据,以非法获取、控制计算机信息系统数据被判处有期徒刑1年5个月至3年不等。

涉事公司在将插件植入刷机软件后,运营部门会通过后台服务端操控,向被静默插件感染的手机推送软件、广告等商业电子信息。当用户手机上网后,该插件会自动激活。他们再通过服务器操作,随意给用户推送广告。



在上述两个事件中,手机便是中了病毒成为“肉鸡”。360网络安全研究院工程师李丰沛介绍,不法分子在机主不知情的情况下,可以控制“肉鸡”做任何事情,获取手机内的所有信息。比如悄无声息地盗走用户网银或第三方支付账号的资金,静默删除短信、静默发送短信及下载App,手机流量也会莫名被“偷走”。

李丰沛介绍,正常互联网赚钱方式主要靠流量,“地下”互联网也一样。网络黑客会用各种方式收集流量。可以用“手机肉鸡”去刷App的下载量,比如在你睡着的情况下,半夜12点手机被控制开始下载,下载后去打开,3点钟结束后自己删掉,作为手机的主人完全不知道有这件事情发生。此外,手机里的通信录、电话号码移动轨迹等所有数据都可以卖钱。

“抓鸡软件”300元学全套

记者调查发现,网络上存在大量的可以购买的“手机肉鸡”攻击服务,花300元即可学会全套“抓鸡”技术。

在搜索引擎中及QQ群搜索服务中输入“黑客肉鸡DDOS”等关键词,页面会自动弹出推广链接,均为提供黑客服务的网站及论坛,并附有大量QQ群号码。

12月8日,记者加入多个含有“肉鸡”“DDOS攻击”等字样的交易群,这些群人数不一,少的130人,多的达1000人。在名为“勉头 ddos/CC攻击销售”的247人QQ群内,每隔十分钟左右,就有不同人发小广告,宣称“接单出‘肉鸡’,收费带徒、主教‘抓鸡’、攻击、入侵等黑客技术”。

多位在群内发送“小广告”的黑客热心地向记者介绍了如何“抓鸡”、攻击等问题后,都表示让记者向其“拜师”深入学习。

网名“秒杀网络”黑客直接提出“拜师”价码,记者向其支付宝账户转账300元后,他改口称记者为“徒弟”。

学徒从获取“抓鸡软件”开始。12月8日,“秒杀网络”给记者发来“手机DDOS”的压缩包,并连接了语音,QQ直播“抓取手机肉鸡流程。”压缩包内含有“安卓自动抓鸡工具”“123APK”木马病毒及“安卓苹果手机DDOS客户端”。

有了专门的“抓鸡”软件,还需要有相应的服务器来运行。“秒杀网络”说,软件会在服务器内自动扫描全网有漏洞的手机,进行抓取,抓到后软件内木马会自动种植在手机上。种植成功后,变身“肉鸡”的手机就会自动上线成为他们App的用户,并显示出手机IP和手机号。

在数十个QQ群中,“抓鸡软件”销售者报出的价格大同小异。“电脑抓鸡软件”是200元,所需服务器也为每月200元。“手机抓鸡软件”是300元,专门的服务器需要600元每月。“不正规的服务器即可,正规的查到会封杀。”

“我一天接几十个单子,等你学得差不多了,我会给你单子接。”“秒杀网络”嘱咐记者不用着急,一个人就可完成“抓鸡”攻击任务。

“秒杀网络”不无炫耀地说,今年才学习了自己编木马及“抓鸡软件”程序,没几个月已先后带过20多位徒弟。目前已经成立了一间工作室,有8人,均是自己的徒弟。

一位从事互联网安全的业内人士透露,网络上的大量黑客收费带徒,存在陷阱。黑客圈内将初学黑客技术的年轻人称为“小白”,利用网络攻击赚钱的黑客,会持续发展“小白”成为他们的下线。师父发给徒弟的软件可能存在“木马”,徒弟利用软件抓取“肉鸡”的同时也就成为“师父”的“傀儡机”。说白了就是“师父”用木马控制“徒弟”的电脑,获取免费“肉鸡”。

“肉鸡”软件推广月入数十万

除了网络攻击、收徒等,记者发现,黑客在抓取“手机肉鸡”后,还会进行出售。病毒制造推广者月入数十万。

“只要你愿意花钱,就可以控制别人的手机。”在网络“手机肉鸡交易”QQ群中,“肉鸡”被明码标价,其中“电脑肉鸡”价格为0.2到1元,而“手机肉鸡”则要贵几倍,需要1元到10元不等。

卖家介绍,现在“手机肉鸡”几乎都是安卓系统的。因为安卓系统手机防御性比较弱。一位网名为“免杀肉鸡DDOS”的卖家称其手中有2万台安卓“手机肉鸡”,“我一直在出货,有人来买。”“免杀肉鸡DDOS”说,因“肉鸡”可多人共享,所以一台“肉鸡”卖过之后可反复再卖。

记者联系上一名自称为婚庆公司购买“肉鸡”的员工,其表示“手机肉鸡”是他们公司主要的广告发布渠道。他们买来海量“手机肉鸡”自动向机主推送婚庆广告。他介绍“手机肉鸡”也兼具刷广告的功能,用“肉鸡”刷网站流量,这样公司在搜索引擎当中的排名也会靠前。

据2013年的一款手机病毒研究报告显示,某团伙用一款后门程序,历时1年多,构建了一个覆盖百万用户、可远程任意操控用户手机的“僵尸网络”,病毒制造者将一款后门程序植入各种被篡改的热门安卓游戏当中,利用应用市场、论坛、搜索引擎等渠道进行推广。手机一旦下载,便会沦为“肉鸡”。报告揭秘,病毒制造者使用恶意推广和点击欺诈等手段,大量骗取广告联盟的广告费和广告主的推广费,可轻松实现每月数十万的收益。

而在前述朝阳区法院审理的案件中,涉事公司运营部门便是通过后台服务端操控“手机肉鸡”。截至2013年8月案发,被植入静默插件的用户已达到40余万,推送广告获利20余万元。

网站发布病毒链接也需担责

记者获得的一份“手机抓鸡软件截图”显示,抓取的“手机肉鸡”会显示在线上客户端内,用户的手机IP、网络状态、手机名称等信息一一暴露。若想监控,甚至可以显示手机的通信录、通话记录、短信、摄像、文件等。

互联网安全业内人士解释,每一部手机只有一个IP,当你的手机存在漏洞时,就可能被黑客利用“抓鸡软件”植入木马。

上述人士表示,这些所谓的“抓鸡教程”的市场需求非常广大,抓“肉鸡”出售或转让,盗“肉鸡”的信息资料等转手出售,控制“肉鸡”点击广告、网站、下载App,甚至偷拍“肉鸡”主人的隐私照片来实施巨额敲诈。

今年2月5日,在工信部发布的《2014年全年及第四季度电信服务情况》中显示,在去年组织的对40家手机应用商店拨测筛查过程中,发现不良软件107款,如《飞语免费网络电话》《碰碰》《微微网络免费电话》等App等,涉及违规收集用户个人信息、恶意“吸费”、软件自动向外发送短信、强行捆绑推广其他无关应用软件等问题。

京润律师事务所律师韩骁介绍,刑法有关于侵犯手机系统犯罪的相关规定。依据《刑法》第285条,控制及销售“手机肉鸡”适用于“非法侵入计算机信息系统罪”“非法获取计算机信息系统数据、非法控制计算机信息系统罪”和“提供侵入、非法控制计算机信息系统程序、工具罪”。情节特别严重的,最高可处七年以下有期徒刑,并处罚金。

韩骁表示,从承担责任上分析,制造和传播该手机病毒的人作为第一责任人,应该承担用户的损失。发布病毒链接的网站平台以及手机通信的运营商也要承担一定的法律责任,他们有责任屏蔽、清除手机病毒,为消费者提供一个安全、良好的消费环境。

(新京)