



木马短信成最新诈骗方式

据了解,手机木马短信已经成为最新的诈骗方式,犯罪分子通过伪基站向周围的手机用户发送木马短信,或者冒充好友在网络聊天中发送木马链接。只要一点击链接,各种网银账号密码、短信验证码就很有可能被木马盗取,然后转发到不法分子手中,后果不堪设想。

腾讯移动安全实验室有关人士说:“我们关注到,网络的黑色产业链在 2014 年底开始就发生了显著的变化,目前手机木马的盗刷事件呈高发态势。”数据显示,2015 年上半年,手机支付木马病毒新增 29762 个,感染用户总数达到 1145.5 万,最高峰的 6 月,平均每天有 6.8 万名用户中毒。

利用手机木马的不法分子,已经形成了由买卖个人信息、制作植入木马病毒、盗刷、线下转移资金等职业化明显的作案团伙。另外,黑产团伙利用互联网技术跨平台进行非法洗钱销赃,也致使多个互联网平台及电商蒙受信誉及实际的经济损失。

个人信息被肆无忌惮买卖

该实验室相关人士说,他们发现,近一年来网络欺诈手段越来越高技术化,其中短信手机木马的发展最为迅速,也是他们和警方近期打击的一个重点。

日前,公安部、工信部、中国人民银行等 23 个部门将联合在全国开展打击治理电信

网络新型违法犯罪专项行动,集中打掉一批犯罪团伙,整治一批重点地区,铲除一批盘踞境内外的犯罪窝点,治理整顿一批提供非法电信业务的线路运营商。

那么,网络不法分子是如何获悉用户个人信息的呢?记者从业内了解到,除了黑客盗取之外,一部分是用户自己主动或被动泄露的。比如,微信上的一些优惠赠送,吸引用户主动填入了相关个人信息;其次是个人信息交易市场猖獗,很多用户收到过退改签机票诈骗信息,经过调查发现,主要来自海南省某市,当地不少人靠此为生,用一切手段拿到信息。在大数据时代,机票信息泄露的渠道很多,从许多第三方软件、机票销售网站等都可以拿到。

个人信息的不慎泄露,往往给不法分子带来可乘之机。有媒体报道,今年 5 月 11 日,河南南阳某公司老板吕某的手机被木马控制,犯罪分子拉取其通讯录,向其他公司负责人冯某发送催款短信,导致冯某被骗 500 万元。

7 家虚拟运营商被监管部门约谈

电信诈骗案频发,也反映出运营商和金融机构在安全防范方面仍有机可乘。有警方微博指出,中国人民银行、工信部近年来一直强调落实发卡实名制,由于利益的驱动,一些银行和电信运营商并未严格执行这一要求。另外,电信诈骗反映的电信运营商和银行安全管理漏洞长期存在,一直没有得到

改善。

最近,工信部官方微博表示,近期工信部信息通信管理局就 170 号段垃圾短信问题约谈了远特通信、贵州朗玛、北京国美、深圳爱施德、天音通信、苏宁云商、分享通信 7 家虚拟运营商。工信部向这些虚拟运营商强调法律法规要求,并督促相关企业切实落实责任,采取务实措施,加强垃圾短信治理。

对此,中国虚拟运营商产业联盟秘书长邹学勇表示,目前有一些 170 号段存在诈骗违法行为,导致用户投诉率高,这对 170 品牌产生了负面效应。记者还了解到,广州某些“6”字开头的固话(中国铁通)也屡屡被骚扰电话或诈骗电话所使用。

如何解决

1.技术对抗,网友举报,联动警方。

根据各大安全企业的成功经验看,一方面,企业后台要及时发现网络犯罪的线索,并将线索移交警方。比如建立起伪基站打击平台,犯罪分子在通过伪基站给周围的用户发木马短信的时候,相关企业就能监测得到,及时协助警方精确打击手机木马的伪基站违法犯罪。另一方面是通过网友举报。

2.加强产品识别和风险拦截。

科技企业要加强风险预警和拦截能力,对手机木马病毒进行拦截,对风险支付进行

控制。比如在今年 8 月 25 日,深圳的吴小姐由于泄露了个人信息,导致银行卡被盗刷 3 万元。相关企业获悉后立即响应,利用风控自定预案机制,成功拦截了被骗资金,整个过程前后花费不足 30 分钟。

3.联合行业合作伙伴,建立安全生态链。

由政府或行业协会牵头成立相关组织,欢迎更多行业伙伴加入,发挥各家公司的优势,共同建立起跨平台、跨行业的联动打击机制。

手机中毒 短信验证码或遭拦截

该网友表示,其亲戚曾收到一条短信,没有网址,都是数字,“他打开看了一下……其他没有什么异常……从来没有登录什么网址。”相关专家认为,一般来说,不法分子通过发送短信,让持卡人点击了网址,就容易感染手机病毒,从而导致短信验证码遭到拦截。“这种病毒其实并不难制作,但是有的病毒是所有的短信都拦截,有的病毒只拦截带有‘验证码’字眼的短信。”猎豹移动安全专家李铁军说。

如果手机中毒,一定是要下载并且安装才可以,因此原因很难鉴别。为了防止手机中毒,别通过短信链接去下载软件。若已发现中毒的,立刻拔出 SIM 卡,装在正常手机上,同时,对原来的手机进行杀毒处理。

(广日)