手机“蝗虫”病毒爆发短信别乱点

全国 50 万部手机中招

通信工作室
负责人:戴黎明
电话:13803769176
E-mail:xyrbsm@163.com

8 月 2 日,有哈尔滨市民向记者反映,收到一条带链接的短信,发短信的人是通信录里的联系人,点开后,却遭遇了手机病毒。

2 日上午,哈尔滨市民周晓梅正准备出门,拿起手机一看收到了朋友发来的信息。周女士告诉记者:“信息里写着,‘周晓梅,看这个,http://cdnXXshenqi.apk’,因为当时在家有wifi,我也没多想,以为是朋友发来的有意思的网站就点开了。”周女士说:“没想到点击之后下载了一款 apk 压缩包应用软件,等了半天我看没反应,以为是朋友恶作剧就没当回事儿。可是没过几分钟,有朋友回复问她链接是什么意思,还给我发来一个短信的截屏。我一看确实是我给他发的信息。这时候我才意识到可能在自己不知情的情况下给通讯录的联系人发了同样的短信。”

随后,周女士删除了刚才下载的软件,但是查询话费后发现自己的话费一下少了 20 多元,相当于给通讯录里的 200 多个好友发送了 200 多条短信,这时周女士确信自己的手机中毒了,于是她开始发短信提醒朋友不要点击短信链接以免也中招。

为此,记者电话采访了相关专家。专家表示:“截至 2 日 14 时到 18 时,“蝗虫” 超级手机木马病毒短信发送 500 万条, 全国受感染手机已经超过 50 万部。

制作传播手机病毒 19 岁大学生被抓

据公安部治安管理局官方微博“公安部打四黑除四害” 消息,2 日凌晨 1 时, 深圳网警陆续接报群众手机感染“XX 神器”木马病毒的警情,立即联合罗湖分局成立专案组开展侦查,后又接到山东潍坊、四川成都等地网警部门案情通报,经过 17 个小时的通宵奋战,于 8 月 2 日 18 时抓获制作传播超级手机木马“蝗虫”的犯罪嫌疑人李某。目前,该案正在进一步侦查中。

据深圳警方 8 月 3 日下午透露,“XX 神器”作者李某,男,19 岁,湖南省新邵县人,中南大学软件系大一学生。李某暑假期间来到深圳父亲身边度假。出于好奇,想自己尝试做一款全国大范围传播的手机软件,于是独自于 7 月 24 日制作了这一款手机木马,后从其自己手机上开始往外传播。

2 日 11 时,腾讯手机管家通过对病毒样本的反编译,迅速找到了犯罪嫌疑人李某在病毒包中预留的手机号码、邮箱号,根据这些信息确定了犯罪嫌疑人在深圳。

软件是安卓安装包只针对安卓手机

此次爆发的群发短信病毒软件究竟从何而来?

有网友称,该安装包最先起源于一些低端视频网站的看片神器,但截至目前此说法未得到官方证实。

记者就此咨询了一名一线网警,他表示,这条短信是一个典型的病毒短信。首先,该短信中的链接使用 CDN 为开头,以 APK 为结尾,熟悉手机软件的专业人士一眼就能看出这个链接是一个不安全的下载软件。

网警解释说,CDN 是内容分发网络,通俗地说就是一个资源管理中心,很多的资源都上传到这里,用户可以在这里下载。APK 就是安卓系统的安装包,相当于 windows 中的 exe 文件,所以这个病毒只会对安卓手机产生影响。

三大运营商拦截“毒”短信千万余条

中国电信、中国移动、中国联通针对 8 月 2 日爆发的超级手机病毒,在全国范围成功拦截该病毒短信千万余条,并阻断病毒下载链接。

中国电信网络安全团队于 8 月 2 日上午首先分析并确认了一例有广泛传播趋势的安卓恶意手机病毒,随即启动了全网处置行动,第一时间在电信全网范围切断了此病毒的传播途径。

同时,中国移动也做出部署,在全网实施拦截和封堵病毒扩散,并通过中国移动官方微博等渠道及时向广大用户预警;中国联通立即采取紧急措施,实施关键字拦截恶意短信,并通过 WAP 网关进行网址链接拦截。

恢复手机出厂设置彻底踢走病毒

针对新型移动互联网恶意木马程序,国家计算机病毒应急处理中心建议:

1.通过恢复手机出厂设置来根除病毒。

2. 用户如果怀疑可能已经被感染,应马上停止网络连接,与运营商联系,核对通信话单,检查短信记录和网络使用记录,发现来源不明的短信发送行为和网络访问请求,并立即更改手机应用的账户密码等隐私信息,尤其是金融支付类、通信类相关的应用,以免造成进一步损失。同时告知通信录中的亲友,请勿轻信可能由本机号码发出各种虚假信息。如果造成经济损失,请保留通信话单、保持手机当前状态,向所属地区公安机关报案。

(据《生活报》)

银监部门警示:

电信网络诈骗出现三大新形式

上海银监局日前警示,电信网络诈骗作案手法正出现三大转变:一是转账方式更多从柜面逐步转向网上银行、自助机具、电话银行、手机银行等离柜途径;二是诈骗内容从冒充亲友、欠费欠税、中奖咨询等向理财、网购、养老补贴等转变;三是诈骗方式从计算机轮候录音拨号向接听者精准施骗转变。

最新统计显示,今年上半年,上海银行业营业网点成功防阻电信网络诈骗案件共 345 起,挽回群众资金损失 2451.1 万元。

为应对当前不法分子诈骗形式新变化,上海银监局会同沪上各银行持续探索推出网银转账防骗提示、限制无序开卡、涉骗“灰名单”预警、新业务推出安全风险评估等源头防骗措施,指导辖内银行深入持久地开展防范电信网络诈骗工作,探索防范新举措。

上海各商业银行也积极行动,在坚持“四问一告知”“四核实”等防阻措施的基础上,结合实际开展新的防骗措施。

上海银监局表示,下一步还将从制度建设着手防范电信网络诈骗。一是进一步推进同一客户借记卡开卡数量设限工作,遏制借记卡交易市场的蔓延;二是尝试建立跨行合作机制,利用警银“点对点”系统推动信息共享,搭建电信诈骗涉案账户快速冻结平台;三是进一步推动银行开发网银系统防欺诈功能,加强网银账户资金流向监控,用足用好手机验证码提示短信的尾字宣传功能。**(据新华网)**

中国手机支付用户达 1.25 亿

同比增长 126%

去年,我国移动支付交易规模增长率为 707%,远高于银行卡收单、互联网支付等增速。移动支付正进入高增长时期,但也暴露出安全性能和稳定性能缺乏等隐患。

这是记者从中国互联网协会与新华社《金融世界》2 日联合发布的《2014 中国互联网金融发展报告》中获悉的。报告显示,去年我国手机支付用户规模达 1.25 亿,同比增长 126%,手机支付、网络银行、金融证券等相关各类移动应用累计下载量超过 4 亿次。其中, 支付宝钱包下载量占比达 58%。交易便捷使得移动支付进入爆发式增长期。

便捷总是以牺牲一定安全性为代价的。中国互联网协会副秘书长石现升说,由于智能手机操作系统的脆弱性、平台开放等特点, 移动支付也受到手机安全漏洞和各类木马的威胁,安全性能和稳定性能不足。

他建议,联合运营商、银行、第三方支付平台等做好技术防范措施, 并通过应用大数据等加强对第三方支付资质的评估与监管,加强对应用软件的审核监督,并呼吁从宏观层面出台统一的手机支付安全标准,完善相应法律法规,确保网络安全。 **(据《京华时报》)**

智能手机管理缺陷

让大多数用户面临风险

据英国路透社 8 月 1 日消息,安全研究人员本周表示,当前智能手机面临的两大威胁可能会让全球 90%的智能手机用户遭遇密码和数据被窃,甚至黑客完全掌控手机的风险。

威胁之一是,苹果、谷歌、安卓以及黑莓等智能手机的制造商执行模糊的行业标准。该标准负责控制从网络接入到用户识别在内的一切活动如何接受管理。

网络安全公司 Accuvant 的手机研究人员 Mathew Solnik 在接受路透电话采访时表示, 这种风险可能会让攻击者远程控制手机,安装恶意软件、访问数据并运行智能手机上的应用等。

另一项威胁是旧金山 Bluebox Security 的研究人员发现的,可影响至少四分之三运行较早版本安卓软件的手机。

Bluebox Security 称,这个被称为“Fake ID”的漏洞可让恶意应用程序骗过安卓设备上运行的 Adobe、谷歌以及其他公司的信任软件,而用户却得不到任何通知。

Bluebox 在声明中表示:“基本上,任何依赖验证签名链的安卓应用程序都会受到这一漏洞影响。”**(据环球科技)**

二季度电信服务申诉率上升

44 款不良软件曝光

工信部近日发布今年第二季度电信服务质量报告:本季度电信服务能力持续提升;通信网络安全畅通;信息消费规模持续扩大;季度百万用户申诉率 7.9 人次,较一季度上升 3.9%;主管部门对垃圾短信、不良手机软件、服务协议和流量收费等问题进行了重点治理。

本季度工信部组织对 40 家手机应用商店拨测筛查,发现不良软件 44 款,主要涉及过度收集用户信息、软件自动向外发送不明短信、恶意操控用户手机、恶意“吸费”、强行捆绑推广其他无关应用软件等违法违规问题。

曝光的应用商店包括安卓应用市场、网易应用中心、91 门户、小米应用商店、搜狗市场等,其中找你妹、实况足球、微信攻略、愤怒的小鸟太空版攻略等应用赫然在列。生活类、攻略类 App 是不良应用的主阵地。

工信部对这些违规软件涉及的应用商店经营者已进行集中诫勉谈话,责令自查整改,下架不良应用软件。**(据新华网)**