手机木马 窃取2000万条通讯录

刷机植入水货手机 后台推送软件广告 10名涉案人员获刑

3家公司研发"静默插件",利用刷机操作将插件装入水货手机,窃取手机用户通讯录近2000万条,涉及用户40万名。记者2月28日获悉,3家公司的10名涉案人员因犯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,被北京朝阳法院一审判处有期徒刑3年半至1年5个月不等的刑罚。

□案情

3家公司勾结作案

朝阳检察院指控3家公司涉案人员杨小慧、陈新等10人犯了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。

据朝阳法院审理查明,这3家公司分别为北京麦德联合信息技术有限公司(以下简称麦德公司)、深圳市安丰易联信息技术有限公司(以下简称安丰公司)、深圳万丰博通信息技术有限公司(以下简称万丰公司)。3家公司中,44岁的杨小慧是麦德公司的实际控制人,37岁的张炳是麦德公司副总;37岁的陈新是安丰公司法定代表人;30岁的罗真运则是万丰公司的法定代表人。3家公司的经营范围包括计算机软件开发、网络技术开发、手机软硬件开发等。

朝阳法院审理查明,自2011年底起,杨小慧、陈新、罗真运、张炳经商议后,便授意马庆沐、林伟东、吴浩、黄光侠研发"静默插件",将该插件通过刷机的方式,植入大量移动终端。杨小慧、张炳等人安排祝春娟、杜雪梅通过后台服务端操控,向植入"静默插件"的移动终端推送软件、广告等商业性电子信息。

远程操控用户手机

经鉴定,该"静默插件"可在用户不知情的情况下获取用户手机位置、读写用户存储卡等多种功能。通过刷机方式,可将该款插件植入大量手机。而麦德公司员工祝春娟、杜雪梅等,便可远程操控后台服务端,向植入"静默插件"的手机推送软件、广告等。同时,该款"静默插件"还可获取大量移动终端存储的通讯录、所处地理位置等数据信息。

据公安人员现场勘验,在杨小慧等所经营的公司服务器内,含有大量的用户移动终端内的信息,被获取移动终端内通讯录近2000万条。

朝阳区检察院指控3公司10名涉案人员的行为触犯了我国《刑法》第285条第2款等相关规定,已构成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。

□供述

公司最初主营刷机

杨小慧供述,2010年,他和陈新、罗真运、张炳在深圳成立了万丰公司、安丰公司后,在2011年又在北京成立了麦德公司,负责安丰下载的运营、手机软件及广告的推广。

万丰公司的主要业务是给水货手机提供rom包,给软件开发商推广软件,将开发商的软件植入rom包,再将rom包刷到水货安卓智能手机里,从中获取软件开发商支付的推广费。

安丰公司主要开发appstore业务,即安丰下载软件,由万丰公司负责推广。

自己制作插件牟利

在2012年初,因线下预装rom包及软件生意不景气,杨小慧便和陈新、罗真运、张炳商量,再制作一个插件植入用户手机。

"静默插件"最初在2011年底,由张炳和陈新提出,由马庆沐和林伟东研发,目的是通过服务端,向使用该插件的手机用户推送软件以获取推广费。经安排,马庆沐、林伟东开发了该款插件。该插件的功能是通过给智能手机刷rom的形式,安装在用户手机里,该插件在手机用户不知情的情况下,以后台方式在手机中运行。

当用户手机上网后,该插件会自动通过互联网联系该插件所在的服务器,该手机即被激活。他们再通过服务器操作,未经用户允许,给用户推送软件及广告信息,从中获利。

插件截获隐私数据

杨小慧称,该插件可以获取用户手机的相关数据,截至2013年8月案发,被植入"静默插件"的用户已40余万,通过在用户手机中植入静默插件,推送广告获利约20余万元。

杨小慧供述其是这3家公司的主要负责人,麦德公司研发部门有张炳、马庆沐,商务推广是祝春娟,运营维护是杜雪梅,这些人均知道公司以"静默插件"方式推送广告及获取用户信息的事。

2012年夏天,杨小慧和陈新、罗真运、张炳、吴浩5个人通过讨论,决定在以前的插件中加入上传手机用户个人资料信息、通讯录的功能,后由吴浩制作该软件,马庆沐参与升级,可将个人信息全部上传至公司的服务器。

据查,该款插件先后更新至5个版本。

通过刷机植入插件

祝春娟在供述中表示,其在2011年10月到麦德公司做商务专员,自己会接到公司发的一个apk格式的文件包,"里面是新研发软件的程序,接到文件包后,我发给技术部门或者运营部门。技术部门会在深圳为水货手机刷机,将文件包里的软件直接预装在手机里。把文件包发给运营部后,运营部会通过推送软件给手机用户发送新软件的广告"。

祝春娟称,2013年1月,麦德公司副总张炳明确跟她说:"做静默推广是为了提高收入,该应用加载到用户手机上后,不经用户同意即可安装软件。"

□判决

3公司10名涉案人员获刑

朝阳法院审理后认为,该案中,杨小慧、陈新、罗真运、张炳,以营利为目的,授意技术人员马庆沐、林伟东、吴浩、黄光侠研发升级"静默插件",并安排祝春娟、杜雪梅通过后台服务端操控的方式向植入"静默插件"的移动终端推送软件、广告等商业性电子信息,从而非法获取计算机信息系统数据,实现对计算机信息系统的非法控制。杨小慧、陈新、罗真运、张炳、马庆沐、黄光侠、吴浩、林伟东、祝春娟、杜雪梅的行为触犯了刑法,均已构成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。

对于杨小慧及其辩护人,陈新、张炳的辩护人所提该案被告人安装"静默插件",其行为没有违反国家规定,杨小慧、陈新、张炳的行为不构成犯罪的辩护意见,朝阳法院认为,根据我国《计算机信息系统安全保护条例》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》等相关法律规定,杨小慧、陈新、张炳等人以营利为目的,共同商量决定研发"静默插件",未经手机用户的同意,通过向用户手机(通信设备)预置"静默插件"的方式侵入计算机信息系统,非法获取身份认证信息,并在手机用户不知情的情况下向用户推送软件、广告等商业性电子信息,其行为已违反国家规定,构成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。

最终,朝阳法院审理认定,以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判处杨小慧有期徒刑3年半,罚款5万元;判处陈新、罗真运、张炳有期徒刑各3年,罚款3万元;判处马庆沐有期徒刑2年,罚款3万元;判处黄光侠有期徒刑1年半,罚款2万元;判处吴浩有期徒刑1年半,罚款2万元;判处林伟东有期徒刑1年5个月,罚款2万元;判处祝春娟、杜雪梅有期徒刑1年5个月,罚款1万元。

□提醒

小心免费APP 卖隐私偷流量

现在大家智能手机上,都安装了免费的"手电筒"APP,你有没有想过,这种免费的手机应用靠什么赚钱呢?近日,360互联网安全中心发布《2014年APP广告插件安全研究报告》显示,免费APP的广告插件存在暗中卖隐私、偷流量赚钱的行为。

记者在手机"安卓市场"里,下载了几款"手电筒"APP。然而,在安装这些不同公司出品的"手电筒"软件时,记者发现,这种仅需使用手机闪光灯的软件,竟然要求手机用户开放包括读取通讯录、通话状态和身份,以及拍照和视频功能等不必要开放的权限。

360互联网安全中心表示,目前,这种免费APP广告插件收集用户隐私信息、滥用隐私权限的情况比较普遍,一旦涉及用户隐私的权限对某个APP放开,就等于把隐私毫无保留地贡献给APP开发商。一般泄露出来的个人信息会被用来分析,还可能通过地下产业进行转卖流转,用于推广或发送广告信息等。

这位专家表示,手机用户装APP时,一定要注意观察软件权限。手机安全软件可以对敏感权限进行关闭,及时对应用程序申请的不必要权限进行管理限制。专家以一款"手机电筒"APP为例,这款手电筒的安装文件大小约为2.9M;而将该应用中的所有广告插件都祛除后重新生成的文件仅为1.1M,二者相差了1.8M。 (据京华时报)