5000万条短信莫名消失的背后

500万台手机被控制，5000万条短信被截取，出售公民信息获利790余万元，受害人遍布全国31个省份。近日，浙江省新昌县公安局侦办的“8·12”特大侵犯公民个人信息案进行了宣判，70余人受到法律的惩处。

在这起案件中，犯罪嫌疑人将目光瞄准老年手机，通过安装木马程序截取老年手机中的各类个人信息，再将这些个人信息出售给他人用来“薅羊毛”。此案是新昌警方近年来破获的涉案金额最大、涉案范围最广、抓获人员最多的一起侵犯公民信息安全案件。

外婆的新手机为何收不到验证码

2019年8月12日，新昌县市民小朱给外婆买了一台新手机，等拿回去用时才发现，外婆的手机无法收到验证码短信。小朱一连试了很多次，还是无法收到验证码，便怀疑外婆的手机被人安装了不法程序。当天，小朱前往新昌县公安局羽林派出所报了案。羽林派出所接警后立即通知了网安大队，网安大队副大队长陈懿立即前往处理。

“我带着技术人员到达现场后，实地测试了一下这台老年机，发现手机卡插入这台老年机中，就无法收到验证码，插入其他手机中，又能正常接收验证码，怀疑这台手机被安装了木马软件。”陈懿告诉记者，网安大队立即开展调查，对这台老年机进行了全面测试。经过反复的试验，警方发现，这台老年机上收到的验证码全部发向某一服务器。

经过查询，这台服务器属于深圳的一家公司。警方还发现，这个现象不是个例，他们陆续检测了20多台同款老年机，都发现了相同的现象。

鉴于案情重大，绍兴、新昌两级公安机关成立了由网安部门牵头的“8·12”侵犯公民个人信息案专案组。在查明了整个犯罪团伙的组织框架后，专案组随即赶赴深圳进行抓捕。经过长达10天的蹲守摸排，专案组掌握了整个公司的人员结构。待公司主要负责人全都到位后，专案组雷霆出击实施抓捕，一举抓获以吴某为首的14名犯罪嫌疑人，扣押电脑主机20余台，扣押作案手机1300余部，现场冻结资金1000余万元。

回忆起当时的抓捕现场，新昌县公安局刑事犯罪侦查大队民警李赟赟告诉记者，那家公司内部有一个“神秘”的小房间，当他们进入这个不足15平方米的小房间后，吃惊地发现房间有三面“手机墙”，每面“手机墙”上有近400只手机在不停闪烁，各种手机软件在屏幕上不停地跳转。在公司工作人员的桌上，还发现了“猫池”机器，上面插着许多手机卡。这家公司就是通过“猫池”手工盗取公民个人信息。

木马软件悄悄潜入老年手机

在吴某等人归案后，根据手机生产商的线索，警方又成功打击了两家手机主板生产商，控制了这两家公司的主要负责人。前期，吴某等人极不配合，避重就轻，推卸责任。经过民警7天的深入讯问，吴某等人的心理防线最终崩溃，如实交代了自己的罪行。

据吴某交代，他们公司与不法手机主板生产商进行合作，将吴某公司生产的木马程序安装到手机主板内，然后流入市场，销售给生产商。这样的手机被销售后，一旦被插卡使用，吴某公司的后台工作人员就能收到该手机的数据，尤其是手机号码和验证码，并可以实时控制该手机发送短信、拦截短信、删除短信的功能。吴某还说，公司的业务现在不仅仅局限于老年手机，还偷偷延伸至普通手机和儿童电话手表。经查，已有2万余只儿童电话手表被安装了木马软件。

吴某等人为什么要大费周折地获取手机号码和验证码呢？这些手机号码和验证码究竟被用来干什么？这两个问题困扰着办案民警。为了解答这两个问题，办案民警向专业人士请求帮助。在专业人士帮助下，民警了解到，这极有可能是一个“薅羊毛”产业链。在清楚吴某犯罪的目的后，民警有针对性地进行讯问，最终，一个完整的犯罪链条逐渐呈现在民警面前。

在这个犯罪链条中，以吴某为首的软件公司和手机主板生产商是上游，负责设计木马软件并将木马软件嵌入手机主板中，再将手机销售给客户，获取客户的手机号码、验证码等信息。之后，吴某等人将收集来的客户手机信息打包销售给例如“番薯”这样的二级批发平台。“这类平台就像公民个人信息的‘批发商’，他们从吴某这样的公司里低价收购个人信息，然后再通过QQ群、微信群加价出售给下游‘薅羊毛’的团伙和个人，从中赚取差价。”新昌县公安局刑事犯罪侦查大队民警王泽远告诉记者。

在王泽远的手机上，记者看到了“番薯”平台。民警将虚拟货币充值进“番薯”平台，就可以选择所需要地区的手机号码，再点击一次“获取”按钮，就有一列列的手机号加载出来供选择。王泽远介绍，买家从“番薯”平台购买公民个人手机号后，可以接收从这些手机号中收到的验证码短信，借此进行“薅羊毛”活动。至于为什么选择老年机来“开刀”，吴某解释道，是因为老年机操作简单，木马软件植入简便，而且老年人一般不会注意到验证码消失的情况，所以选择在老年机上安装木马软件。

一台台老年手机、一条条手机号码和验证码，公民的个人信息就这样在地下黑市场中“裸奔”，再被层层买卖、使用获利，在全国范围形成了一张庞大的犯罪网络。

“薅羊毛”盯上了商家福利

“薅羊毛”案件是一类新型犯罪案件，在浙江省内不多发。为更好地了解掌握此类案件的特点，“8·12”专案组特向发生类似“薅羊毛”案件的公安机关了解情况，派人前往取经，调取相关材料，并进行讨论研究，理清了案件其中的原理和新的抓捕思路。新昌县公安局组织侦查民警集中对山东、江西、江苏等地的犯罪嫌疑人进行抓捕，经过3个月的抓捕行动，共抓获在“番薯”平台中购买手机号码和验证码用于“薅羊毛”的犯罪嫌疑人105名。

随着犯罪嫌疑人的到案，“薅羊毛”案件也不再神秘。根据梳理，民警发现，犯罪嫌疑人主要通过“拉新”“套取”“倒卖”三种方式进行“薅羊毛”操作。以“拉新”为例，据犯罪链条“下游”人员董某供述，许多网络购物平台或者外卖平台有鼓励拉新人活动，老账号将邀请码推送给新用户，新用户在注册平台账号时填写该邀请码，老账号就可以获取5至20元不等的无限制抵用券，用这些无限制抵用券，他们专门挑价格相对便宜的商品购买，这样一来，就可以实现“0元购”。

怎么“套现”？一些商家推出现金红包活动，只需要将红包二维码推广给其他用户，让其他用户点击，待点击次数达到一定标准后，就可以拿到现金。犯罪嫌疑人将买来的手机号不断注册此类商家的用户，不停套取商家的现金红包，以此牟利。此外，警方还发现，一些人通过手机号码注册大量账号在App中刷点赞数、刷流量赚钱。

“这些电商平台的活动主要针对的是新用户，而新用户的识别标准就是手机号码，只要你有未曾注册的手机号码用于注册就可以领取相关福利，于是这条黑色产业链就诞生了。”新昌县公安局刑事犯罪侦查大队相关负责人告诉记者，仅从“番薯”平台上看，这条黑色产业链的范围就遍布全国各个省市，从获取的手机号码来看，归属地包含各个地区。警方查明，自“番薯”平台成立以来，从平台上购买信息的用户就达上万人，涉案资金流水达2500余万元。

吴某“薅羊毛”团队作案手机

相关链接>>>

330余万部手机出厂就被植入木马 非法获取个人信息500余万条

当前网络黑灰产已形成生态圈，为犯罪持续“输血供粮”。利用公民个人信息实施网络犯罪日益高发，获取信息方式日趋隐蔽。最高人民检察院今年1月公布了一起涉网络黑灰产的典型案例。330余万部手机在出厂时被植入木马程序，非法获取公民个人信息500余万条，严重侵害公民个人隐私和人身、财产权利，社会危害巨大。

2017年11月至2019年8月底，深圳云某科技有限公司（以下简称“云某公司”）实际控制人吴某等人在与多家手机主板生产商合作过程中，将木马程序植入手机主板内。后经出售，吴某等人通过该程序控制手机回传短信，获取手机号码、验证码等信息，并传至公司后台数据库。

随后，该公司商务组人员联系李某理（在逃）、管某辉等人非法出售手机号码和对应的验证码。期间，云某公司以此作为公司主要获利方式，共非法控制330余万部手机，获取相关手机号码及验证码数据500余万条，获利790余万元。

其中，李某理等人向云某公司购买非法获取的手机号码和验证码后，利用自行开发的“番薯”平台软件贩卖给陈某峰等人。陈某峰等人将非法购买的个人信息用于平台用户注册、“拉新”“刷粉”、积分返现等，非法获利80余万元。管某辉从云某公司购买手机号码和对应的验证码后，也用于上述用途，非法获利3万余元。

2019年12月31日，浙江省绍兴市新昌县公安局将本案移送新昌县检察院审查起诉。2020年6月19日，新昌县检察院对吴某等5人以非法控制计算机信息系统罪，对陈某峰、管某辉等14人以侵犯公民个人信息罪提起公诉。2020年11月18日，新昌县法院以非法控制计算机信息系统罪分别判处吴某等5名被告人有期徒刑二年至四年六个月不等，并处罚金；以侵犯公民个人信息罪分别判处陈某峰、管某辉等14名被告人有期徒刑六个月至三年六个月不等，并处罚金。

最高检提示社会公众要提高对个人信息的保护意识，不轻易点击、下载来源不明的链接和程序，务必在正规商店购买正规厂家生产的电子设备，不轻易向外透露个人信息。相关部门要加强监管，从网络硬件的生产、流通、使用各环节规范数据收集，规范网络平台、APP软件等收集、使用公民个人信息的行为，监督相关企业建立数据合规制度。

（来源：《人民公安》杂志、中国青年报、正义网等）