新买手机竟被植入木马

县公安局打掉涉及31个省市570多万部手机的“薅羊毛”黑色产业链

特约记者 孙文涛

为招揽客户,一些电商平台会选择给新注册用户发放优惠券或新人红包,而网上专人搜集各类优惠券和红包的行为被称为“薅羊毛”。想要“薅羊毛”,就要用新手机号进行注册,那么新号码从哪里来呢?有人将目光对准老年手机,通过植入木马,拦截验证码完成注册再去“薅羊毛”。

去年8月,县公安局打掉一条“薅羊毛”黑色产业链,破获一起涉及全国31个省市570万多部手机的非法控制计算机案。近日,包括吴某在内的20多位嫌疑人被移送审查起诉。

外婆的手机收不到验证码?

去年8月12日,我县市民小朱在使用外婆手机时发现,手机收不到验证码短信。“试了很多次,还是收不到,我怀疑外婆的手机被人控制了。”当天,小朱向县公安局报警。

接警后,县公安局网安大队介入调查。大队民警对小朱外婆的手机进行现场测试,发现除无法收到验证码、密码之类的短信外,其余短信均能正常收发。

小朱外婆手机的“不正常”会不会只是个例呢?县网安部门迅速组织围绕涉案手机销售渠道展开调查,先后询问本地购买同款手机的37人,勘验手机25部,发现短信收发不正常的手机有15部。之后,民警对手机里的木马程序进行司法鉴定,发现手机主板被植入特殊的木马程序,能把需要的短消息上传至服务器。

那么,究竟是谁在这些老年机里植入木马程序?拦截含有验证码的短信有什么用途?被植入木马程序的手机到底有多少部?鉴于案情重大,绍兴、新昌两级公安机关成立由网安部门牵头的“2019.8.12”侵犯公民信息专案组,全力展开侦查。

500多万部手机被控制

专案组民警首先围绕验证码短信发去哪里展开调查,集合话单分析后,民警发现用于接收回传短信的是深圳的一个手机号码。围绕这个号码进行深挖后,犯罪嫌疑人吴某和卢某进入民警视线,并最终确认该团伙在深圳市南山区一园区内的办公地点。

2019年8月29日,专案组抽调30名警力在深圳开展第一轮抓捕行动。在此次抓捕行动中,民警起获大量后台服务器数据和与上下游链条交易合同。

经查,以犯罪嫌疑人吴某为总经理的这家公司,制作可以控制手机、识别拦截短信的木马程序,并与主板生产商合作,将木马程序植入手机主板中。“被植入木马程序激活的手机有500多万部,涉及功能机型号4500多种,受害者遍布全国31个省、直辖市、自治区。”办案民警说。

随后,专案组民警顺藤摸瓜,在深圳抓获其中一个手机主板制造商,现场查获大量植入木马程序的手机主板。又先后在厦门、杭州抓获利用非法购买公民个人手机号和验证码进行“薅羊毛”的嫌疑人14人。

同时,专案组通过公安部发起“2019净网行动”集群战役,对下游非法买卖手机号、验证码等公民信息进行“薅羊毛”的黑灰产业链进行全产业链打击。

犯罪分子是如何“薅羊毛”的?

对案件进行梳理后,民警发现,该案制作的木马主要针对老年机、儿童电话手表等功能机,而使用此两类功能机的机主相对不会关注短信验证类信息。此前,该团伙尝试针对智能机种植木马,但由于智能机使用人群范围比较广,很快会因为收不到短信而投诉,于是他们终止智能机业务。

那么,手机主板是如何被植入木马程序的?犯罪分子又是怎么“薅羊毛”的呢?

据介绍,被做了手脚的手机,只要插入电话卡,主板里的木马程序就会运行,并向后台发送短信,犯罪团伙就可以实时对这部手机进行控制。

犯罪嫌疑人吴某是专门负责木马病毒和对码平台的搭建。犯罪嫌疑人邓某是一家手机主板生产厂家的技术负责人,他们把吴某提供的木马病毒嵌入手机主板后,销售给手机生产商。民警介绍,厂家生产一块老年机主板只有几毛钱的利润,但安装木马程序后,厂家可以拿到三倍的利益。

在这条黑色产业链上,木马制作公司的下游包括对码、接码、“薅羊毛”环节。吴某团伙利用木马程序获取的手机号、验证码就流向这三个环节。对码平台,是手机号和验证码的接收平台,他们要确保每个验证码和对应的手机号相一致;接码平台相当于二级批发商,他们从吴某公司的对码平台获得手机号和验证码,然后再通过QQ群销售给“薅羊毛”的团伙或个人。这些人在购买手机号和验证码后,注册电商平台获取新人红包,这就是最后的“薅羊毛”环节。

民警拉练助力防诈骗宣传

通讯员 王金婷

近日,县公安局城东派出所基础防范中队结合南明志愿警察组织开展拉练活动。明明是一场拉练却一举三得,这是怎么回事呢?

城东派出所辖区班竹村是近年新建设的风景区,因景色优美、民风淳朴、娱乐设施完善,吸引游客前往,而游客被骗现象也随之出现。近日,新冠肺炎疫情逐渐转好,班竹村景区的游客量逐渐增多,治安压力也随之增大。

对此,城东派出所基础防范中队副所长丁良樑组织拉练活动,结合近日游客增多现象进行反诈骗宣传,同时对班竹村旅游景点街面进行巡逻。“不仅有助于提高游客和当地居民的反诈骗意识,而且有利于提高街面见警率,发扬新时代“枫桥经验”“五小工程”,切实提升百姓的安全感和满意度。另外,也是为更好地完成县局大练兵活动要求,此乃一举三得。”丁良樑说。

说做就做。当天下午2时,全体成员共25人在城东派出所列队结合,统一前往班竹村风景区。到达目的地后,通过统一列队、布置任务,25名队员共分成五组,对班竹村风景区展开巡逻、发放宣传单。队员们仔细讲解,游客和村内老人耐心听讲,共发放宣传单236份,达到较好的宣传效果。

再次集合后,丁良樑带领全体队员进行爬山活动,一路爬至第一平台。为更好地锻炼身体,激发大练兵精神,丁良樑拿出提前设置好的抽奖纸条(设有一、二、三等奖和10、20、30个俯卧撑、蛙跳等奖项),再次激励大家的锻炼热情。全体队员们纷纷上阵参与抽奖,大练兵氛围良好。

此次拉练,一方面加强社区工作,另一方面丰富和活跃队员们的日常生活,进一步强健警员身体素质,增强团队意识和集体观念,体现县公安局关键时候“拉得出、打得响”的良好素质,同时也切切实实提高人民群众的安全感、满意度和幸福感。

拖欠多人工资 民警帮忙追回

通讯员 张丹丹

“真是太感谢王警官了!如果不是他帮忙,我们17个人的工资还不知什么时候才能拿回来。”4月8日上午,在县公安局治安大队内,我县市民陈先生拿回3.5万元欠薪后激动地说。

在县公安局的帮助下,当天早上,包括陈先生在内的17名市民拿回被拖欠1年多的工资,共计10多万元。激动之余,这些市民还给民警送上锦旗表示感谢。

2018年,陈先生被我县某制衣有限公司聘为管理员,每月工资5000元,之后因工厂经营不善,工作10个月的陈先生只拿到1.5万元工资。

“我被拖欠1万元工资,原先老板承诺过段时间就会发,我们相信他,想着大家都有困难的时候。”市民朱阿姨是该制衣厂的老员工,她说因为生意不好,制衣厂于2018年11月停产,17名员工没有拿到工资,老板蔡某表示会想办法筹钱发工资。

在多次催讨无果下,去年3月,陈先生联合大家去劳动部门反映情况。劳动仲裁部门找到蔡某,蔡某表示将于5月和8月分批发放拖欠工资。“哪知道过了一段时间,他不但电话打不通,连人也找不到。”朱阿姨说。

去年11月,劳动部门将欠薪案移交给县公安局,该局治安大队于12月立案侦查。“我们调查发现,蔡某在新昌有房有车,但去年他已将车子房子卖了,原先的手机号也停用。”该大队行动中队民警王高春说,考虑到临近过年,大家都急着用钱,他们抓紧追查速度。

通过调查,民警发现蔡某夫妻在奉化溪口打工。新冠肺炎疫情持续向好后,3月31日,民警赶赴奉化抓获蔡某。经民警反复做思想工作,蔡某表示想办法筹钱支付拖欠1年多的工资。目前,蔡某因涉嫌拒不支付劳动报酬被依法取保候审。

开学在即民警线上授课护安全

通讯员 王淑英

“同学们大家好,我本来应该在校园里给大家上这堂安全讲座课,没想到变成‘十八线网络主播’,和大家线上见面。”近日,县公安局儒岙派出所民警郭经福在儒岙中学八(4)班的网课上现身,通过钉钉直播,给同学们带来一堂生动实用的安全教育课,为复学返校提供安全保障。

直播中,郭经福以“安全第一、健康成长”为主题,从安全素质教育、防电信诈骗和新冠肺炎疫情防疫三方面展开,从同学们应掌握的法律常识和如何防范为切入口,并结合实际案例进行讲解,内容详实,生动实用。

“感谢派出所民警百忙之中为我们讲解校园安全,内容贴近生活,同学们受益匪浅。”八(4)班班主任王老师说。儒岙中学潘校长则希望这堂安全教育课能剪辑成视频,让全校师生观看,普及安全知识,强化学生安全意识。

接下来,儒岙派出所将继续加强安全宣传,提高辖区学校的防范和应急处置能力,助力辖区学校有序复学返校。

停 电 预 告

2020/4/14 8:30- 2020/4/14 12:30 35kV沙溪变:龙皇堂P387线-龙皇堂线下庄支线跌落式熔断器后段 新昌县-沃洲镇(龙皇堂行政村-下后午自然村,祝家庄行政村-新庄自然村)

2020/4/14 13:30- 2020/4/14 17:30 35kV沙溪变:龙皇堂P387线-龙皇堂4#变配变令克后段 新昌县-沃洲镇-龙皇堂行政村-龙皇堂自然村

2020/4/16 8:00 - 2020/4/16 12:00 35kV小将变:茅洋P450线首端,茅洋1051线茅洋P1035开关,茅洋1051线茅洋P1059开关之间 新昌县-小将镇-桥里房行政村(赤房山自然村,染里自然村,桥头王自然村),小将镇-五埠行政村(海角坑自然村,埠头自然村,外坑自然村,雷峰自然村,孙家坪里坑自然村,孙家坪自然村),小将镇(道士岙行政村-道士岙自然村,芹塘行政村-芹塘自然村);浙江省-绍兴市-新昌县-小将镇-里宅行政村-中国移动通信集团浙江有限公司新昌分公司,小将镇-五埠行政村(新昌县新特农产品专业合作社,中国移动通信集团浙江有限公司新昌分公司,中国电信股份有限公司新昌分公司),小将镇-里东行政村(中国铁塔股份有限公司绍兴市分公司,新昌县罗坑山农产品专业合作社)

2020/4/16 7:30- 2020/4/16 13:30 110kV儒岙变:双溪P015线-双溪P015线双溪P1035开关后段 新昌县-儒岙镇-王渡里行政村(坑下山自然村,毛洋山自然村,王渡里自然村),儒岙镇(王渡口行政村-王渡口自然村);儒岙镇-儒一行政村-中国铁塔股份有限公司绍兴市分公司,儒岙镇-王渡里行政村(新昌县儒岙镇王渡里村坑下山水电站,新昌县儒岙镇王渡里村三级电站,新昌县儒岙镇王渡里村二级水电站,新昌县儒岙镇王渡里村一级电站),儒岙镇-王渡口行政村(新昌县仓潭水电站,新昌县苍潭水电站,新昌县儒岙镇儒王友谊水电站)

2020/4/16 8:30- 2020/4/16 17:30 110kV塔山变:五都P706线-杨梅山三变支线12#杆后段 新昌县-七星街道(杨梅山行政村-杨梅山自然村)