

上海徐汇区善恒婚姻介绍所, 遗失银行开户许可证, 开户许可证核准号: J2900107766601, 声明作废, 特此公告。

上海明聚机电安装工程有限公司遗失营业执照正、副本, 证照编号: 29000000202005030210(209), 声明作废。
上海五雁环境科技有限公司遗失营业执照副本, 证照编号: 29000000201608260461, 声明作废。

上海凤睿经贸有限公司经股东决定解散, 并己成立清算组。请债权人自本公告刊登之日起45日内向本公司清算组申报债权, 特此公告。

上海市崇明区市场监督管理局撤销行政许可听证告知书
沪市监崇撤听告[2021]716435号
上海邦环工贸有限公司、苗鹏程、贺晓东:

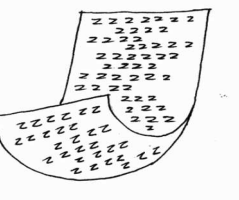
由本局调查的关于苗鹏程申请撤销上海邦环工贸有限公司设立登记行政许可一案, 已调查终结。现将本局拟作出撤销该行政许可的事实、理由、依据及内容告知如下:
上海邦环工贸有限公司2018年5月16日向本局提交的设立登记材料中苗鹏程的身份证及复印件系2016年9月21日前遗失的身份证。上海邦环工贸有限公司此次设立时所提交的《指定代表或者共同委托代理人》、《上海邦环工贸有限公司章程》、《股东会决定》等材料中“苗鹏程”签名非苗鹏程本人签署, 该公司的设立也不是苗鹏程的真实意思表示, 而是其他人冒用苗鹏程的身份办理的。苗鹏程本人并不知情。
上述事实有苗鹏程提供的撤销设立申请材料、相关证明及其询问笔录、上海三星经济开发区职员的询问笔录、安徽省舒城县公安局河棚派出所出具的户籍证明、国家税务总局上海市崇明区税务局的证明材料、浙江泰隆商业银行股份有限公司上海宝山支行的证明材料、上海润家生物医药科技有限公司司法鉴定所鉴定意见书、设立登记档案材料及其他材料等予以证明。
根据《中华人民共和国行政许可法》第六十九条第二款的规定, 本局拟决定撤销2018年5月16日作出上海邦环工贸有限公司设立登记的行政许可。
对上述拟作出的决定, 你(单位)有要求举行听证的权利。如果要举行听证, 可以自接到本告知书之日起五个工作日内以书面形式提出举行听证的要求。逾期未提出听证要求视为放弃听证权利。
联系人: 陈毅铭、戴婷
联系电话: 59629212
地址: 崇明区城桥镇东门路388号政策法规科 邮编: 202150
上海市崇明区市场监督管理局 2021年9月18日

上海市青浦区市场监督管理局公告
根据润盈生物工程(上海)有限公司申请, 本局已于2021年9月16日核准该企业变更(备案)登记, 因该企业无法将原营业执照正本原件交回, 现公告作废润盈生物工程(上海)有限公司原营业执照(正本编号: 29000000201703280342; 副本编号: 29000000201703280343)。上海市青浦区市场监督管理局公告 2021年9月23日

陆宽 遗失注销减资登报传媒 021-59741361 13764257378(微信同号)

环保公益广告

重复使用, 多次利用



双面使用纸张 = 减少一半的废纸产生

优先购买绿色食品



健康安全 无污染

拒绝使用一次性用品



6000~8000 双一次性筷子 ≈ 一株20岁的大树

微信“清粉”背后的陷阱

“系统正在检测删除我的人, 勿回” “清粉请见谅, 扫描二维码可免费检测” “检测一下看谁把你拉入了黑名单?”

当微信成为人们常用的即时通信工具后, 常常会看到这些“清粉”的消息出现, 一不小心, 就可能掉进犯罪分子设下的陷阱。

8月19日, 江苏省南通市通州区公安局民警开展反诈宣传时, 特意将微信“清粉”列入宣传内容, 提醒群众切勿随意使用“清粉”软件。

“清粉”后微信“失控”

一键清理“僵尸粉”, 释放手机内存。为图省事和方便, 部分微信用户会选择一些来路不明的“清粉”服务。2020年, 一些微信用户使用“清粉”软件后发现, 有陌生人或通过自己分享的二维码扫码进群, 或者自己被拉入了一些广告群, 自己的微信号还发生批量关注微信公众号等情况, 如“失控”一般。更可怕的是, 相关操作引起系列连锁反应, 还有人因此被网络诈骗、赌博等犯罪团伙盯上, 最终造成财产损失。对于这些“中招”的用户, 不法分子有多种“吃”法: 先是赚销售“清粉”服务的钱; 还可以通过控制用户的微信账户, 到处散发各种营销广告信息获利; 再就是盗取受害用户个人信息, 售卖牟利。

“清粉”服务成了非法数据交易产业链的重要“上游”, 不法分子通过相关软件攫取的数据在被分类后经由信息“地下市场”交易。

2020年6月, 南通市公安局网安支队民警在工作中发现, 部分微信朋友圈和群聊中散播的“清粉”软件存在很大的安全隐患。警方调查发现, “清粉”软件的原理就是通过应用集群控制软件控制微信账号, 自动向所有

斩断背后利益链条

专案组通过对嫌疑人的“清粉”二维码进行解析, 调取嫌疑人租用的10余台服务器镜像数据发现, 嫌疑人利用服务器搭建了微清系统、用户微信群二维码过滤系统、后台管理系统。虽然犯罪嫌疑人使用的是非实名信息注册以逃避公安机关打击, 但侦查员盯案不放, 反复梳理线索后, 在已停用的服务器上取得重大突破, 最终成功挖出团伙成员刘某、何某等人的真实身份, 一个以“清粉”为幌子的违法犯罪集团渐渐浮出水面。

2020年7月22日, 专案组民警兵分3路开展集中抓捕, 在广东韶关、仁化, 湖北天门等地公安机关的支持下, 最终将涉案的5名犯罪嫌疑人全部抓获归案。这个团伙究竟是如何运作、如何牟利的?

通州警方深入调查发现, 2020年初, 犯罪嫌疑人张某、李某等5人共谋开发了这个能非法获取用户微信群二维码的“清粉”软件。

该犯罪团伙分工明确, 由何某负责软件开发, 刘某负责服务器租赁、平台的搭建和维护, 张某负责“清粉”二维码的图片制作, 李某负责销售非法获取的用

好友群发消息, 再由软件自动识别哪些是“僵尸粉”并予以删除。但犯罪嫌疑人在取得微信账号的控制权限后, 却借机非法获取用户微信群二维码信息, 再倒卖给诈骗、赌博等犯罪团伙获利。

2020年7月3日, 南通市公安局成立由网安、法制部门和通州区公安局相关单位组成的专案组, 并指令通州区公安局主办此案, 全力侦破。专案组研判发现, 2020年2月以来, 多个地区频繁出现陌生人扫码进群散布赌博、营销等非法广告, 甚至实施诈骗, 关联案件达1500余起, 涉及20多个省市。

另据腾讯公司反馈, 微信群聊二维码泄露现象发生后, 他们依法配合多地公安机关抓获了多个出售和利用微信群聊二维码作案的犯罪团伙, 但警方始终未能查明这些二维码的泄露源头。专案组通过对大量“清粉”软件开展侦查, 最终锁定一款名为“微清”的软件有重大嫌疑。嫌疑人精心制作了“极速清粉”的广告图, 号称官方认证、只需要1分钟就检测完毕。为吸引人使用, 这款软件打着官方“清粉”团队的旗号, 通过各种途径在微信用户群体中传播, 一旦有人点击扫描登录检测, 就可以通过后台服务器直接登录受害人微信, 获取用户的所有权限。

户群二维码牟利, 以及检测群二维码是否过期; 谭某负责为微信公众号引流牟利。

据嫌疑人交代, 所谓的官方认证、放心访问只是为了降低使用者的警惕心理, 他们并没有获得官方授权, 而是租用服务器自行搭建系统, 他们制作的“清粉”图片中包含二维码, 二维码对应一个链接, 打开后显示为“获取二维码, 扫描登录即可清粉”。产生风险的关键点就在扫码授权登录这个环节。受害人点击获取二维码后, 实际得到的是微信PC端登录的二维码, 受害人扫描后, 嫌疑人通过“微清”系统在后台服务器就可以直接登录受害人的微信, 并获取所有的用户权限。这就相当于把自己的微信使用权拱手相让。

嫌疑人将制作好的“清粉”图片通过微信好友、微信群、朋友圈等途径进行大肆传播。在骗取用户授权登录后, 嫌疑人使用“微清”系统为他人批量关注大量微信公众号和刷阅读量、点赞量。还使用“微清”系统批量扫描受害人的群二维码, 并以图片形式保存在服务器上。他们还向下游出售微信群二维码, 许多微信群二维码被下游犯罪团伙用于加群并发布诈骗、赌博等非法信息。



资料图片

案件报道>>>

利用“清粉”软件控制用户账号强加关注 八人被诉获刑

据《扬子晚报》报道, 张某某、何某某等8人分别系网络公司法定代表人、程序员。2020年1月至7月, 张某某等人为谋求利益, 在未获得腾讯公司授权的情况下, 开发为用户识别已经单方面将自己删除的微信好友的应用软件(即“清理微信僵尸粉”软件, 以下简称“清粉”软件)。用户使用该软件后, 软件即以“清粉”为名发送授权请求, 取得用户微信账号登录凭证, 使用账号登录, 进而控制用户账号。该软件控制用户微信账号后, 可以向用户微信好友群发信息, 获取用户微信群二维码, 强制用户添加关注微信公众号等。张某某等人通过“清粉”软件控制他人微信账号, 获取用户微信群二维码后予以出售, 并且强制用户添加关注指定的微信公众号收取提成, 共计获利260万余元。

记者了解到, 该案为全国首例利用微信“清粉”软件非法获取信息案件, 是公安部督

办案件。本案的争议焦点在于, 利用微信“清粉”软件控制用户账号后, 获取群二维码信息并强制添加关注公众号的行为, 应当如何认定。就本案而言, 笔者同意上述第二种意见, 即张某某等人的行为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。具体分析如下:

根据“两高”相关司法解释, 刑法保护的计算机信息系统, 是指具备自动处理数据功能的系统, 包括计算机、网络设备、通讯设备、自动化控制设备等。根据国务院《计算机信息系统安全保护条例》, 计算机信息系统是指由计算机及其相关的和配套的设备、设施(含网络)构成的, 按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。因此, 数据和应用程序处理功能, 对信息进行采集、加工等处理, 是刑法界定计算机信息系统的核心要件。微信属于一种快速的即时通讯程序, 具有多人群聊功能, 支持发送语音短信、视频、图片、文字

等, 支持腾讯微博、QQ信箱等插件, 显然具有数据采集、加工、存储、传输等功能, 能够认定为刑法保护的计算机信息系统。张某某等人违反国家规定, 违背用户意愿, 通过技术手段侵入用户计算机信息系统即微信程序, 获得相关操作权限, 继而获取用户的计算机信息系统数据即微信群二维码, 非法控制微信强制用户添加关注指定公众号, 其行为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。

2020年12月15日, 江苏南通通州区人民检察院对张某某、何某某等8人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提起公诉。2021年3月2日, 南通通州区人民法院作出一审判决, 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分别判处张某某等人有期徒刑一年六个月至四年, 并处罚金五千元至十万元。一审宣判后, 张某某等人并未上诉, 检察机关亦未抗诉, 判决产生法律效力。

敛财 200 多万元

警方初步查明, 短短3个月, 该犯罪团伙共非法获取用户微信群聊二维码2000余万个, 批量出售给了福建龙岩等地的诈骗、赌博犯罪团伙, 涉及全国千余起诈骗案件, 性质十分恶劣, 危害极大。同时该团伙为他人批量关注微信公众号和刷阅读量、点赞, 先后获利200余万元。

专案组循线追踪, 陆续抓获为该犯罪团伙提供资金或者帮助收取、转移犯罪所得的张某某、李某某、李某泉。

该犯罪团伙平台化、专业化、精细化程度高, 隐蔽性极强。从非法获取微信用户的相关个人信息, 到下游的广告、营销和其他网络犯罪, 已经形成一个各环节相互独立又紧密协作的产业链。在侦办这起案件的过程中, 办案民警通过分析作案手法、犯罪事实, 在腾讯公司

和南京森林警察学院的支持配合下, 开展身份刻画追踪、海量数据分析、后台数据支撑等工作, 最终案件得以成功告破。

犯罪嫌疑人通过技术手段非法获取受害人微信群二维码等计算机信息系统数据, 并通过出售数据获利5000元以上, 涉嫌违反刑法第二百八十五条第二款规定, 构成非法获取计算机信息系统数据罪, 且违法所得已经超过追诉标准5倍以上, 属于情节特别严重情形。

今年3月, 当地法院对该案进行了集中宣判。张某某等8名被告人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而获刑, 被判处有期徒刑一年六个月至四年不等的刑期, 并分别处以相应的罚金。4月以来, 8名罪犯陆续被投送至江苏宜兴、江宁监狱服

刑。

南通通州警方提醒广大微信用户, “清粉”软件猫腻多, 一旦同意使用这类“清粉”软件, 就意味着自己的账号完全让人“接管”, 不法分子将轻易获取相关个人信息。这不但会将自己的个人隐私完全暴露, 连工作、身份、联系方式、社会关系、财务信息等也会被他人获得。如果已经使用过“清粉”软件, 要尽快检查自己的账号是否出现异常, 并立刻取消相关登录授权。还可以在手机微信设置里, 找到账号与安全目录下的登录设备管理, “踢掉”陌生的登录设备。建议广大网友尽量不要使用破坏官方协议或具有外挂功能的插件和软件, 有效规避可能遇到的安全风险。

(来源: 《人民公安》杂志)