

诈骗App背后隐现技术开发灰色产业链

产品名称	诈骗App背后隐现技术开发灰色产业链
公司名称	东莞市微三云大数据科技有限公司
价格	.00/件
规格参数	
公司地址	东莞石排瑞和路一号
联系电话	18002820787 18002820787

产品详情

去年下半年经历的一次与手机App有关的离奇遭遇，至今让北京市顺义区的郭女士百思不得其解。

郭女士手机上的某财富管理App看起来和身边朋友们的毫无二致，起初投资收益颇丰，没想到投入200万余元巨款后，系统显示“账户异常”无法提现，随后这款App再也无法登录。

警方介入调查后发现，这款外观设计“高大上”、起初各类功能看似正常的App，实为“山寨版”，系在安徽一家网络科技公司旗下的“微导流”平台封装而成。

经查，“微导流”平台管理者的亲戚桂某利用其权限，没有在该平台实名注册即为他人封装多款名为该财富管理的虚假App，后被他人利用实施电信诈骗。

办理该案的顺义区人民检察院检察官任巍巍介绍，所谓封装，是将网址、应用名、LOGO、启动图打包形成一个App应用包，使网站以App形式呈现。“一次违规封装，就可以让诈骗工具披上正版手机软件的外衣，令无数家庭倾家荡产。”

中青报·中青网记者梳理发现，2019年以来，中国裁判文书网公布多起与虚假App有关的电诈案，涉及虚拟币投资、赌博、套路贷等多个领域（详见本报11月26日报道《为赚快钱 IT青年沦为新型电诈案“制刀者”》）。大量“量身定制”的涉诈App背后，有的公司从接单、开发，到封装、分发、售后等，提供“一条龙”服务，诈骗App背后隐现技术开发灰色产业链。

今年4月底被查封的湖北晟昌网络科技有限公司即是其中之一。参与办案的武汉市洪山区公安分局网安大队民警张晟介绍，该公司由25人组成，分为技术、销售、美工等部门。技术开发人员分工明确，负责编写程序代码、购买域名、租用服务器、封装……一番操作下来，一款App制作周期大多不会超过1个月。因其中一些App需要实现的功能类似，同类App可“批量开发”。该公司还为下线买家组建微信群，负责后期功能调试、运维等。

在湖南，一家由多名名校毕业的年轻人创办的“明星”企业，甚至“组团犯罪”，远赴海外开发诈骗App。2019年11月，客户张某找上门来提出，请该公司制作某证券App的“相似款”。该公司3名主要负责人明知这款软件可能被用以犯罪，仍接下业务，派遣4名员工先后两次前往泰国，帮助张某开发、维护两款虚假证券App。

团伙作案之外，一些涉诈App案中，有的技术人员私下“接单”、参与其中关键环节，从中非法渔利。

11月初，浙江省金华市人民检察院披露了一起涉App裸聊敲诈勒索案。案件中，明知该App是不法分子用来实施犯罪的工具，计算机专业毕业的00后孙某某仍为其提供软件平台搭建、后台技术维护服务。不到3个月，孙某某非法获利22820元，近日被提起公诉。

“我真不应该为一点蝇头小利去做违法犯罪的事情，毁了自己的大好前程……”面对检察官的讯问，孙某某悔不当初。

今年7月以来，国家反诈中心接连公布两批共计644个涉诈App。这些仿冒App，由公安机关对电信网络诈骗案件梳理后整理而出，内容涵盖社交、贷款、投资、博彩、购物、短视频、手机安全等多个领域。

诈骗App背后隐现技术开发灰色产业链

诈骗App背后隐现技术开发灰色产业链