2025.1.24 星期五
责编 金钟 | 美编 周洁 | 校对 王欣
江南晚报

22日晚上，无锡市社会福利中心的食堂内格外热闹，从这里走出去的成年孤儿纷纷回“家”，一起来见见“亲人”。据了解，这样的年夜饭已坚持了多年。

社会福利中心里的团圆

这顿坚持多年的年夜饭格外香

后厨团队忙了整整两天

当天下午4点多，食堂大厅的餐桌上已摆好了五香牛肉、盐水鸭、烤肠、蒜泥长豆等冷盘。负责这顿年夜饭的大厨蒋守璐介绍，团队忙了整整两天，从冷菜到热菜，所有的菜品都是大家亲手做的，“每年的这顿年夜饭是大家的集体期盼，后厨团队也变着花样给大家惊喜。”

今年的菜里有一道“硬菜”京葱海参，这是后厨团队特意烹制的。“他们即便在外面成家立业了，一般家中也不太会做这道菜，关键不用吐骨头。”老蒋表示，不少成年孤儿身有残疾，菜肴少刺少骨，是后厨准备菜单时要考虑的。大家在无锡长大，喜欢吃无锡的甜口，像走油蹄髈、蟹粉蹄筋等菜肴都很受欢迎。

蒋守璐回忆，他是2002年从部队转业后来到社会福利中心工作的，这样的年夜饭，除了疫情那几年暂停外，年年都置办。有的成年孤儿因为上班安排等原因说来不了，可突然发现有空了，即便迟到也要赶来。后厨一般都会多备上一桌。很多人是拖家带口一起来的，多的时候要办上11桌，今年也有8桌。

这里永远都是“避风港”

47岁的刘女士一家是第一个到福利中心的家庭。她和老公一起在残疾人之家做些手工活，现在小儿子大学毕业，在一家待遇不错的企业工作，全家人的日子越来越好。她介绍，这里有她从小一起长大的姐妹，平时大家忙很少聚会，就想趁着吃年夜饭碰个面。

“我向单位请了个假”，小王一家开了40多分钟车，从胡埭赶来吃年夜饭。在这里，小王还有一个专属的名字，仿佛又回到了10多年前的时光。每年回来小王都会拍不少照片留存，这里有她许多幼时的记忆。

她是幸运的，助养家庭一路资助她。但曾有一段时间，养父母生意特别忙，她又回到中心上学。她知道，“自己背后是有人托底的”。

43岁的小路带着还在上小学的儿子前来，她表示，有了孩子后，一段时间特别难熬，很多事不知道怎么办。因为带孩子，她不能上班，经济上捉襟见肘。中心负责人了解到这一情况，帮她联系了好心人，为她捐助了奶粉、尿不湿等物资。

“成年后，中心帮我们申请了廉租房，装修也是大家一起完成的”，小华表示，有时路过中心，还会来蹭顿饭吃，这里就是他的家。

过上自食其力的生活

“我每月收入5000元朝上，具体多少不告诉你”，来吃年夜饭的小夏当天刚发了工资，热情地要请大家吃外卖，被大家一把拉住。这个小伙子当年可是出了名的淘气，他在大家的帮助下，由好心人资助学了技能，有了份好工作。

聋哑小伙小钢戴上了助听器，这也是中心帮助他申请的。他大学毕业后，曾在上海工作，租房压力太大。回到无锡后，他暂时回到福利中心过渡，在这里不用为食宿发愁。“我现在送外卖，同时也在找份稳定的工作”，小钢在手机上打字表示，有“家”的感觉真安心。

市社会福利中心的负责人冯浸介绍，该中心通过社会化安置的孤儿有41人，年龄从20多岁到50多岁不等。他们出嫁迎娶时，中心都会按照无锡风俗置办礼物，并为他们证婚。一年一度的年夜饭更是大家亲情的维系，“这一举措也是在告诉这些走上社会的成年孤儿，这里是永远的家。”（晚报记者 黄孝萍/文、摄）

点了一个链接，公司财务被“领导”骗了186万元

骗子通过木马病毒链接，诱骗财务人员点击后掌控其办公电脑，“鸠占鹊巢”在群里变身为“老板”，要求财务人员进行大额转账实施诈骗。近日，法院以提供侵入、非法控制计算机信息系统程序、工具罪及偷越国（边）境罪，数罪并罚判处被告人覃某有期徒刑四年三个月，并处罚金11万元。

/ 不明的链接 /

2024年1月初的一天，无锡某公司财务人员张女士如同往常一样在电脑前处理财务事务。这时，当地会计群聊里有人发了一个名为“2024年1月税务稽查局企业搜查名单”的链接，张女士随即在电脑上点击了该链接，电脑显示自动下载了一个压缩包。解压两次没有成功后，张女士删除了该压缩包，没再理会这件事。

同年1月10日下午，张女士被拉进一个小群，此时群内已有两名成员，分别是公司负责人“周总”及副总经理“周副总”。张女士特意返回日常工作群中，查看了两位领导的头像和昵称，确认与日常工作群中的账号信息一致。群内的“周总”安排“周副总”和张女士盯紧公司一笔98万元款项的到账情况。在查看公司账户后，张女士如实向群内两位“领导”在线报告了并未收到款项的情况。

不久后，按照群内“周总”和“周副总”的指令，张女士将公司账户内的186万元分三次转入另一对公账户。次日，仍未收到98万元款项的张女士向企业负责人周总当面汇报情况，才得知周总从未安排过转账。惊觉被骗后，张女士当即报了警。

/ 真相被揭开 /

公安机关经过侦查后发现，原来张女士的工作电脑被安装了木马程序。该木马程序的来源正是“2024年1月税务稽查局企业搜查名单”的链接。在她点击的瞬间，一个名为“wolf”的木马病毒便侵入了她的电脑。此后，电脑上的所有操作、公司内部信息都被犯罪嫌疑人一览无余。正是获取了这些信息，犯罪嫌疑人先伪装成公司领导获取信任，再逐步对其下达转账指令，从而骗取钱财。

根据木马程序回传的IP地址、服务器等相关信息，警方很快锁定了犯罪嫌疑人覃某、吴某（已分案处理）。经查，2019年，吴某编制了一款远程控制工具软件“wolf”，该软件主控端使用用户名、密码登录，能一键生成可伪装的木马文件。该木马文件可绕过杀毒软件，直接写入并非法控制被控制端，从而实现对被控制端远程开关机、注销、上传下载、屏幕后台监控、键盘记录、视听监控等操作。

自行编译出木马文件后，吴某经常在社交平台和视频网站发布编程相关技巧，吸引网友关注。2023年8月，覃某看到吴某编程视频后，通过留言，添加了吴某的社交账号。随后，覃某向吴某购买了“wolf”的独家代理权并将该软件转售给境外诈骗团伙，并承诺给吴某抽成。

境外诈骗团伙通过查询企业邮箱，冒充客户将“wolf”软件伪装成税务通知、电子发票等发送至邮箱、群聊内，公司的财务人员一旦点击，其使用的电脑就会被木马程序侵入。

/ 获刑并罚款 /

覃某始终与吴某保持“合作”，为了让吴某更积极地维护该木马程序，覃某还与吴某约定，在分销所得的利润中视情况抽取“辛苦费”给吴某。此外，为方便销售木马程序，覃某采用坐车、步行等方式偷渡至越南，在越南继续从事非法木马程序销售活动。2024年4月，覃某再次以相同方式偷渡回国。

经查，吴某在2023年8月至2024年1月间，通过出租木马软件使用权限和下家分成，非法获利31368USDT虚拟币（折合人民币22万余元）。2024年7月，该案侦查终结，被移送至江阴市检察院审查起诉。受案后，承办检察官对覃某的犯罪事实进行审查，并引导公安机关就覃某被抓获前在越南实施的犯罪行为以及犯罪期间虚拟币USDT价格折算情况进行补充侦查取证。由于虚拟币的金额、价值、来源难以准确认定，覃某非法所得情况取证面临现实困难，最终，承办检察官以覃某打给吴某的分红数额作为共同犯罪金额认定。

经江阴市检察院提起公诉，近日，法院以提供侵入、非法控制计算机信息系统程序、工具罪及偷越国（边）境罪，数罪并罚判处被告人覃某有期徒刑四年三个月，并处罚金11万元。（王佳）