94万部手机成“肉鸡”，专刷“10万+”

犯罪团伙通过木马控制用户手机，为微信公众号刷阅读量牟利

据《扬子晚报》报道，微信公众号的营销像是一个波谲云诡的江湖，谁都想从中分一杯羹。有些“网红”公众号，发一条微信，分分钟就能收获“10万+”的阅读量，背后团队为此付出了艰辛的劳动。可有些公众号的“光环”，却来自一条“危险的捷径”。

日前，江苏省邳州市公安局破获一起特大非法控制计算机信息系统案件，撬开了依附于微信上的增粉、刷量灰色产业链的冰山一角。这个犯罪团伙通过木马程序植入，将全国各地94万部手机当成随意玩弄的“肉鸡”（指可以被黑客远程控制的机器），给一些花钱的公众号增粉、点赞，刷阅读量，获利高达100余万元。

嫌疑人被抓捕归案（资料图）

警方缴获的作案工具（资料图）

微信偶尔“闪退”，背后竟有玄机

闲暇之余，刷刷微信朋友圈，看看公众号文章，成了很多人打发时间的方式。邳州市民王先生就是这样，可今年4月的一天，他发现微信有些异常。

“下班后把手机给孩子玩，孩子下了个程序后，我发觉微信‘闪退’。我上网查了，说可能中了木马病毒。因为微信绑了银行卡，我就挺担心的。”当邳州市公安局运西派出所社区民警来走访时，王先生跟民警说了这种情况，关机重启后微信依然会“闪退”，疑似中了木马。民警随后进行初查，并上报邳州市公安局网安大队。

生活当中，微信“闪退”时常出现，可多数人并未在意，因为重启后手机能照常用。可这次王先生的微信“中招”，委实有点怪。网安大队扩大侦查后有了新收获，王先生的微信“闪退”并非个案，而是由一款专门针对微信制作的木马造成的，全国各地不少人“中招”。

94万台智能手机，被这伙人控制

邳州市公安局随即成立专案组，经过追踪，发现受害人遍布全国各地，背后有一个以非法控制计算机信息系统进行牟利的作案团伙，而这个团伙在北京、深圳等地均设有联络点。

随后，专案组兵分四路，前往北京、深圳、秦皇岛、南昌组织抓捕。在当地警方协助下，4个抓捕组蹲守近5个小时后，于5月19日中午一举抓获11名犯罪嫌疑人，当场缴获手机、笔记本电脑等作案工具。

经过突审，一个分工明确、人员学历高、作案技术手段强的计算机信息犯罪团伙的架构逐渐清晰起来。“这个团伙共13人，分为3个小队，一队负责木马技术的开发，一队负责将木马植入手机，还有一队负责联系有需要的公众号进行应用推广。”办案民警李棒棒说，他们的学历基本是大专以上，曾从事过互联网软件开发，案发前一直有合作。他们智商较高，是为了多赚点钱才决定铤而走险，从事这个“时髦行业”的。

邳州市公安局网安大队大队长冯雷说，这个犯罪团伙已经涉嫌非法控制计算机信息系统罪。根据刑法及相关司法解释，这个罪名一般来说，控制20台就可定罪，而该团伙控制了94万台智能手机，显然是“情节特别严重”了。

目前，这个团伙主要犯罪嫌疑人严某、张某、黄某已被邳州市人民检察院依法批准逮捕，其他嫌疑人也被采取了强制措施，案件还在进一步办理中。

■ 深度揭秘

A 植入木马却不动银行卡，原来另有目的

王先生手机中了木马病毒之后，微信除了“闪退”外，其他功能正常，与微信绑定的银行卡、微信红包等财产并未受到损失。不图财，他们图什么？

邳州市公安局网安部门立即与腾讯公司微信安全团队联系。微信安全团队分析后发现，这款木马攻破了微信的安全设置，能自动终止微信的进程，修改相关文件，最终实现在手机用户不知情的情况下，关注一些微信公众号，并对公众号发布的文章阅读、点赞。

也就是说，不法分子开发这款木马程序，目的是为一些公众号拉粉、点赞，刷阅读量，从而获取利益。随着犯罪嫌疑人落网，专案组揭开了这个团伙的具体运作方式。

深圳公司控制人严某擅长软件开发，今年初，在破解了微信安卓客户端的加密方式后，他立马意识到，赚大钱的机会来了。他联系了常年合作的北京某公司的张某。经过一番合谋，他们决定利用这种手段为公众号“刷量”从而获利，并把宣传推广的重任交给了张某。

张某颇有人脉，很快与北京一家专门从事手机软件开发的公司联系，利用该公司开发的手机软件“后门”（指绕过安全性控制而获取对程序或系统访问权的方法），诱骗用户下载root软件，在用户不知情的情况下，通过远程指令下载安装木马，修改微信客户端文件，把用户手机当作“肉鸡”，“无私”地替公众号“刷量”。

B 安卓手机还没卖，就被植入木马

据介绍，严某、张某等人采用两种方式投放操作木马。一种是线上投放，在手机软件安装包内加入带有root功能的加速软件。

当手机用户在玩手游时，会弹出一个对话提示框告诉你手机运行慢，可以下载安装这个加速项。只要用户安装了，他们就会获得root权限，相当于在手机上开了“后门”。

“只要手机处于黑屏状态，他们就可以用微信肆意地加粉、刷阅读量，但线上投放的‘安全系数’低，被发现的概率大，所以他们一般采取线下投放。”冯雷说，线下投放主要针对即将投放市场的安卓系统手机，先从批发商、销售商处下手，通过预装手机系统把root刷进去，以便掌握“后门”，获取这些手机的最高权限。这些手机卖到用户手中并被使用后，他们就能远程控制手机，实施加粉、刷阅读量等行为。

“目前这个软件技术还没完全开发成功，只能针对安卓系统的手机进行控制。”冯雷说，“木马能自动识别手机是否在黑屏状态，一旦是黑屏，仅需一两秒，就可以神不知鬼不觉地关注某个公众号、点击某篇文章。”

C 涨粉2毛，点赞1元，轻松刷出“10万+”

据初步统计，截至案发时，这个团伙已控制全国各地手机94万余台，通过加粉、刷阅读数等获利100多万元。

那么，这个团伙都为哪些公众号提供了这种“加粉”“刷量”服务，又是怎么收费的呢？

记者了解到，该团伙的客户主要是一些商业推广公司控制的公众号、个人公众号，甚至还有部分政府机关的公众号。收费标准则是目前行内“统一价”：涨1个粉0.2元，点1个赞1元，图文阅读500次5元，原文阅读100次8元，分享转发到朋友圈100个25元，量大价格可以优惠。

“他们掌握了90多万部手机，要给某个微信公众号增加上万粉丝，或者给某篇文章刷个‘10万+’，几百元上千元就搞定了，真是轻而易举。”办案民警说。

业内人士告诉记者，庞大的点赞和阅读量，能为微信公众号争取粉丝和更多的广告收入，这是公众号商业运用的基本模式。

此外，读者看到拥有高阅读量文章的公众号，基于从众心理，自然对该公众号产生信赖感和关注兴趣。所以，一些不愿踏踏实实靠内容和活动一点点“涨粉”的微信公众号，就开始寻觅捷径。微信“刷粉”业务顺势而生。

■ 记者调查

“微信刷阅读量”在网上明码标价

从微博、微信诞生开始，刷粉丝、刷阅读量这种事就有了，如今更是大行其道。

记者在淘宝上搜索“微信刷粉”“阅读量”“公众号加粉”等关键词时，出现了大量标价为1元的店铺。

记者以买家身份联系了其中两家销量较高的卖家。其中一家卖家说，标价显示1元只是为了方便服务，阅读量的价格实时报价，阅读量1000次是26元，但要等到明天早上才能完成。如需10多分钟内就上涨阅读量，则要多收10元。

至于“刷粉丝”的收费，“僵尸粉”为6元100个，“真人粉”30元100个。在谈及两者的区别时，卖家表示，区别就是小号质量不同，“僵尸粉”是电脑控制手机、掉粉包补，而“真人粉”是手工加的，掉粉不补。

当问及“这种刷量操作会不会被发现导致封号”时，一个卖家表示，不会，很安全。

■ 网警提醒

网络环境隐患多 及时预防很重要

为了保护自己的手机安全，切记以下几点——

首先，不要随意从网上下载软件，切记手机不要越狱或者root，否则系统安全威胁将大大提升；其次，到正规渠道下载ROM和软件客户端，不要下载来历不明或安全性不确定的软件包；第三，可以安装一些专业手机安全软件，定期查杀木马和病毒。

（王子琦 韩琪 陈贺 于英杰）