来源:检察日报

原标题 “挖矿”两年，获利1500万


办案人员查获的部分作案工具

每一名网游爱好者，都希望自己永远是赢家。倘若要问如何才能成为赢家，有人会说，有一种被称为“游戏外挂”的过关“神器”，保你百战百胜。“游戏外挂”自产生，就备受网游者青睐——帮人作弊、替人“挖矿”，甚至人为操纵他人计算机实施犯罪。

贺翔成，山东青州城区的一名网吧管理员，是一名“外挂高手”，仗着盖世“武功”混迹网络江湖，通过在网络游戏中安装木马程序，用收集的数据换取虚拟币（这种手法俗称为“挖矿”）的“绝活”维生。

何为“挖矿”

“挖矿”，“矿”为何物？即是由特定字符串组合而成的数据值。“挖矿”，指的非法控制他人的计算机信息系统，通过大量计算机运算获取数字货币。这是一种计算机系统下的犯罪行为。

“挖矿”的通常过程是，犯罪嫌疑人将事先开发出来的外挂程序（木马程序）安装到配置高、运行快的目标电脑上，一般是网吧电脑。只要电脑一开机，这些外挂程序就在后台自动运行且不断升级，在此过程中犯罪嫌疑人趁“机”（目标电脑）寻找特定字符串进行数据收集。只要找到特定数据值，就能得到来自虚拟币矿池的奖

励，即获得虚拟币。

虚拟币矿池是一个全自动的开采平台，它会根据“矿工”的贡献算力（比特币网络处理能力的度量单位）占比大小进行奖励分配。一般来说，虚拟币矿池建在犯罪嫌疑人的电脑服务器上，不仅实现了由单个“矿工”单独挖矿到多个“矿工”协同“挖矿”的算力集结，更提升了比特币等虚拟币开采稳定性，使“矿工”收获趋于稳定。当“矿工”们的虚拟币达到一定数量时，可以提取并到相关网站进行人民币兑换，实现非法获利。

贺翔成通过“挖矿”名声大震，拥有了“天下网吧论坛”的版主、辽宁省大连市晟平网络有限公司（下称晟平公司）迅推平台的大客户经理等众多头衔。网络带给他财富，也带给他梦魇，让他的人生变得飘忽不定。如今，梦想已灰飞烟灭，留下的只有罪恶。

8月3日，山东省青州市检察院以涉嫌非法控制计算机信息系统罪批准逮捕贺翔成及同伙贾峰、励芸（贾峰的妻子）等9名犯罪嫌疑人。自2015年起，该团伙利用黑客技术控制电脑主机389万台、挖矿主机100多万台，非法获利1500余万元。据悉，此案系山东省检察机关办理的首例利用木马程序非法控制他人计算机信息系统，通过“挖矿”获取收益的新型犯罪案件。

从“论坛版主”撬开“冰山一角”

贺翔成是如何进入警方视线的呢？原来，腾讯公司的安全团队检测到一款游戏外挂暗藏木马程序，这正是贺翔成开发的“绝地求生”外挂程序。他伙同其他人员利用这款外挂程序非法控制了607台计算机来进行“挖矿”，直到案发，该木马程序感染了数十万台用户电脑。

腾讯公司网络安全部工作人员告诉记者，用户一旦下载了“绝地求生”这款游戏外挂程序，电脑就会被植入木马程序。“杀毒手段不断升级，木马也不断升级。真可谓‘道高一尺，魔高一丈’！”办案检察官赵树芬感慨道。

赵树芬介绍，这款挖矿程序会自动检测电脑的使用情况，当CPU（中央处理器）使用率在一定范围内时，该木马就会自动启动，在后台静默挖矿，电脑的使用者是觉察不到的。这对计算机CPU、GPU（图形处理器）资源和电力资源的耗费相当大。贺翔成为何如此谙悉计算机，又怎样潜伏下来默默“挖矿”？一连串的问号困扰着办案检察官。

这要从三年前说起。当时32岁的贺翔成是当地一家网吧的网管。一个偶然机会，他成了“天下网吧”论坛的版主。贺翔成利用版主的身份，建立了多个外挂讨论群，

不仅在群文件中共享外挂程序，还悄无声息地将含有木马的外挂程序上传到“天下网吧”论坛供网民下载。平时，贺翔成还利用木马程序，给电脑用户投放广告弹窗，借此获取广告受益，用户每点击1000次，贺翔成获得零点几元的受益。单看一笔受益很小，但是天长日久，获利也不是小数。

不久，贺翔成成功“研发”出名为“绝地求生”等游戏新款外挂程序，具备“自动瞄准”“透视”“子弹加速”“子弹跟踪”等功能，通过社交群和论坛宣传，并供网民免费下载发展大量用户。

随着“事业”越干越大，贺翔成已不满足于“小打小闹”。喜好钻研的他仿冒“爱奇艺”，编写了酷艺VIP影视服务端和客户端，在全国范围内发展了60多个代理，以年卡、月卡等方式向全国网吧兜售。至案发，贺翔成共向全国2465家网吧卖出年卡5774张，季卡282张，半年卡116张，月卡3285张，非法牟利20万余元。

除此之外，贺翔成还有一个重要的身份，就是58迅推平台的大客户经理。贺翔成利用58迅推的增值客户端控制了3万余台网吧主机，非法获利26.8万余元。

2017年10月以来，贺翔成又对58迅推的增值客户端、挖矿程序进行修改，内嵌了自己的HSR（红烧肉币）钱包地址，被挖主机在挖矿时挖到矿币后会转到其HSR钱包中。截至案发，贺翔成已挖取了8552枚币（最高价格252元/枚，目前市值42元/枚）。

顺藤摸瓜挖出“幕后东家”

58迅推增值联盟源于一家网络公司——晟平公司。这家公司2014年成立，坐落在大连市甘井子区。公司旗下有两个网站：一个是迅推，另一个是速推。两个网站在分工上各有侧重，迅推主要是做广告增值和云增值（就是“挖矿”，即挖取虚拟货币）；速推则做手机App。

2014年试运行之后，公司幕后控制人贾峰指使公司副总兼运营主管张焕亮组织所谓的“研发”，也就是先研发挖矿监控软件，再集成挖矿程序。很快，该公司形成了以闫石为技术主管，以赵乐乐、丛宁一、彭立山等人为技术骨干的研发团队，将寻找到的挖矿程序进行完善，制作成“EXE”木马程序。程序研发后交由测试部测试员白桦进行测试，一旦测试成功就投放公司的迅推客户端平台，再由郭宜杰、费林洋等客服部工作人员通过客服、QQ等方式向市场推广。客服部肩负“发展下线带领并指导使用”的双重任务，在向市场推广的过程中，成功“吸纳”了贺翔成、张数等若干下线。

贺翔成和其他下线从迅推平台下载增值客户端程序后，通过多种方式将增值客户端

非法植入到网吧主机中，并静默下载挖矿监控软件和挖矿程序运行。挖到的矿币会转移到贺翔成等人的虚拟货币钱包中，由公司财务主管励芸随时变现提现，并按照控制的终端数向代理分发提成。这些虚拟货币主要有DGB（极特币）、XMR（门罗币）、Zcash（零币）等类型。至案发，团伙成员非法控制389万多台电脑主机做广告增值收益，在100多万台电脑主机静默安装挖矿程序，两年间共挖取DGB（极特币）2600余万枚。这些虚拟货币大部分都已经卖出，嫌疑人共非法获利1500余万元。

下线悉数落网

与贺翔成同时加入58迅推增值联盟的杜良晖、张数、高曰然，也是发展较为迅猛的三条“下线”。

33岁的广东佛山人杜良晖是晟平公司成立之初发展的客户，算是资历较深的“雇员”。他通过从迅推网页上下载晟平公司提供的一份EXE格式的客户端程序，并将这个软件进行编辑，把它绑定到自己编写的一个消除网吧广告的小软件里面，在消除网吧接受其他广告的同时，仍可以接受晟平公司的广告。杜良晖还将编写的这个软件分享给了一个网管QQ群里，让其他的网管朋友帮忙做推广，很多人用得不错，就自行下载安装到网吧系统里，此时罪恶的黑手已经伸向这些网吧。就这样，杜良晖利用网吧维护人员身份，将迅推网站“推广”的“EXE”木马程序静默式植入网吧电脑中，案发时杜良晖已经非法控制了9495台计算机进行“挖矿”，牟利100余万元。

36岁的黑龙江籍青年张数和同龄同乡好友高曰然，也忙碌在“挖矿”的第一线，他俩与贾峰形成“铁三角”。早在2014年贾峰就与张数相识，那时候，贾峰在搞广告弹窗，而张数则是一家网络公司的法定代表人，负责维护“净网先锋”网站，该网站本身就有一个推送功能，这为日后挖矿留下“口子”。

2017年6月至2018年4月间，张数伙同高曰然利用管理“净网先锋”网吧管理系统的便利条件，将晟平公司提供的“EXE”木马程序植入“净网先锋”的服务器，非法控制黑龙江一亩园网吧、银河舰队网吧、大伽网吧等486家网吧，共计15772台计算机来“挖矿”进而牟利。晟平公司在张数、高曰然作案时负责木马程序的正常运行、统计挖取虚拟货币的数量并变现、提现，其中，返利给张数30余万元。

2018年4月，青州市公安机关抽调精干力量50余人赶赴大连，在当地公安机关的协同配合下，经过紧张的侦查工作，终将涉嫌非法控制计算机信息系统犯罪嫌疑人贾峰、励芸等16人全部抓获。至此，警方一举破获这起特大非法控制计算机信息系统案，抓获了涉案的20名犯罪嫌疑人，成功捣毁涉案网络科技公司2个，扣押涉案电脑52台，查缴游戏黑客程序1款、vpn加速器1款、酷艺VIP影视木马控制程序1款；

同时，公安机关还查缴58迅推木马增值客户端、挖矿程序及挖矿监控程序157款。

据办案检察官介绍，此类新型犯罪案件，因具有很强的隐秘性，被害人对犯罪分子的“挖矿”行为鲜有觉察，电脑被外挂程序后大多数情况下也是浑然不知，这不仅直接影响到计算机的GPU和CPU的正常运行，还对电力资源造成巨大浪费。（嫌疑人、涉案公司均为化名）