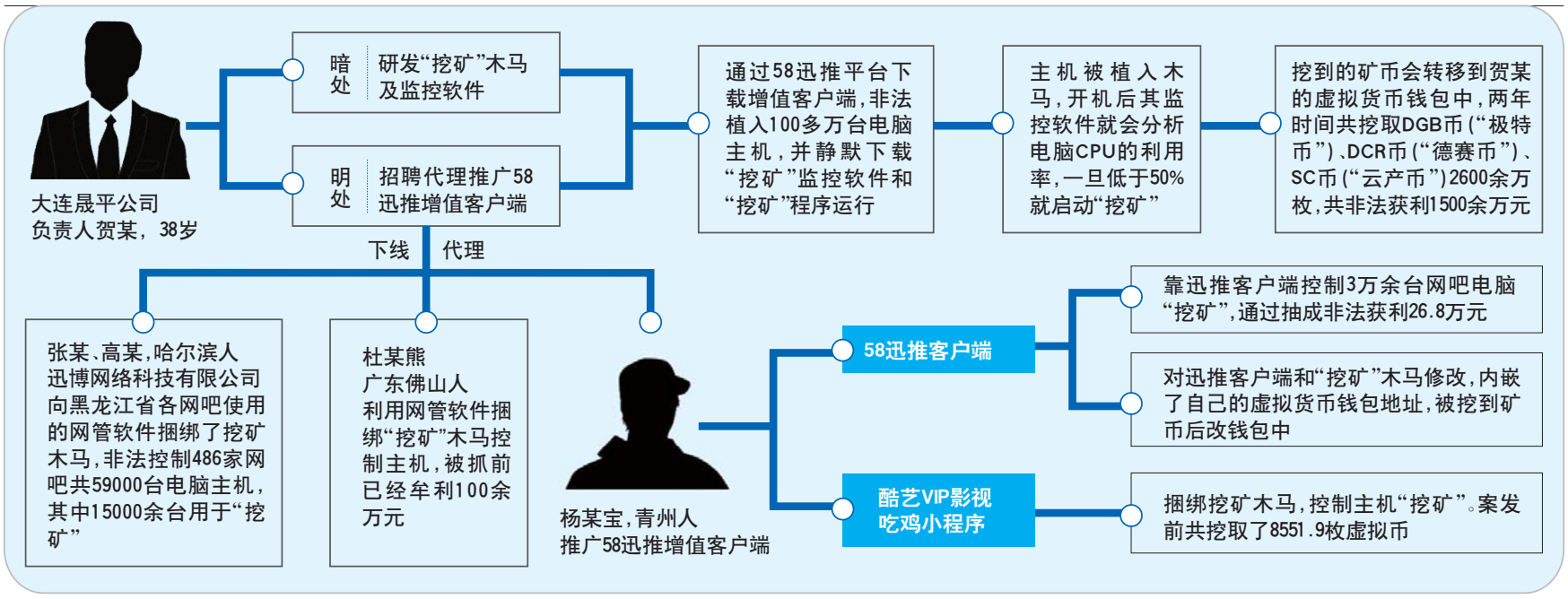


# 百万台电脑被木马控制“挖矿”

## 部分靠“吃鸡”外挂植入，三年挖取虚拟货币2600余万枚获利1500余万元

本报记者 杜洪雷

zhi liao 知了

**当你惬意地在电脑上玩着“吃鸡”游戏时，其实你的电脑正在被木马程序控制着，为千里之外的一家科技公司“挖矿”获取虚拟数字货币。自2015年起，大连晟平网络科技有限公司在全国各地招聘代理，来推广捆绑着挖矿程序的木马58迅推增值客户端，一旦客户端植入电脑主机，就会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公司控制人贺某的虚拟货币钱包中。该公司非法利用黑客技术控制电脑主机389万台、挖矿主机100多万台。**

专案组突击在大连晟平公司开展抓捕行动。警方供图

### 青州男子开发“吃鸡”外挂木马

近两年，俗称“吃鸡”的“绝地求生”游戏风靡网络，成为众多游戏玩家的最爱。为了能够在游戏中“所向披靡”，许多玩家就使用该款游戏的外挂程序，从而具备更多的能力，例如“自动瞄准”“透视”“子弹加速”等，其中多数外挂号称免费，其实内存猫腻。

去年12月20日，腾讯守护者计划安全团队发现“绝地求生”游戏中一个名为“吃鸡小程序”的外挂暗藏一款木马程序，该木马程序具备后台静默挖矿功能（挖矿即通过大量计算机运算获取数字货币－虚拟货币奖励，主要耗费计算机CPU、GPU资源和电力资源），初步统计该木马程序感染数十万台用户机器。

随后，线索转交给潍坊市公安局网安支队进行侦查。

民警通过互联网提取到外挂木马样本，找到木马开发者建立的木马交流群，初步侦查发现该款木马程序开发者在青州市。潍坊市局网安支队、青州市局成立专案组，对该案立案侦查。

通过侦查，专案组确定交流群群主身份为杨某宝（男，35岁，山东省青州市人）。民警侦查发现杨某宝通过多个途径来传播这个隐藏挖矿木马程序的外挂，其一是建立了多个外挂讨论群，在群文件中共享外挂程序，另外他利用“天下网吧论坛”版主的身份，将含有木马的外挂程序上传到“天下网吧”论坛，通过百度网盘进行分享下载。

3月8日，专案组制定了详细的抓捕方案，在家中将杨某宝抓获。

### 大专学历网管竟是有名“黑客”

仅仅是大专学历的杨某宝在上大学的时候将多数时间用于计算机程序学习，利用所学的编程语言来编写外挂程序和修改游戏，并在网络上有一定的名气。此后，他在青州一家网吧内干网管，从而接触更多的“黑客技术”来实现挣钱的目的。

最初，他仿冒“爱奇艺”，编写了“酷艺VIP影视”服务端和客户端，全国范围内发展了60多个代理，以年卡、月卡方式向全国网吧兜售。杨某宝共向全国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余万元。

此外，杨某宝开发了名为“吃鸡小程序”的外挂程序，并供网民免费下载发展大量用户，得以进入众多的电脑主机。

2017年，杨某宝在天下网吧论坛接触到用于广告增值服务的58迅推客户端，并与该平台的开发公司大连晟平网络科技有限公司（下文简称“大连晟平公司”）联系，获知该客户端捆绑着“挖矿”的木马程序，能够通过推广该客户端来控制主机“挖矿”获利。

杨某宝手上控制着大量的网吧主机，从而成为推广平台的大客户。杨某宝利用此前推广软件发展的用户来推广58迅推增值客户端，从而控制3万余台网吧电脑来为大连晟平公司“挖矿”，其通过有效控制的终端数来抽成，非法获利26.8万元。

看到控制他人主机“挖矿”牟利很大，杨某宝发挥其才能，对58迅推客户端和捆绑的“挖矿”木马程序进行修改，内嵌了自己的HSR（“红烧肉币”，一种虚拟货币）钱包地址，被控主机在挖矿时挖到矿币后会转到自己的HSR钱包中。

此外，杨某宝将这个挖矿木马程序捆绑到此前研发的“酷艺VIP影视”服务端和“吃鸡小程序”中，然后通过升级这两个程序，将“挖矿”木马程序植入到装有这两款程序的主机上面，从而控制更多的主机为其“挖矿”。经统计，自2017年10月份至案发，杨某宝共挖取了8551.9枚HSR币（最高价格252元/枚，目前42元/枚）。

### “挖矿”木马背后是正规网络公司

“经过深入调查，我们发现‘杨某宝’仅仅是58迅推平台的一个代理，背后更大的犯罪集团是大连晟平公司。”青州市公安局网安大队大队长田爱伟称，他们调查发现这家公司是正规注册的网络计算机公司，有40多名员工。

专案组曾经三赴大连对该公司进行调查，“我们摸清楚了公司的幕后控制人为贺某，38岁，吉林人，公司财务主管是陈某，32岁，是贺某的妻子，同样也是吉林人。”潍坊市公安局网安支队民警王万涛称，贺某平常都在家里，很少去公司，其妻子陈某在公司主持日常的工作。

4月11日，潍坊市公安局网安支队与青州市公安局抽调精干力量50余人赶赴大连。经过周密部署，专案组突击在大连晟平公司和贺某家中开展抓捕行动，抓获全部涉案嫌疑人16名。通过审查，贺某、陈某等12人涉嫌非法控制计算机信息系统罪被刑事拘留，赵某从等4人被取保候审。

随后，专案组对大连晟平网络科技有限公司的下线进行梳理并展开抓捕。4月18日，专案组在哈尔滨打掉迅博网络科技有限公司，抓获张某（男，36岁，哈尔滨人）、高某（男，36岁，哈尔滨人）。两名嫌疑人利用职务之便，向黑龙江省各网吧使用的网管软件捆绑了挖矿木马，非法控制486家网吧共5万9千台电脑主机，其中15000余台电脑用于“挖矿”。

4月19日，专案组在佛山将杜某熊（男，33岁，广东佛山人）抓获，查缴一款dll挖矿程序。“这名嫌疑人也是一个网管，利用网管软件捆绑‘挖矿’木马控制主机。该嫌疑人是大连晟平公司最大的一个代理，被抓前已经牟利100余万元。”王万涛介绍道。

### 自动监测CPU利用率低于50%就启动挖矿

38岁的贺某是大连晟平公司的实际控制人，也是一名非法控制计算机信息系统的老手，此前都是在南方活动，2014年曾因此被打击处理。

2014年下半年，贺某在大连成立公司开展广告增值服务，最初只有几个人，后来发展到40多个人。“所谓的广告增值服务，也是游走在灰色地带，通过开机广告、弹窗广告和隐藏广告来帮着其他公司进行推广，根据实际点击数来收取费用。”王万涛称，这个也需要通过招聘代理推广客户端来实现，而贺某的客户端就是58迅推增值客户端。

2014年开始，以比特币为代表的虚拟数字货币火起来，从而出现众多的虚拟数字货币。看到这个“风口”，贺某开始不甘于仅仅推广增值客户端，从2015年开始指使公司副总兼运营主管张某宁组织研发、测试部门对“挖矿”木马进行研发。

为此，公司研发部负责研发“挖矿”监控软件、集成“挖矿”程序；测试部负责测试，客服部负责发展下线代理并指导使用。下线代理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某的虚拟货币钱包中。其中杨某宝等人就是其下线代理。

“一旦主机被植入木马，只要是主机开着机，其监控软件就会分析电脑CPU的利用率，一旦低于50%就启动‘挖矿’程序进行‘挖矿’。如果CPU利用率高就停止‘挖矿’，防止被发现。”田爱伟称，即便被杀毒软件发现查杀，其公司依然可以通过更改部分数据进行升级程序来规避杀毒软件。

经统计，2015年以来，贺某等人非法控制389万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，近三年来共挖取DGB币（“极特币”）、DCR币（“德赛币”）、SC币（“云产币”）2600余万枚，共非法获利1500余万元。

办案民警称，违法犯罪人员通常提前调研市面上挖取难度较低的虚拟货币，非法控制用户的电脑主机，植入这种虚拟货币的挖矿程序进行挖矿，在挖取到大量矿币后迅速进行变现提现，牟取高额利润，而被植入挖矿木马的用户电脑主机，在经常长期高负荷运转挖矿的情况下，显卡、主板、内存等硬件会提前报废，严重损害网络用户的权益。