潍坊青州公安破获部督特大非法控制计算机信息系统案

本报讯 记者徐鹏通讯员刘贵增 王艳 正常用着的电脑，却被非法控制，正替别人“干活”，用户浑然不知。原来，电脑被植入了挖矿程序及挖矿监控程序，监控程序只要监测到电脑CPU利用率低于50%，挖矿程序就会在后台静默启动，通过大量耗费被控电脑的CPU、GPU资源和电力资源，持续不断地挖取虚拟货币，并将这些虚拟货币转至控制者处，从而提现牟取暴利。

近期，潍坊市公安局网安支队会同青州市公安局在公安部、省公安厅指导下，在腾讯守护者计划安全团队协助下，按照公安部和省公安厅“净网2018专项行动”部署要求，成功破获部督“1.03”特大非法控制计算机信息系统案，目前抓获犯罪嫌疑人20名，取保候审11名，批捕9名。

经查，大连昇平网络科技有限公司研发挖矿监控软件、集成挖矿程序后，通过发展下线代理，非法控制了全国389余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。两年期间共挖取DGB币（“极特币”）、DCR币（“德赛币”）、SC（“云产币”）币2600余万枚，共非法获利1500余万元。

游戏外挂暗藏挖矿木马程序

2018年1月3日,潍坊市公安局网安支队接腾讯守护者计划安全团队报案称，腾讯电脑管家检测到一款游戏外挂暗藏了一款木马程序，该木马程序具备后台静默挖矿功能。

“挖矿，就是通过大量计算机运算获取数字货币 - 虚拟货币奖励，这个过程对电脑硬件配置要求比较高，主机经常长期高负荷运转，显卡、主板、内存等硬件会提前报废，对电脑的损害极大。”办案民警介绍。

办案民警说，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，通过云计算、显卡云计算业务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，用户对此毫无察觉，只要电脑处于开机状态，挖矿程序就在后台静默运转，在挖取到大量矿币后迅速转至控制者那里变现提现，牟取高额利润。

初步统计，该木马程序感染数十万台用户机器。潍坊市公安局网安支队接案后，迅速研判案件线索，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，初步落查发现该款木马程序开发者在青州市。市局网安支队将该案情通报青州市公安局，由市局网安支队、青州市局成立专案组，对该案立案侦查。

专案组确定交流群群主身份为杨某宝。通过侦查发现，杨某宝一是建立了多个外挂讨论群，在群文件中共享外挂程序；二是利用“天下网吧论坛”版主的身份，将上传含有木马的外挂程序到“天下网吧”论坛供网民下载；三是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。

科技公司研发木马程序发展代理

经审讯，杨某宝对利用外挂、“酷艺VIP影视”非法控制计算机信息系统的犯罪事实供认不讳。该杨交代曾为58迅推增值联盟雇佣，利用该平台增值客户端非法挖矿共同获利。

专案组迅速查清58迅推增值联盟的幕后公司为大连晟平网络科技有限公司，掌握了这家公司的组织架构，摸清公司幕后控制人为贺某、公司财务主管为陈某（贺某妻子）。

4月11日，专案组抽调精干力量50余人赶赴大连，经过周密部署，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。

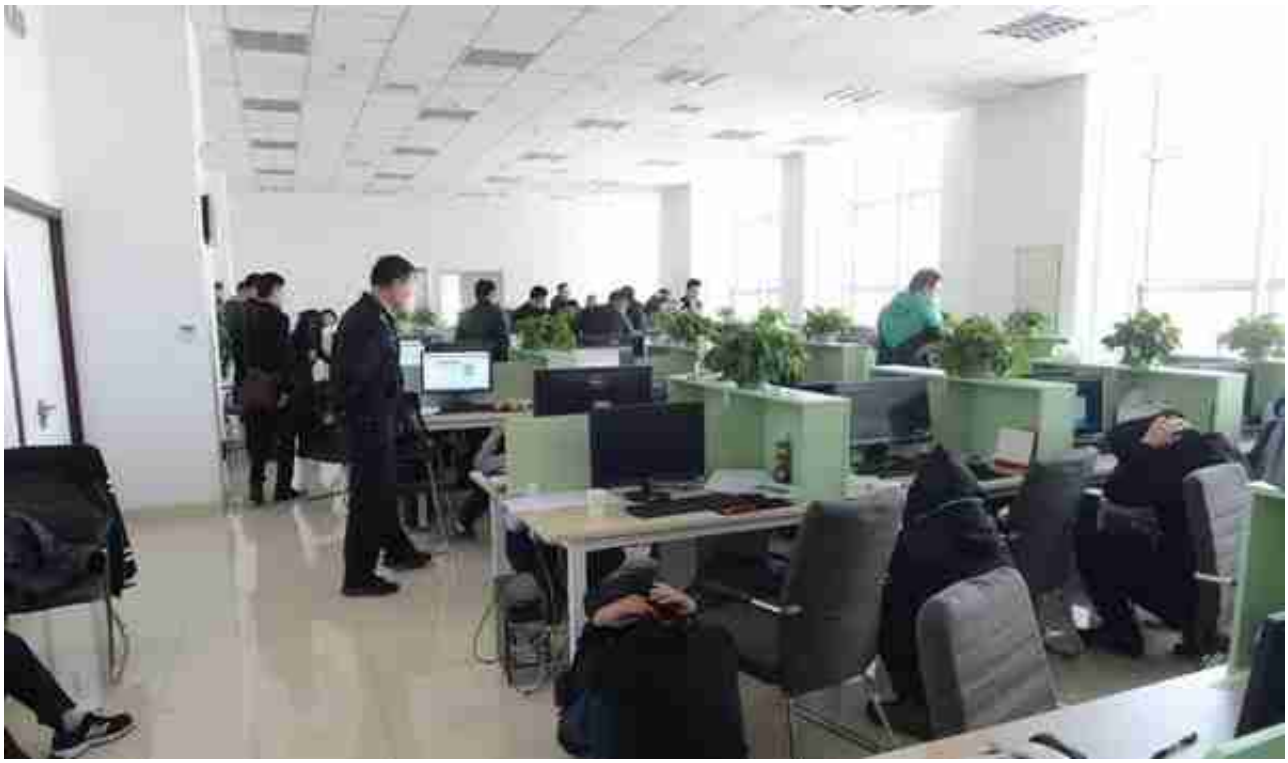
随后，专案组对大连晟平网络科技有限公司的下线进行梳理，并开展抓捕。

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、高某，查清该二人利用职务之便向黑龙江省各网吧使用的某网管软件捆绑了挖矿木马，非法控制近6万台电脑主机。

4月19日，专案组在佛山将杜某熊抓获，查缴一款dll挖矿程序。

“大连晟平网络科技有限公司是上线，提供技术支持，研发了挖矿监控软件、集成挖矿程序，然后发展了全国几百名下线从事代理。”办案民警介绍，这些下线手中掌着全国389万台电脑的庞大资源，大连这家公司一一与下线达成合作协议，不仅向这389万台电脑发送广告获利，还选择其中100多万台进行后台静默挖矿，这两部分的利润由上线与下线按比例分成。

据了解，虽然非法控制电脑的违法犯罪屡见不鲜，但是数量达到如此之巨，而且能够植入静默挖矿程序进行挖矿变现，这在全国是比较少见的。



揭示挖矿木马牟利产业链

通过审讯查清，杨某宝涉嫌侵犯著作权非法牟利，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。该杨共向全国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。

同时，杨某宝开发了外挂程序，具备“自动瞄准”、“透视”、“子弹加速”、“子弹追踪”、“物品显示”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。

“杨某宝通过上述两种渠道掌握了大量电脑资源，共计有3万多台电脑主机。作为大连晟平网络科技有限公司的大客户，他利用其迅推的增值客户端控制了这些电脑

，植入挖矿木马程序后，大连这家公司提取虚拟货币套现，和杨某宝分成，杨某宝共非法获利26.8万余元。”办案民警介绍。

对于大连晟平网络科技有限公司，经查，从2015年以来，贺某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研发，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。

“就像杨某宝一样，全国几百名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，陈某随时进行变现提现，陈某按照控制的终端数向代理分发提成。”办案民警说。

据了解，杨某宝曾做过网吧管理工作，在电脑编程方面自学成才，非常有研究，尝到甜头的他后来不满足于受制于上线，他对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，被控主机在挖矿时挖到的矿币后会转到自己的HSR钱包中。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）。

警方提醒，不要贪图蝇头小利安装来源不明的软件程序、点击来源不明的网站链接和访问非法网站，否则电脑很容易被非法控制。同时，要安装正规杀毒软件及时更新升级，电脑卡顿、温度过热时，利用杀毒软件查杀或者请技术人员进行检查。