文丨王伶玲 来源丨法制晚报

虚拟货币虽然眼花缭乱但却有据可循，运用区块链算法进行计算获得货币从而变现。但是有一种挖矿病毒却在用你高配置的电脑为他人掘进牟利，导致电脑速度变慢不说还极大的损害硬件。眼下这种黑色产业链却风生水起，凭借零成本、高收益的优势成了黑客们的新宠。

近日，山东警方在辽宁大连破获了“tlMiner”挖矿木马黑产公司。该公司非法控制用户电脑终端达389万台，非法获利1500余万元。

案例

398万电脑为黑客赚1500万

日前，山东警方在辽宁大连一举破获了“tlMiner”挖矿木马黑产公司。据悉，该公司为大连当地高新技术企业，为非法牟利搭建木马平台，招募发展下级代理商近3500个，通过网吧渠道、吃鸡外挂、盗版视频软件传播投放木马，非法控制用户电脑终端389万台，进行数字加密货币挖矿、强制广告等非法业务，合计挖掘DGB（极特币）、HSR（红烧肉币）、XMR（门罗币）等各类数字货币2000万枚，非法获利1500余万元。

该案为国内首例利用挖矿木马组建僵尸网络，非法控制计算机挖矿的案件。据警方统计，这家公司控制的电脑中，100万台性能最好的电脑用来挖矿，其余200多万台用做弹窗广告。

“所谓僵尸网络，就是电脑是你的，但是不归你管，别人想在你电脑上干什么都可以，挖矿只是他做的最无害的一个动作。他还可以拿着你的数据，控制你家里的摄像头，还可以让这么多电脑，去集中地攻击某一个网站，300多万台足以让被攻击的网站瞬间瘫痪。”协助此次破案的腾讯电脑管家高级安全专家李铁军告诉记者。

揭秘

虚拟货币火爆 黑客找人掘金

2009年，比特币横空出世。得益于其去中心化的货币机制，其受到许多行业的青睐，交易价格也是一路走高。受此影响，许多基于区块链技术的数字货币纷纷问世，例如以太币、门罗币等。这类数字货币并非由特定的货币发行机构发行，而是依据特定算法通过大量运算所得。而完成如此大量运算的工具就是挖矿机程序。

挖矿机程序运用计算机强大的运算力进行大量运算，由此获取数字货币。由于硬件性能的限制，数字货币玩家需要大量计算机进行运算以获得一定数量的数字货币，因此，一些不法分子通过各种手段将挖矿机程序植入受害者的计算机中，利用受害者计算机的运算力进行挖矿，从而获取利益。这类在用户不知情的情况下植入用户计算机进行挖矿的挖矿机程序就是挖矿木马。

据360安全报告显示，挖矿木马最早出现于2013年，受利益驱使，2017年底开始挖矿木马成为最流行的木马，控制肉鸡电脑挖矿成为掘金最快的网络黑产。

机主浑然不知 硬件损害极大

电脑被黑客们控制挖矿，机主真的察觉不到吗？答案是肯定的。

有网友反映，自己在用外挂“吃鸡”的时候，电脑过热，或者风扇声音变大，但他们都认为那是正常的，因为“吃鸡”的时候本来就会对电脑进行高消耗。但也有网友反映，待机状态电脑风扇会自动运转并且电脑发热。那么你的电脑可能正在“挖矿”。

李铁军告诉记者，挖矿木马隐蔽性强，犯罪分子通常会筛选配置较高的电脑进行木马植入。记者梳理发现，挖矿木马“tlMiner”有几大特点：机器CPU利用一旦超过50%，木马会停止工作；如果挖矿的行为要占用40%的进程时也会自动退出；机主在“吃鸡”时，挖矿木马通常不会工作，而当电脑息屏或者待机状态时，挖矿会全速进行。

“当前个人电脑的主流配置性能很强的时候，即使木马已经在挖矿，性能变差的直观感受也并不明显。只有挖矿木马启动挖矿程序，同时用户启动较耗资源的应用，比如大型游戏，此时才会感觉电脑速度变慢、温度升高。据悉，挖矿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。”李铁军表示。

几百元控制千台电脑获利上万

如果说勒索病毒是暴露在大众视野中的“恶魔”，那么挖矿木马就是潜藏在阴暗之处的“寄生虫”，而且成本低，获利高。

记者搜索发现，网络上已经有人出售“电脑肉鸡”程序，这些程序往往能够轻易地控制别人的电脑。在慧聪网上，有人以标价0.1元的价格供应电脑肉鸡，最小起订量2000个。这意味着，用户只需要花费几百元的成本，就能控制上千台电脑盗取电脑里的资料、接单攻击网站和服务器、利用电脑进行“挖矿”等非法获利，获得上千

元甚至上万元的非法利益。挖到的虚拟货币还能兑换成人民币。

2017年底，温州市瓯海公安分局就曾破获一个12人组成的黑客团伙，他们攻击、控制了全国5000多台电脑，买卖电脑控制权，并利用这些电脑给自己“挖矿”，获取门罗币等数字货币1000多枚，目前查实获利60余万元。

“互联网往哪个方向走，黑色产业就往哪个方向走，基本上是一一对应的关系。”李铁军介绍，黑产在早期可能就是控制别人的机器来弹广告，做广告分发，之后是软件分发，黑产主动在后台在用户不知情的情况下装很多软件，弹广告、锁主页、推广软件，这些套路都没变过。直到2017年挖矿，改变了整个黑产行业的作战形式，大家都去挖矿了，挣钱特别直接。可以看到其他恶意软件的行为变少了，都在挖矿，控制的肉鸡规模越大，收益就越高。

专家建议

外挂需谨慎 不明文件要拒绝

挖矿木马的崛起源于数字货币交易价格的持续走高，从当前的情况看，数字货币交易价格还将持续攀升，这也将可能导致挖矿木马数量的激增。因此，如何防范挖矿木马是重中之重。

李铁军建议用户，要养成良好的安全习惯，比如不随便打开来历不明的文件，不随便按网站的提示关闭或退出杀毒软件等。

“很多外挂或游戏辅助工具的网站会欺骗用户说，杀毒软件会误报，要用这个外挂就要先退出杀毒软件。我们希望用户不要轻信，保持警惕，最大可能减少主动运行病毒的机会。另外，建议用户经常使用腾讯电脑管家修复系统漏洞，开启杀毒软件，这样中毒的机会会少很多。”李铁军称。