来源:新京报

7月25日，比特币价格突破8500美元大关，其价格在7月以来已经上涨超40%。虚拟货币繁荣背后，黑色数字产业链却已经悄然将方向转向“挖矿”（利用电脑硬件计算出虚拟货币的位置并获取该货币的过程）领域。

7月初，山东省青州警方破获了一起制造木马病毒感染普通电脑，并利这些电脑闲置的CPU资源“挖矿”的案件。涉案的大连某高新技术企业控制了包含389万台电脑的“僵尸网络”（指被木马感染，可由远程控制的电脑网络），涉案案值超1500万元。

新京报记者采访了相关办案民警、电脑安全专家等，揭露黑色数字产业链发展的上下游，以及黑产如何围绕互联网流量进行变现。

吃鸡“外挂”暗藏“挖矿”木马

“我们是按‘非法控制他人计算机’罪名立案的。”山东省青州市公安局的李警官介绍，该案犯罪嫌疑人杨某，仿冒“爱奇艺”编写“酷艺VIP影视”，还提供吃鸡游戏“外挂”程序（游戏作弊软件）供网民免费使用，但杨某在程序中暗置木马程序“挖矿”，专门挖HSR虚拟货币。至案发，杨某已挖取了8551.9枚HSR币（最高252元/枚，目前42元/枚）。

该案中，杨某将带有木马病毒的软件大规模扩散，是由于其“天下网吧论坛”版主的身份，以及大连晟平网络科技有限公司（下称晟平网络）的推广。晟平网络表面业务是广告营销、软件推广，背地里却在其增值客户端和推广的软件中植入“tlMiner”挖矿木马。经过该企业及其3500个代理商的推广，挖矿木马感染了超100万台电脑。

据李警官介绍，晟平网络共控制了389万台电脑的“僵尸网络”，经济收益超1500万。其中，利用高性能计算机挖取DGB币（极特币）、DCR币（德赛币）、SC（云产币）币2600余万枚；其他200余万台进行广告弹窗、应用下载业务。而单独售卖“外挂”，单月单人仅能获益不到百元。

电脑为别人“挖矿”，用户却不知情

据警方信息，该案的线索来自于网络安全大数据监控。2017年年底，腾讯电脑管家（PC端）及安全大脑（云端）发现“tlMiner”木马在一天之内感染超20万台电脑，并且具有暗中挖矿、以正常应用程序带木马等行为。警方经过近半年时间的侦破，上述案件告破。

腾讯电脑管家高级安全专家李铁军介绍，相较过去的木马程序，挖矿木马不会改动用户首页、隐藏文件，甚至具有选择性占用用户内存的特点，不易被感染者发现；此类病毒直接挖矿改变了数字黑产的变现方式，无需再与下游企业结算，可直接卖币获利。

虽然目前该木马感染用户计算机后，只占用闲置CPU资源挖矿，但与其他木马类似，服务器可对被感染计算机做任何事情，比如调用摄像头、查看重要文件等。同时，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，对电脑的损害大。

此外，此类挖矿木马除了植入在游戏外挂中，还会植入在号称可以看视频网站付费内容的“仿冒”播放器中。以上软件在运行时，都会提醒用户“暂时关闭安全软件、防火墙等”，让用户电脑处于无防护状态。

“挖矿”木马成黑产更直接变现手段

“现在，市面上的木马病毒一般只做两种事情，一种是挖矿，一种是勒索”，李铁军告诉新京报记者。去年大面积爆发的勒索病毒就是木马病毒，只是其在入侵用户计算机后，通过检测用户信息，了解用户身份，进而对高净值人群进行勒索。今年以来，勒索病毒大面积爆发减少，但精准性增强，针对政府、医院及企业高净值人群的案件增多。最近的新趋势是，以木马控制“僵尸网络”给直播、短视频网红点赞、刷评论、弹幕等，但并非主流趋势。

业内专家介绍，以前木马的制造者，会通过控制“僵尸网络”打Ddos攻击（分布式拒绝服务攻击，可短时间致使某网站瘫痪）、运行弹窗广告，以及暗中下载应用软件等，目前这些行为都在减少。这反映出木马黑产背后的产业链正在变短。

从变现角度讲，原来木马黑产需要通过各种手段入侵电脑，控制“僵尸网络”，然后转让给其他控制者，打Ddos攻击获利；或者给广告主做弹窗广告，给应用程序做非法下载，再由下游公司进行结算，这些都是间接变现。而挖矿木马的出现，让黑产上游可以直接将挖到的虚拟币存入钱包，直接交易变现。

“木马行业的黑产都是围绕流量变现展开的，互联网产业往哪个方向走，黑色产业就往哪个方向走，基本上是一一对应的关系”，李铁军告诉新京报记者，早期是广告，因为早期互联网软件都是利用广告弹窗的方式来变现，黑产就控制别人的机器来弹广告。后来软件分发成为一个趋势，黑产就在用户不知情的情况下装很多软件；直到现在的挖矿，改变了整个变现形式，挣钱特别直接。“锁定主页、弹窗广告、下载软件等行为变少了，因为都在挖矿。”（记者 白金蕾 实习生 赵炜）