责编:钱 虹
制版:赵 芳
内蒙古法制报

揭秘“网络黑色产业链”新套路

由0和1组成的比特世界,看似规则清晰、简单有序,但实际上,只要是能够承载人性欲望的地方,就永远少不了正邪较量。日新月异的科技手段只是工具,正义者用其造福人类,邪恶者则用其谋取私利。

中国拥有全球最庞大的互联网用户群体,另一方面我国也成为网络黑产的重灾区。根据阿里云方面提供的数据,如今发生在全球范围内的DDoS攻击(指分布式拒绝服务,攻击者利用自己控制的终端对目标网站在较短时间内发起大量请求,大规模消耗目标网站的主机资源,使其无法正常服务),有一半以上发生在中国,平均每分钟就发生一次DDoS攻击。据科技市场研究机构IDC估算,全球每年因网络攻击造成的损失超过千亿美元,中国占比超过十分之一。

玩游戏也可能中招

为了能够顺畅讨论网络黑产,可能需要先了解几个“术语”:

暗网传统搜索引擎能够“看到”的表面网络,只是网络空间非常小的一部分,业内人士估计只有4%左右,而大量存储在网络数据库的内容,不能通过超链接访问,需要通过动态网页技术才能获取,这就是暗网。

暗网中有大量非法信息和违禁商品在售,比如身份账户信息、枪支毒品、色情视频、假证伪钞……据说,被称为“黑暗版淘宝”的暗网平台“silk road”上,还有信用评级体系出售,甚至还在“黑五”搞促销。而比特币就是暗网世界的通行货币,黑客敲诈案件索要的大多是比特币。

肉鸡指受黑客远程控制的电脑、手机。大量已经沦为肉鸡的电脑、手机构成了僵尸网络(Botnet),黑客可以以一对多的形式控制网络上的设备,并通过远程操控进行各种不法活动牟利。你或许会觉得这都是电视剧里的剧情,事不关己。但其实很多人都游走在网络黑产的边缘,甚至可能已经跌落其中,只是并不知晓。

今年4月,山东警方在辽宁大连破获了一起“tlMiner”挖矿木马黑产大案。一家当地知名的高新科技企业,竟然掌控着一个拥有389万台电脑终端的僵尸网络。

警方最后查实,因为这家公司表面上伪装成一家软件公司,因此互联网渠道资源非常丰富,分发一个病毒就变得非常容易。这家公司为非法牟利搭建木马平台,招募发展下级代理商近3500个,主要通过网吧渠道、“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。

通过这个超大的僵尸网络,这家公司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)、SHR(超级现金币)、BCD(比特币钻石)、SIA(云储币)等各类数字货币超过2000万枚,非法获利1500余万元。

李铁军透露,这个团伙控制了300多万台电脑,只拿其中100多万台“挖矿”,其他的用来做弹广告、推广等“传统业务”。“他们挑选了系统性能最好的电脑‘挖矿’,‘吃鸡’游戏玩家的电脑配置都比较高,非常适合用来‘挖矿’。”

为何“盯上”虚拟数字货币

“从2017年至今,我们观察到一个明显的趋势:这两年围绕虚拟数字货币的病毒木马最为多见。挖矿病毒在2018年上半年尤其突出,这种情况跟这两年区块链经济火热有关,虚拟数字货币行情很好,变现相对容易,且具有匿名性,不方便警方追查。”亚信安全通用安全产品总经理童宁告诉记者。

根据亚信安全发布的《2018年第一季度网络安全威胁报告》,挖矿病毒已经成为不法分子利用最为频繁的攻击方式之一。“挖矿病毒具备非常好的隐蔽性,没有广告弹窗、也不会通过文件加密来勒索用户,被用户主动发现的几率很小,再加上挖矿病毒广泛存在于PC、移动设备中,所以会出现大量受害者。”童宁介绍说。

无论采取什么样的手段和方式,网络黑产的最终目标是赚钱。记者采访的多位安全专家都表示,这么多年来,黑色产业链的本质并没有变过,就是流量变现。哪里能够最有效地变现,黑产的触手就会伸向哪里。最早,互联网主流的变现方式是广告,主流互联网公司靠广告盈利,黑产也是如此。黑产通过木马建立僵尸网络,一个广告看似被上百万用户看到和点击,但实际上都是僵尸肉鸡在点击,对于广告主来说毫无价值。即使到今天,弹广告、锁主页、推广软件,这些套路都没变过。

后来移动互联网兴起,软件分发成为一个盈利渠道。通过木马,黑产从业者把软件在用户不知觉的情况下,装到电脑或者手机上,甚至还卸载不了。

但广告和软件分发还需要建立代理网络,与很多人分成,而随着区块链的火爆,挖矿可以直接变现。

李铁军表示,区块链现在已经成为网络黑产的新风口,挖矿病毒增长非常快,勒索病毒也都索要比特币,可以说现在的黑产犯罪大多与区块链有关,这也是当下网络黑产的重要特征。

黑产也在追“风口”

《2018年第一季度网络安全威胁报告》指出,挖矿病毒对于个人中毒者来说,会出现计算机运行缓慢、耗电量大增、死机、电脑寿命降低等后果;而对于企业来说,会破坏企业内部IT环境、数据中心的正常运行秩序以及关键应用的交付。

李铁军表示,表面上看,相比弹广告、锁首页、删文件勒索、窃取信息的木马病毒,挖矿木马的危害好像比较轻,因为它只是消耗用户电脑的资源,增加耗电量而已。而且现在的挖矿木马还特别“良心”,它只会占用用户系统资源的一部分,基本会控制在50%以下,还会随着用户的使用情况自动调整用量,达到让人不易察觉,从而长期挖矿的目的。

“但是,其中隐藏的风险是巨大的。因为一旦电脑被远程控制,也就意味着他人可以在用户的电脑上干任何事,比如获取用户数据、控制摄像头……更可怕的是,如果近400万台电脑组成的僵尸网络攻击某个网站,其基本上瞬间就会瘫痪。”李铁军介绍说。

童宁指出,虚拟货币在网络黑产的另一重要角色是作为地下交易的介质。在网络地下黑色市场的运行中,基于区块链技术的虚拟货币由于去中心化、可自由交易等特性,为网络黑产的交易提供了非常便捷的交易手段。

“为了增强交易的稳定性,现在很多虚拟货币的网络以及交易所开始重视网络安全。比如加强与网络安全公司的合作,向社会招募相应的漏洞挖掘者进行悬赏,悬赏金额从5000到1万美元不等。”童宁说。

“挖矿让网络黑产的产业链变短了,门槛降低了,原本个体黑客只是一个有技术能力的人,可能没有刷流量变现的渠道,又不敢打DDoS,但现在可以去挖矿。”李铁军说。在“tlMiner”案件中,“吃鸡”外挂的“作者”发现自己的“作品”被这家大连公司植入了挖矿木马从而盈利丰厚,于是后来就在外挂中留了“后门”,也为自己挖矿。

据记者了解,目前大多数挖矿病毒都在挖一些山寨币,因为只需要用CPU的算力就能挖。而挖比特币的大多是专业矿机,必须有高性能的CPU,黑产者获取比特币更有效的方式是勒索。

李铁军表示,从去年下半年到现在,电脑病毒基本上有两大类,一是勒索病毒,二是挖矿病毒。“DDoS攻击目前是公安部的头号打击对象,而且一旦几万台电脑集中攻击,国家互联网应急处理中心系统马上会监测到,所以现在不是特别流行了,一般也不敢搞了。”他说。

但是,黑产有自己的办法,就是缩小攻击范围,做“精准打击”,这样范围较小,更隐蔽。因此,从各类安全报告提供的数据看,今年以来,勒索病毒在感染数量上有所下降,但这并不意味勒索病毒的危害减轻了,而是攻击者调整了策略:精确打击最可能付费的企业、事业单位等高价值目标,基本放弃了中招就选择重装系统的普通网民。

“过去勒索病毒都是大面积攻击,不管三七二十一,先把所有用户电脑上的数据文档都加密。但这几年变化挺大的,现在控制者会先在云端浏览用户电脑里的数据信息,识别出这是一个有钱人的电脑还是普通人的电脑,是一个普通职员的电脑还是企业高管的电脑,尤其是医疗机构、政府部门等电脑,都会被筛选出来,进行小范围勒索。普通用户中了勒索病毒基本就是重装系统,他们挣不到钱。”李铁军说。

另外一个近年来的热门发财之道就是刷单,比如一些微博、直播、短视频平台为了打造网红或者营销号想扩大影响力,就会下单雇佣黑产者帮助做流量、做粉丝、点赞、发评论……“这条路现在也非常赚钱,因为市场需求很大。”李铁军说,自己就亲身经历过,在出差时连接了酒店的免费WiFi,然后就发现自己的微博账号在不停给人点赞。

黑产新套路:黑吃黑、做周边

国家互联网应急中心将“网络黑产”界定为三类:一是发动涉嫌拒绝服务式攻击的黑客团伙,即“黑客攻击”;二是盗取个人信息和财产账号的盗号团伙,即“盗取账号”;三是针对金融、政府类网站的仿冒制作团伙,即“钓鱼网站”,这些都是典型的网络违法犯罪行为。

据统计,我国网络犯罪已占犯罪总数的三分之一,并以每年30%以上的速度增长。

童宁认为,目前网络黑产呈现出越来越明显的组织化与专业化趋势。由于暗网的存在,不法分子可以通过互联网的“地下黑市”买到网络诈骗所需要的用户数据、恶意软件等产品与服务,在不需要了解攻击技术的情况下,很多不法分子也可以通过网络黑色产业链进行攻击,这让网络黑产的门槛大幅降低。

另一方面,这也使黑产间的竞争加剧了。腾讯电脑管家安全团队监控发现,挖矿木马之间也会“黑吃黑”。随着挖矿木马的流行,出现了很多重复感染的情况,即一个肉鸡感染了多个挖矿木马。这就使木马之间开始“斗法”,看谁率先把其他木马干掉,让这个肉鸡全身心为自己挖矿。

更有甚者干脆“截胡”,在其他黑客挖币成功后,控制矿机与矿池之间的数据沟通,直接篡改矿机接收矿池奖励的地址为自己的钱包地址。

随着传统企业的数据化转型,也增加了黑客们的捞金空间,甚至产生了“周边”行业,比如现在火爆的“勒索病毒破解”,只要在百度搜索勒索病毒破解、解密,就会找到很多提供此类上门服务的公司。

“要知道,勒索病毒加密后基本是解不了的。”李铁军说,“大部分这类公司其实是扮演‘谈判中介’的角色,大部分勒索索要比特币等数字货币,很多被勒索者根本不知道去哪里买数字货币以及如何转账,而这些公司比较熟悉数字货币的交易,可以帮被勒索者与勒索者讨价还价,赚取差价,并非真能解开加密。这个行业已经很成熟了,也不排除有一边放毒,一边过来解密收钱的不法分子。”

对于个人用户来说,中了黑产的招,很大一部分原因就是安全意识不够,存在侥幸、贪财等心理,这些因素会导致用户比较容易受到诈骗信息的影响。因此,首先要增强网络安全保护意识,在网络生活中尽量减少对于个人信息的泄露,并主动拒绝存在安全隐患的应用。另外,个人用户在生活中最好能关注手机、电脑的安全状况,发现异常情况后通过杀毒软件等方式进行清理。最后,个人用户应该具备理性的判断能力,对疑似网络诈骗的活动进行核实,避免受骗。

(孙冰)

广告发行部电话:(0471) 4687563 广告经营许可证:呼工商广字1501004000013 邮编:010010 本报激光照排印刷:呼和浩特日报社印刷厂 本报零售:每份1.6元