腾讯安全《2018 上半年区块链安全报告》

发表时间：2018-08-02

目录

序言

2018 年，是公认的区块链大年。与区块链有关的讨论不仅遍存在于中关村的创业咖啡，更是存在于街头巷尾、地铁公交、微博微信，几乎无处不在。然而，伴随着区块链技术的不断发展，区块链领域本身的安全问题逐渐凸显，与区块链相关的诈骗、传销等社会化安全问题日益突出。

随着区块链的经济价值不断升高，促使不法分子利用各种攻击手段获取更多敏感数据，“盗窃”、“勒索”、“挖矿”等，借着区块链概念和技术，使区块链安全形势变得更加复杂。据网络安全公司 Carbon Black 的调查数据显示，2018 年上半年，有价值约 11 亿美元的数字加密货币被盗，且在全球范围内因区块链安全事件损失金额还在不断攀升。

为了护航区块链产业健康发展，6 月 21 日“中国区块链安全高峰论坛”上，中国技术市场协会、腾讯安全、知道创宇、中国区块链应用研究中心等政府指导单位、网络安全企业、区块链相关机构及媒体等二十余家机构、单位联合发起“中国区块链安全联

盟”，联盟成立后着手建立区块链生态良性发展长效机制，着重打击一切假借区块链名义进行变相传销、诈骗等敛财行为。

区块链安全正受到越来越多的关注，除了广大用户特别关心的会不会踩雷“空气币”，腾讯安全联合实验室的关注点还在于围绕区块链，存在哪些安全风险，以及面对风险怎样才能避免出现重大损失。基于此，腾讯安全联合实验室联合知道创宇，梳理了2018年上半年围绕区块链爆发的典型安全事件，并给出防御措施，希望尽可能帮助用户避开区块链的“雷区”。

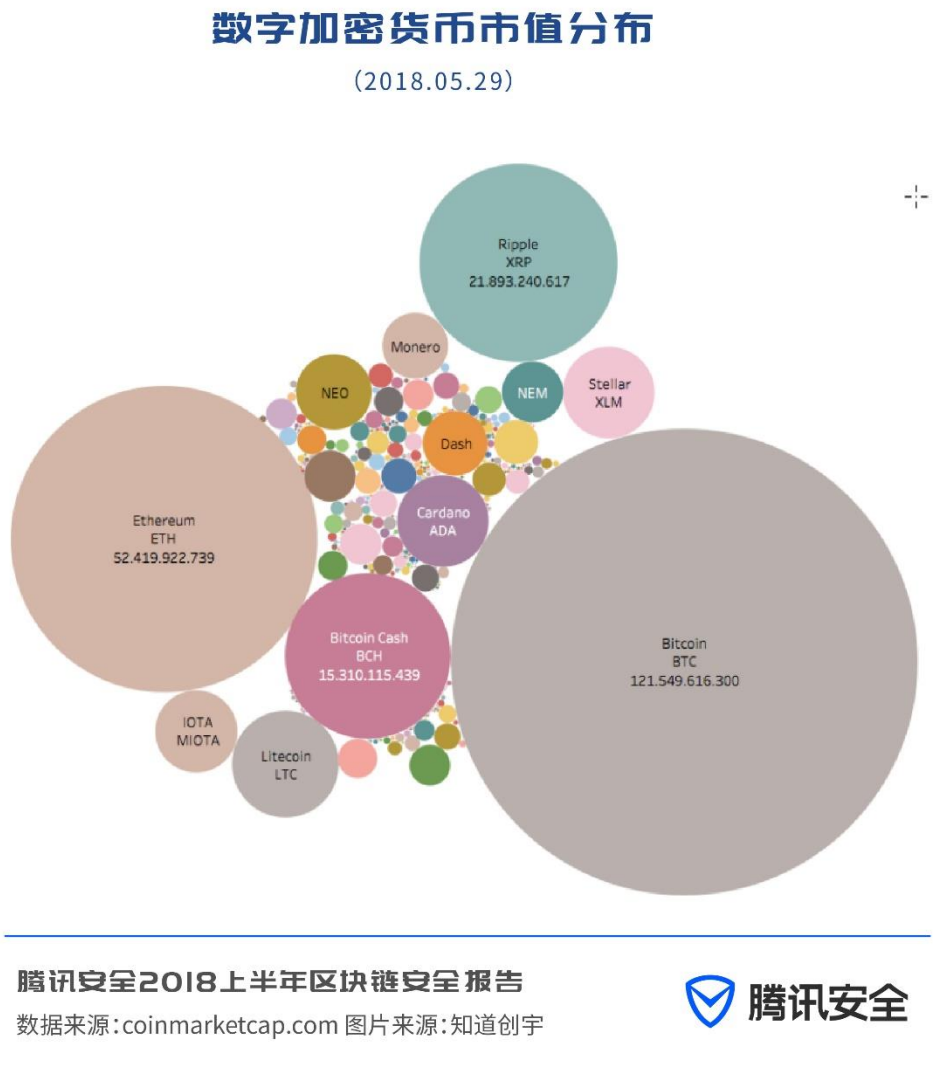
一、区块链安全事件频发，案值过亿屡见不鲜

1.数字加密货币撑起6000亿美元的市值

数字加密货币，是按照一定的数学算法，计算出来的一串符号。信仰者认为这串符号，代表一定的价值，可以像货币一样使用。因为其仅存在于计算机中，人们常称之为“数字加密货币”。

不同于由政府发行、并以政府信用做担保，用于商品流通交换的媒介——法币。数字加密货币，是由某个人或某个组织发行，通过一定算法，找到一串符号，然后宣称其是“XX币”。世界上首个数字加密货币由日本人中本聪发现，被他称作比特币。在比特币成功取得黑市交易硬通货的地位之后，引发了数字加密货币发行狂潮。至今，全球出现过的数字加密货币已超过1600种，是地球上国家总数的8倍多。

这1600多种数字虚拟币中，存在大量空气币，被认为一文不值。但这1600多种数字虚拟币，在高峰时期，却撑起了6000亿美元的市值。排名前十的加密数字货币，占总市场的90%，其中比特币、以太坊币分别占总市值的46.66%和20.12%。



关于 ICO

一家上市公司发行股票，需要向证券交易场所提交 IPO 申请，当一种虚拟数字货币需要上市发行时，会寻求数字虚拟币交易所申请 ICO。ICO 机构并不像 IPO 机构那样由各国政府机构依法建立，有强大的财经、政治实力做保障，ICO 组织均为民间自发形成的组织或联盟，类似自由市场。部分 ICO 机构的实际表现，实际上更接近于跨国诈骗组织。空气币在全球范围内满天飞，群雄四起的 ICO 机构功不可没。

2. 区块链安全事件爆发率逐年增加，案值增大

加密数字货币一经诞生，安全性就是人们关注的焦点，遗憾的是各类重大安全事件层出不穷。就比如下面这些惊人的案例：

2013 年 11 月，澳大利亚广播公司报道，当地一位 18 岁的青年称，自己运营的比特币银行被盗，损失 4100 个比特币；

2014 年 3 月，美国数字货币交易所 Poloniex 被盗，损失 12.3%的比特币；

2014 年 Mt.gox 盗币案——85 万枚，价值 120 亿美元；

2015 年 1 月，Bitstamp 交易所盗币案——1.9 万枚比特币，当时价值 510 万美元；

2015 年 2 月，黑客利用比特儿从冷钱包填充热钱包的瞬间，将比特儿交易平台冷钱包中的所有比特币盗走，总额为 7170 个比特币,价值 1 亿美元；

2016 年 1 月 1 日，Cryptsy 交易平台失窃 1.3 万比特币，价值 1.9 亿美元；

2016 年 8 月 1 日，全球知名比特币交易平台 Bitfinex 盗币案——约 12 万枚，价值 18 亿美元；

2017 年 3 月 1 日，韩国比特币交易所 yapizon 被盗 3831 枚比特币，相当于该平台总资产的 37%，价值 5700 万美元；

2017 年 6 月 1 日，韩国数字资产交易平台 Bithumb 被黑客入侵，受损账户损失数十亿韩元；

2017 年 7 月 1 日，BTC-e 交易所盗币案——6.6 万枚，价值 9.9 亿美元；

2017 年 11 月 22 日 Tether 宣布被黑客入侵，价值 3100 万美元的比特币被盗；

2017 年 11 月 23 日，Bitfinex 发生挤兑 3 万比特币瞬间被提走；

据美国财经网站 CNBC 报道，网络安全公司 Carbon Black 的调查数据显示，2018 年上半年，有价值约 11 亿美元的数字加密货币被盗。

二、区块链安全威胁分类

1.引发区块链数字加密货币三大安全问题

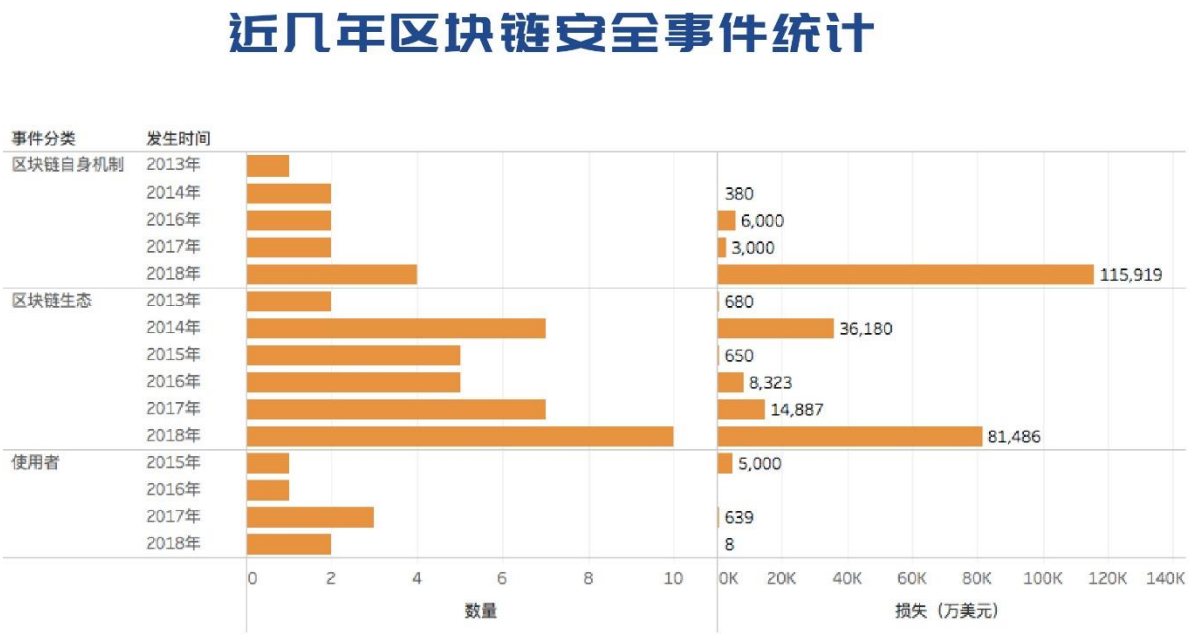
与数字加密货币有关的安全事件为何影响如此严重呢？产生安全风险的原因在哪儿？腾讯联合安全实验室和知道创宇公司认为：基于区块链加密数字货币引发的安全问题来源于区块链自身机制安全、生态安全和使用者安全三个方面。

发表时间：2018-08-02

目

上述三方面原因造成的经济损失分别是 12.5 亿、14.2 亿和 0.56 亿美元。

总的趋势是，随着数字虚拟货币参与者的增加，各种原因导致的安全事件也显著增加。



细分来观察：

区块链自身机制安全问题

——智能合约的问题

——理论上存在的 51%攻击已成现实

区块链生态安全问题

——交易所被盗（如前所述、触目惊心）

——交易所、矿池、网站被 DDoS

——钱包、矿池面临 DNS 劫持风险（劫持数字虚拟币交易钱包地址的病毒已层出不穷）

——交易所被钓鱼、内鬼、钱包被盗、各种信息泄露、账号被盗等

使用者安全问题

——个人管理的账号和钱包被盗

——被欺诈、被钓鱼、私钥管理不善，遭遇病毒木马等。

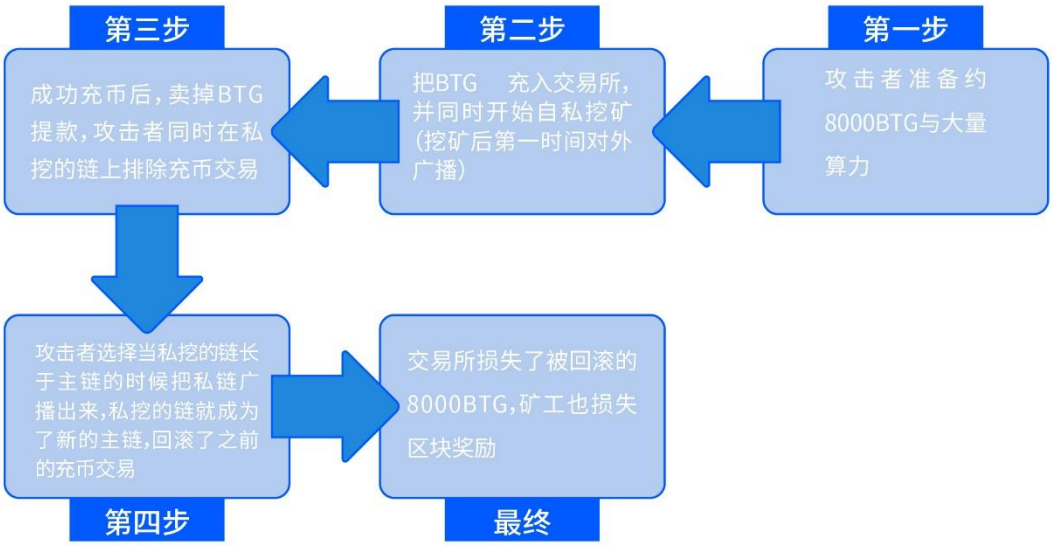
2. 区块链数字加密货币安全事件详解

2.1 因比特币自身机制而出现的安全事件

2018 年 5 月，比特币黄金（BTG）遭遇 51%双花攻击，损失 1860 万美元。

2017 年 10 月，比特币网络遭遇垃圾交易攻击，导致 10%以上的比特币节点下线。

51%双花攻击最为典型，所谓 51%攻击就是有人掌握了全网 51%以上的算力之后，就可以像赛跑一样，抢先完成一个更长的、伪造交易的链。比特币只认最长的链。所以伪造的交易也会得到所有节点的认可，假的也随之变成真的了；“双花”（Double Spending）从字面上看，就是一笔钱被花出去了两次。以 BTG 事件为例，就是黑客临时控制了区块链之后，不断地在交易所发起交易和撤销交易，将一定数量的 BTG 在多个钱包地址间来回转，一笔“钱”被花了多次，黑客的地址因此能得到额外的比特币。



腾讯安全2018上半年区块链安全报告

图片来源:知道创宇

腾讯安全

2.2 因区块链生态系统原因导致的安全事件

比如交易所面临的风险，被 DDoS 攻击的事件常有发生。还有交易所账户被黑客控制，攻击者控制交易行情，场外套利。

2018 年 3 月，号称世界第二大交易所的“币安”被黑客攻击，大量用户发现自己账户被盗。黑客将被盗账户中所持有的比特币全部卖出，高价买入 VIA（维尔币），致比特币大跌，VIA 暴涨 110 倍。

2.3 区块链使用者面临的风险

数字虚拟币钱包，要理解或完全掌握这些交易工具的使用有较高的门槛，要求使用者对计算机、对加密原理、对网络安全均有较高的认知。然而，许多数字虚拟币交易参与者并不具有这些能力,非常容易出现安全问题。

2017 年 7 月 1 日，中原油田某小区居民 188.31 个比特币被盗。油田警方几个月后将位于上海的窃贼戴某抓获，价值 280 万美元；

2017 年 10 月，东莞一名 imToken 用户发现 100 多个 ETH（以太坊币）被盗，最终确认是身边的朋友盗取他的数字加密货币。

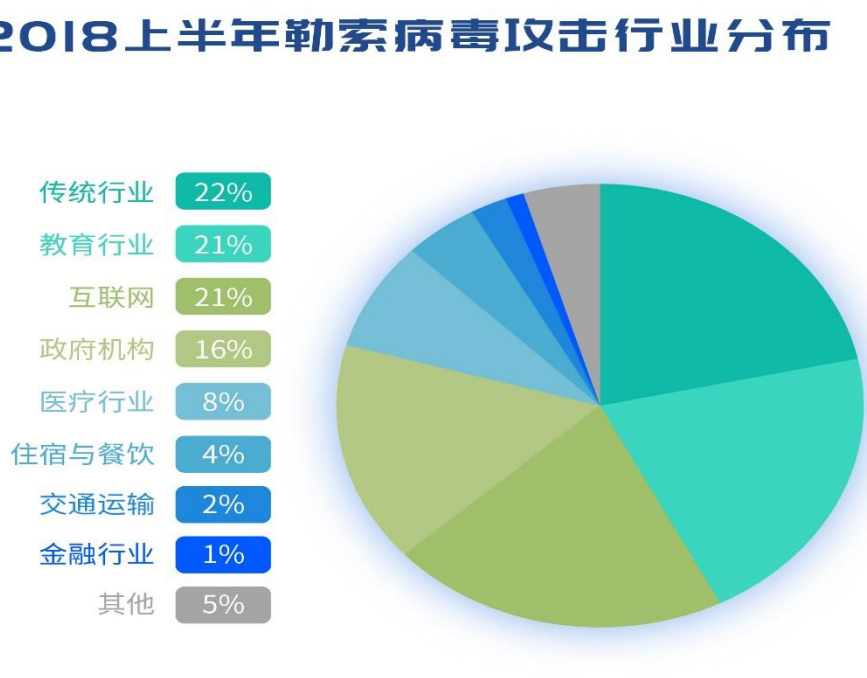
三、区块链数字货币“热”背后的三大网络安全威胁

1.数字货币勒索事件频发，基础设施成勒索病毒攻击重点目标

勒索病毒是 2018 年上半年危害互联网最严重的病毒之一。勒索病毒加密受害者电脑系统，并要求受害者向某些指定的比特币钱包转帐，其危害范围日益扩大，影响到事关国计民生的各个行业。

1.1 上半年勒索病毒攻击特征与三大勒索病毒家族

从受攻击行业分布上看，传统工业、互联网行业、教育行业和政府机构是受勒索病毒攻击的重灾区，医疗行业紧随其后。医疗由于其行业特殊性，一旦遭受到病毒攻击导致业务停摆，后果将不堪设想。

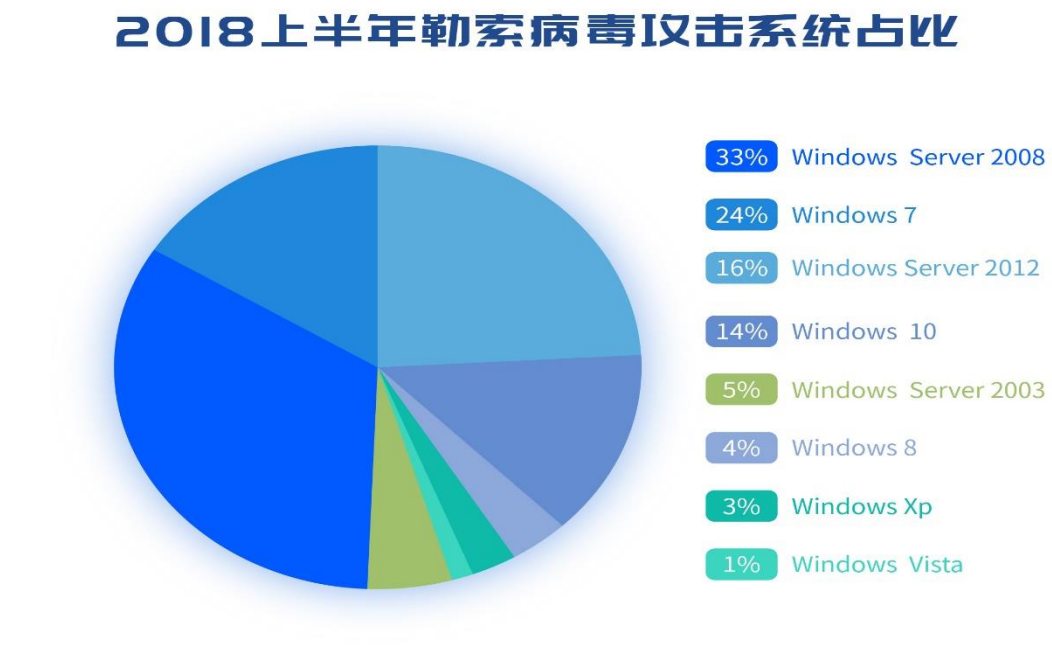


腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

观察 2018 上半年勒索病毒攻击系统占比可知，Windows Server 版本系统受攻击次数占比大于普通家用、办公系统。Windows Server 版本系统中 Windows Server 2008 版本系统受勒索病毒攻击占比最大，造成该现象的主要原因为企业服务器数据价值一般情况下要远远高于普通用户，中招后更加倾向于缴纳勒索赎金，这一特性进一步刺激了攻击者有针对性地对服务器系统的设备实施攻击行为。

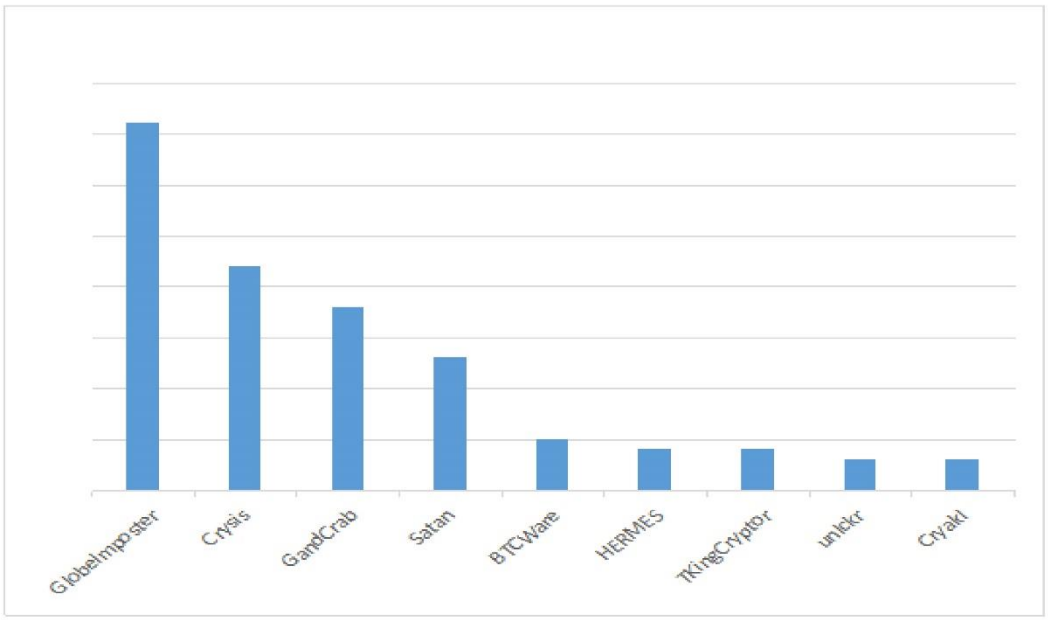


腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

2018 上半年以 GlobeImposter，Crysis，GandCrab 为首的 3 大勒索家族展开的攻击活动占据了网络勒索事件的绝大部分。此外，Satan 家族在 2018 上半年时段展开的攻击也有明显上升，其它老牌家族依然有不同程度的活跃。



腾讯安全2018上半年区块链安全报告

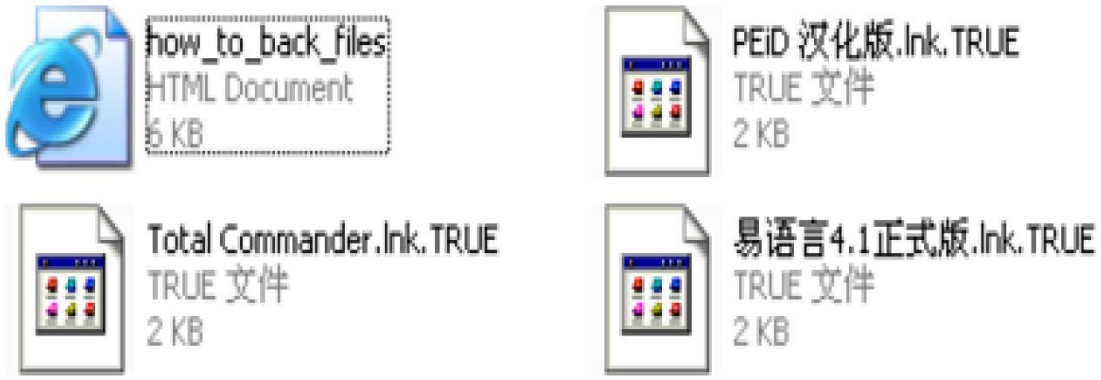
图片来源:腾讯御见威胁情报中心

腾讯安全

Top1：GlobeImposter 勒索病毒家族

2018 年 2 月，春节过后不久，包括医疗行业在内的多家国内公共机构的服务器就遭到最新的 GlobeImposter 家族勒索病毒变种的攻击，黑客在突破企业防护边界后释放并运行勒索病毒，加密破坏数据库文件，最终导致系统被破坏，正常工作秩序受影响。

该勒索病毒变种将加密后的文件重命名为.GOTHAM、.Techno、.DOC、.CHAK、.FREEMAN、.TRUE、.TECHNO 等扩展名，并通过邮件来告知受害者付款方式，使其获利更加容易方便。



腾讯安全2018上半年区块链安全报告

图片来源:网络

腾讯安全

Top2：Crysis 勒索病毒家族

Crysis 家族最早可以追溯到 2016 年 3 月，进入 2017 年后开始针对 windows 服务器发起持续攻击。Crysis 勒索病毒家族的攻击模式主要为黑客通过爆破远程登录后，手动传播勒索病毒并执行。

Crysis 勒索病毒在 2017 年 5 月万能密钥被公布之后，消失了一段时间，但在 2018 上半年中新的变种依然比较活跃。Crysis 家族变种也有多种，较为流行的加密后缀多为.arena、.arrow 等，并且附加上的后缀中还会带有受害者 id 和勒索者联系邮箱，如 1.txt.id-EE5106A8.[decrypthelp@qq.com].arrow。赎金金额需要受害者自行联系黑客方可获知。

版本	V1	V2	V3	V4
出现时间	2018年1月	2018年3月5日	2018年5月3日	2018年7月5日
传播方式	Seamless恶意广告软件和RIG、GrandSoft漏洞利用工具包	邮件传播	邮件传播	邮件传播，软件供应链传播
勒索货币	达世币	达世币	没有明确指明	达世币或比特币
文件后缀	.GDCB	.CRAB	.CRAB	.KRAB
特点	1. 1.5个达世币，约合1200美元。 2. 已有解密工具可解密部分加密文件	1.0.72达世币，约合400美元 2.使用CC地址 malwarehunterteam.bit挑衅安全分析人员 3.二维码获取付款地址	1.替换桌面背景 2. 运行后会强制关机，同时添加开机启动项 3.没有明确指出勒索金额、勒索货币等。 4.取消了二维码功能	1.勒索文档要求使用Tor工具进一步获得勒索信息。 2.要求指定时间内支付998美元的数字币赎金，过期翻倍。 3.要求使用达世币或比特币交易

腾讯安全2018上半年区块链安全报告

图片来源:腾讯安全反病毒实验室

腾讯安全

Top3：GandCrab 勒索病毒家族

GandCrab 勒索病毒家族堪称 2018 年勒索病毒界的“新星”，自 1 月腾讯御见威胁情报中心捕获到首次盯上达世币的勒索病毒 GrandCrab 起，短短几个月的时间，GrandCrab 历经四大版本更迭。

第一版本的 GandCrab 勒索病毒因 C&C 被海外安全公司与警方合作后控制而登上各大科技媒体头条，两个月后 GandCrab V2 版本勒索病毒出现，勒索软件作者为了报复安全公司与警方控制了其 V1 版本的 C&C 服务器，在 V2 版本中直接使用了带有安全公司与警方相关的字符做为其 V2 版本的 C&C 服务器，因而又一次登上科技新闻版面。

两个月后的 GandCrab V3 版本结合了 V1 版本与 V2 版本的代码隐藏技术，更加隐蔽。GandCrab V3 勒索病毒使用 CVE-2017-8570 漏洞进行传播，漏洞触发后会释放包含“안녕하세요”（韩语“你好”）字样的诱饵文档。与以往版本的该家族的勒索病毒相比，该版本并没有直接指明赎金金额，而是要求用户使用 Tor 网络或者 Jabber 即时通讯软件与勒索者联系。

GandCrab V4 版本为该家族系列病毒中目前最新迭代版本，相比较以往的版本，V4 版本文件加密后缀有了进一步变化（.KRAB），传播渠道上也有了进一步的扩展，病毒通过软件供应链劫持，破解软件打包病毒文件，进一步传播到受害者机器实施勒索攻击。

此外，4 月 3 号发现“魔鬼”撒旦（Satan）勒索病毒携“永恒之蓝”漏洞卷土重来，变种不断出现，对企业用户威胁极大。该病毒会加密中毒电脑的数据库文件、备份文件和压缩文件，再用中英韩三国语言向企业勒索 0.3 个比特币，该病毒的最新变种除了依赖“永恒之蓝”漏洞在局域网内攻击传播，还会利用多个新漏洞攻击，包括 JBoss 反序列化漏洞（CVE-2017-12149）、JBoss 默认配置漏洞(CVE-2010-0738)、Tomcat 漏洞（CVE-2017-12615）、Tomcat web 管理后台弱口令爆破、Weblogic WLS 组件漏洞（CVE-2017-10271）等等。

1.2 下半年勒索病毒的传播趋势

（1）勒索病毒与安全软件的对抗加剧

随着安全软件对勒索病毒的解决方案成熟完善，勒索病毒更加难以成功入侵用户电脑，病毒传播者会不断升级对抗技术方案。

（2）勒索病毒传播场景多样化

传统的勒索病毒传播主要以钓鱼邮件为主，勒索病毒更多利用了高危漏洞（如永恒之蓝）、鱼叉游戏攻击，或水坑攻击等方式传播，大大提高了入侵成功率。以 GandCrab 为例，该家族勒索病毒传播同时利用了钓鱼邮件、水坑攻击、网页挂马和漏洞利用四种方式。

（3）勒索病毒攻击目标转向企业用户

个人电脑大多能够使用安全软件完成漏洞修补，在遭遇勒索病毒攻击时，个人用户往往会放弃数据，恢复系统。而企业用户在没有及时备份的情况下，会倾向于支付赎金，挽回数据。因此，已发现越来越多攻击目标是政府机关、企业、医院、学校。

（4）勒索病毒更新迭代加快

以 GandCrab 为例，当第一代的后台被安全公司入侵之后，随后在一周内便发布了 GandCrab2，现在已升级到 3.0 版本。病毒早期发布时存在漏洞，使得安全公司可以解密被加密的文件，随后更新的版本已无法被解密。

（5）勒索赎金提高

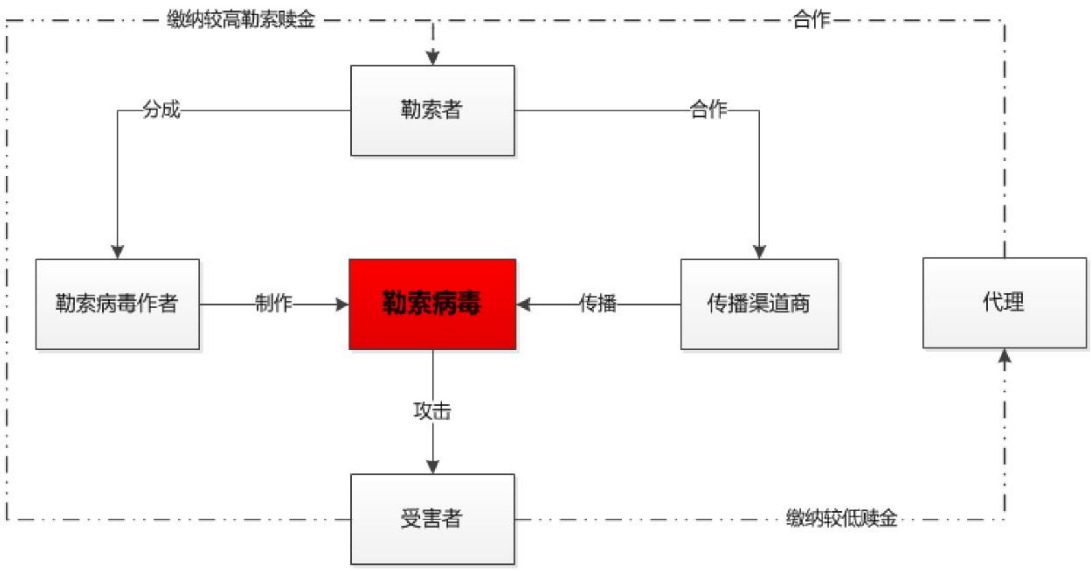
随着用户安全意识提高、安全软件防御能力提升，勒索病毒入侵成本越来越高，赎金也有可能随之提高。上半年某例公司被勒索病毒入侵后，竟被勒索 9.5 个比特币。如今勒索病毒的攻击目标也更加明确，或许接下来在赎金上勒索者会趁火打劫，提高勒索赎金。

（6）勒索病毒加密对象升级

传统的勒索病毒加密目标基本以文件文档为主，现在越来越多的勒索病毒会尝试加密数据库文件，加密磁盘备份文件，甚至加密磁盘引导区。一旦加密后用户将无法访问系统，相对加密而言危害更大，也有可能迫使用户支付赎金。

（7）勒索病毒黑色产业链形成

随着勒索病毒的不断涌现，腾讯御见威胁情报中心甚至观察到一类特殊的产业诞生：勒索代理业务。当企业遭遇勒索病毒攻击，关键业务数据被加密，而理论上根本无法解密时，而勒索代理机构，承接了受害者和攻击者之间谈判交易恢复数据的业务。



腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

2.挖矿木马“异军突起”，成币圈价值“风向标”

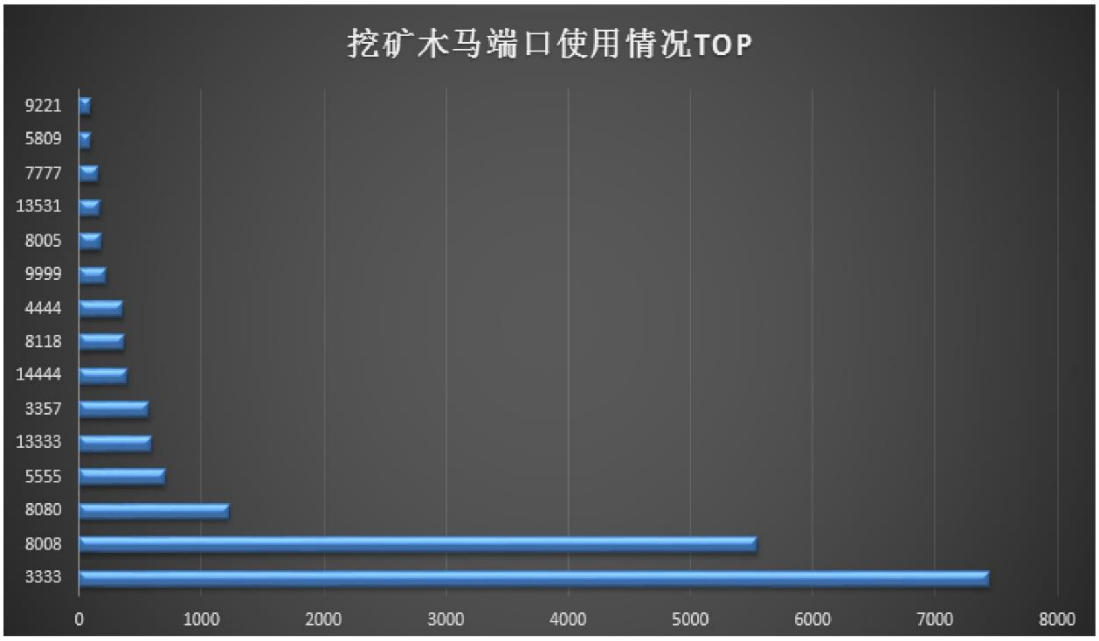
挖矿病毒发展成为 2018 年传播最广的网络病毒，且挖矿热度往往与币种价格成正比。由于挖矿病毒的控制者可以直接通过出售挖到的数字虚拟货币牟利，挖矿病毒的影响力空前高涨，已经完全取代几年前针对游戏玩家的盗号木马、针对网购用户的交易劫持木马、甚至是用于偷窥受害者家摄像头的远程控制木马。

当受害者电脑运行挖矿病毒时，计算机 CPU、GPU 资源占用会上升，电脑因此变得卡慢，如果是笔记本电脑，会更容易观察到异常：比如电脑发烫、风扇转速增加，电脑噪声因此增加，电脑运行速度也因此变慢。挖矿年年有，但进入 2018 年以来，PC 端挖矿木马以前所未有的速度增长，仅上半年爆出挖矿木马事件 45 起，比 2017 年整年爆出的挖矿木马事件都要多。

2.1 上半年挖矿木马样本分析与传播特征

腾讯御见威胁情报中心对数十万挖矿病毒样本进行归类，对挖矿木马使用的端口号、进程名、矿池地址进行了总结。

挖矿木马最偏爱的端口号是 3333，其次是 8008、8080、5555 等端口。



腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

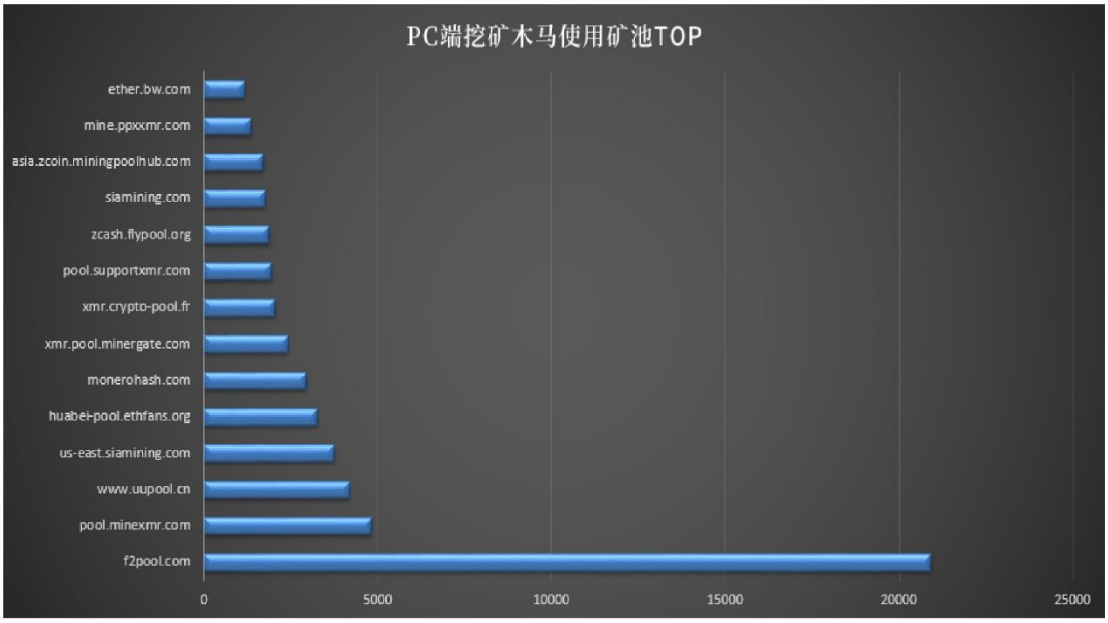
木马最爱的借用的进程名是 svchost.exe 以及 csrss.exe，这两个名字原本属于 windows 系统进程，现被挖矿木马利用来命名以迷惑用户。

腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

矿池就是一个开放的、全自动的挖矿平台，目前挖矿木马主要通过连接矿池挖矿，矿工将自己的矿机接入矿池，贡献自己的算力共同挖矿，共享收益。上半年 PC 端僵尸网络挖矿应用最广泛的矿池为 f2pool。



腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

与以往挖矿木马相比，2018 上半年挖矿木马出现新的传播特征：

（1）瞄准游戏高配机，高效率挖矿

辅助外挂是 2018 上半年挖矿木马最喜爱的藏身软件之一。由于游戏用户对电脑性能要求较高，不法分子瞄准游戏玩家电脑，相当于找到了性能“绝佳”的挖矿机器。

2018 年 1 月，腾讯电脑管家曝光 tlMiner 挖矿木马隐藏在《绝地求生》辅助程序中进行传播，单日影响机器量最高可达 20 万台。随即在 3 月份配合腾讯守护者计划安全团队，协助山东警方快速打击木马作者，并在 4 月初打掉这个链条顶端的黑产公司。据统计，该团伙合计挖掘 DGB（极特币）、HSR（红烧肉币）、XMR（门罗币）、SHR（超级现金）、BCD（比特币钻石）等各种数字加密货币超过 2000 万枚，非法获利逾千万。

2018 年 2 月，腾讯电脑管家发现一款门罗币挖矿木马藏身在上百款《荒野行动》辅助二次打包程序中传播，并在 2 月中下旬通过社交群、网盘等渠道传播，出现明显上涨趋势。

2018 年 5 月，腾讯御见威胁情报中心感知到一款名为“520Miner”的挖矿木马通过游戏外挂传播，控制数千台机器挖了好几天的矿，最终收获 67 枚 VIT 币，总价值不到一毛钱人民币，可以说是史上最能穷折腾的挖矿木马。

（2）利用网页挂马，大范围传播

挖矿木马的传播渠道不限于通过伪装成电脑软件下载，还普遍采用了网页挂马这种最高效率的传播方式。

2018年4月12日,腾讯御见威胁情报中心监测到国内一起大规模的网页挂马事件。当天包括多款知名播放器软件、视频网站客户端、常见的工具软件在内的 50 余款用户量千万级别的电脑软件遭遇大规模网页挂马攻击。

攻击者将攻击代码通过某广告联盟的系统主动分发带毒页面，而这个带毒页面被内嵌在 50 余款千万级别用户群的常用软件中，这些用户的电脑一开机会主动连网下载广告资源，电脑会因此下载若干个病毒，其中就包括挖矿病毒。腾讯电脑管家当天拦截超过 20 万次病毒下载。

此外，腾讯御见威胁情报中心还监测到一款挖矿病毒感染量异常增高，经病毒溯源分析发现，受害者电脑上的挖矿木马均来自某些打着“人体艺术”旗号的色情网站。

当网民浏览这些网站时，由于部分系统存在 Flash 高危安全漏洞，打开网页会立刻中毒。之后，受害者电脑便会运行挖矿代码，电脑沦为一名矿工。攻击者会控制大量矿工电脑集中算力挖矿，并以此牟利。

（3）入侵控制企业服务器，组建僵尸网络云上挖矿

随着各种数字加密货币的挖矿难度越来越大，通过普通用户的个人电脑难以实现利益最大化。而实施短时间内的大范围挖矿，除了网页挂马，最普遍的作法就是控制肉鸡电脑组建僵尸网络挖矿。服务器性能强、24 小时在线的特征，吸引更多不法矿工将攻击目标转向企业、政府机构、事业单位的服务器实现云上挖矿。

腾讯御见威胁情报中心曾发现一个感染量惊人的“PhotoMiner 木马”，通过入侵感染 FTP 服务器和 SMB 服务器暴力破解来扩大传播范围。查询木马控制的门罗币钱包地址，发现该木马控制肉鸡电脑挖到 8 万枚门罗币，挖矿累计收益达到惊人的 8900 万人民币，是名副其实的“黄金矿工”。

腾讯安全云鼎实验室通过对 DNS 请求的矿池地址进行统计和归类，发现云上挖矿币种主要是 XMR（门罗币）、以太币（ETH）和 ETN（以利币）。对云主机服务器上挖矿木马最常连接的矿池地址进行了统计，发现 xmr.pool.minergate.com 使用频率最高。

云主机服务器上挖矿木马最常连接的矿池		
矿池地址	影响值	算力
xmr.pool.minergate.com	234	26.5MH/s
pool.minexmr.com	231	103MH/s
fee.xmrig.com	192	/
xmr.crypto-pool.fr	102	1.72MH/s
xmr.xmr5b.ru	57	/
pool.supportxmr.com	50	78MH/s
donate.xmrig.com	44	/
donate.xmr-stak.net	41	/
xmr.f2pool.com	33	30MH/s
xmr-eu1.nanopool.org	32	96MH/s
xmr.kiss58.org	24	/
xmr-eu2.nanopool.org	21	96MH/s
pool.monero.hashvault.pro	21	10MH/s
xmr.yiluzhuanqian.com	14	/

其中部分在国内流行的挖矿木马使用了自建矿池的方式进行挖矿，这主要是出于使用第三方矿池，第三方矿池会收取一定的手续费，而使用自建矿池的方式可以减少这些不必要的费用支出。

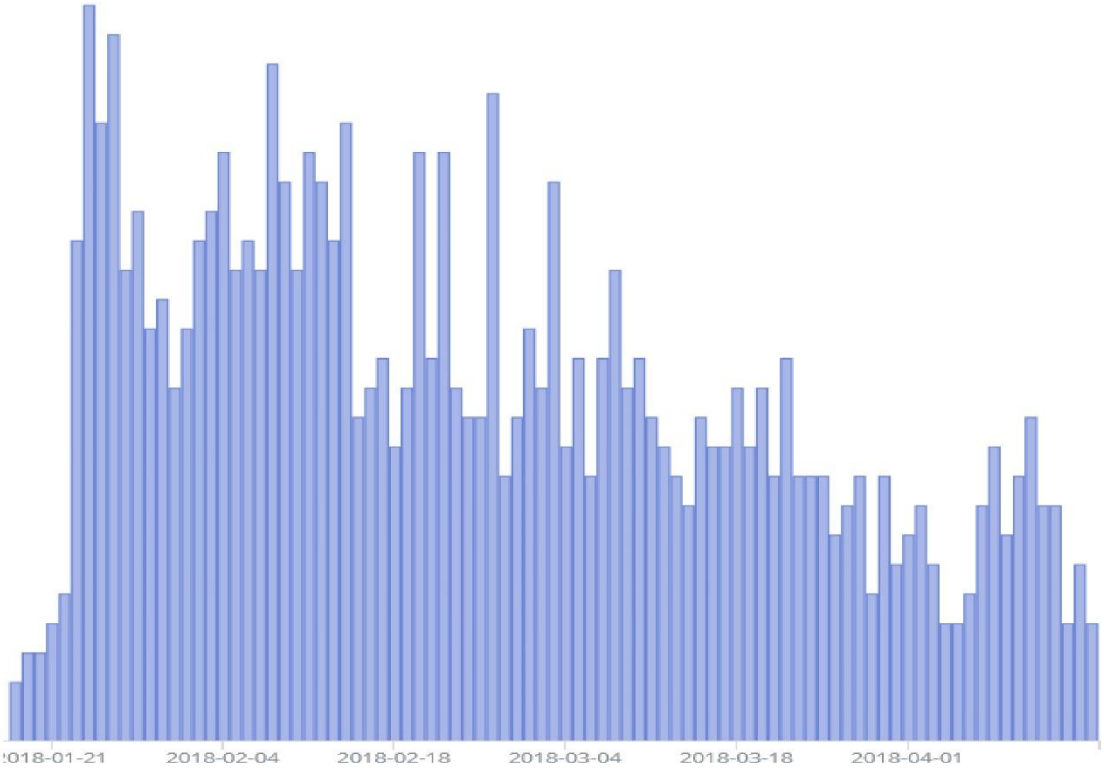
通过对数字货币的价格走势和挖矿热度进行关联分析，发现挖矿的热度与币种价格成正比关系。这也再次验证，网络黑产的目标就是追求利益的最大化。观察 ETN（以利币）的价格走势，我们可以发现从其从 1 月中旬开始呈下降趋势：

腾讯安全2018上半年区块链安全报告

图片来源:网络

腾讯安全

而观察其对应矿池的访问，发现也是下降趋势：

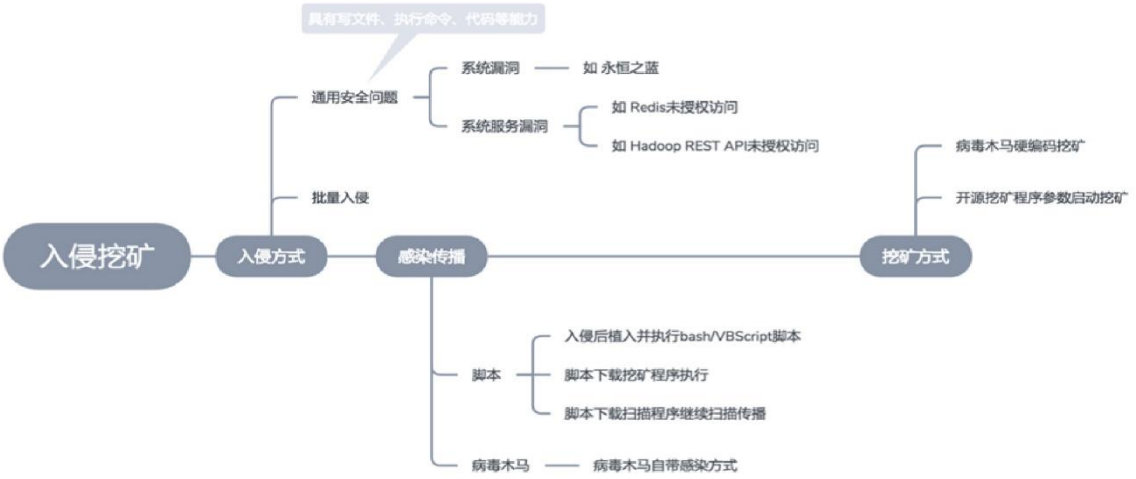


腾讯安全2018上半年区块链安全报告

图片来源:腾讯安全云鼎实验室

腾讯安全

通过对历史捕获挖矿案例的分析，云上挖矿通常是一种批量入侵方式，而由于其批量入侵的特性，所以利用的也只能是通用安全问题，比如系统漏洞、服务漏洞，而最常见的是永恒之蓝、Redis 未授权访问问题、Apache Struts 2 漏洞导致企业 Web 服务器被批量入侵。



腾讯安全2018上半年区块链安全报告

图片来源:腾讯安全云鼎实验室

腾讯安全

攻击者还擅长使用挖矿木马生成器、弱口令攻击字典等攻击工具入侵服务器，再大量扩散挖矿木马。

腾讯安全2018上半年区块链安全报告

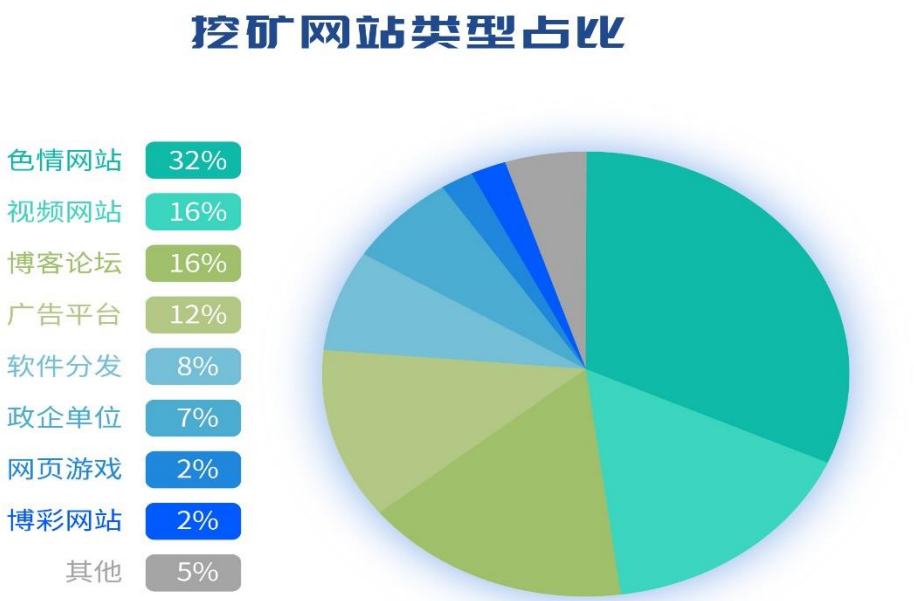
图片来源：网络

腾讯安全

（4）网页挖矿：在正常网址插入挖矿代码

由于杀毒软件的存在，许多挖矿木马文件一落地到用户电脑就可能被拦截，不利于扩大挖矿规模，更多攻击者倾向实施网页挖矿：通过入侵存在安全漏洞的网站，在网页中植入挖矿代码。访客电脑只要浏览器访问到这个网页，就会沦为矿工。

在挖矿的网站类型中，色情网站占比最高，其次是视频网站和博客、论坛。用户在此类网站观看视频、阅读文章，停留时间较长，黑客利用这些网站进行挖矿，可以获取较高的收益。

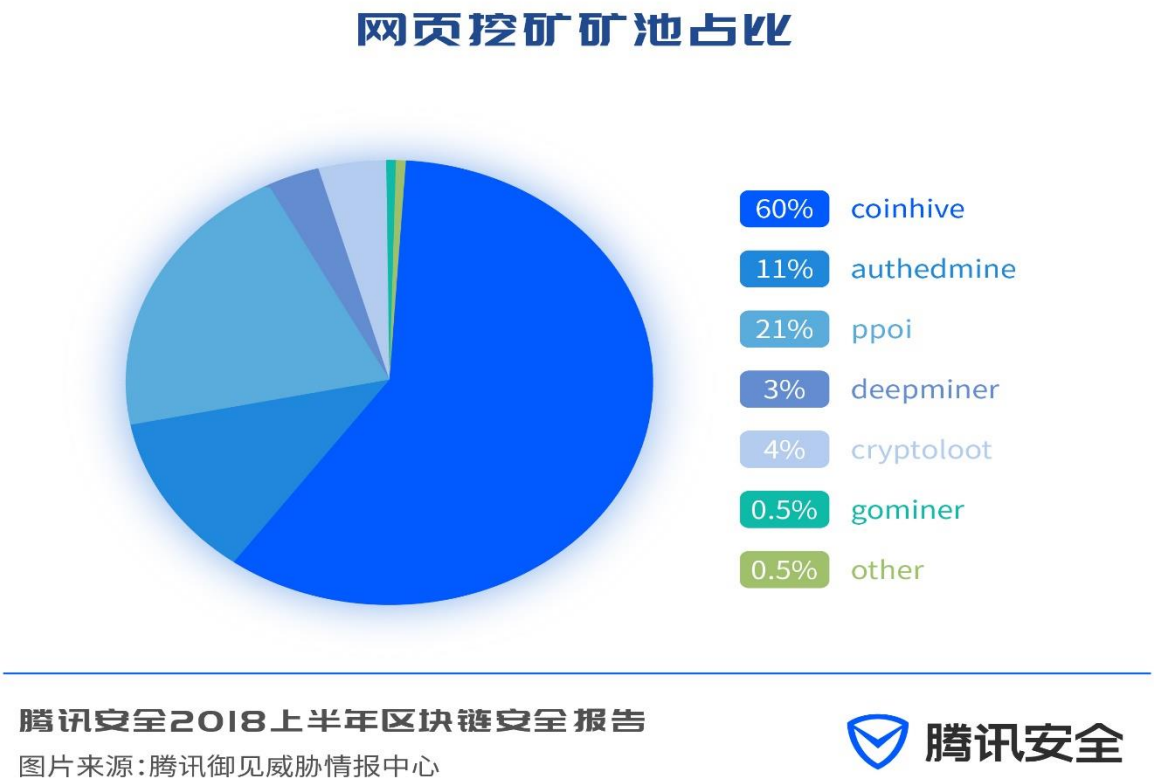


腾讯安全2018上半年区块链安全报告

图片来源:腾讯御见威胁情报中心

腾讯安全

在矿池方面最早出现的 coinhive 矿池占据网页挖矿中的最大比例，与 coinhive 同一平台的 authemine 矿池占 11%；基于 coinhive 建立的 ppoi 矿池和 cryptoloot 矿池分别占比 21%、4%。



2.2 下半年挖矿木马的传播趋势

数字加密货币在 2018 年上半年持续暴跌，比特币已从去年年底的 2 万美元，跌至现在不足 7000 美元，“炒币”热似在降温，但这并没有影响挖矿木马前进的脚步，毕竟挖矿木马是靠肉鸡挖矿赚钱，勿需投入物理设备，而从最近爆出的挖矿木马事件中发现，挖矿木马可选择的币种越来越多，设计越来越复杂，隐藏也越来越深，下半年的挖矿将会持续活跃，与杀毒软件的对抗会愈演愈烈。

（1）全能型挖矿木马产生，同时带来多种危害

PC 病毒的名字通常包含了病毒的来源、传播路径、目的等信息，如“Trojan.StartPage”代表这是一类锁主页木马，“Backdoor.GrayBird”属于灰鸽子后门病毒，如今在杀软的强力打击之下，病毒木马“栖息地”越来越少，拓展“业务”已成为众多病毒木马的首要任务，挖矿木马也不例外。

上半年出现的“Arkei Stealer”木马，集窃密、远控、DDoS、挖矿、盗币于一体，可谓木马界“全能”。下半年的挖矿木马或将集成更多的“业务”，通过各种渠道入侵至用户机器。

（2）隐藏技术更强，与安全软件对抗愈加激烈

病毒发展至今，PC 机上隐藏技术最强的无疑是 B/Rootkit 类病毒，这类木马编写复杂，各模块设计精密，可直接感染磁盘引导区或系统内核，其权限视角与杀软平行，属于比较难清除的一类病毒。

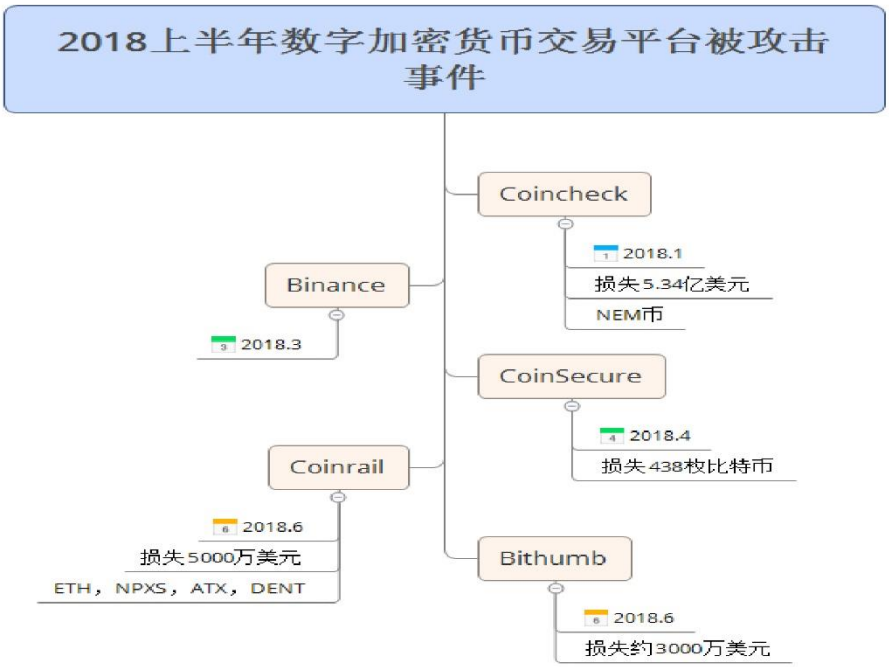
此类病毒常用于锁主页及勒索，而近期发现 R/Bookit 技术也被应用于挖矿木马中，使挖矿木马的隐藏技能提升几个档次。下半年数字加密货币安全形势依然严峻，挖矿木马的隐藏对抗或将更加激烈。

3. 数字劫匪“铤而走险”攻击交易所，半年获利约 7 亿美元

除了勒索病毒造成的损失，盗窃行为也同样可对数字加密货币持有者造成大量损失，从数字加密货币诞生初期，数字加密货币被盗的新闻就层出不穷。目前盗取数字加密货币的方式大致 4 种：入侵交易所，入侵个人用户，“双花攻击”，漏洞攻击。

3.1 数字加密货币交易平台被攻击

数字加密货币交易所被攻击，仅 2018 年上半年就损失了约 7 亿美元。



图片来源：腾讯御见威胁情报中心

（1）2018 年 1 月日本最大的数字加密货币交易所 Coincheck 被盗走价值 5.34 亿美元的 NEM（新经币）；

（2）2018 年 3 月 7 日，Binance 交易锁被入侵，此次为大规则通过钓鱼获取用户账号并试图盗币事件；

（3）2018 年 4 月 13 日，印度数字加密货币交易所 CoinSecure 被 438 枚比特币，疑为内部人员监守自盗；

（4）2018 年 6 月 10 日，韩国数字加密货币交易所 Coinrail 被攻击，损失超过 5000 万美元；

（5）2018 年 6 月 20，韩国数字加密货币交易所 Bithumb 被黑客攻击，价值 3000 万美元的数字加密货币被盗，这是 Bithumb 第三次被黑客攻击了。

3.2 个人账号遭入侵

（1）通过植入病毒木马窃取钱包文件

2018 年 2 月腾讯电脑管家发现大量利用 Office 公式编辑器组件漏洞（CVE-2017-11882）的攻击样本，通过下载并运行已被公开源码的 Pony 木马，窃取用户比特币钱包文件等敏感信息。

2018 年 3 月，一款基于剪切板劫持的盗币木马在国内出现，该木马使用易语言编写，通过激活工具、下载站到达用户机器，木马会监视用户剪切板，一旦发现有钱包地址，则替换为木马的钱包地址，木马内置 30 多个钱包地址，且部分钱包已经有盗取记录。

此外，腾讯御见威胁情报中心分析发现，越来越多的病毒会尝试劫持数字加密币交易钱包地址，当受害者在中毒电脑上操作数字加密货币转帐交易时，病毒会迅速将收款钱包地址替换为病毒指定的地址，病毒行为就如同现实中的劫匪。类似病毒在电脑网购普及时也曾经出现，病毒在交易完成的一瞬间，将受害者资金转入自己指定的交易账户。

（2）内部盗取加密货币

2018 年 3 月份，北京某互联网攻击员工利用职务便利，在公司服务器部署恶意代码，盗取该公司 100 个比特币，目前已经被依法逮捕，这是北京首例比特币盗窃案。

3.3“双花攻击”

“双花攻击”是控制某数字加密货币网络 51%算力之后，对数字加密货币区块链进行攻击，可实现对已经交易完成的数据进行销毁，并重新支付，这样就可获得双倍服务。

2018 年 5 月，BTG（比特黄金）交易链被黑客攻击，黑客向交易所充值后迅速提币，并销毁提币记录，共转走了 38.8 万枚 BTG，获利 1.2 亿人民币。

3.4 漏洞攻击

2018 年 4 月，BEC 智能合约中被爆出数据溢出漏洞，攻击者共盗取 579 亿枚 BEC 币，随后 SMT 币也被爆出类似漏洞。

四、安全建议

区块链技术，仍是众多互联网公司乃至国有银行系统重点研究的领域。区块链的应用并不等同于数字虚拟货币，安全专家并不鼓励人们炒币，在此对炒币行为不做赘述。

对于区块链安全来讲，从系统架构上，建议相关企业与专业区块链安全研究组织合作，及时发现、修复系统漏洞，避免导致严重的大规模资金被盗事件发生；

对于参与数字虚拟币交易的网民来讲，应充分了解可能存在的风险，在电脑端、手机端使用安全软件，避免掉进网络钓鱼陷阱，避免数字虚拟币钱包被盗事件发生；

对于普通网民而言，应防止电脑中毒成为被人控制的“矿工”，谨慎使用游戏外挂、破解软件、视频网站客户端破解工具，这些软件被人为植入恶意程序的概率较大。同时，安装正规杀毒软件并及时更新升级，当电脑卡顿、温度过热时，使用腾讯电脑管家进行检查，防止电脑被非法控制，造成不必要的损失；

对于企业网站、服务器资源的管理者，应部署企业级网络安全防护系统，防止企业服务器被入侵安装挖矿病毒，防止受到勒索病毒侵害。企业网站应防止被黑，及时修补服务器操作系统、应用系统的安全漏洞，避免企业服务器沦为黑客挖矿的工具，同时也避免因服务器被入侵而导致企业网站的访客电脑沦为“矿工”。