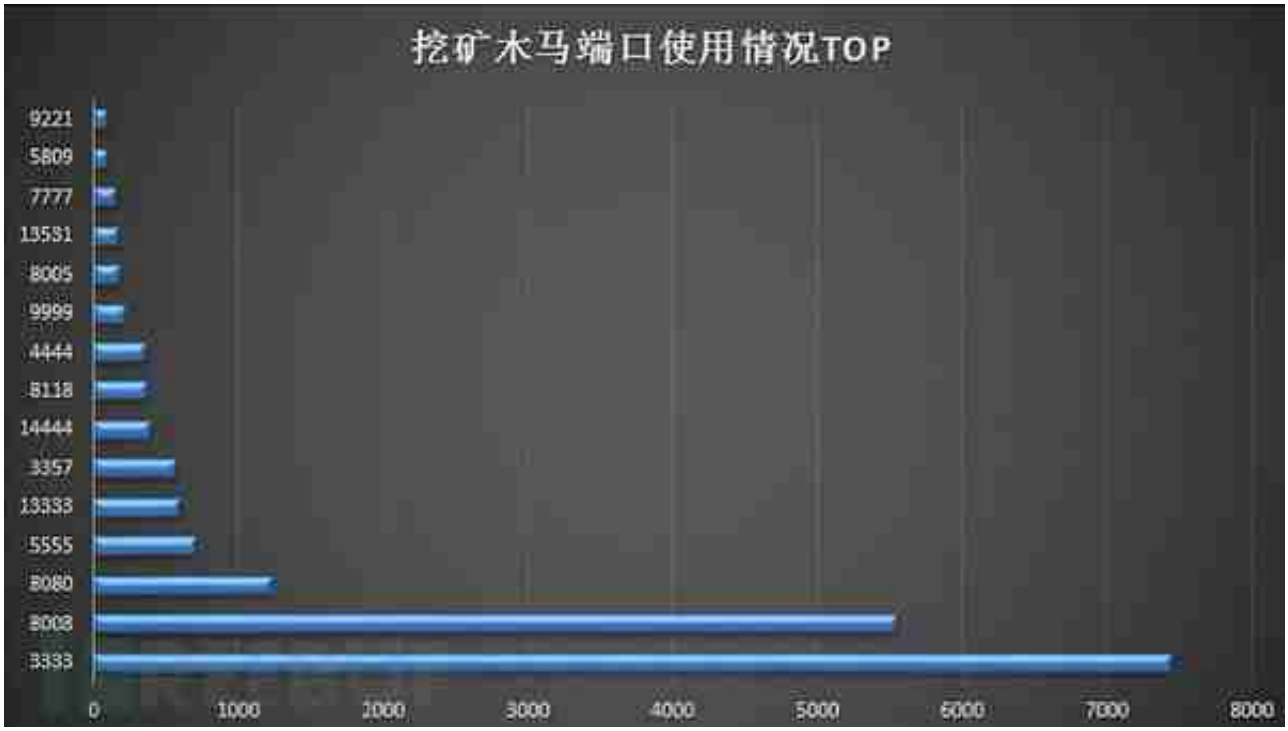
一、概述

根据腾讯御见威胁情报中心监测数据，2018年挖矿木马样本月产生数量在百万级别，且上半年呈现快速增长趋势，下半年上涨趋势有所减缓。由于挖矿的收益可以通过数字加密货币系统结算，使黑色产业变现链条十分方便快捷，少了中间商（洗钱团伙）赚差价。数字加密币交易系统的匿名性，给执法部门的查处工作带来极大难度。

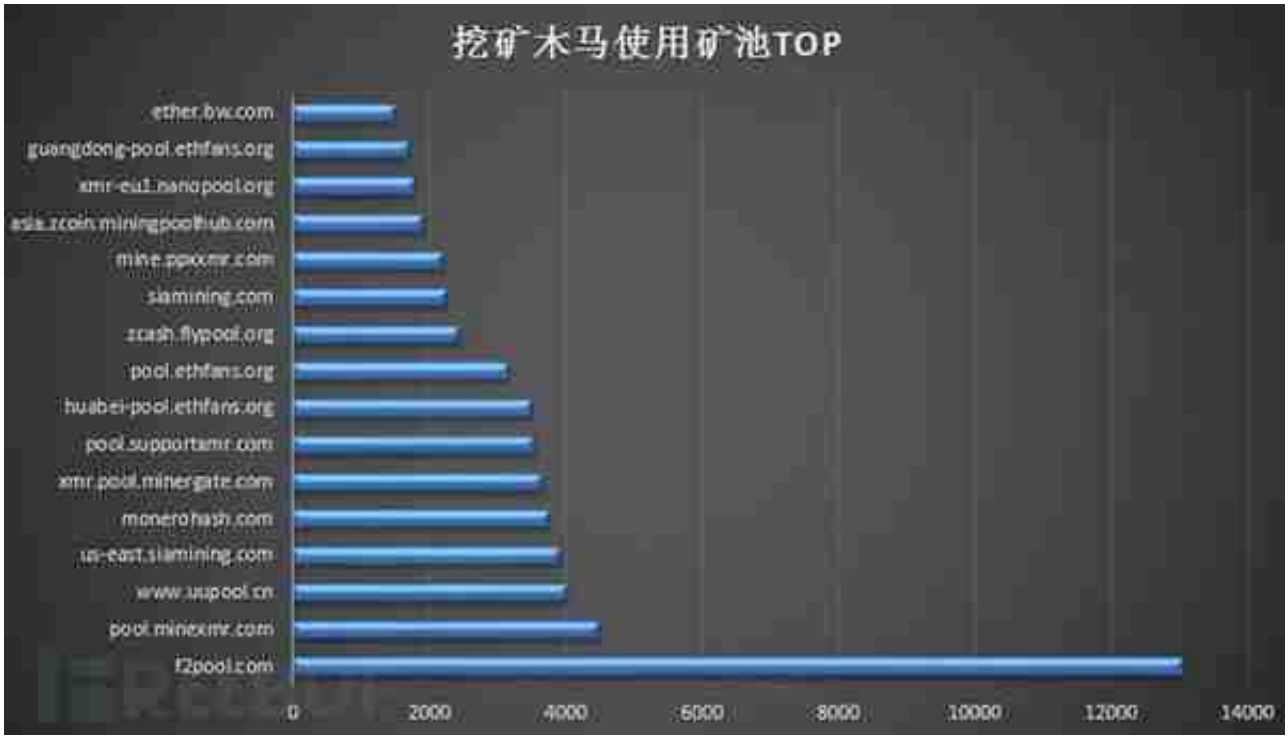
在过去的2018年，挖矿病毒的流行程度已远超游戏盗号木马、远程控制木马、网络劫持木马、感染型病毒等等传统病毒。以比特币为代表的虚拟加密币经历了过山车行情，许多矿场倒闭，矿机跌落到轮斤卖的地步。但即使币值已大幅下跌，挖矿木马也未见减少。因为控制他人的肉鸡电脑挖矿，成本为零。

当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。但是也有挖矿木马故意控制挖矿时占用的CPU资源在一定范围内，并且设置为检测到任务管理器时，将自身退出的特性，以此来减少被用户发现的几率。

根据腾讯御见威胁情报中心监测数据，2018年挖矿木马样本月产生数量在百万级别，且全年呈现增长趋势。



挖矿木马喜欢将自身进程名命名为系统进程来迷惑用户，除了部分挖矿进程直接使用xxxminer外，最常使用的进程名为windows系统进程名：svchost.exe以及csrss.exe。



二、2018年挖矿木马传播特点

1．瞄准游戏高配机，高效率挖矿

辅助外挂是2018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。

案例1：tlMiner挖矿木马利用《绝地求生》玩家的高配置机器，搭建挖矿集群

2017年年底腾讯电脑管家发现一款名为“tlMiner”的挖矿木马，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。经溯源分析发现，该木马在2017年12月8号辅助新版发布后开始植入辅助工具，其间有过停用，但巨大的利益驱使不法分子在12月25号重新开放辅助及挖矿功能。

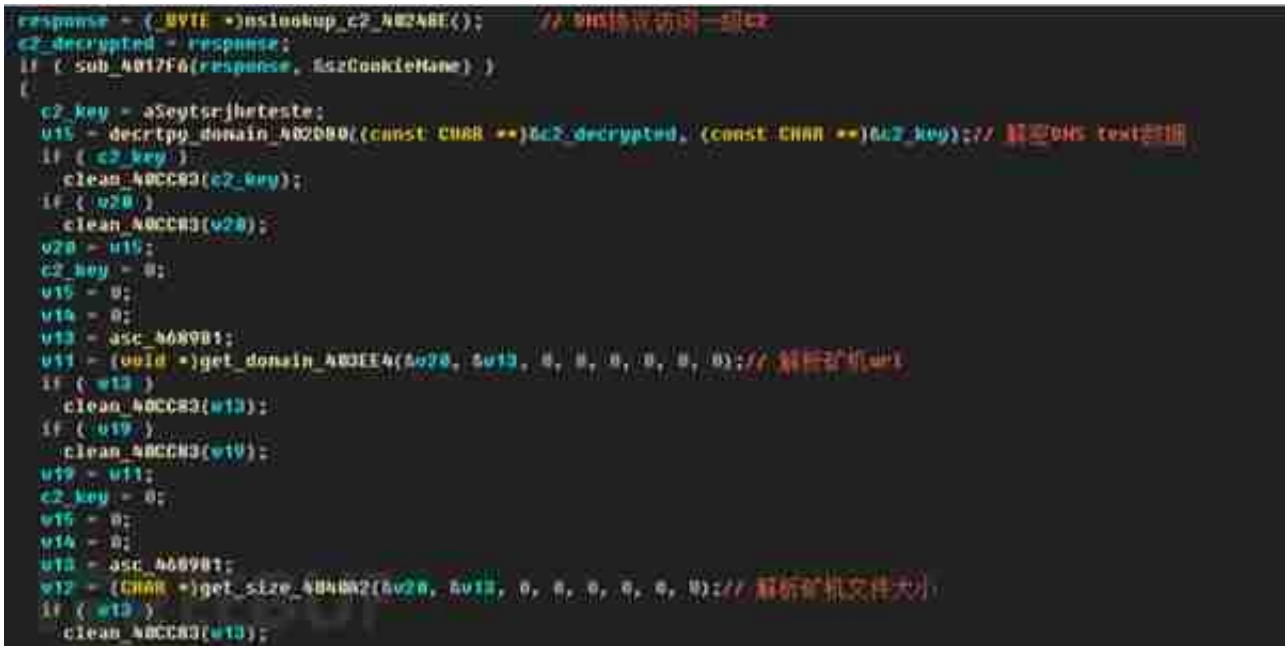
2018年1月腾讯电脑管家对tlMiner挖矿行为及传播来源进行曝光，随即在3月份配合腾讯守护者计划安全团队，协助山东警方快速打击木马作者，并在4月初打掉这

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。

案例2：藏身《荒野行动》辅助的挖矿木马

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6月，致力于传播勒索病毒的病毒作者xiaoba也盯上了《荒野求生》辅助外挂，在网站xiaobaruanjian.xyz上提供荒野行动游戏辅助，并将挖矿木马等植入其中。一旦从该网站下载运行所谓的吃鸡辅助，电脑CPU会被大量占用挖矿。



3．挖矿木马版本快速升级

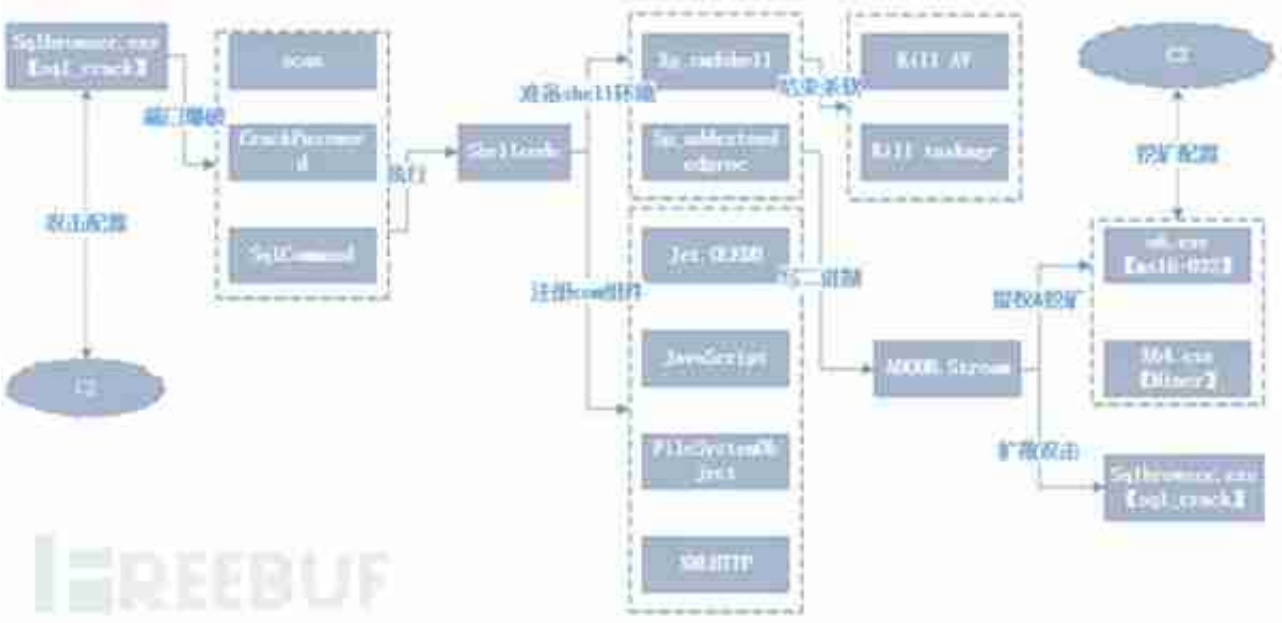
案例1：Apache Struts2高危漏洞致企业服务器被入侵安装KoiMiner挖矿木马

2018年7月腾讯御见威胁情报中心发现有黑客利用攻击工具检测网络上存在Apache struts2漏洞(CVE-2017-5638)服务器，发现存在漏洞的机器后通过远程执行各类指令进行提权、创建账户、系统信息搜集，然后将木马下载器植入，进而利用其下载挖矿木马netxmr4.0.exe。

由于挖矿木马netxmr解密代码后以模块名“koi”加载，因此将其命名为KoiMiner

。

通过多个相似样本进行对比，发现木马作者在一个月内更新发布了4个挖矿木马版本。



版本2：

2018年12月腾讯御见威胁情报中心再次检测到KoiMiner活动，此次的样本仍然专门针对企业SQL Server 服务器的1433端口爆破攻击，攻击成功后会首先植入Zegost远程控制木马（知名远控木马Gh0st的修改版本，安装后会导致服务器被黑客完全控制），控制机器进一步植入挖矿木马。黑客攻击时使用的SQL爆破工具CSQL.exe加密方法与7月发现的样本一致，解密后以模块名“koi”加载执行。

通过SQL爆破工具的解压路径“1433腾龙3.0”进行溯源，发现与攻击事件相关联的一个黑客技术论坛（腾龙技术论坛），并通过信息对比确认相关的论坛活跃成员“*aoli**22”，论坛传播的挖矿木马生成器“SuperMiner v1.3.6”,以及该成员注册C2域名使用的姓名和电话号码。

4．暴力入侵多家医院，威胁医疗系统信息安全

案例：多家三甲医院服务器遭暴力入侵，黑客赶走50余款挖矿木马独享挖矿资源

医疗业务系统正在快速实现信息化，医疗业务系统成为黑客攻击的重点。2018年7月腾讯御见威胁情报中心检测到多家三甲医院服务器被黑客入侵，攻击者暴力破解医院服务器的远程登录服务，之后利用有道笔记的分享文件功能下载多种挖矿木马

。

攻击者将挖矿木马伪装成远程协助工具Teamviewer运行，并且挖矿木马会检测多达50个常用挖矿程序的进程，将这些程序结束进程后独占服务器资源挖矿。木马还会通过修改注册表，破坏操作系统安全功能：禁用UAC（用户帐户控制）、禁用Windows Defender，关闭运行危险程序时的打开警告等等。已知样本分析发现，攻击者使用的挖矿木马拥有多个矿池，开挖的山寨加密币包括：门罗币（XMR）、以太坊（ETH）、零币（ZEC）等等，从矿池信息看，目前攻击者已累积获利达40余万元人民币。

5．应用NSA武器攻击，木马、蠕虫狼狈为奸

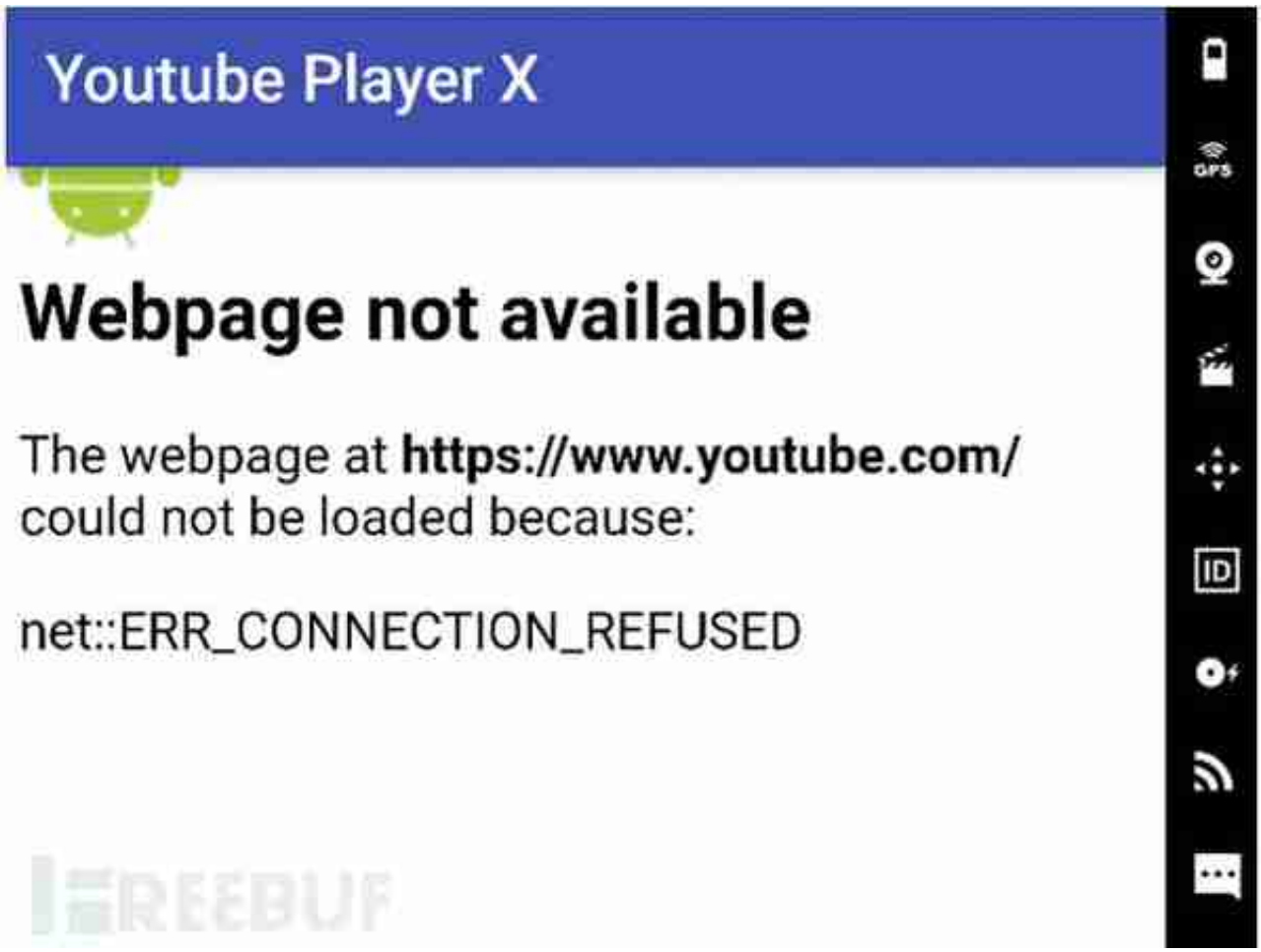
自从NSA武器库工具泄露以来，一直倍受黑客垂青，该工具包经过简单的修改利用便可达到蠕虫式传播病毒的目的。2018年腾讯御见威胁情报中心发现大量的挖矿木马团伙应用NSA武器库工具传播挖矿木马，这使挖矿木马拥有蠕虫病毒的传播能力。

案例1：精通NSA十八般兵器的NSAFtpMiner感染约3万台电脑

2018年9月腾讯御见威胁情报中心发现黑客通过1433端口爆破入侵SQL Server服务器，再植入远程控制木马并安装为系统服务，然后利用远程控制木马进一步加载挖矿木马进行挖矿。随后，黑客还会下载NSA武器攻击工具在内网中攻击扩散，若攻击成功，会继续在内网机器上安装该远程控制木马。

木马加载的攻击模块几乎使用了NSA武器库中的十八般武器：

Eternalblue(永恒之蓝)、Doubleplsar(双脉冲星)、EternalChampion(永恒冠军)、Eternalromance（永恒浪漫）、Esteemaudit（RDP漏洞攻击）等漏洞攻击工具均被用来进行内网攻击，攻击主进程伪装成“Ftp系统核心服务”，还会利用FTP功能进行内网文件更新。其攻击内网机器后，植入远程控制木马，并继续从C2地址下载挖矿和攻击模块，进行内网扩散感染。



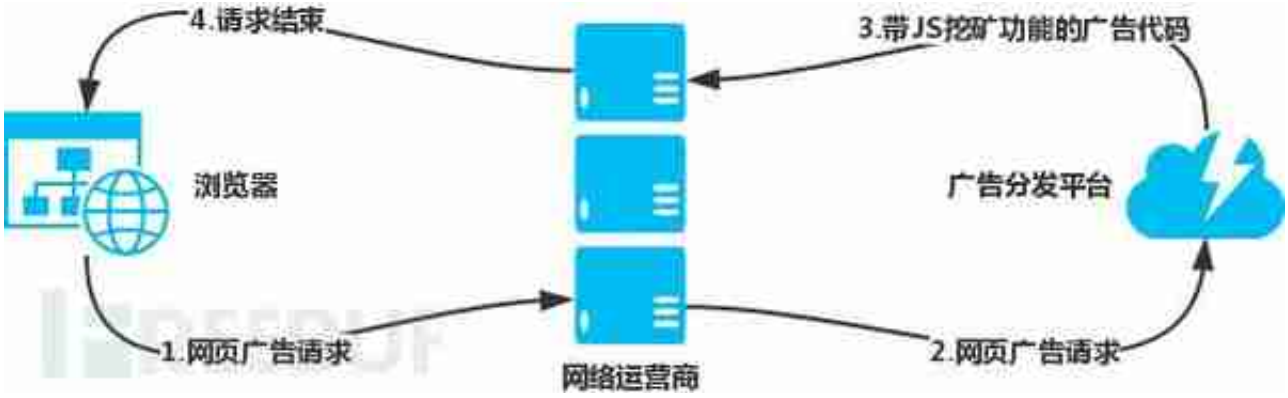
2018年12月御见威胁情报中心通过蜜罐系统部发现了利用Aapche Struts2-045（CVE-2017-5638）漏洞攻击Linux服务器,并通过计划任务植入的挖矿木马。并通过进一步分析发现了针对Windows系统和Linux系统进行攻击的挖矿木马，且不同平台的挖矿木马最终均使用了相同的矿池及钱包。

7．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，而以往利用网页挂马传播最多的是盗号木马。

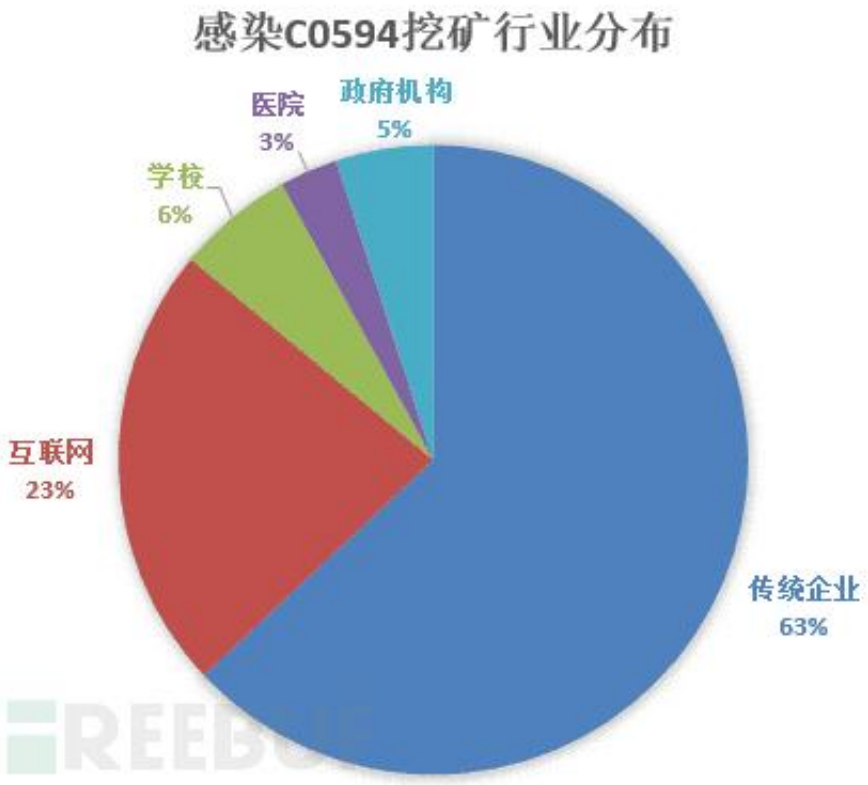
案例1：广告联盟的分发系统被挂马，传播挖矿木马等病毒

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。



此次恶意JavaScript代码存放在国内某电商平台服务器上。页面中导入恶意JS脚本为Coinhive JavaScript
Miner代码，该代码基于CryptoNight挖矿算法，挖取数字加密货币—门罗币。

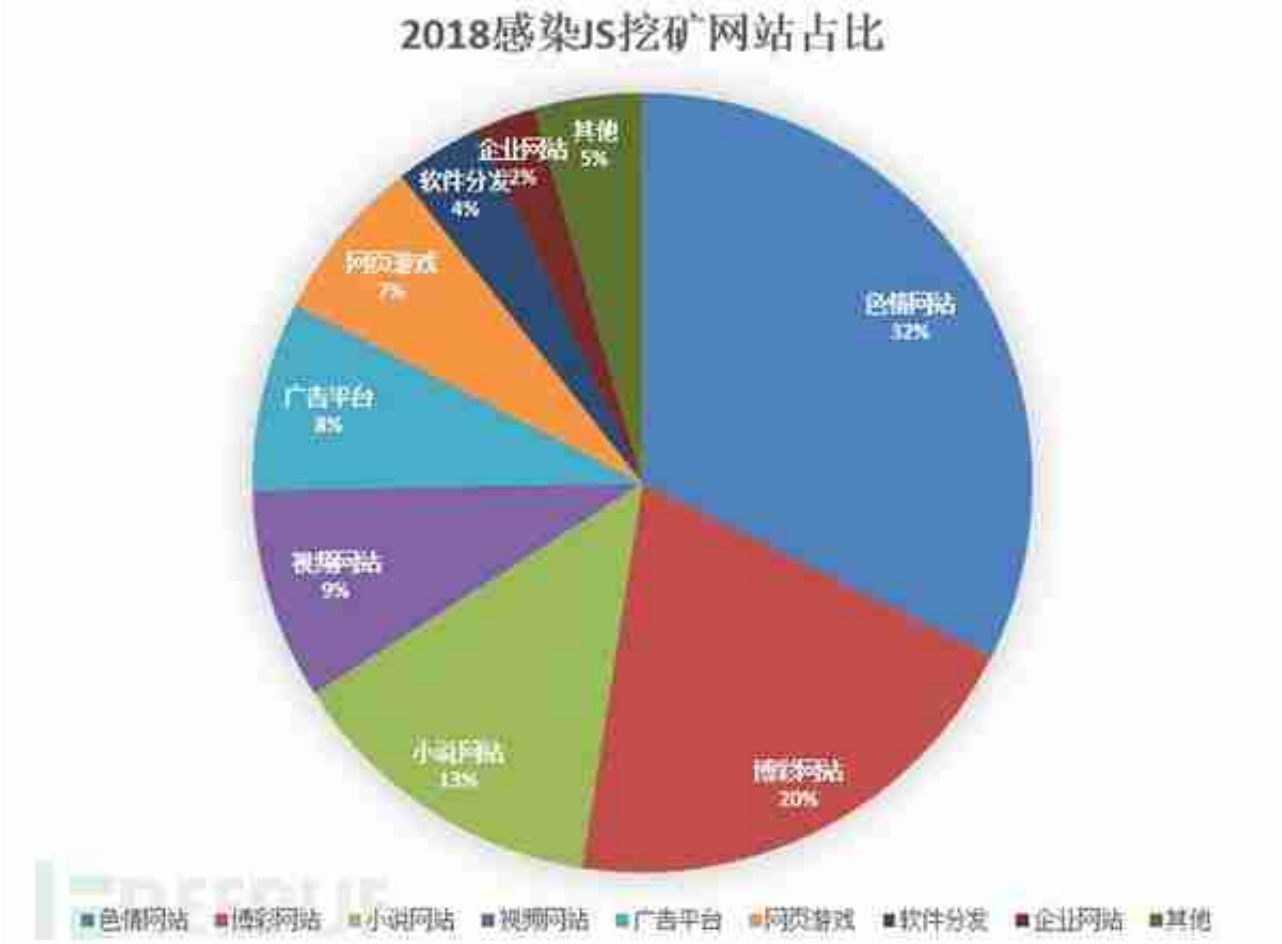
此外，为了不被轻易发现，该挖矿脚本仅在非IE浏览器内运行，并通过Math.random()设置50%的启动概率。这就意味着，当用户发现电脑卡顿、CPU占用率过高，怀疑有恶意程序运行进而进行确认时，挖矿环境并不一定重现。



案例3：使用Drupal系统构建的网站遭遇大规模JS挖矿攻击

2018年5月腾讯御见威胁情报中心监测到，大批使用Drupal系统构建的网站遭到JS

挖矿攻击。经分析，受攻击网站所使用的Drupal系统为存在CVE-2018-7600远程代码执行漏洞的较低版本。黑客利用Drupal系统漏洞将混淆后的挖矿JS注入到网站代码中进行挖矿。



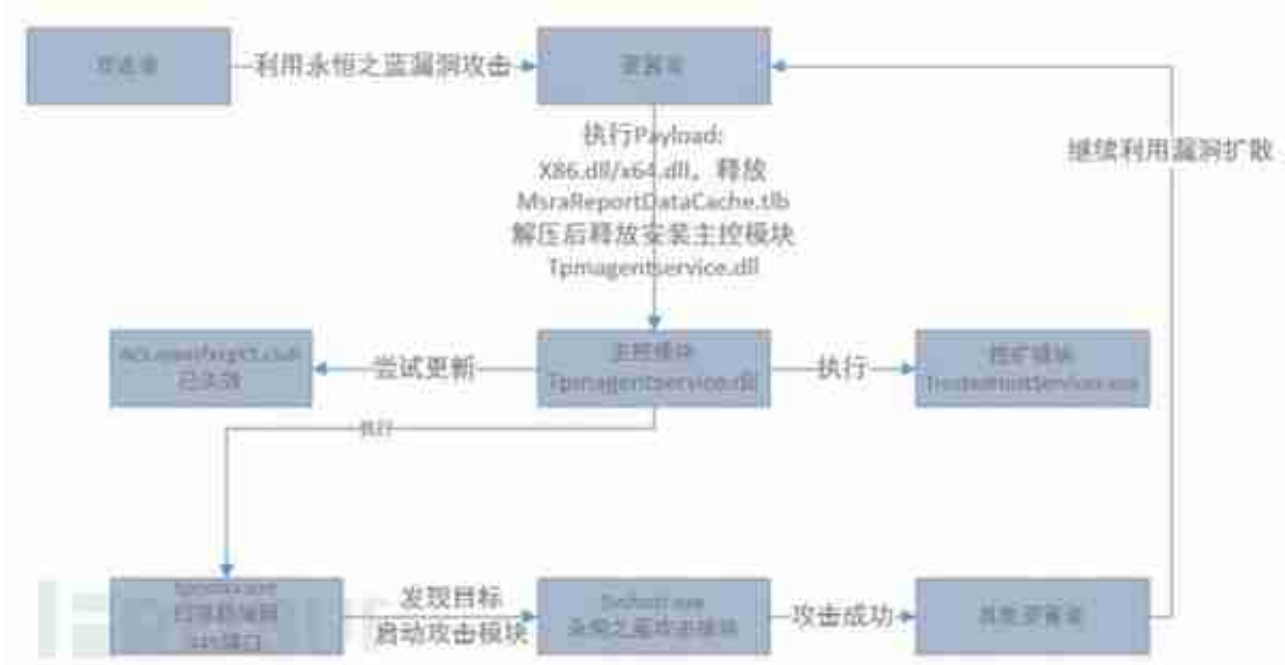
三、挖矿僵尸网络

僵尸网络通过多种攻击方法传播僵尸程序感染互联网上的大量主机，从而形成庞大的受控集群，接收同一个个木马控制端的指令完成相应的行为。挖矿木马变得流行起来后，许多大型僵尸网络也开始将挖矿作为其系统功能的一部分，从而更快地获取收益。2018年活跃的挖矿僵尸网络包括MyKings，WannaMiner等。

1．MyKings>/h3>

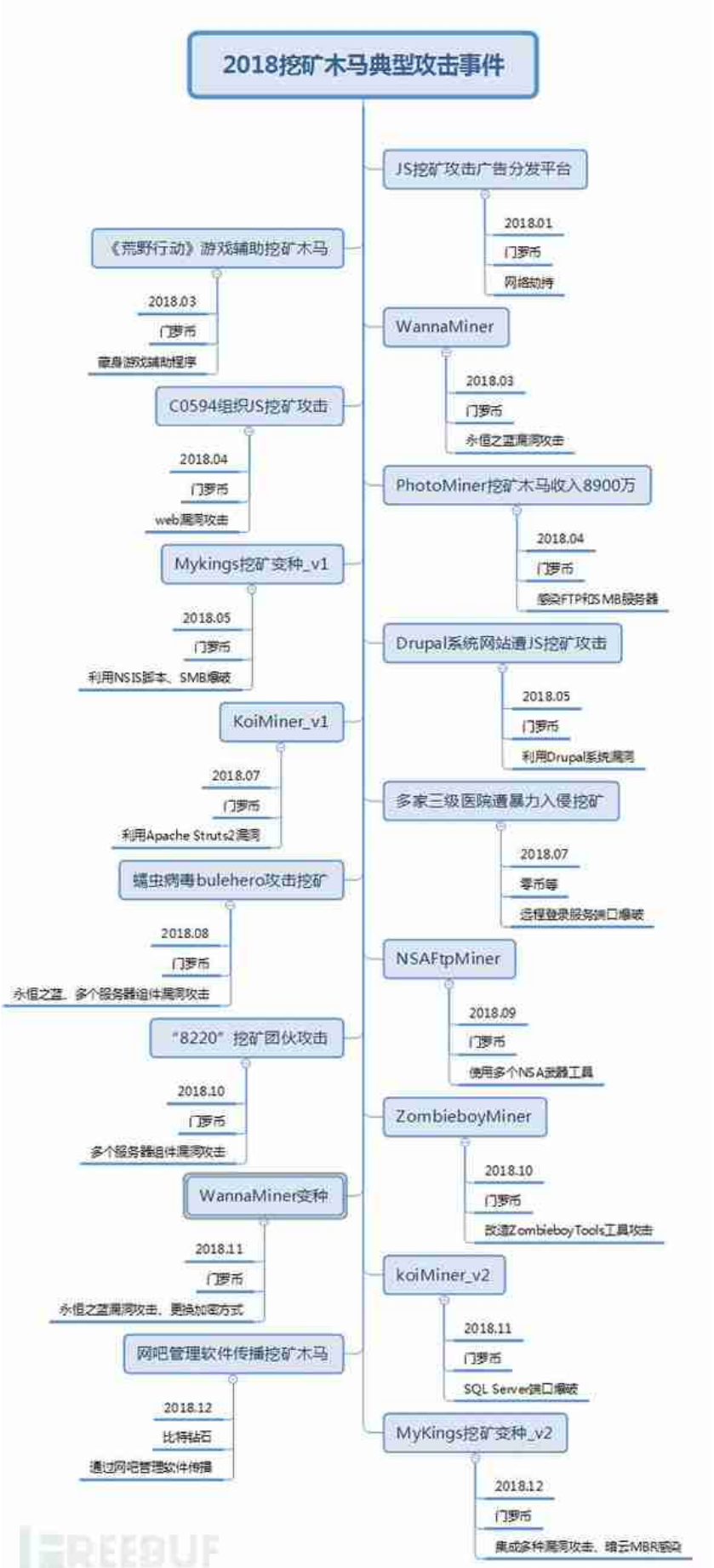
Mykings僵尸网络是目前发现的最复杂的僵尸网络之一，其攻击手段主要为“永恒之蓝”漏洞利用，SQL Server密码爆破等，并在失陷主机植入挖矿模块，远程控制模块，以及扫描攻击模块进行蠕虫式传播。

2018年12月御见威胁情报中心发现Mykings僵尸网络攻击方式升级，在其攻击模块中集成永恒之蓝漏洞、闭路电视物联网设备漏洞、MySQL漏洞攻击以及RDP爆破、Telnet爆破弱口令爆破等多种攻击方式。并且首次发现其使用“暗云”木马感染器感染机器MBR，感染后payload会下载配置文件执行主页锁定和挖矿功能。



2018年11月腾讯御见威胁情报中心发现WannaMiner最新变种攻击，该变种病毒

利用永恒之蓝漏洞在企业内网快速传播。变种的主要变化为，漏洞攻击成功后释放的母体文件由压缩包变为特殊格式的加密文件，因此木马在使用该文件时由简单的解压变为解密，特殊的加密方式给杀软查杀造成了一定难度。


2018挖矿木马典型攻击事件
JS挖矿攻击广告分发平台
2018.01
门罗币
网络劫持
《荒野行动》游戏辅助挖矿木马
2018.03
门罗币
WannaMiner
2018.03
门罗币
永恒之蓝漏洞攻击
C0594组织JS挖矿攻击
2018.04
门罗币
web漏洞攻击
PhotoMiner挖矿木马收入8900万
2018.04
门罗币
Mykings挖矿变种_v1
2018.05
门罗币
利用NSIS脚本、SMB爆破
Drupal系统网站遭JS挖矿攻击
2018.05
门罗币
KoiMiner_v1
2018.07
门罗币
利用Apache Struts2漏洞
多家三级医院遭暴力入侵挖矿
2018.07
蠕虫病毒bulehero攻击挖矿
2018.08
门罗币
永恒之蓝、多个服务器组件漏洞攻击
NSAFtpMiner
2018.09
门罗币
"8220"挖矿团伙攻击
2018.10
门罗币
多个服务器组件漏洞攻击
ZombieboyMiner
2018.10
门罗币
WannaMiner变种
2018.11
门罗币
永恒之蓝漏洞攻击、更换加密方式
koiMiner_v2
2018.11
门罗币
网吧管理软件传播挖矿木马
2018.12
比特钻石
MyKings挖矿变种_v2
2018.12
门罗币

五、币圈疲软，挖矿木马还有未来吗？

数字加密货币在2018年经历了持续暴跌，比特币已从去年年底的2万美元，跌至现在不足4000美元，通过“炒币”暴富的希望似乎越来越渺茫，但这并没有影响挖矿木马的热度，相对于投资矿机来说，控制肉鸡电脑挖矿成本为0。

而从2018年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，因此我们认为2019年挖矿木马仍会持续活跃，与杀毒软件的对抗也会愈演愈烈。除非币圈持续爆跌到一文不值，挖矿黑产才会有新的变化。

综合分析，我们估计2019年，挖矿木马产业会有以下特点：

（1）利用多种攻击方法，短时间快速传播

漏洞利用攻击是木马传播的重要手段之一，挖矿木马将受害者机器作为新的攻击源，对系统中的其他机器进行扫描攻击，达到迅速传播的效果，例如WannaMiner挖矿木马的爆发，几天之内可以达到感染数万台设备，如何快速响应和阻止此类木马是安全厂商面临的考验。

（2）针对服务器攻击，企业用户受威胁

企业设备上往往运行着数量庞大的应用程序，例如提供对外访问的web服务，对企业内部提供的远程登录服务等，这些服务作为企业服务的一个窗口，也成为了不法份子瞄准的弱点。一旦入侵内网，再利用大量廉价的攻击工具可以快速组成挖矿僵尸网络。

例如对服务器远程登录端口爆破，利用服务器组件攻击传播的挖矿木马攻击，未来需要更加有效的解决方案。

（3）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Bootkit/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，属于顽固难清除的一类病毒，可以最大限度在受害电脑系统中存活。

例如在2018年12月发现的Mykings木马最新变种，加入了“暗云”MBR感染功能，通过修改系统系统启动引导扇区加载挖矿模块，使得其难以彻底清除。2019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。

六、针对挖矿木马的应对措施

1、 不要下载来历不明的软件，谨慎使用破解工具、游戏辅助工具。

2、 及时安装系统补丁，特别是微软发布的高危漏洞补丁。

3、 服务器使用安全的密码策略
，使用高强度密码，切勿使用弱口令，防止黑客暴力破解。

4、 企业用户及时修复服务器组件漏洞，包括但不限于以下类型：

Apache Struts2漏洞、WebLogicXMLDecoder反序列化漏洞、Drupal的远程任意代码执行漏洞、JBoss反序列化命令执行漏洞、Couchdb的组合漏洞、Redis未授权访问漏洞、Hadoop未授权访问漏洞；

5、监测设备的CPU、GPU占用情况，发现异常程序及时清除，部署更完善的安全防御系统。个人电脑使用杀毒软件仍是明智之举。

*本文作者：腾讯电脑管家，转载请注明来自FreeBuf.COM