**挖矿流量调研**

**一、目前挖矿流量识别的相关产品**

**产品一：金晴云华公司产品**

**（https://www.aqniu.com/vendor/74993.html）**

金晴云华公司对于恶意挖矿流量的识别主要分为挖矿前期的木马识别和挖矿时的通信流量检测。

木马识别阶段主要使用挖矿木马家族使用的C&C域名、恶意文件hash、相关漏洞利用规则这些威胁情报以及密码爆破检测、AV、沙箱、文件基因检测等方法来对挖矿木马进行识别。

**挖矿流量识别主要通过Stratum协议通信行为、门罗币挖矿行为等流量规则、以及挖矿池域名和IP、挖矿木马使用的加密货币钱包地址等威胁情报进行对通信流量进行检测。**

除此之外，该公司还针对恶意硬盘挖矿提出了监控硬盘以及特定端口的硬盘挖矿行为检测，并提出未来使用ai来识别加密流量特征的畅想。

**产品二;minerBlock**

**https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl?hl=en**

该产品主要使用url、js文件名拦截和js检测的方法来阻止网页挖矿

查看该产品的url、js拦截列表（一共748条）以及该产品的简介发现，主要拦截的url是矿池域名和常用的挖矿js脚本文件名。js检测主要使用的是脚本中的潜在采矿行为来识别挖掘脚本。

**产品三：Panabit公司产品**

该公司针对挖矿流量检测矿池域名、ip列表检测、挖矿通信协议检测、挖矿js脚本引擎网站（实际上还是矿池，不过提供了网页js）检测等方法。

**二、检测挖矿流量的方法**

目前关于挖矿流量检测的方法可以分为

基于深度包检测的方法、

基于矿池服务器列表检测的方法、

基于流量特征分析的检测方法、

基于挖矿网页和挖矿软件木马的挖矿行为检测

**深度包检测**通过对网络流量与已有的检测规则进行匹配来检测挖矿流量，匹配准确率高，但是无法对加密流量的载荷进行检测。

**基于矿池服务器列表**检测的方法是通过将流量的ip和域名与矿池服务器列表进行匹配，通信ip或域名为矿池服务器的即为挖矿流量。基于矿池服务器列表检测的方法可以对加密矿池流量进行检测，但是矿池服务器列表容易失效或被绕过，列表需要持续更新。

**基于流量特征分析**的检测方法是指通过分析挖矿流量和非挖矿流量的特征差异，来区分挖矿流量和非挖矿流量。该方法的优点是可以发现隐藏的矿池服务器，但目前的方法在现实应用中的准确率有待提高。

在挖矿通信流量未发生之前，识别带有挖矿脚本的网站和恶意软件木马在挖矿流量发生之前进行挖矿行为的预先识别。

以下是四种方法的具体介绍。

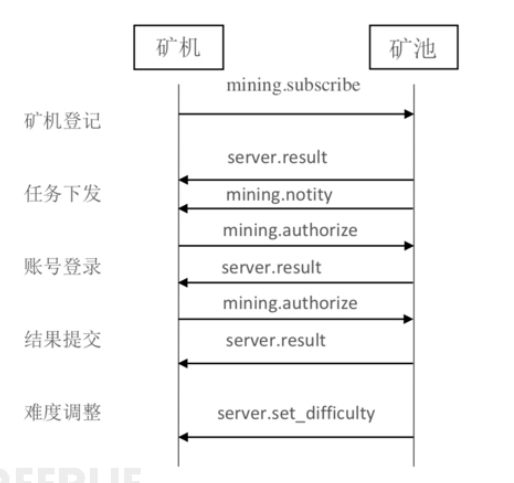
**方法一：深度包检测**

深度包检测方法是将网络流量与已有的检测规则进行匹配来检测挖矿流量。

stratum协议是目前最常用的矿机和矿池之间的TCP通讯协议。因此可以从stratum协议内容出发来制定挖矿流量匹配规则。

**1.协议分析**

矿机和矿池间的一般通信过程主要分为矿机登记、任务下发、账号登录、结果提交与难度调整等部分。



* 任务订阅

矿机启动，首先以mining.subscribe方法向矿池连接，用来订阅工作。

矿池以mining.notify返回订阅号、ExtraNonce1和ExtraNonce2\_size。

Client:{"id":1,"method":"mining.subscribe","params":[]}

Server:{"id":1,"result":[["mining.notify","ae6812eb4cd7735a302a8a9dd95cf71f"],"08000002",4],"error":null}

其中：

ae6812eb4cd7735a302a8a9dd95cf71f是订阅号；

08000002是ExtraNonce1，用于构建coibase交易；

ExtraNonce2\_size为4，矿机ExtraNonce2计数器的字节数。

* 任务分配

该命令由矿池定期发给矿机，当矿机以mining.subscribe方法登记后，矿池应该马上以mining.notify返回该任务。

Server:{"params":["bf","4d16b6f85af6e2198f44ae2a6de67f78487ae5611b77c6c0440b921e00000000", "010000000100000000000000000000000000000000000000000000000000000000000000 00ffffffff20020862062f503253482f04b8864e5008", "072f736c7573682f000000000100f2052a010000001976a914d23fcdf86f7e756a64a7a9688ef9903327048ed988ac00000000",["c5bd77249e27c2d3a3602dd35c3364a7983900b64a34644d03b930bfdb19c0e5", "049b4e78e2d0b24f7c6a2856aa7b41811ed961ee52ae75527df9e80043fd2f12"], "00000002","1c2ac4af","504e86b9",false],"id":null,"method":"mining.notify"}

其中：

任务号：”bf”；

前个区块HASH：

"4d16b6f85af6e2198f44ae2a6de67f78487ae5611b77c6c0440b921e00000000"；

coinbase第一部分：

"010000000100000000000000000000000000000000000000000000000 00000000000000000ffffffff20020862062f503253482f04b8864e5008"；

coinbase第二部分：

"072f736c7573682f000000000100f2052a010000001976a914d23fcdf86f7 e756a64a7a9688ef9903327048ed988ac00000000"；

交易ID列表：

["c5bd77249e27c2d3a3602dd35c3364a7983900b64a34644d03b930bfdb19c0e5", "049b4e78e2d0b24f7c6a2856aa7b41811ed961ee52ae75527df9e80043fd2f12"]；

区块版本号：”00000002″；

nBit:”1c2ac4af”；

当前时间：”504e86b9″；

清理任务：如果为true,则矿机中止所有任务，马上开始新任务；如果是false则等当前任务结束才开始新任务。

* 矿机登录

矿机以mining.authorize方法，用某个帐号和密码登录到矿池，密码可空，矿池返回true登录成功。该方法必须是在初始化连接之后马上进行，否则矿机得不到矿池任务。

Client:{"params":["miner1","password"],"id":2,"method":"mining.authorize"}

Server:{"error":null,"id":2,"result":true}

* 结果提交

矿机找到合法share时，就以”mining.submit“方法向矿池提交任务。矿池返回true即提交成功，如果失败则error中有具体原因。

Client:{"params":["miner1","bf","00000001","504e86ed","b2957c02"],"id":4,"method":"mining.submit"}

Server:{"error":null,"id":4,"result":true}

其中：

用户名：”miner1″；

任务号：”bf”；

ExtraNonce2：”00000001″；

当前时间：”504e86ed”；

nonce:”b2957c02″；

* 难度调整

难度调整由矿池下发给矿机，以mining.set\_difficulty方法调整难度，params中是难度值。矿机会在下一个任务时采用新难度，矿池有时会马上下发一个新任务并且把清理任务设为true，以便矿机马上以新难度工作。

Server:{"id":null,"method":"mining.set\_difficulty","params":[2]}

**2.规则制定**

* 文献1根据以上挖矿通信协议进行分析，提取了以下suricata挖矿流量检测相关规则。

Login行为规则（suricata自带规则）（可以看出content部分主要包含了登录数据包的相关载荷）：

alert tcp $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET POLICY Crypto Coin Miner Login"; flow:to\_server,established; content:"|7b 22|method|22 3a|"; depth:10; fast\_pattern; content:"|22|login|22 2c|"; distance:0; within:9; content:"|22|params|22 3a|"; distance:0; within:10; content:"|7b 22|login"; nocase; distance:0; within:8; content:"agent|22 3a|"; nocase; distance:0; metadata: former\_category POLICY; reference:md5,d1082e445f932938366a449631b82946; reference:md5,33d7a82fe13c9737a103bcc4a21f9425; reference:md5,ebe1aeb5dd692b222f8cf964e7785a55; classtype:trojan-activity; sid:2022886; rev:3; metadata:affected\_product Any, attack\_target Client\_Endpoint, deployment Perimeter, tag Bitcoin\_Miner, signature\_severity Audit, created\_at 2016\_06\_09, malware\_family CoinMiner, performance\_impact Low, updated\_at 2017\_10\_12;)

alert tcp-pkt $HOME\_NET any -> $EXTERNAL\_NET any (msg:"ET POLICY Cryptocurrency Miner Checkin"; flow:established,to\_server; content:"|7b 22|id|22 3a|"; nocase; depth:6; content:"|22|jsonrpc|22 3a|"; nocase; distance:0; content:"|22 2c 22|method|22 3a 22|login|22 2c 22|params|22 3a|"; fast\_pattern; content:"|22|pass|22 3a 22|"; nocase; content:"|22|agent|22 3a 22|"; nocase; content:!"<title"; nocase; content:!"<script"; nocase; content:!"<html"; nocase; metadata: former\_category POLICY; classtype:policy-violation; sid:2024792; rev:4; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, deployment Perimeter, signature\_severity Minor, created\_at 2017\_10\_02, updated\_at 2018\_06\_15;)

submit操作检测：

alert tcp $HOME\_NET any -> $EXTERNAL\_NET any (msg:"Cryptocurrency Miner Check By Submit"; flow:to\_server,established; content:"|22|method|22 3a|"; fast\_pattern; content:"|22|submit|22 2c|"; distance:0; within:10; content:"|22|params|22 3a 7b|"; distance:0; within:15; content:"result|22 3a|"; nocase; distance:0; sid:3013015; rev:1; metadata:Detecting Mining Rules;

矿池响应矿工的流量检测规则：

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"Pools Response Cryptocurrency Miner"; flow:to\_client,established; content:"|22|method|22 3a|"; nocase; content:"|22|params|22 3a|"; nocase; content:"|22|blob|22 3a|"; nocase; content:"|22|job\_id|22 3a|"; nocase; sid:3013016; rev:1; metadata:Detecting Mining Rules;)

网页挖矿行为也可以通过以下规则进行检测：

alert http $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ET CURRENT\_EVENTS CoinHive In-Browser Miner Detected"; flow:established,from\_server; file\_data; content:"coinhive.min.js"; nocase; fast\_pattern; content:"start"; nocase; distance:0; content:"script"; content:"var"; distance:0; pcre:"/^\s\*(?P<var>[a-zA-Z0-9]{3,20})\s\*=\s\*new\s\*CoinHive\s\*\.\s\*[^\(]+\(\s\*[\x22\x27][A-Za-z0-9]+\s\*[\x22\x27]\s\*(?:\x2c\s\*\x7b\s\*\w+\x3a\s\*\d\.\d\x7d)?\)\s\*\x3b\s+(?P=var)\s\*\.\s\*start/Ri"; metadata: former\_category CURRENT\_EVENTS; classtype:policy-violation; sid:2024721; rev:2; metadata:affected\_product Any, attack\_target Client\_Endpoint, deployment Perimeter, signature\_severity Minor, created\_at 2017\_09\_18, performance\_impact Moderate, updated\_at 2018\_05\_08;)

* snort发布了关于检测挖矿流量的相关的规则：

Snort 有一系列用于处理挖矿相关活动（从防止下载挖矿程序到阻止挖矿命令和访问挖矿池，再到恶意软件本身的命令和控制基础设施）的规则。

**处理加密挖矿活动的 Snort 规则可以分为三组：**

**①　用于阻止传入客户端（包括挖矿程序下载）的规则**： SID：44692- 44693、45265- 45268、45809- 45810、45949- 45952、46365- 46366、46370- 46372。

**②　用于阻止已经明确知道会在受害者网络中挖矿的恶意软件及变体的规则**： SID：20035、20057、26395、28399、28410-28411、29493- 29494、29666、30551- 30552、31271-31273、31531- 1533、32013、33149、43467-43468、44895- 44899、45468- 45473、45548、45826-45827、46238- 46240。

**③　侧重于识别和阻止加密货币矿工使用的协议的规则**： SID：26437、40840- 40842、45417、45549-45550、45825、45955。

使用深度包检测的方法检测挖矿流量的优点是匹配准确率较高，**缺点是无法对加密流量载荷进行检查**，同时因为需要对数据包进行深度解析导致代价较高。

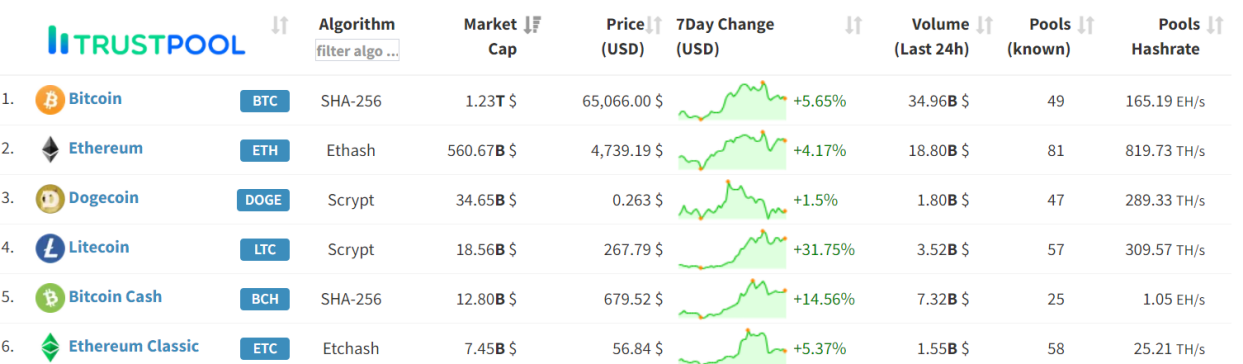
**方法二：基于矿池服务器列表检测**

文献3提出了一种自动列举矿池及其子域，并将它们转换为 IP 地址的方法，利用矿池服务器域名和ip可以检测加密挖矿流量。具体的实现方案如下。

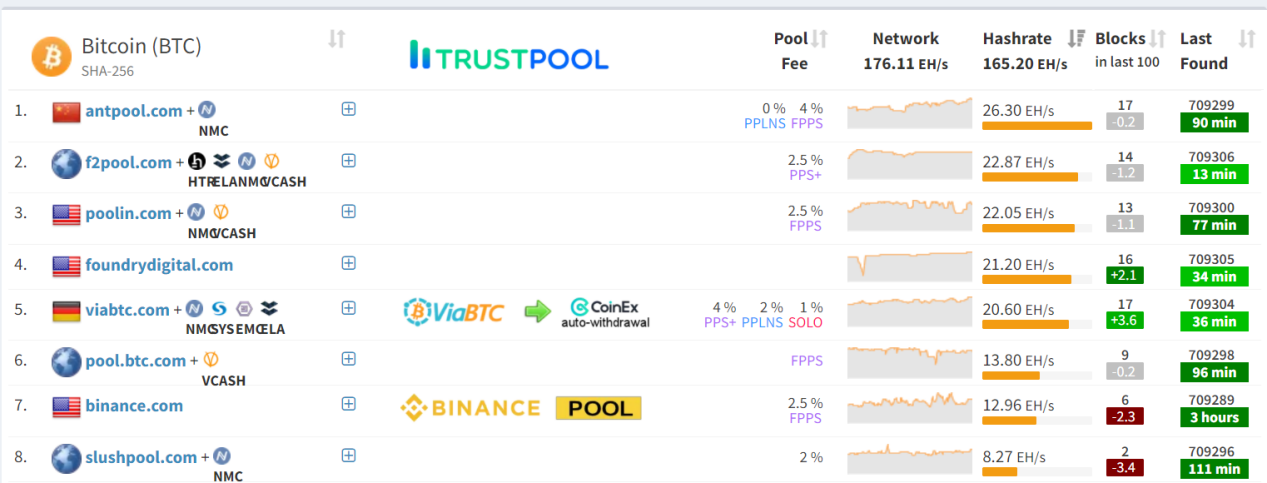
**1. 列举矿池**

第一步是收集活跃的采矿池列表。根据网上公开的信息可以获取大部门公开矿池的相关网站。例如，Google搜索矿池列表关键字，第一个搜索结果：

<https://miningpoolstats.stream/>，该网站列举了目前主流加密货币的相关息



点击货币名称，即可查看目前货币的主要矿池网站及网站的相关信息。以bit币为例。



**2. 列举矿池服务器域名**

矿池网站通常包含有如何将矿工连接到矿池的信息，其中详细说明了矿池服务器的域名或 IP 地址。文献3观察到一些网站使用类似的网络框架，并将信息存储在同一位置，可以自动访问 Web 请求和 调用API ，以下载矿池网站的 Web 内容并解析池服务器的域名。（文献三未具体描述自动化方法和存放位置）

点击antpool的具体矿工配置可以得到以下矿池服务器域名和端口的相关信息。



**3. 列举矿池服务器子域名**

矿池网站的域名通常与接收采矿流量的单个池服务器的域名不同。文献3观察到，大多数池服务器域遵循来自池的网站域的类似命名惯例，例如：

池网站域名 池服务器域

f2pool.com xmr.f2pool.com

nanopool.org xmr- us-west1.nanopool.org

miningpool.fun xmr.miningpool.fun

2miners.com xmr.2miners.com

hashcity.org xmr.hashcity.org

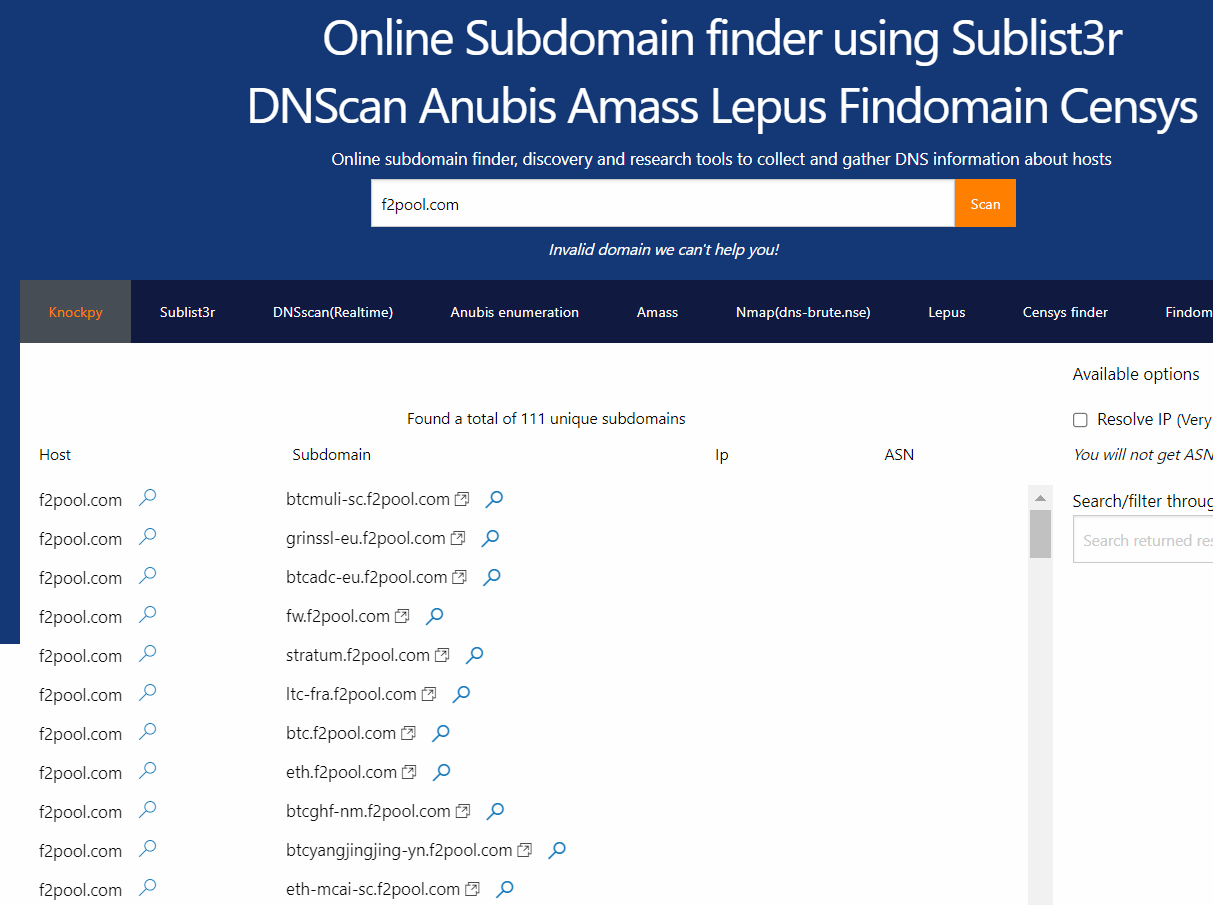
hashvault.pro pool. hashvault.pro

minexmr.com pool. minexmr.com

supportxmr.com pool. supportxmr.com

大多数池服务器域名可能会包含和加密货币相关的关键字。可以使用 findomain 、Sublist3r、subdomainfinder这些工具来查找与特定根域相关的任何子域。然后过滤显示包含加密货币关键字的相关子域。

使用<https://www.nmmapper.com/sys/tools/subdomainfinder/>，查询f2pool.com的子域名如下图所示：



根据以上方法确定域名并查找其对应的ip。

**4.手动验证池服务器ip**

文献2提出了一种主动探测池服务器ip的方法。

文献2向可疑的ip主动发送经过精心构造的数据包，通过服务器的反应来判定是否为矿池服务器ip。通常服务器有3种反应，如果探测成功，即视为矿池服务器ip。

* DOWN-探测失败，连接未建立
* LISTEN-指定端口接受连接，但服务器使用的挖矿协议与测试的挖矿协议不同，或者端口被占用无法正确响应。
* UP-探测成功，正确响应。

根据以上方法即可整理出大部分矿池服务器域名及ip列表。通过匹配网络流量的域名和ip来检测挖矿流量。

使用矿池服务器ip进行检测的优点是检测效率高，成本低。缺点是覆盖面有限，只能尽可能收集矿池服务器ip和域名，总有遗漏，矿池也很容易通过绕过ip列表。

**方法三：基于流量特征分析**

文献2提出了一种使用**加密流量特征**来识别加密客户端的方法，通过识别挖矿客户端，进一步挖掘。

**1.分析挖矿客户端流量特征**

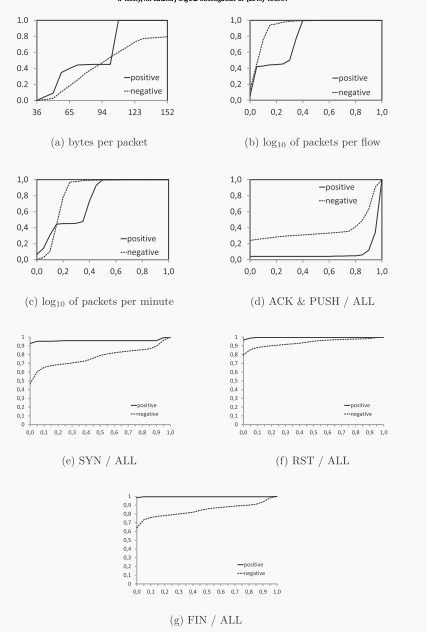
文献2观察了目前常见的挖矿客户端流量，总结了以下流量特点。

* 矿工和矿池之间的通信通常会持续几个小时。数据包一般很小，数据包大小通常在40到120字节之间。
* 目标端口小于源端口。
* 大多数流都包含ACK&PUSH标志位。
* 双方通常不会主动发送FIN标志位断开连接，即大多数流都不包含FIN标志位。
* 大多数流不包含RST标志。

一个长连接长期不释放，那么多半在搞事情，流中数据包无Fin标志也无RST标志。

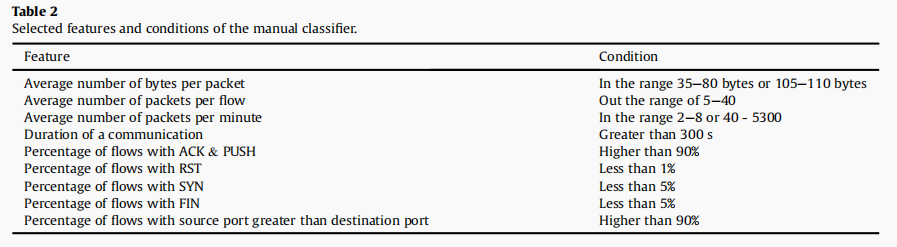
之后在捷克国家研究和教育网络上收集了超过5万个用户的流量数据，对挖矿、非挖矿客户端的流量特征进行了具体的分析。其中挖矿客户端设为positive，其他设为negative。以下是文献2的一些分析结果。

* 图a代表40％的挖矿客户端数据包平均大小在36-80之间，超过50％的挖矿客户端数据包平均大小在105-110之间。
* 图d，e，f表示挖矿客户端流量中都很少包含SYN、FIN、RST标志位，与正常流量有所不同。



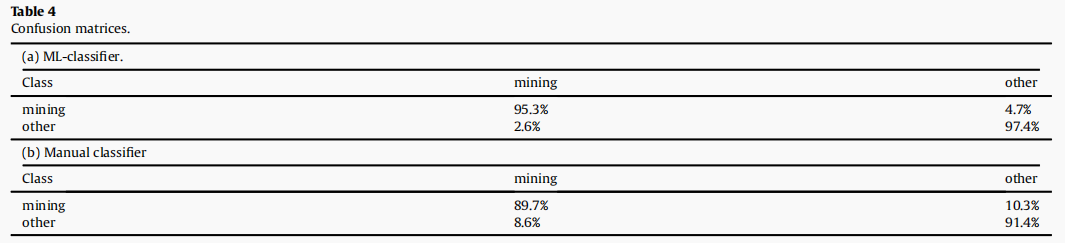
**2.提取挖矿客户端流量特征**

基于以上的数据分析，文献2提取了流量的以下特征



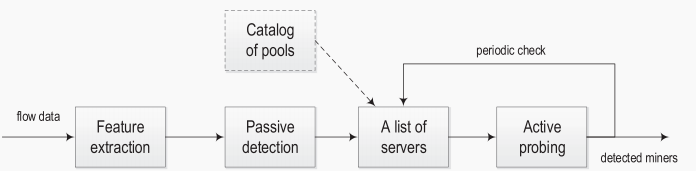
**3.使用机器学习方法对挖矿客户端和非挖矿客户端进行分类**

之后文献2作者使用机器学习算法和以上特征对挖矿客户端和非挖矿客户端进行分类，准确率达90％以上，以下是混淆矩阵。



**4.结合方法二主动验证的方法发掘隐藏的矿池服务器信息**

文献2结合了在检测出挖矿客户端的基础上结合方法二的主动验证部分来发掘隐藏的矿池服务器信息。主动探测可以维护池列表，通过ip、域名等给被动检测提供可靠的训练数据。被动检测可以发现隐藏的矿池服务器信息，使用主动探测可以确定新发现矿池服务器信息是否正确。



**方法四：识别挖矿的恶意网站和软件**

本方法是指通过**识别带有挖矿脚本的网站**和恶意软件木马在挖矿流量发生之前进行挖矿行为的预先识别。

**1.网页挖矿识别**

网页挖矿是一种利用网站前端javascript进行挖矿的一种行为，目前主要利用CoinHive和JSEcoin这两个手段进行网页挖矿，除此之外还有利用Webmine，Cryptoloot，Webmine等进行挖矿。

以下针对使用CoinHive脚本挖矿的流程进行介绍:



这种挖矿与普通的挖矿不同，采用coinhive网页挖矿是攻击者将自己的钱包地址给了第三方，然后通过与第三方的代理矿池交互去实现的网页挖矿。第三方会收取一定的比率的算力，是一种代理挖矿的模式。

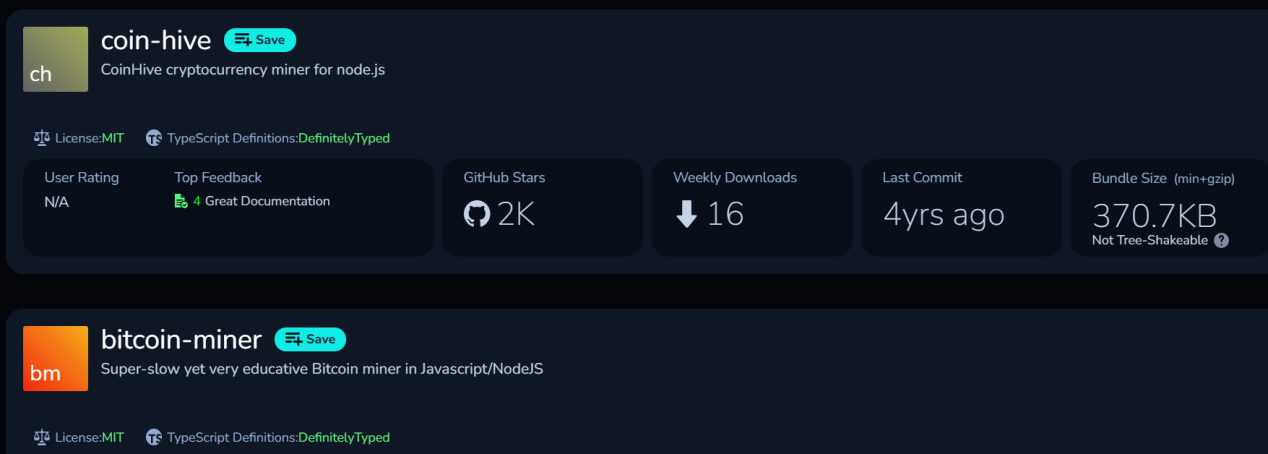
针对具体的挖矿流程如下：

* 浏览器会请求coinhive服务器中的coinhive.min.js文件；
* 执行coinhive的JS代码，会去请求代理矿池；
* 开始与代理矿池交互；
* 代理矿池会与总矿池交互；
* 在代理矿池中挖取的门罗币会发送到js中提交的钱包地址里面。(如果网站是被劫持挖矿的，js脚本里的钱包地址会被替换为黑客的钱包地址)

**1.1获取js脚本引擎的网站**

主要通过公开信息

如（https://openbase.com/categories/js/best-nodejs-cryptocurrency-libraries）查找主要的js脚本引擎的网站，得到网站的相关域名信息。



**1.2 获取网页挖矿的网站列表**

有相关机构（https://webtechsurvey.com/technology-type/cryptominer）、Pixalate总结了一些使用各种挖矿脚本的网站。访问这些机构网站可以获得一部分网页挖矿列表。



**1.3 获取网页挖矿的可疑网站**

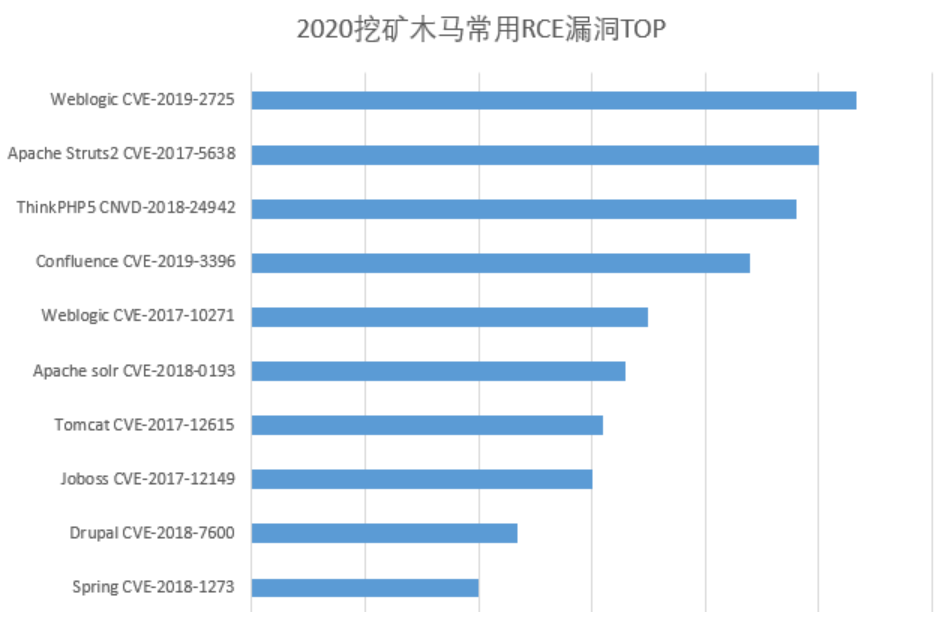
通过相关开源搜索引擎fofa（https://fofa.so/）、PublicWWW的扫描发现具有挖矿脚本引擎网站（coinhive.com）域名来查找可疑的网页挖矿的网站。



**1.4 通过主动的js检测来检测网站是否为挖矿网站。**

通过主动访问可疑挖矿网站查看页面js内容以及查看hash计算次数、堆栈调用次数等来片段网站是否为挖矿网站。

1. **恶意挖矿木马**



恶意挖矿木马的识别方法主要通过两个方面：

* 识别恶意挖矿木马的cnc域名以及木马的流量通信规则。

Snort中收录了用于阻止已经明确知道会在受害者网络中挖矿的恶意软件及变体的规则： SID：20035、20057、26395、28399、28410-28411、29493- 29494、29666、30551- 30552、31271-31273、31531- 1533、32013、33149、43467-43468、44895- 44899、45468- 45473、45548、45826-45827、46238- 46240。

* 对邮件、web等方式下载的文件进行动静态主动分析是否为恶意木马。

**三、总结**

目前挖矿检测相关的方法主要包括挖矿前期检测和挖矿时检测。挖矿前期主要时对挖矿网页和挖矿木马检测，主要使用方法方法四。挖矿时检测主要利用已知的挖矿协议规则以及矿池域名、ip（方法一、二）进行检测，方法三时对于加密挖矿流量检测未来探索的方向。

可以将方法二与方法三集合起来，利用挖矿客户端访问域名的共性来发掘隐藏矿池服务器。

1.使用确定的矿池服务器列表、snort规则、以及机器学习的方法来识别出挖矿流量和挖矿客户端。

2.通过比对挖矿客户端访问域名的共性，来进一步发掘隐藏的矿池服务器信息。（因为同为挖矿客户端，很有可能会访问相同的未被发现的其他矿池服务器）

3.使用主动探测的方法来确认第二步可疑的矿池服务器ip和域名的正确性，扩充矿池服务器列表，不断的迭代更新。

挖矿流量相关资源

【1】 <https://github.com/nesfit/DI-cryptominingdetection> 包含文献2的原始挖矿流量pcap包、特征csv文件、主动探测工具、采矿服务器ip list。

【2】 <https://miningpoolstats.stream/> 矿池相关信息网站

【3】 <https://www.nmmapper.com/sys/tools/subdomainfinder/> 、

https://github.com/Edu4rdSHL/findomain/releases、<https://github.com/aboul3la/Sublist3r>

子域名查找工具

参考文献：

【1】<https://www.freebuf.com/articles/network/195171.html>

【2】[1]V Veselý, M Ždník. How to detect cryptocurrency miners? By traffic forensics![J]. Digital Investigation, 2019.

【3】

<https://www.reliaquest.com/blog/mining-for-better-threat-intelligence-cryptominer-pools/>

【4】

https://www.lyon-county.org/AgendaCenter/ViewFile/ArchivedAgenda/\_08022018-1072