挖矿行为发现&治理解决方案

目 录

01

相关基础知识

虚拟货币是什么

“挖矿”挖的是数字货币，也称“虚拟货币”。

数字货币是一种数字化的货币，通常由开发者发行和管理，被“特定”虚拟社区、或者区域所接受和使用。

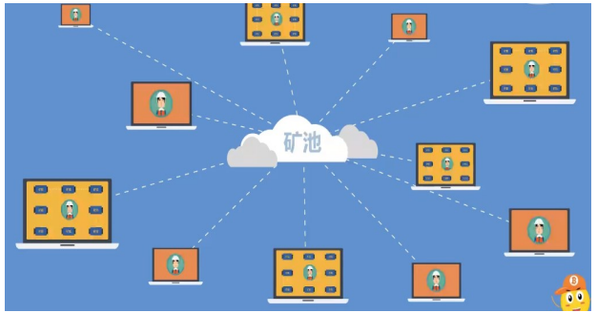
Bitcoin (BTC)

最早发行的虚拟货币是**比特币**，中本聪于2008年发表了一篇名为《比特币:一种点对点式的电子现金系统》的论文，描述了一种被他称为“比特币”的电子货币及其算法。2009年，他发布了首个比特币软件，并正式启动了比特币金融系统，总数量被永久限制在2100万个 。

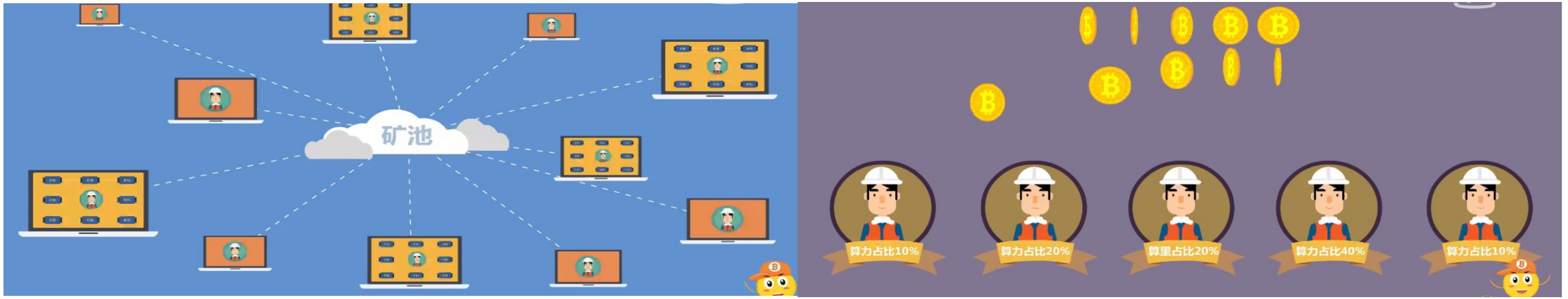
类似货币还有：以太坊 、起亚、门罗、莱特、 狗狗等。

“挖矿”相关名词

名词	说明
挖矿	是对加密数字货币（比如比特币）开采的俗称； 开采比特币就像是求解一道数学题，最先得到答案，就获得相应的奖励，所以整个求解并验证的过程就叫做挖矿。
矿机	用于破解数字答案的设备就称为矿机。
矿工	运行矿机，获得收益的人群就被成为矿工。
矿场	矿场是很多台矿机组合到一起，使得算力增强
矿池	矿池是突破地址位置的限制，将各地的算力汇聚起来增强算力，并把收益平分给所有算力。
钱包	像一张银行卡一样，拥有一个唯一卡号（地址）来接收或发送你的数字货币，矿池挖到币以后，给你发到这个地址上，币就进入了你的钱包。



什么是矿池



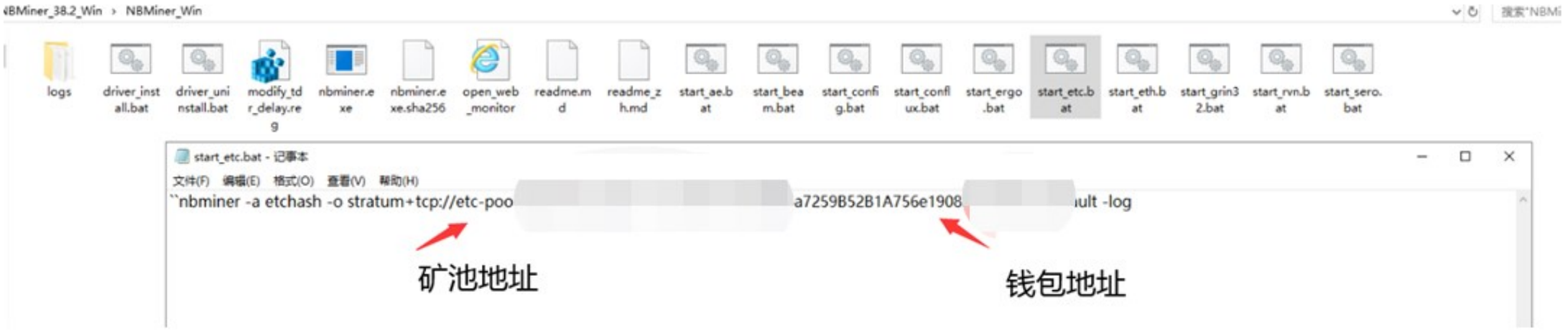
矿池:随着参与挖矿的人越来越多，比特币全网的算力不断上涨,单个设备或者少量的算力都很难再挖到比特币,这个时候矿池就产生了，矿池是突破地址位置的限制，将各地的算力汇聚起来增强算力，并把收益平分给所有算力，保证矿池参与者收入稳定。那么所有队伍中的人会根据每个人的电脑性能进行分红。

由于挖矿主机需要和矿池通讯，因此我们如果知道矿池的相关域名或者IP地址，我们就可以发现内网那些主机和矿池相关IP地址通讯；通过禁止矿池相关IP的通讯，也可以阻断挖矿行为。

怎么挖矿— 挖矿软件

挖矿模式1：软件挖矿。

通过运行在Linux或者Windows的软件进行挖矿，例如：**矿工、长*矿工之类的，这种是傻瓜式的挖矿只要把钱包地址填进去，选择币种和矿池开始挖矿就行了，这种简单方便，但是他抽成比较高。



此外，也有一些黑客，通过非法手段上传“挖矿”木马程序到计算机或者服务器上，然后通过设置计划任务或者修改系统文件权限等方式，实现“挖矿”木马程序的持久化运行。

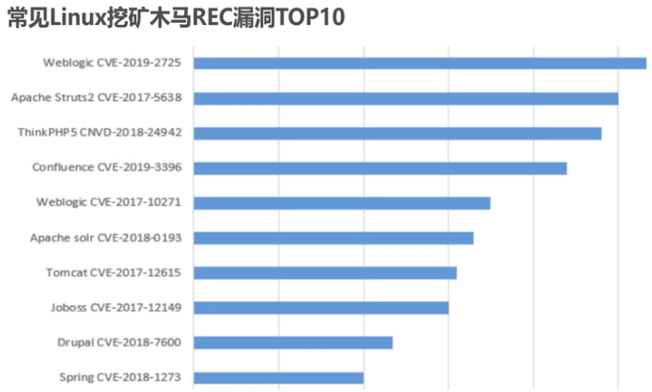
怎么挖矿— 脚本模式

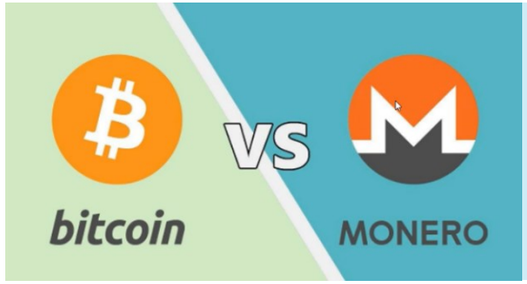
Panabit®

挖矿模式2：基于网站脚本方式

基于网站脚本的方式是通过JavaScript等编写的“挖矿”脚本在浏览器中执行，通过在网站中嵌入含有“挖矿”代码的脚本，当浏览器访问带有“挖矿”脚本的网站时，浏览器将解析并执行“挖矿”脚本（如Coinhive、JSEcoin等），在后台进行“挖矿”。这种方式比传统的基于程序的“挖矿”方式更加隐蔽，难以被发现。

此外，也有一些黑客，通过非法手段上传“挖矿”木马程序到计算机或者服务器上，然后通过设置计划任务或者修改系统文件权限等方式，实现“挖矿”木马程序的持久化运行。





罗门币挖矿病毒，该病毒程序利用了“永恒之蓝”高危漏洞在局域网内蠕虫式传播并且使用中毒电脑挖取一种与“比特币”类似的虚拟数字货币“门罗币”牟利。

挖矿收益和支出

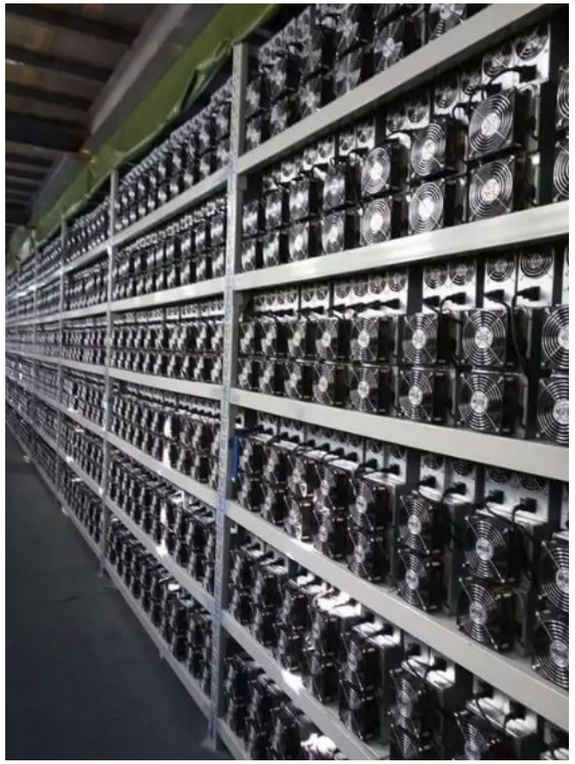
算力：(也称哈希率)是比特币网络处理能力的度量单位。即为计算机(CPU、GPU等)计算哈希函数输出的速度。比特币网络必须为了安全目的而进行密集的数学和加密相关操作。

每M日产出	0.00086378	ETC
币价	414.2016	¥
拥有算力	12	MHash
总功耗	2430	W
机器成本	0.00	¥
电费	0.5	¥/度

开始计算　用APP计算

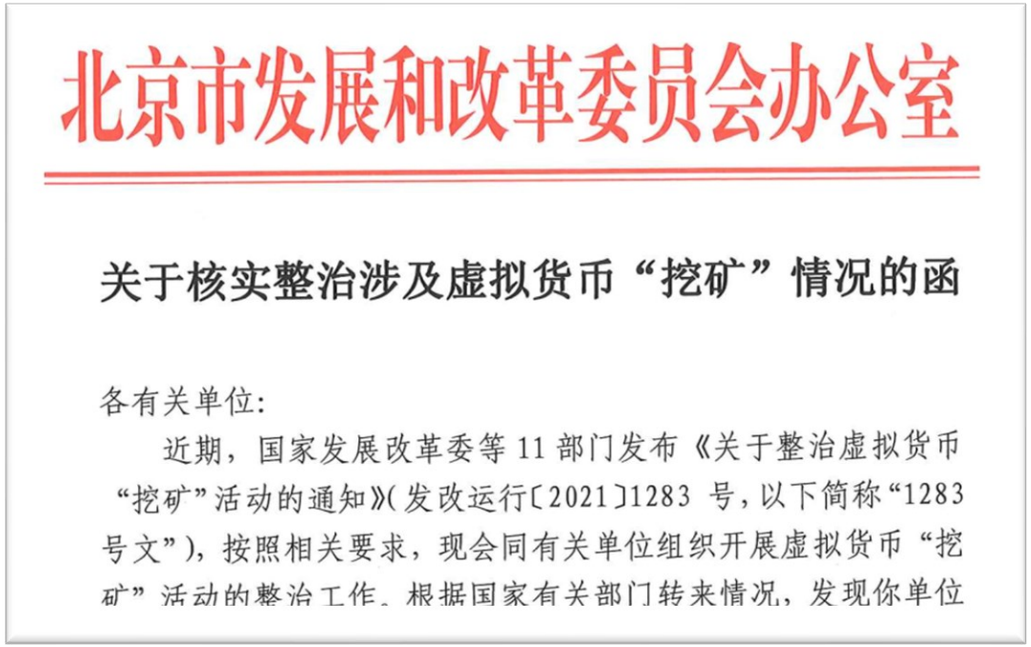
周期	产出	用电量	电费	净收益
每日	4.29 元 0.01036536 ETC	58.32 度	29.16 元	-24.87 元
每周	30.05 元 0.07255752 ETC	408.24 度	204.12 元	-174.07 元
每月	128.80 元 0.31096080 ETC	1749.60 度	874.80 元	-746.00 元
每年	1567.07 元 3.78335640 ETC	21286.80 度	10643.40 元	-9076.33 元

电费占比	100%
关机币价	2813.22 元 / ETC
回本时间	静态回本周期为 -



挖矿收益和支出：
通过算力，软件帮你算得清清数数，能挣多少，亏多少..
例如：某电脑显卡GTX 1050Ti，由于电费支出非常大，完全亏本的。
因此，会出现有人利用单位/公共资源的电和算力资源来进行挖矿。

国家政策

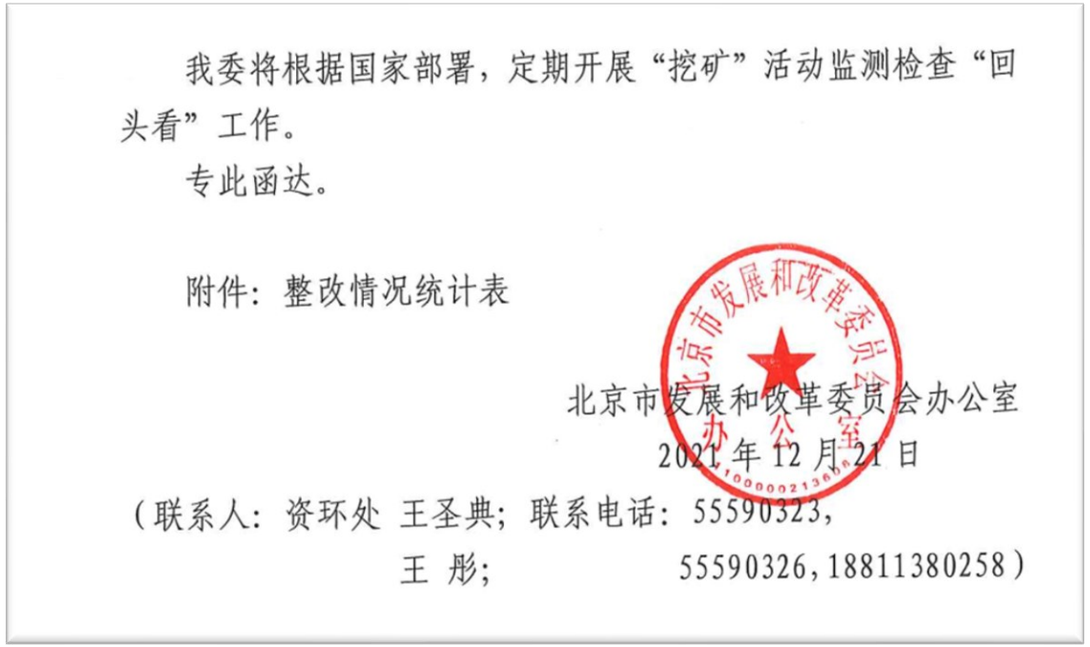


北京市发展和改革委员会办公室

关于核实整治涉及虚拟货币“挖矿”情况的函

各有关单位：

近期，国家发展改革委等11部门发布《关于整治虚拟货币“挖矿”活动的通知》（发改运行〔2021〕1283号，以下简称“1283号文”），按照相关要求，现会同有关单位组织开展虚拟货币“挖矿”活动的整治工作。根据国家有关部门转来情况，发现你单位



我委将根据国家部署，定期开展“挖矿”活动监测检查“回头看”工作。

专此函达。

附件：整改情况统计表

北京市发展和改革委员会办公室

2021年12月21日

（联系人：资环处 王圣典；联系电话：55590323，

王 彤；55590326，18811380258）

- 为保护社会公众的财产权益，保障人民币的法定货币地位，防范洗钱风险，维护金融稳定，2013年12月5日，央行等五部委联合发布了《关于防范比特币风险的通知》。
- 2016年到2018年之间，代币暗藏的商机被资本们发现，一时间引爆金融市场，包括2017年受重挫的P2P金融产业在内，很多公司都转型开始做起了代币生意，也因此，国内涌现了大批的“空气币”，疯狂收割国民财富，割完就跑，一片云彩都没留下。基于此，2017年9月4日，央行联合银监会等七大部门发布关于防范代币发行融资风险的公告。
- **2021年9月24日，中国人民银行发布进一步防范和处置虚拟货币交易炒作风险的通知。通知指出，虚拟货币不具有与法定货币等同的法律地位**

部分“挖矿”的通报

案例一：利用办公电脑“挖矿”，受到党内警告处分

绍兴市上虞区职业教育中心机房管理员丁某某伙同劳务派遣人员何某某，利用办公电脑并购置3台“矿机”放置于信息技术楼，从事挖取渡鸦币活动累计111天，获利1.5万元，丁某某受到党内警告处分并扣除绩效考核奖3个月；何某某被解聘。湖州市德清县自然资源和规划局下属事业单位地理信息中心副主任虞某及工作人员吴某某利用办公电脑“挖矿”，分别挖得以太币0.03枚、0.76枚（查获时该币价值为每枚22560元），虞某受到批评教育，责令作出检查，并扣除一个季度绩效考核奖金，吴某某受到党内警告处分并扣除三个季度绩效考核奖金。（案例来源：中央纪委国家监委网站）

案例二：使用公司服务器“挖矿”，获刑三年

从“挖矿”、变现到被判3年，一位百度员工在短短7个月内走完了这三部曲。“挖矿”用的是百度的搜索服务器，在最近公布的一份裁判文书中，公布了百度运维安某的“薅羊毛”细节。从2018年1月底到5月底，安某薅了155台服务器的羊毛，用来挖比特币、门罗币，卖掉一部分之后获利10万元。但事发之后，不仅这笔钱被没收，还额外被罚了11000元，另外还有3年的有期徒刑。近日，中国裁判文书网公布刑事裁定书，披露了案件细节。（案例来源：雪球网）

案例三：制作植入“挖矿”代码的游戏软件，获刑一年

不仅仅是国内开展了整治虚拟货币非法“挖矿”行为，在其他国家非法“挖矿”也会受到处罚。据日媒《河北新报》报道，日本2018年7月3日宣判了首例因恶意利用他人电脑“挖矿”的案例。犯罪者是庫県尼崎市的无业者安田成利（24岁），他向一款游戏作弊软件内植入了“挖矿”代码，并将该软件挂到自己博客上供人下载，使用该软件的人就会在不知情的情况下，为安田“挖矿”。截止被查获，该软件一共下载了90次，安田共获利5000日元（约合人民币300元）。法院判处安田成利1年有期徒刑，缓期三年执行，法官加藤亮称“被告利用技术的巧妙犯罪伤害了人们对计算机程序的信任”。

个人“挖矿”行为不是盲区，国家对虚拟货币“挖矿”的监管不留死角，直至达到虚拟货币“挖矿”清零的目标。广大师生要时刻树牢安全意识、遵纪守法，杜绝主动“挖矿”，避免因感染病毒等原因导致被动“挖矿”。学校成立了工作专班严肃查处整治虚拟货币“挖矿”行为，定期对监测发现的违规违纪行为进行通报。

(文内图片来自网络)

2022-03-21	网信办、网络与计算中心 华中科技大学 新闻网	“挖矿”危害大，违法代价高——虚拟货币“挖矿”警示案例解析 http://news.hust.edu.cn/info/1003/44124.htm https://open.work.weixin.qq.com/wwopen/mpnews?mixuin=tgMyCgAABwCm-tOhAAAUAA&mfid=WW0321-VjvtAAAABwAGdy1tFrkaDwpTrDr63&idx=0&sn=8662a17ea090e6162538438081e4f960&notreplace=true

02

如何查询挖矿主机

挖矿排查

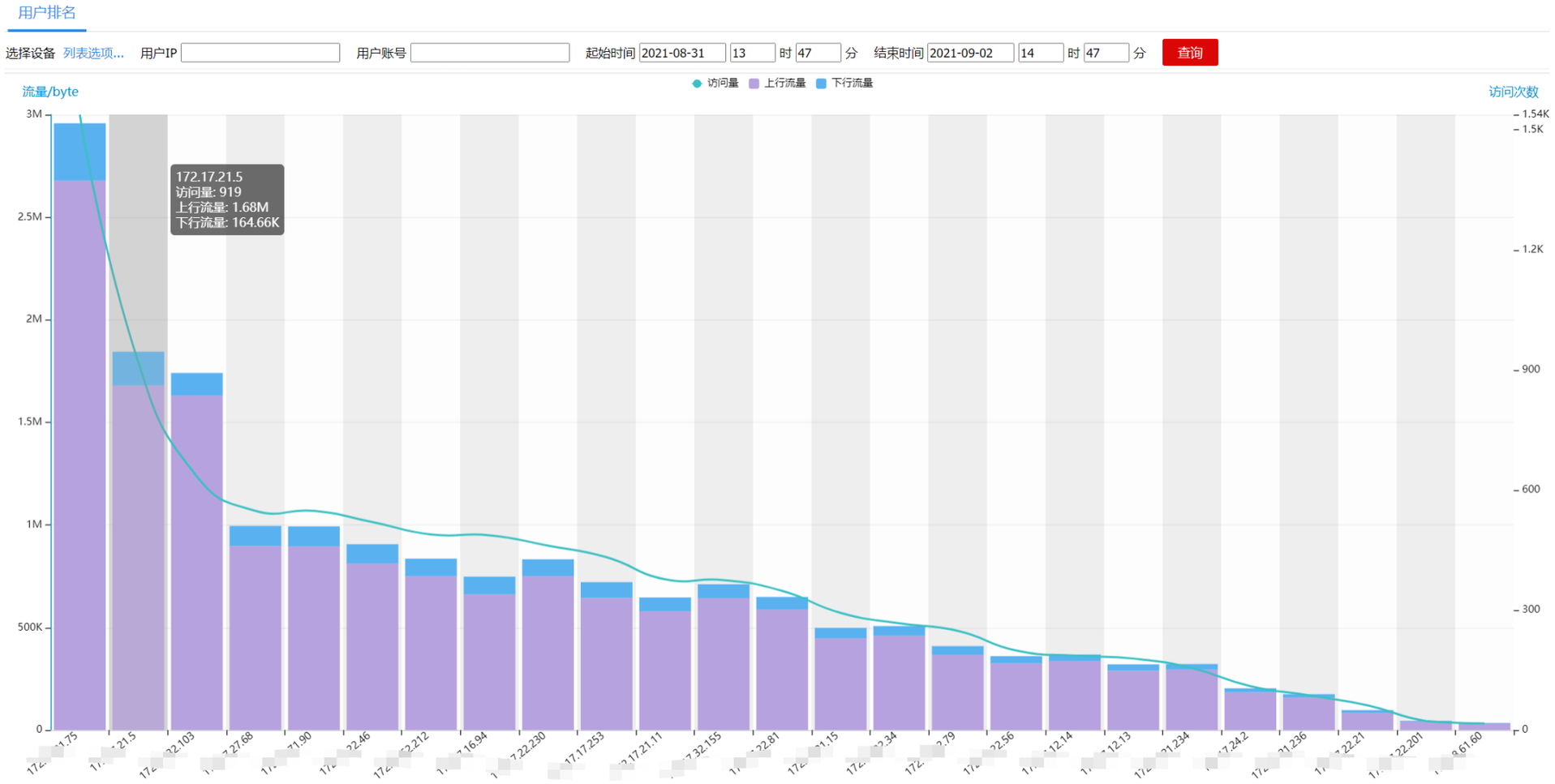
由于挖矿行为有2大类，挖矿排查也分为两种(DPI排查和威胁情报排查)。

1、在Panalog中【内容分析】-【虚拟货币】中查询，基于虚拟货币的协议锁定（主要针对挖矿软件）。

2、在Panalog中【安全分析】-【威胁情报】中查询，先定位威胁情报中挖矿域名或者IP，然后再查询内网IP用户。（主要针对网页脚本挖矿）

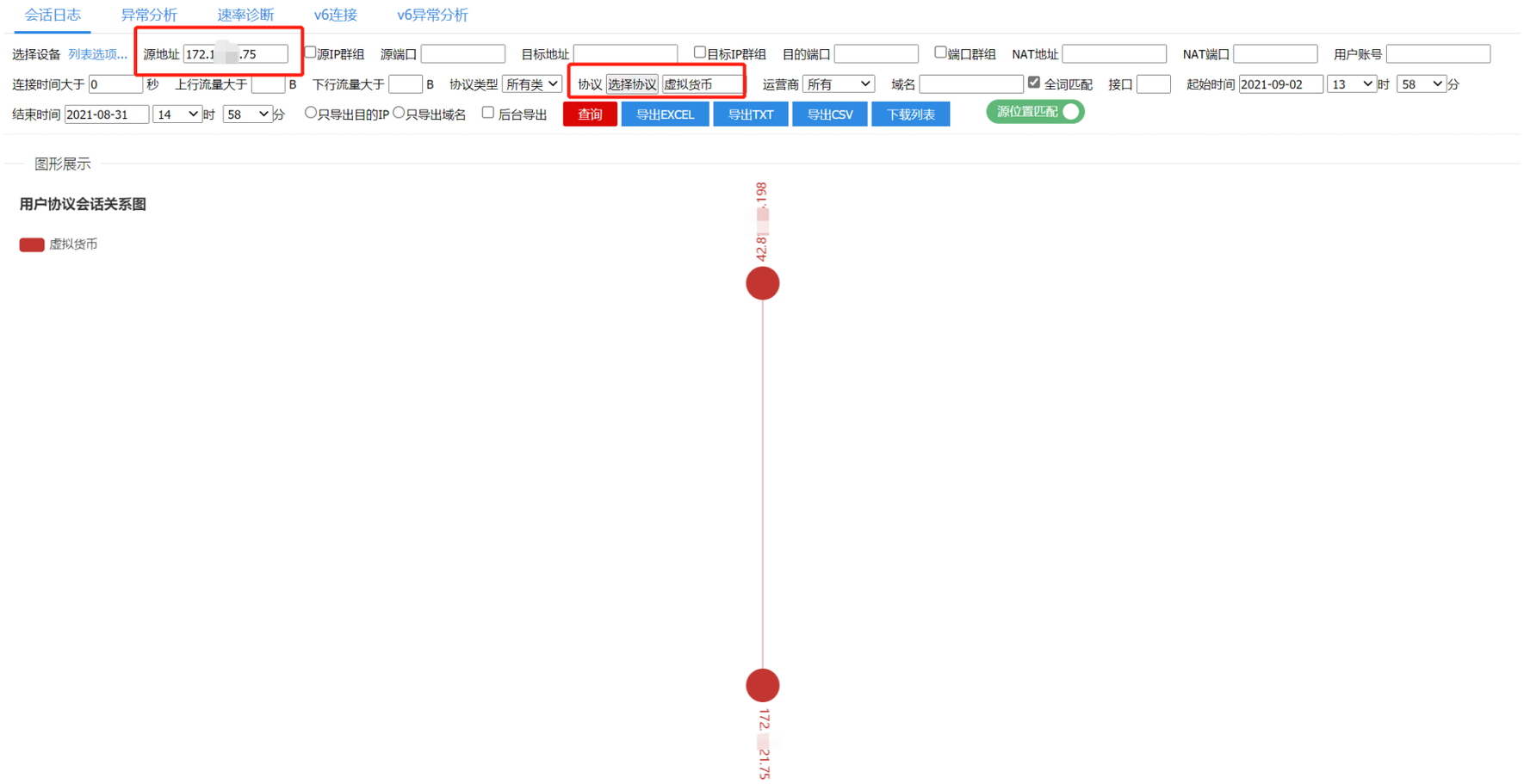
挖矿排查方法1—DPI排查

在【虚拟货币】中直接选中某一个时间段查询，凡是排名靠前、上行流量明显高于下行流量、上行流量速率超过1M的IP地址为主要排查对象。可以在页面中导出IP地址列表。



挖矿排查方法1—DPI排查

在【会话日志】中选择排名第一的IP地址作为源IP，协议选择“虚拟货币”，进行查询



挖矿排查方法2—威胁情报排查

Panabit®

系统升级

升级之后，如果页面没有任何变化或者显示比较杂乱，请清除浏览器缓存后重新登录，或者使用快捷键CTRL+F5进行页面强制刷新。

LOG升级最新版本

当前版本：流量分析管理系统 MARS(火星)r10p5Cluster，创建于2021/12/06 16:58:00 [FreeBSD_11.1]

选择文件

威胁情报升级到最新版本

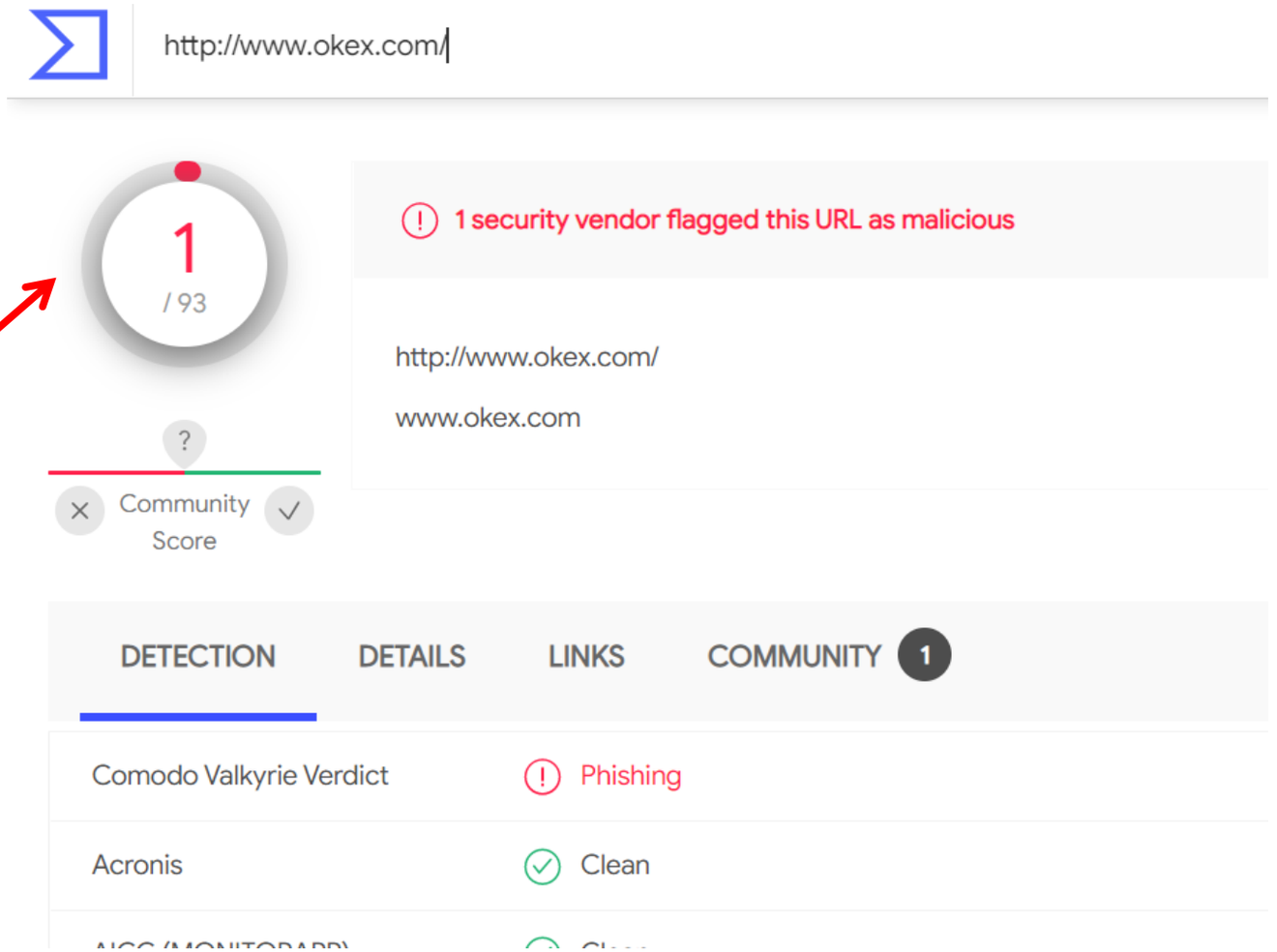
挖矿排查方法2—威胁情报排查

在【安全分析】【威胁情报】中查询，在类别中输入挖矿应用类别“bitcoin”如下所示：

序号	URL	访问次数	类别	来源
1	k1pool.com/ 情报校验	1645	bitcoin	Panabit
2	www.okex.com/ 情报校验	741	bitcoin	Panabit
3	asia2.ethermine.org/ 情报校验	163	bitcoin	Panabit
4	cn.eth.k1pool.com/ 情报校验	52	bitcoin	Panabit
5	crypto.com/ 情报校验	28	bitcoin	Panabit
6	us1.ethpool.org/ 情报校验	26	bitcoin	Panabit
7	freebitco.in/ 情报校验	16	bitcoin	Panabit

威胁情报由派网合作伙伴天际友盟提供

挖矿排查方法2—威胁情报排查



通过威胁情报查询出的域名，可以点击“情报校验”到VT网站上进行核实。

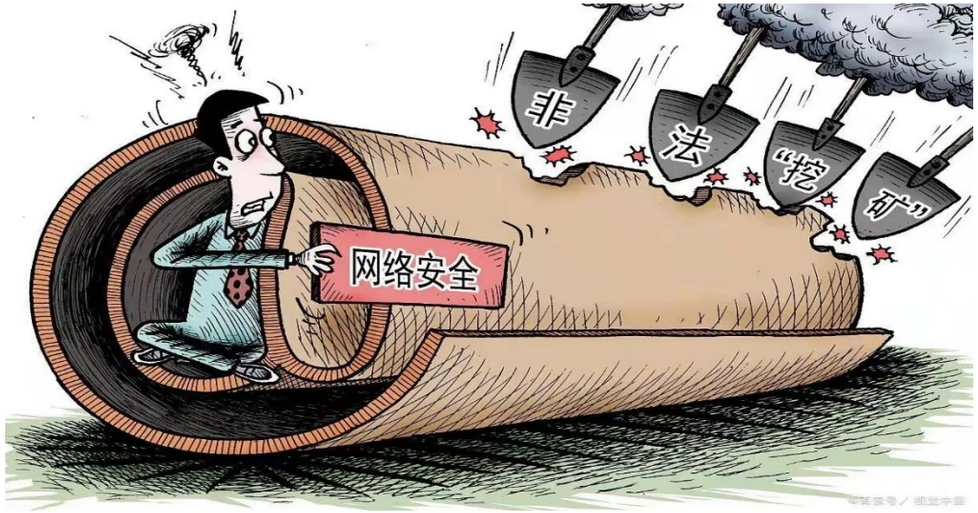
挖矿排查方法2—威胁情报排查

点击对应的域名，便可以看到内网那些用户访问过这些域名，以及访问的次数。

03

如何阻断挖矿应用

挖矿行为阻断



阻断方案1：基于“虚拟货币”协议识别的阻断

阻断方案2：通过矿池黑名单HTTP阻断策略

阻断方案3：基于挖矿域名的DNS解析管控策略

阻断方案4：基于动态威胁情报的管控策略

挖矿行为阻断1—通过DPI阻断

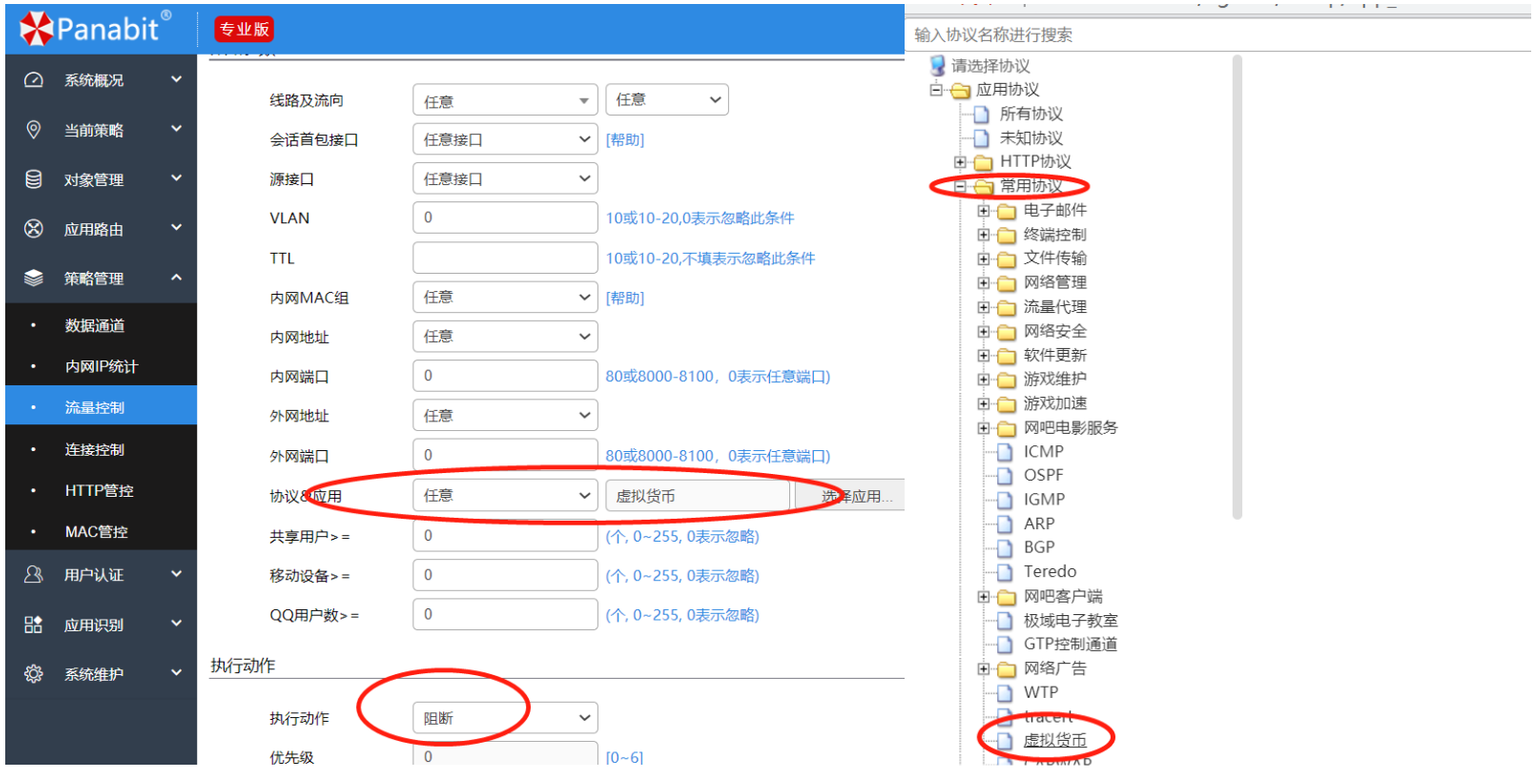
阻断方案：

基于虚拟货币协议识别的阻断，主要用于挖矿软件的阻断

配置方式：

1. 通过【流量控制策略】，将“虚拟货币”作为流量控制匹配条件。

2. 配置阻断动作为“丢弃”，实现对挖矿应用流量进行阻断



挖矿行为阻断2—通过矿池黑名单阻断（域名+IP）

阻断方案：

通过矿池黑名单阻断，黑名单有一些是域名，也有一些是IP地址。

配置方式：

1. 创建矿场的“域名群组”。

2. 通过【HTTP管控策略】，创建的 “虚拟货币域名群组”作为流量管控的匹配条件。

3. 配置阻断动作为“丢弃”，实现对挖矿应用流量进行阻断

挖矿行为阻断3—基于矿池黑名单DNS管控（域名）

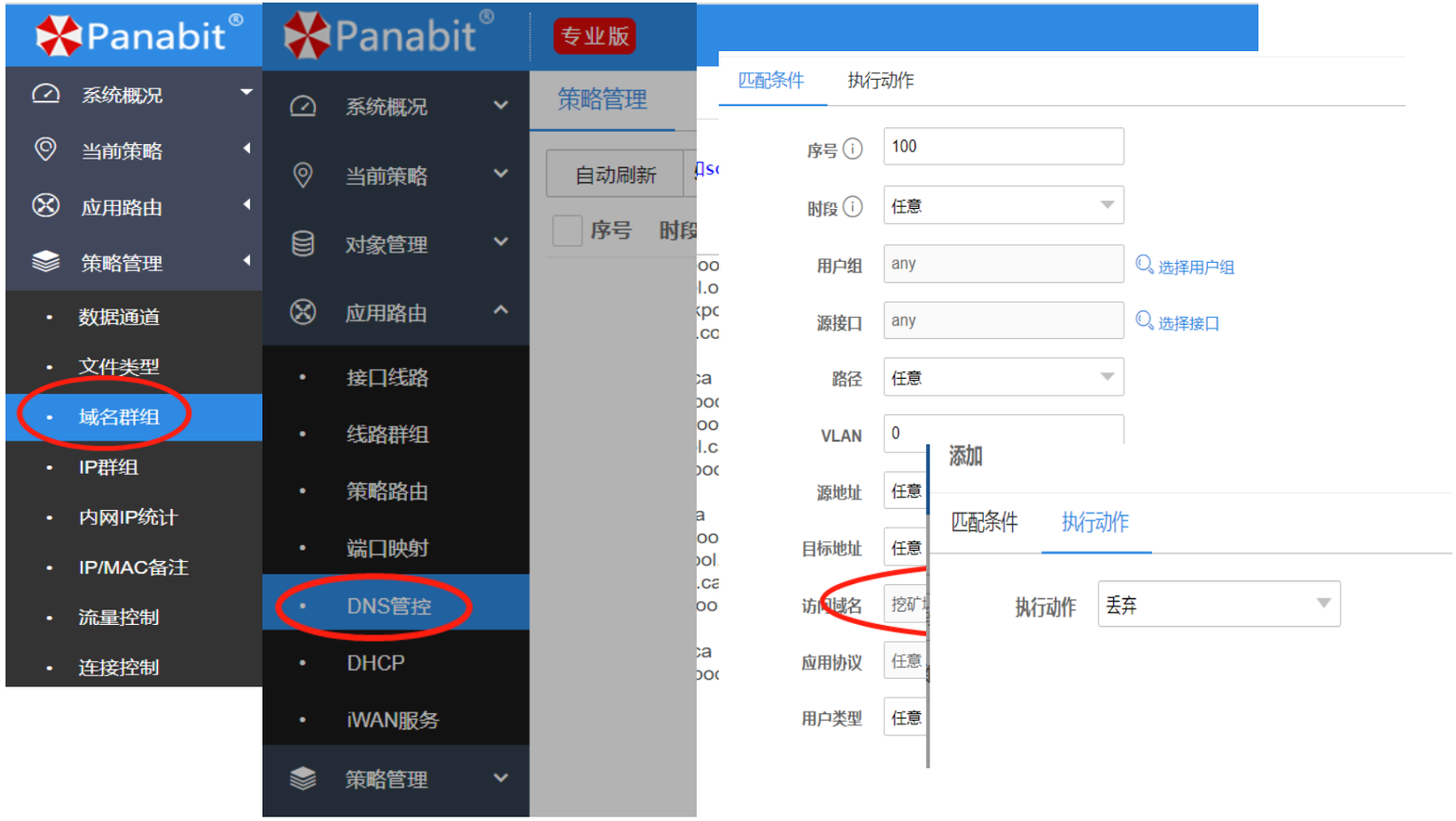
阻断方案：

基于挖矿域名的DNS解析策略

防止由于DNS解析导致的通报。

配置方式：

1. 创建矿场的“域名群组”。
2. 通过【DNS管控】，创建的 “虚拟货币域名群组”作为流量管控的匹配条件。
3. 配置阻断动作为“丢弃”，实现对挖矿应用流量进行阻断



挖矿行为阻断4— 动态威胁情报

阻断方案：

基于动态威胁情报的挖矿Http管控策略

配置方式：

1. 通过APP来动态获得挖矿域名。首先需要安装“威胁情报IOCs同步”APP，然后进行情报同步。
2. 情报同步后，在域名群组就可以看到相关的威胁情报域名。
3. 通过【DNS管控】、【HTTP管控】，策略中进行配置匹配策略。
4. 配置阻断动作为“丢弃”，实现对挖矿应用流量进行阻断

【严重度说明】：
H：高严重度，建议执行“阻断”策略
M：中严重度，建议执行“告警”策略
L：低严重度，建议执行“提示”策略

挖矿行为阻断4— 动态威胁情报

阻断方案：

基于动态威胁情报的挖矿Http管控和DNS管控策略

配置方式：

1. 通过APP来动态获得挖矿域名。首先需要安装“威胁情报IOCs同步”APP，然后进行情报同步。
2. 情报同步后，在域名群组就可以看到相关的威胁情报域名。
3. 通过【DNS管控】、【HTTP管控】，策略中进行配置匹配策略。
4. 配置阻断动作为“丢弃”，实现对挖矿应用流量进行阻断

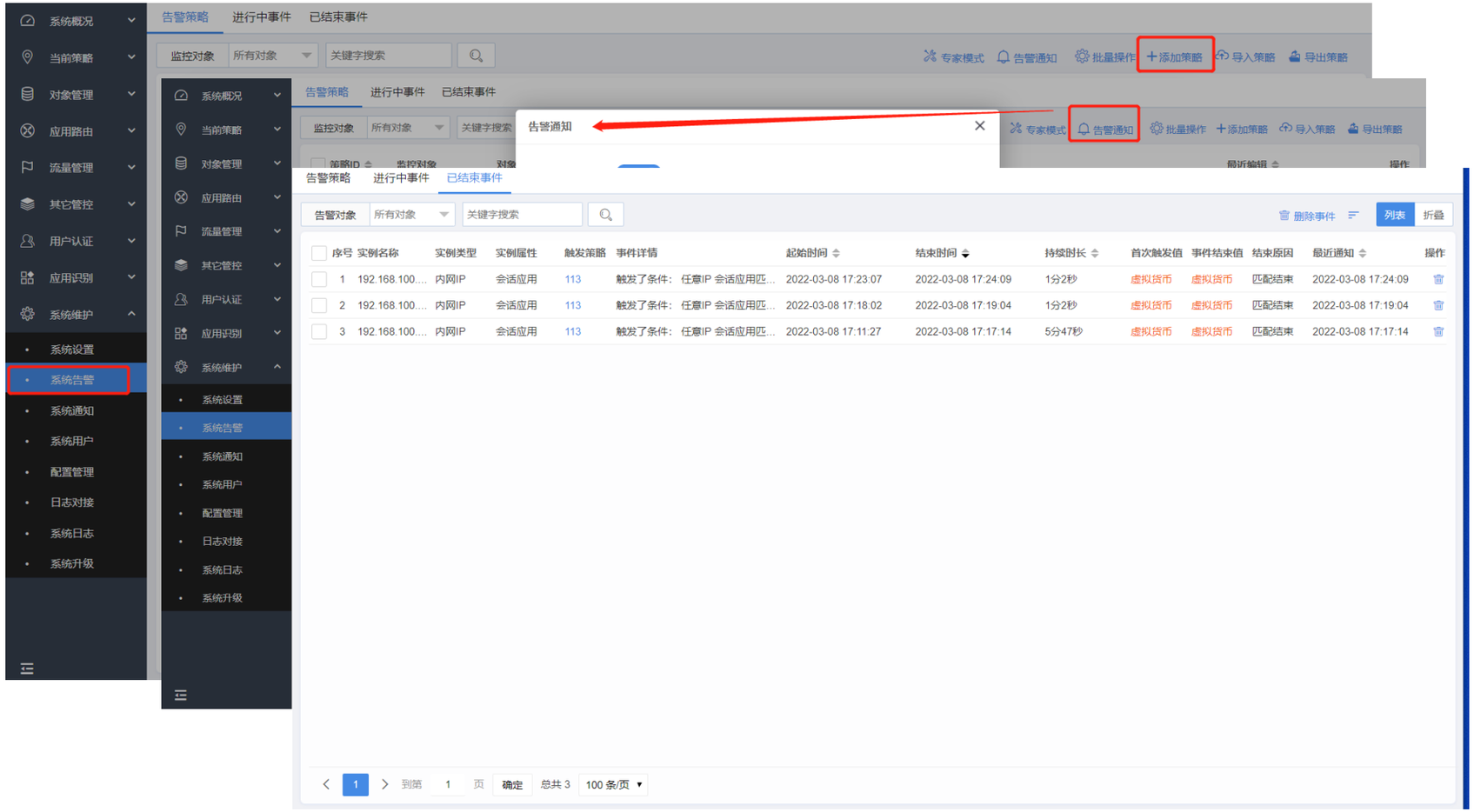
挖矿行为告警— 可通过微信，钉钉，邮件等通知

挖矿告警：

基于“虚拟货币”规则检测的告警

配置方式：

1. 在【系统告警】中添加“虚拟货币”的告警策略。
2. 设置告警通知方式，可支持微信公众号通知，企业微信通知，钉钉通知，邮件通知等方式、。



其他说明

问题1：

我校已经通过DNS服务器的域名黑名单作了挖矿阻断，还需要派网上作阻断策略吗？

回答：需要

1. 矿池是动态，因此相关黑名单也必须是动态的，矿池库需要不断更新。
2. 矿池有的是域名，有的是IP地址，DNS服务器只能针对于域名来作策略，无法针对IP地址。
3. 校内有一些用户喜欢手工配置DNS，例如：114.114.114.114,8.8.8.8之类的公网DNS，在校内DNS服务器作策略，无法对这些用户生效。
4. 审计的需要。挖矿阻断后，我们仍然需要内网有哪些用户存在挖矿行为，因此，需要分析阻断日志，发现内网IP和用户。

其他说明

问题2

派网产品作挖矿阻断时候，产品如何部署？

回答：

推荐部署模式：网关或者网桥，可以通过HTTP管控、DNS管控全面对挖矿行为进行阻断；

旁路部署：可以通过TCP RST对挖矿域名和IP进行重置，从而达到阻断的挖矿的目的。但无法对挖矿的DNS请求进行阻断（因为DNS请求是UDP报文）

其他说明

问题3

通过威胁情报，除了可以对挖矿行为进行发现和阻断，还可以实现啥功能呢?

回答:

派网设备配合不同类别的威胁情报，实现的功能也不一样。具体如下:

数字货币	包括矿池地址、矿池域名和IP信息，用于检测内部终端的挖矿行为。
C&C节点	包含各种恶意软件回连的命令&控制端IP地址等信息,用于检测内部失陷或受控终端。
恶意软件	包含检测后门、间谍软件、欺诈软件等各种恶意软件相关的域名和IP地址。
恶意软件下载	包含直接或隐藏下载各类恶意软件的网站链接，用于检测内部终端下载恶意代码的行为。
僵尸网络	包含被僵尸网络控制的IP信息。
Tor节点	包含Tor服务器节点信息，用于检测内部终端与Tor网络的通信行为。
Proxy节点	包含Proxy服务器节点信息，用于检测内部是否有人通过海外代理访问。

THANK YOU