

哈尔滨工程大学信息化处文件

信息化处发〔2022〕 20 号

关于印发《虚拟货币“挖矿”行为日常监测与 处置规范》的通知

各办公室：

《虚拟货币“挖矿”行为日常监测与处置规范》经 2022 年第 14 次处长办公会讨论通过，现印发给你们，请认真贯彻执行。

哈尔滨工程大学信息化处
2022 年 6 月 8 日



虚拟货币“挖矿”行为日常监测与处置规范

为有效遏制校内虚拟货币“挖矿”行为的发生，营造安全有序的校园网络环境，保障 IDC 数据中心的运行环境安全，实现对虚拟货币“挖矿”行为的日常监测分析、阻断及溯源，特制订本规范。

第一章 日常监测与处置工作 AB 角负责人

（一）IDC 数据中心日常监测与处置的 AB 角负责人

1. 通过 IDC 流量日志分析系统进行“挖矿”行为监测：

A 角-孙彦飞、B 角-徐千

2. 通过网络威胁感知系统进行“挖矿”行为监测：

A 角-孙璟瑶、B 角-孙彦飞

3. 通过 IDC 网络威胁检测系统进行“挖矿”行为监测：

A 角-孙彦飞、B 角-孙璟瑶

4. 通过 DNS 系统进行“挖矿”行为阻断：

A 角-王建、B 角-孙彦飞

5. 通过 IDC 防火墙进行“挖矿”行为阻断：

A 角-孙彦飞、B 角-徐千

6. 通过 IDC 流量日志分析系统和 DNS 系统进行“挖矿”行为溯源：

A 角-孙彦飞、B 角-王建

(二) 校园网日常监测与处置的 AB 角负责人

1. 通过校园网流量日志分析系统进行“挖矿”行为监测:

A 角-高岩、B 角-刘振广

2. 通过校园网网络威胁检测系统进行“挖矿”行为监测:

A 角-高岩、B 角-刘振广

3. 通过校园网认证计费系统、防火墙及流控设备全方位进行“挖矿”行为阻断:

A 角-高岩、B 角-刘振广

4. 通过校园网流量日志分析系统和流量用户会话日志分析监测系统进行“挖矿”行为溯源:

A 角-高岩、B 角-刘振广

第二章 日常监测周期

由 IDC 数据中心和校园网 AB 角负责人联合进行“挖矿”行为日常监测,早(8:00-8:30)、中(11:00-11:30)、晚(16:30-17:00)分别监测上一时间段是否存在“挖矿”行为,同时将疑似“挖矿”行为信息报送至 IT 安全部。

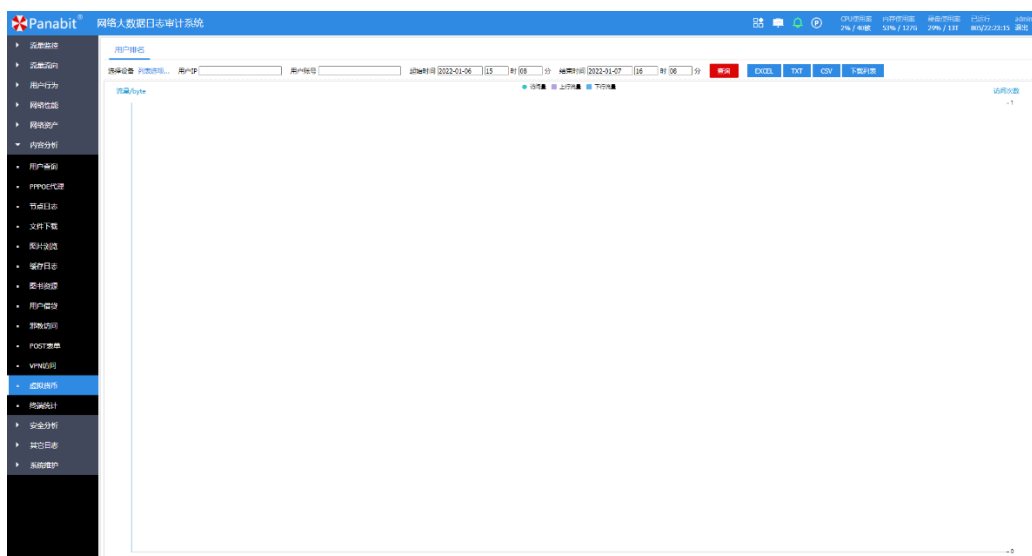
第三章 虚拟货币“挖矿”行为监测

(一) IDC 数据中心“挖矿”行为监测

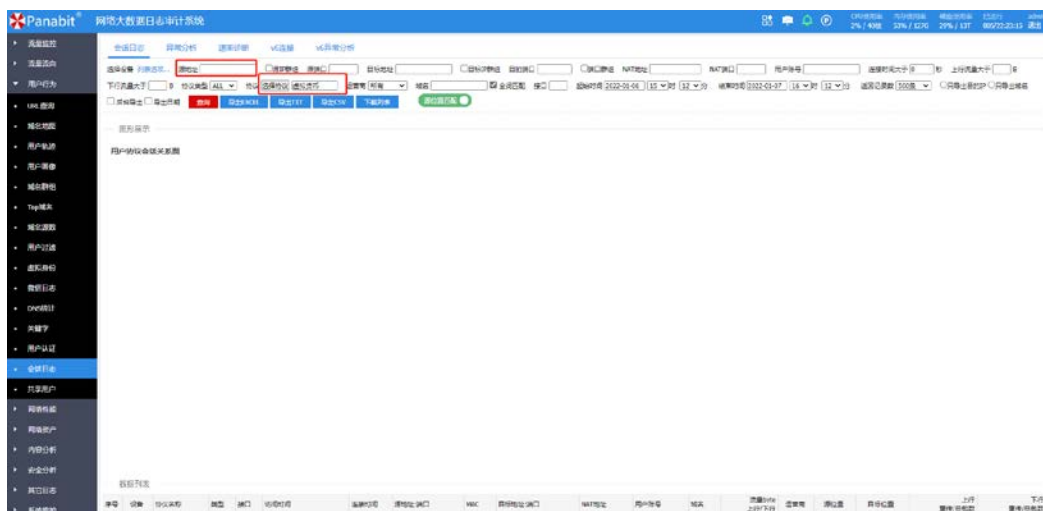
1. 通过 IDC 流量日志分析系统进行“挖矿”行为查询如下:

方式一：

(1) 在 IDC 流量日志分析系统的“内容分析”-“虚拟货币”模块中查询，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，查询疑似使用虚拟货币应用的 IP 地址。

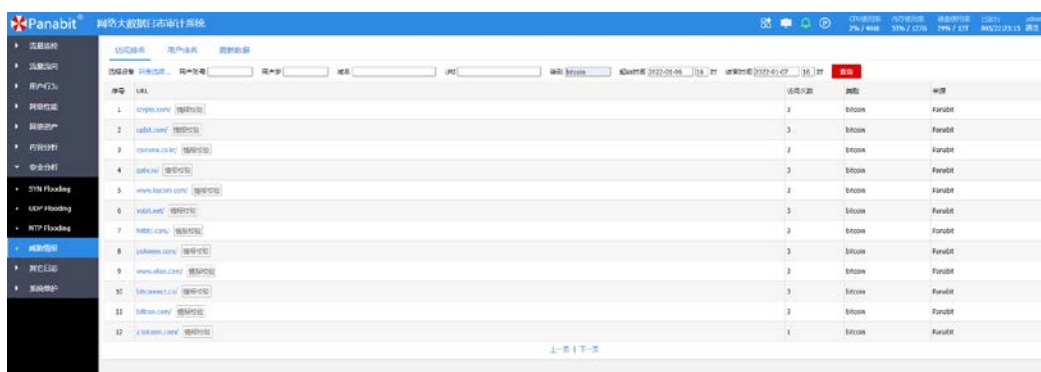


(2) 在“会话日志”模块中根据步骤 1 排查的 IP 地址作为源 IP，协议选择“虚拟货币”，查询此 IP 地址访问信息详情。



方式二：

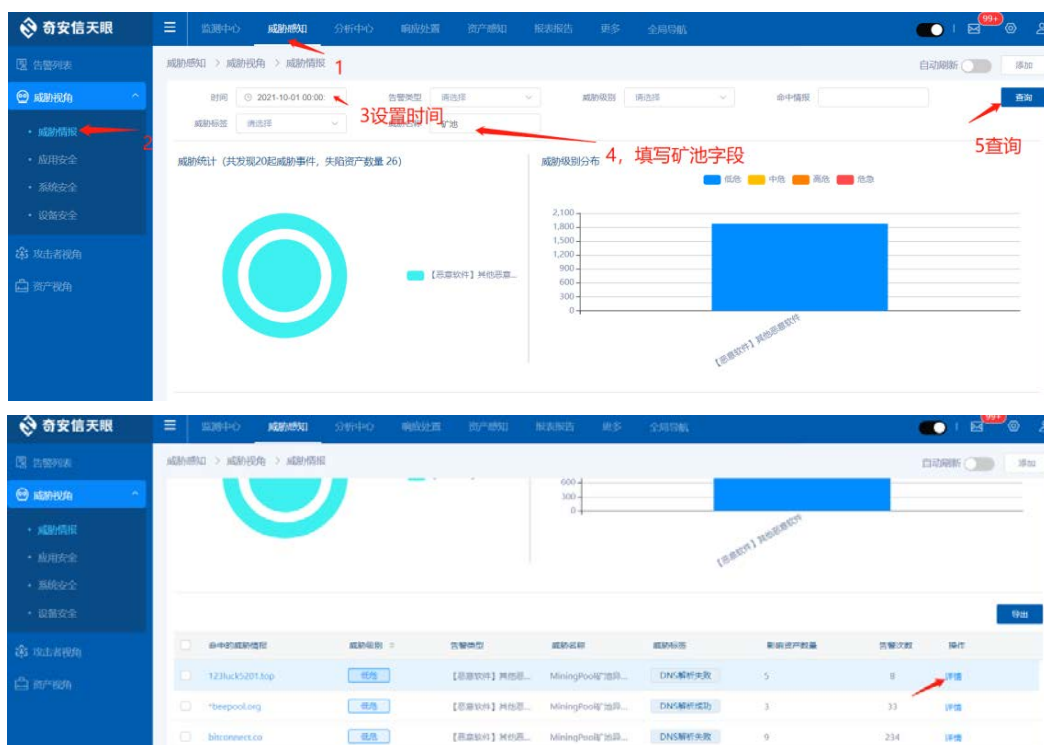
在 IDC 流量日志分析系统“安全分析”-“威胁情报”模块中查询，类别中输入挖矿应用类别“bitcoin”，先定位威胁情报中挖矿域名或者 IP，然后再查询内网 IP 用户。



序号	URL	域名	威胁	来源
1	cryptocoin.com	挖矿应用	3	Bitcoin
2	cryptocoin.com	挖矿应用	3	Bitcoin
3	cryptocoin.com	挖矿应用	3	Bitcoin
4	cryptocoin.com	挖矿应用	3	Bitcoin
5	cryptocoin.com	挖矿应用	3	Bitcoin
6	cryptocoin.com	挖矿应用	3	Bitcoin
7	cryptocoin.com	挖矿应用	3	Bitcoin
8	cryptocoin.com	挖矿应用	3	Bitcoin
9	cryptocoin.com	挖矿应用	3	Bitcoin
10	cryptocoin.com	挖矿应用	3	Bitcoin
11	cryptocoin.com	挖矿应用	3	Bitcoin
12	cryptocoin.com	挖矿应用	1	Bitcoin

2. 通过网络威胁感知系统进行“挖矿”行为查询如下：

(1) 在网络威胁感知系统的“威胁感知”-“威胁视角”-“威胁情报”模块中查询，失陷的威胁为主要排查对象。



(2) 查看涉及此威胁情报的详情，确认哪些是受害资产。

123luck5201.top

威胁情报详情 受害资产列表 告警列表

标记已读 标记未读 请选择批量变更事件状态的: ▾

导出

☐	最近发生时间	受害IP	攻击IP	告警类型	威胁名称	攻击结果	操作
☐	2021-10-13 17:00:31	219.229.203.124		【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白
☐	2021-10-13 16:36:12	219.229.204.218		【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白
☐	2021-10-13 16:24:47	219.229.198.129		【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白
☐	2021-10-13 15:28:46	219.229.195.101		【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白

共 4 条 10条/页 < 1 > 前往 1 页

关闭

(3) 通过告警列表中的受害 IP，查看受害资产。

123luck5201.top

威胁情报详情 受害资产列表 告警列表

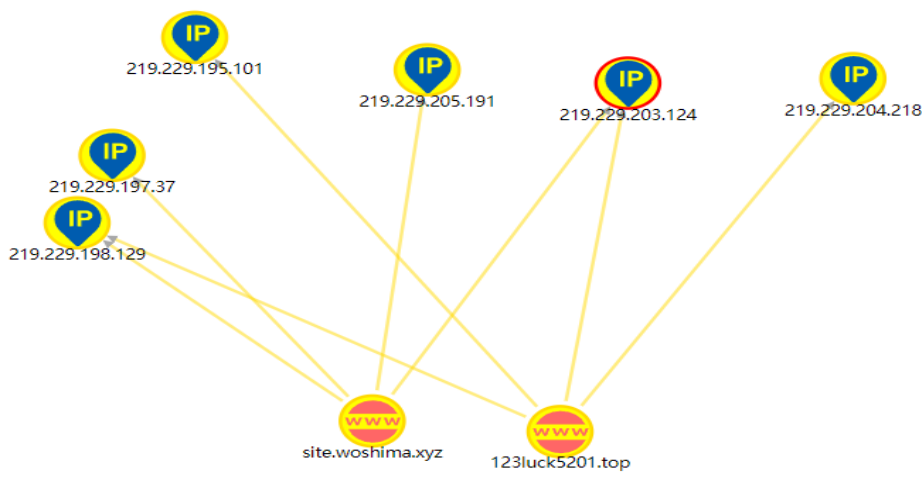
标记已读 标记未读 请选择批量变更事件状态的: ▾

导出

☐	最近发生时间	受害IP	攻击IP	告警类型	威胁名称	攻击结果	操作
☐	2021-10-13 17:00:31	219.229.203.124		【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白
☐	2021-10-13 16:36:12			【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白
☐	2021-10-13 16:24:47			【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白
☐	2021-10-13 15:28:46	219.229.195.101		【恶意软件】其他恶意软件	MiningPool挖矿异...	失败	详情 处置 加白

共 4 条 10条/页 < 1 > 前往 1 页

(4) 通过攻击测绘详细查看哪些资产 IP 访问过此矿池域名。



(5) 通过 ti.qianxin.com 进行研判。

123luck5201.top IOC反查

MiningPool C&C

流行度	★★★★★	最近看到	-	注册人	-	主办单位名称	-
动态域名	否	域名注册时间	-	注册人所属组织	-	主办单位性质	-
隐私保护	否	注册更新时间	-	管理员邮箱	-	网站备案/许可证号	-
白名单	否	注册过期时间	-	国家	-	备案审核时间	-

相关安全报告: 没有数据

威胁情报 (2) 域名解析 注册信息 (0) 关联域名 数字证书 AI判定 网页结果

开源情报

情报源	最近看到	威胁类型
USS2.0	2021/12/07	远程及命令服务器

(6) 针对 IOC 和“挖矿”这种 DGA 域名威胁，存在两种情况：

第一种是只有解析行为，但是没有解析成功，这种情况应高级关注，有可能是资产已经存在恶意软件，但是 IOC 威胁告警的

域名未启用解析,所以没成功,后期攻击者启用此域名解析就会产生通讯流量。

第二种情况,就是已经有通信行为,受害资产已经与矿池产生了通信,说明“挖矿”行为正在进行,需要排查一下资产的进程与网络连接情况,清理“挖矿”木马等恶意软件。

3. 通过 IDC 网络威胁检测系统进行“挖矿”行为查询如下:

在 IDC 网络威胁检测系统的“事件分析”-“威胁分析”-“威胁事件”模块中查询。选择好“时间范围”后,在“检索条件”里面搜索挖矿相关的关键词(首字母大写,并用||隔离开),常搜索的关键词如下: Xmrig || Miner || Minepool1, 多条件聚合检索。



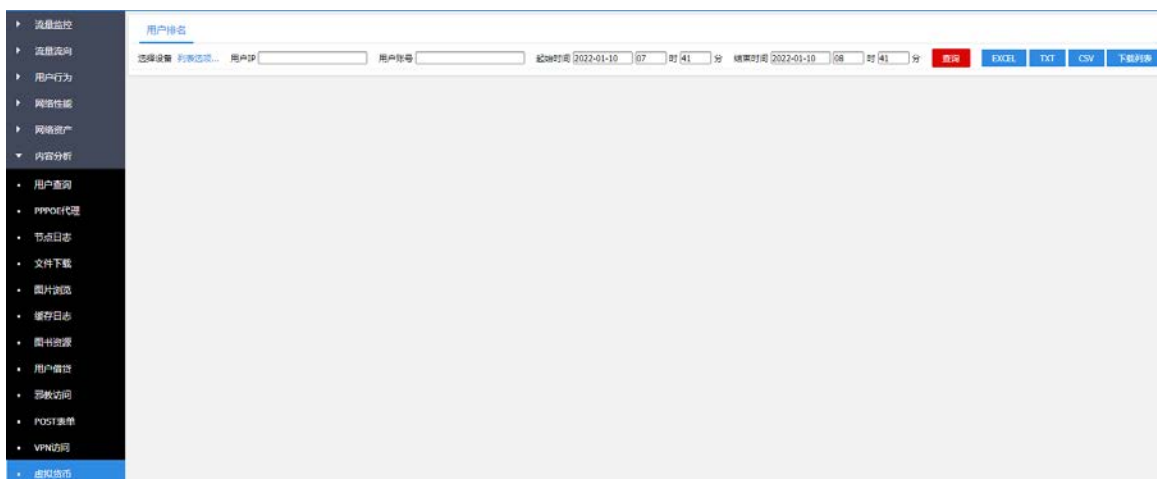
(二) 校园网“挖矿”行为监测

我校所有校园网用户上网行为都经过流控设备(Panabit),

已将流控设备日志全部导入到 PanabitLog 设备（校园网流量日志分析系统）中，在该设备中可以进行“挖矿”行为查询。

1. 通过校园网流量日志分析系统进行“挖矿”行为查询如下：
方式一：

（1）在校园网流量日志分析系统的“内容分析”-“虚拟货币”模块中查询，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，查询疑似使用虚拟货币应用的 IP 地址。

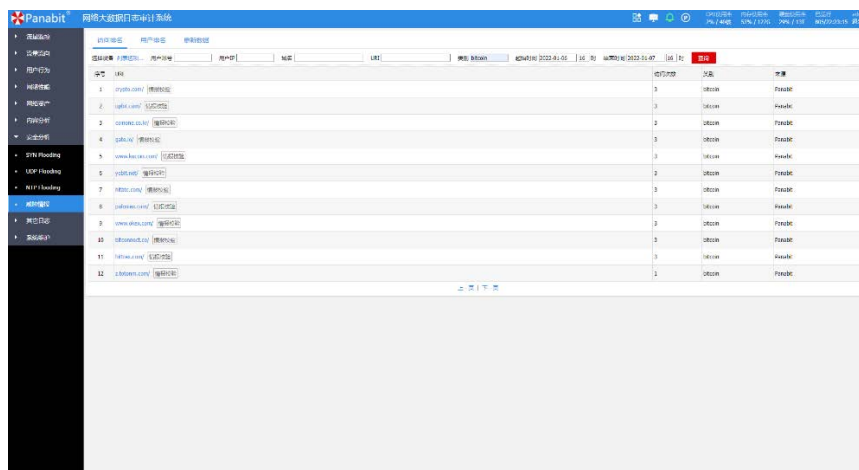


（2）在“会话日志”模块中根据步骤 1 排查的 IP 地址作为源 IP，协议选择“虚拟货币”，查询此 IP 地址访问信息详情。



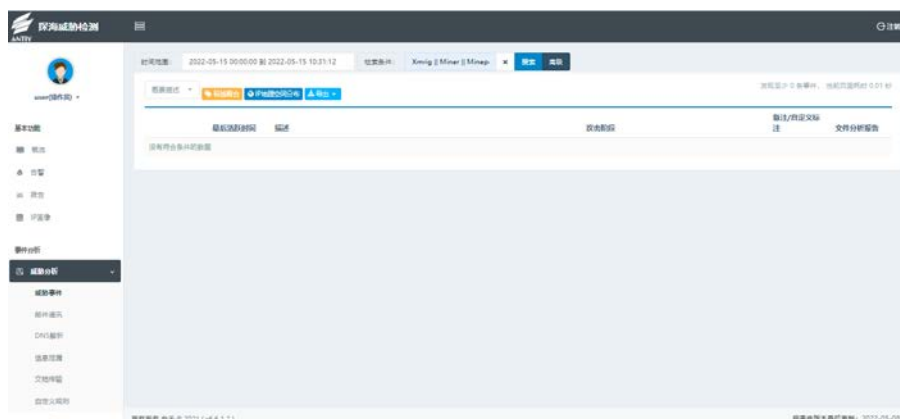
方式二：

在 IDC 流量日志分析系统“安全分析”-“威胁情报”模块中查询，类别中输入挖矿应用类别“bitcoin”，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。



2. 通过校园网网络威胁检测系统进行“挖矿”行为查询如下：

在校园网网络威胁检测系统的“事件分析”-“威胁分析”-“威胁事件”模块中查询。选择好“时间范围”后，在“检索条件”里面搜索挖矿相关的关键词(首字母大写,并用||隔离开),常搜索的关键词如下: Xmrige || Miner || Minepool, 多条件聚合检索。

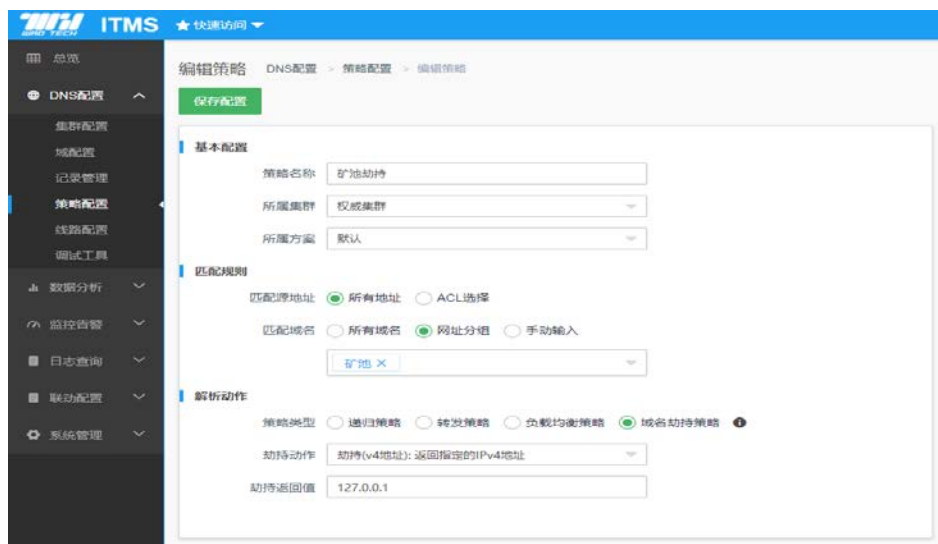


第四章 虚拟货币“挖矿”行为阻断

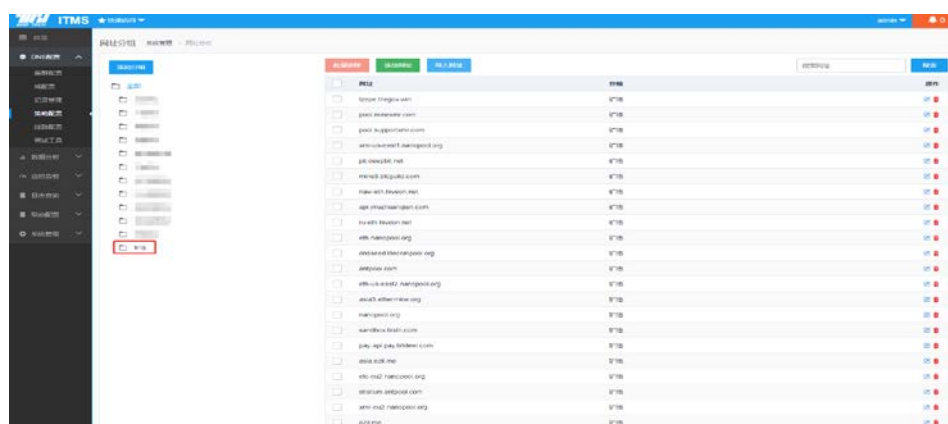
（一）IDC 数据中心“挖矿”行为阻断

1. 通过 DNS 系统进行“挖矿”域名劫持，步骤如下：

(1)在 DNS 系统策略配置中新增矿池阻断策略,对“挖矿”域名进行 DNS 劫持,用户访问“挖矿”域名劫持返回为 127.0.0.1,阻断网络传输。

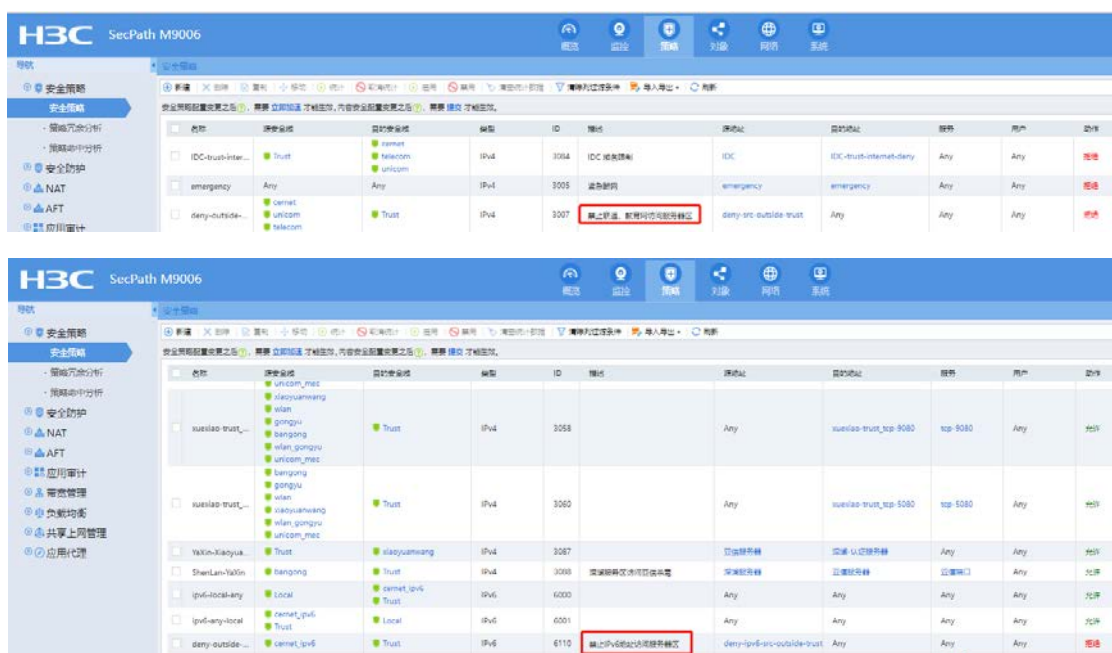


(2) 对于新增“挖矿”域名同步更新至矿池劫持策略, 保证进一步预防“挖矿”行为的发生。



2. 通过 IDC 防火墙阻断访问“挖矿”域名的 IP 地址访问 IDC 服务器区，步骤如下：

根据安全公司每日监测，提供访问“挖矿”域名的 IP 地址，直接在防火墙的“安全策略”模块内禁止此类 IP 地址访问 IDC 服务器区。



(二) 校园网“挖矿”行为阻断

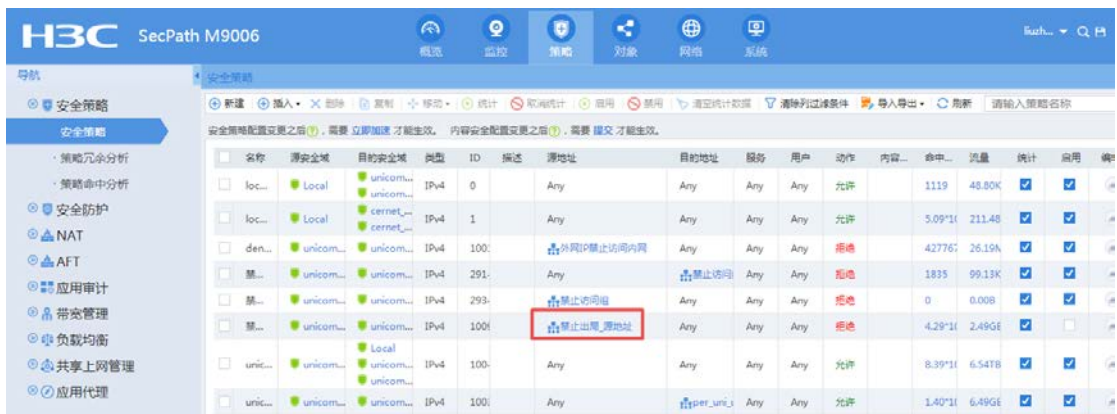
方式一：

根据查询，IT 安全部现场排查进行确认，确认用户确实存在违规行为之后，针对非固定 IP 用户，直接在校网认证计费系统禁用用户账号，待 IT 安全部检查用户整改完成后，通知可以开通时，再开通。



方式二：

根据查询，IT 安全部现场排查进行确认，确认用户确实存在违规行为之后，针对固定 IP 用户，直接在防火墙禁止 IP 出校园网，待 IT 安全部检查用户整改完成后，通知可以开通时，再放行。



方式三：

根据安全公司提供的“挖矿”行为阻断方式及“挖矿”域名，进行了 DNS 管控、HTTP 管控和流量控制的方式进行了全局阻断。

通过在域名群组模块添加已经确定为“挖矿”的域名，进行 DNS 劫持。

Panabit 专业版														
策略管理 QPS 策略														
序号	时段	源地址	源端口	目标地址	目标端口	应用协议	用户类型	执行动作	策略ID	策略名称	策略状态	策略描述	策略备注	策略操作
5	any	any	any	any	any	图书馆U...	any	any	any	any	any	any	any	any
8	any	any	any	any	any	图书馆U...	any	any	any	any	any	any	any	any
100	any	any	any	any	any	any	any	any	any	any	any	any	any	any
600	any	any	any	any	any	无线教学	any	教学放行	any	any	any	any	any	any
620	any	any	any	any	any	any	any	any	any	any	any	any	any	any
630	any	any	any	any	any	any	any	any	any	any	any	any	any	any
750	any	any	any	any	any	无线教学	any	any	any	any	any	any	any	any

系统概况

当前策略

对象管理

账号管理

临时账号

RADIUS

文件类型

域名群组

IP群组

IPMAC备注

应用路由

策略管理

用户认证

编辑

说明:系统采取后缀匹配算法,比如sohu.com相当于*sohu.com,^sohu.com精确匹配sohu.com

域名群组

域名列表

wk行为

^aapool.cn
^aax.com
^abcc.com
^aex.com
^ataix.com
^bhex.com
^big.one
^bkex.com
^btc.com
^btc.top
^btse.com
^bw.com
^f9.cn
^gj.com
^hpt.com
^kc.com
^okex.com
^rhy.com
^stex.com
^taal.com
^zb.com
^zbg.com
0.0lnki.swan.miningpool.online

通过流控系统动态获得“挖矿”域名，进行“挖矿”域名 HTTP 管控。

Panabit 专业版														
HTTP 策略管理														
序号	源地址	源端口	目标地址	目标端口	应用协议	用户类型	执行动作	策略ID	策略名称	策略状态	策略描述	策略备注	策略操作	策略备注
50	any	any	any	any	any	any	any	any	any	any	any	any	any	any
100	any	any	any	any	any	any	any	any	any	any	any	any	any	any
200	any	any	图书馆Library	any	any	any	any	any	any	any	any	any	any	any
300	any	any	图书馆Library	any	any	any	any	any	any	any	any	any	any	any

通过流控系统管控规则，阻断用户访问“虚拟货币”应用。

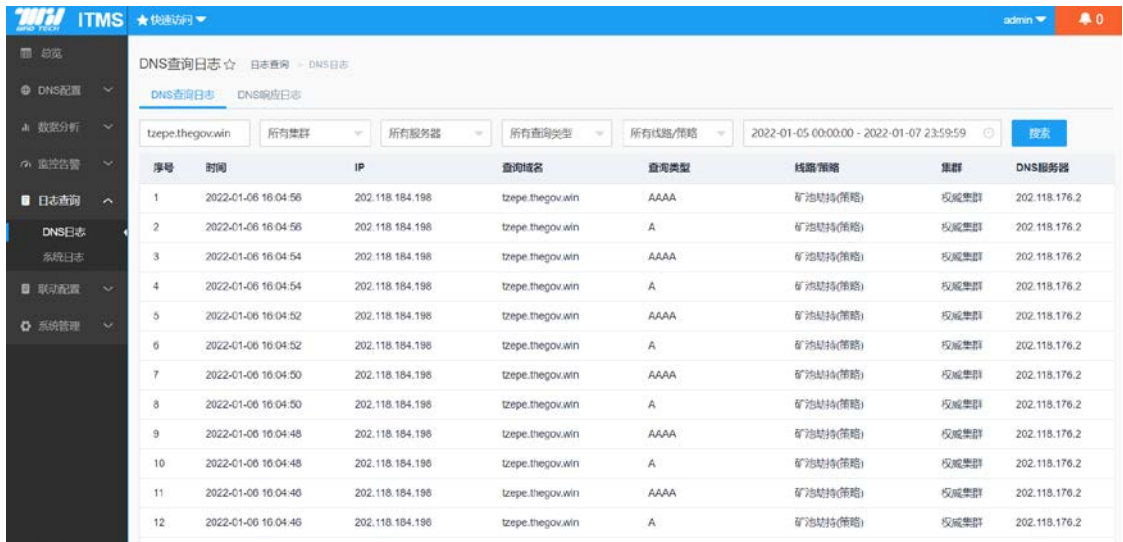


序号	线路	源地址	源端口	目的地址	目的端口	应用	动作	带宽	备注
1	any	any	any	any	any	禁止访问目的	禁止	0/0	
2	any	any	any	any	any	流量控制	禁止	3.92M/3.92M	测试
3	any	any	any	any	any	禁止访问目的	禁止	0/0	
5	any	any	any	any	any	虚拟货币	禁止	0/0	wiki行为
10	any	any	any	any	any	禁止访问目的	禁止	0/0	
40	any	any	any	any	any	图书馆	禁止	0/0	
50	any	any	上行	any	any	图书馆	禁止	0/0	
60	any	any	下行	any	any	图书馆	禁止	0/0	

第五章 虚拟货币“挖矿”行为终端及用户溯源

（一）IDC 数据中心“挖矿”行为终端及用户溯源

根据流量日志分析系统进行“挖矿”行为查询后，通过 DNS 系统日志进行分析，定位访问“挖矿”域名的源 IP 地址，告知 IT 安全部负责人，网络部确认是否为校内用户 IP，并对用户 IP 溯源，如为 IDC 数据中心 IP，IDC 数据中心人员进行溯源。IT 安全部进行现场取证确认后，消除该“挖矿”行为，形成闭环处理。



序号	时间	IP	查询域名	查询类型	线路/策略	集群	DNS服务器
1	2022-01-06 16:04:56	202.118.184.198	tzepe.thegov.win	AAAA	矿池劫持(策略)	权威集群	202.118.176.2
2	2022-01-06 16:04:56	202.118.184.198	tzepe.thegov.win	A	矿池劫持(策略)	权威集群	202.118.176.2
3	2022-01-06 16:04:54	202.118.184.198	tzepe.thegov.win	AAAA	矿池劫持(策略)	权威集群	202.118.176.2
4	2022-01-06 16:04:54	202.118.184.198	tzepe.thegov.win	A	矿池劫持(策略)	权威集群	202.118.176.2
5	2022-01-06 16:04:52	202.118.184.198	tzepe.thegov.win	AAAA	矿池劫持(策略)	权威集群	202.118.176.2
6	2022-01-06 16:04:52	202.118.184.198	tzepe.thegov.win	A	矿池劫持(策略)	权威集群	202.118.176.2
7	2022-01-06 16:04:50	202.118.184.198	tzepe.thegov.win	AAAA	矿池劫持(策略)	权威集群	202.118.176.2
8	2022-01-06 16:04:50	202.118.184.198	tzepe.thegov.win	A	矿池劫持(策略)	权威集群	202.118.176.2
9	2022-01-06 16:04:48	202.118.184.198	tzepe.thegov.win	AAAA	矿池劫持(策略)	权威集群	202.118.176.2
10	2022-01-06 16:04:48	202.118.184.198	tzepe.thegov.win	A	矿池劫持(策略)	权威集群	202.118.176.2
11	2022-01-06 16:04:46	202.118.184.198	tzepe.thegov.win	AAAA	矿池劫持(策略)	权威集群	202.118.176.2
12	2022-01-06 16:04:46	202.118.184.198	tzepe.thegov.win	A	矿池劫持(策略)	权威集群	202.118.176.2

（二）校园网“挖矿”行为终端及用户溯源

1. IP 相关信息是出口 NAT IP 的溯源

根据日常检查信息，首先通过 NAT IP 条件进行查询，得到校园网用户源 IP 地址，然后通过源 IP、目的 IP、源端口、目的端口、时间等信息在校园网流量日志分析系统和校园网流量用户会话日志分析监测系统进行用户详细信息查询与核对，即对用户进行溯源。

（1）校园网流量日志分析系统

Panabit® 网络大数据日志审计系统

会话日志 异常分析 速率诊断 V6连接 V6异常分析

选择设备 列表选项... 源地址 源端口 目标地址 目标端口 NAT地址

NAT地址 用户ID 连接时间大于 0 秒 上行流量大于 8 下行流量大于 8 协议类型 所有类型 协议 选择协议 任意

运营商 所有 域名 全库匹配 接口 起始时间 2022-01-07 21 时 4 分 结束时间 2022-01-07 22 时 4 分

只导出目的IP 只导出域名 后台导出 导出日期 查询 导出EXCEL 导出TXT 导出CSV 下载列表 源位置匹配

图形展示

数据列表

序号	设备	协议名称	类型	接口	访问时间	连接时间	源地址:端口	MAC	目标地址:端口	NAT地址	用户ID	域名	流量类型 上行/下行	运营商	源位置	目标位置	上行 流量/总流量	下行 流量/总流量
----	----	------	----	----	------	------	--------	-----	---------	-------	------	----	---------------	-----	-----	------	--------------	--------------

（2）校园网流量用户会话日志分析监测系统

审计设备 127.0.0.1

开始时间 2021-07-01 00:00

结束时间 2021-07-02 06:06

查询条件

源IP 目的IP 155.235.104.207 源端口 目的端口 协议 应用 设备IP

地址匹配条件

NAT IP 111.42.134.97 NAT IP 操作

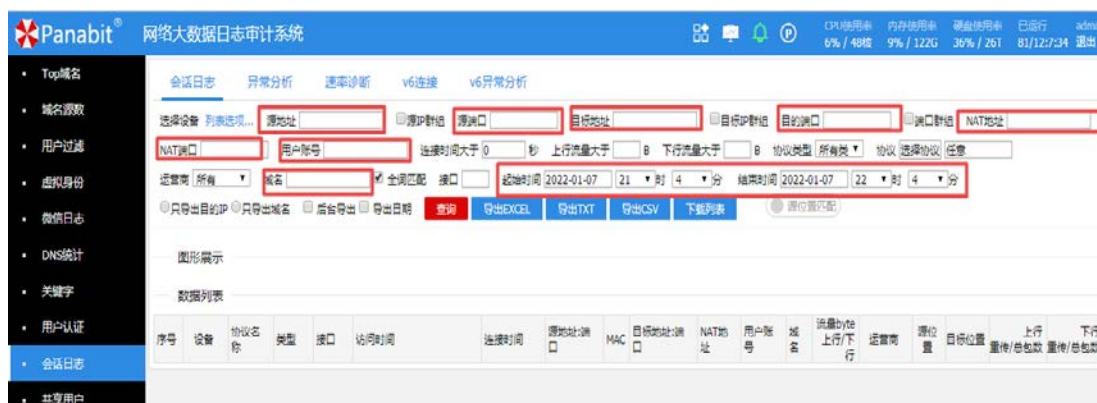
统计

2. IP 相关信息是校园网用户真实 IP 的情况

根据日常检查信息，直接通过源 IP 地址条件进行查询，然后通过源 IP、目的 IP、源端口、目的端口、时间等信息在校园网流量日志分析系统和校园网流量用户会话日志分析监测系统

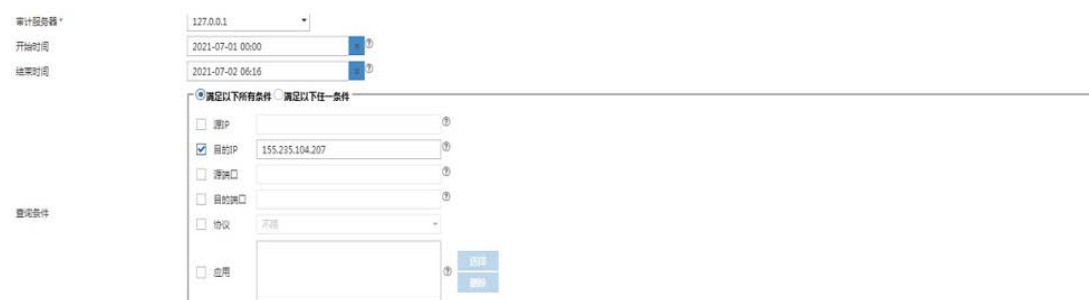
进行用户详细信息查询与核对，即对用户进行溯源。

(1) 校园网流量日志分析系统



The screenshot shows the Panabit network data log audit system interface. The top navigation bar includes '会话日志' (Session Log), '异常分析' (Anomaly Analysis), '速率诊断' (Rate Diagnosis), 'v6连接' (v6 Connection), and 'v6异常分析' (v6 Anomaly Analysis). The main search area contains several input fields for filtering logs, such as '选择设备' (Select Device), '源地址' (Source Address), '源端口' (Source Port), '目标地址' (Destination Address), '目标端口' (Destination Port), 'NAT地址' (NAT Address), '用户账号' (User Account), '连接时间' (Connection Time), '上行流量' (Upstream Traffic), '下行流量' (Downstream Traffic), '协议类型' (Protocol Type), and '协议' (Protocol). There are also buttons for '查询' (Search), '导出EXCEL' (Export to Excel), '导出TXT' (Export to TXT), '导出CSV' (Export to CSV), and '下载列表' (Download List). A table of search results is displayed at the bottom, with columns for '序号' (Serial Number), '设备' (Device), '协议名称' (Protocol Name), '类型' (Type), '接口' (Interface), '访问时间' (Access Time), '连接时间' (Connection Time), '源地址:端口' (Source Address:Port), 'MAC' (MAC), '目标地址:端口' (Destination Address:Port), 'NAT地址' (NAT Address), '用户账号' (User Account), '域名' (Domain Name), '流量字节' (Traffic Bytes), '上行/下行' (Up/Down), '源位置' (Source Location), '目标位置' (Destination Location), '重传/总包数' (Retransmission/Total Packets), and '下行/总包数' (Down/Total Packets).

(2) 校园网流量用户会话日志分析监测系统



The screenshot shows the campus network traffic user session log analysis and monitoring system interface. The top navigation bar includes '会话日志' (Session Log), '异常分析' (Anomaly Analysis), '速率诊断' (Rate Diagnosis), 'v6连接' (v6 Connection), and 'v6异常分析' (v6 Anomaly Analysis). The main search area contains several input fields for filtering logs, such as '选择设备' (Select Device), '源地址' (Source Address), '源端口' (Source Port), '目标地址' (Destination Address), '目标端口' (Destination Port), 'NAT地址' (NAT Address), '用户账号' (User Account), '连接时间' (Connection Time), '上行流量' (Upstream Traffic), '下行流量' (Downstream Traffic), '协议类型' (Protocol Type), and '协议' (Protocol). There are also buttons for '查询' (Search), '导出EXCEL' (Export to Excel), '导出TXT' (Export to TXT), '导出CSV' (Export to CSV), and '下载列表' (Download List). A table of search results is displayed at the bottom, with columns for '序号' (Serial Number), '设备' (Device), '协议名称' (Protocol Name), '类型' (Type), '接口' (Interface), '访问时间' (Access Time), '连接时间' (Connection Time), '源地址:端口' (Source Address:Port), 'MAC' (MAC), '目标地址:端口' (Destination Address:Port), 'NAT地址' (NAT Address), '用户账号' (User Account), '域名' (Domain Name), '流量字节' (Traffic Bytes), '上行/下行' (Up/Down), '源位置' (Source Location), '目标位置' (Destination Location), '重传/总包数' (Retransmission/Total Packets), and '下行/总包数' (Down/Total Packets).

以上两种情况查询到源 IP 地址后，根据用户源地址 IP、上网账号等信息，在校园网认证计费系统中查询用户详细信息，根据用户详细信息确定准确上网用户和客户端设备。针对固定 IP，都有相关负责人，同时根据 MAC 地址、校内 IP 地址可以通过交换机设备逐层追溯到上网终端，对应上网人员。

系统概况

用户管理

策略管理

财务管理

日志管理

操作日志

上网明细

认证日志

账号

IP地址

VLAN ID

MAC地址

2022-01-07 00:00:00

下线时间

选择产品

NAS IP

搜索

Vlanid模糊查询

高级筛选

搜索结果

导出Excel

导出CSV

账号	上线时间	下线时间	总时长	IP地址	VLAN ID	MAC地址	下线原因	NAS IP	端口标识
t280450201	2022-01-07 15:32:33	2022-01-07 22:08:33	6小时36分 钟0秒	118.203.176.40	30280147	00e0.7034.6926	NAS-Request设备请求	172.16.254.201	ae3:3028-147

系统概况

用户管理

搜索用户

添加用户

开户模板

在线用户

修改密码

缴费

退费

在线表

代理在线表

运营商在线

账号

IP地址

MAC地址

上线时间

下线时间

选择产品

外层VLAN

VLAN ID

NAS IP

搜索

模糊搜索账号

高级筛选

搜索结果

导出

IP地址	上线时间	VLAN ID	账号	NAS IP	MAC地址	操作
10.43.46.221	2022-01-07 22:10:19	1080000	2019051425	172.18.246.34	9cbc.f0a6.ede9	下线

本规定自发布之日起施行，由信息化处网络信息安全办公室负责解释和修订。