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-孙琭瑶、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-孙琭瑶

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。

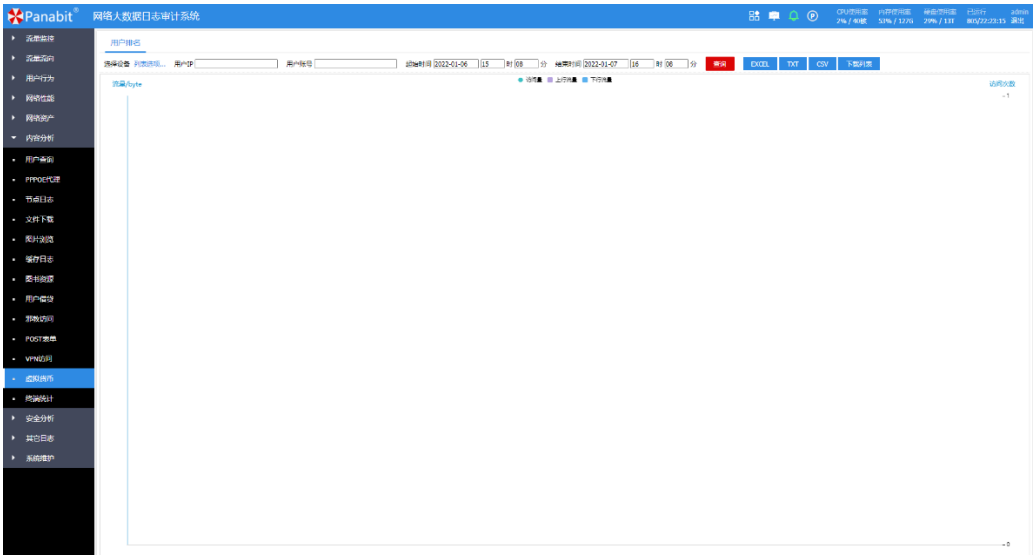
第三章　虚拟货币“挖矿”行为监测

（一）IDC 数据中心“挖矿”行为监测

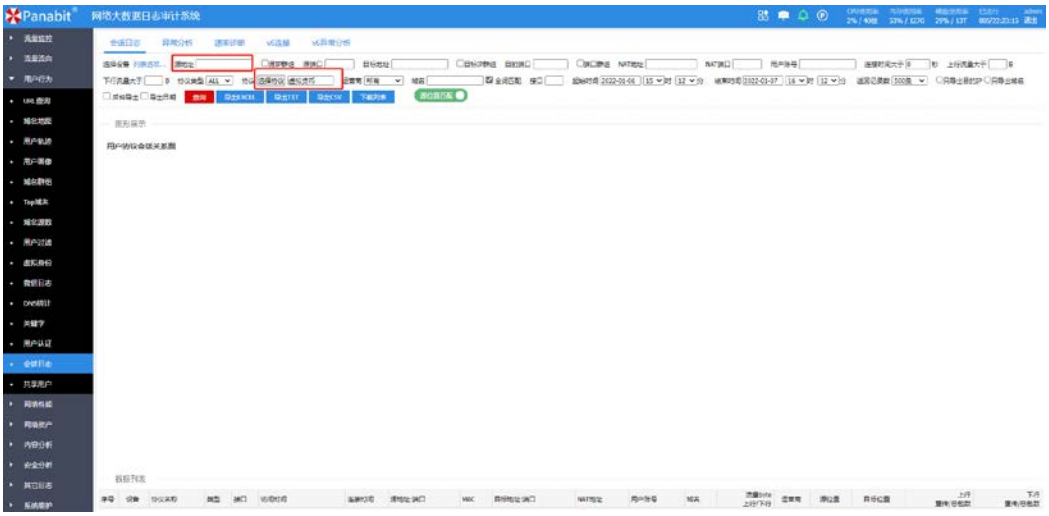
1.通过 IDC 流量日志分析系统进行“挖矿”行为查询如下:

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。

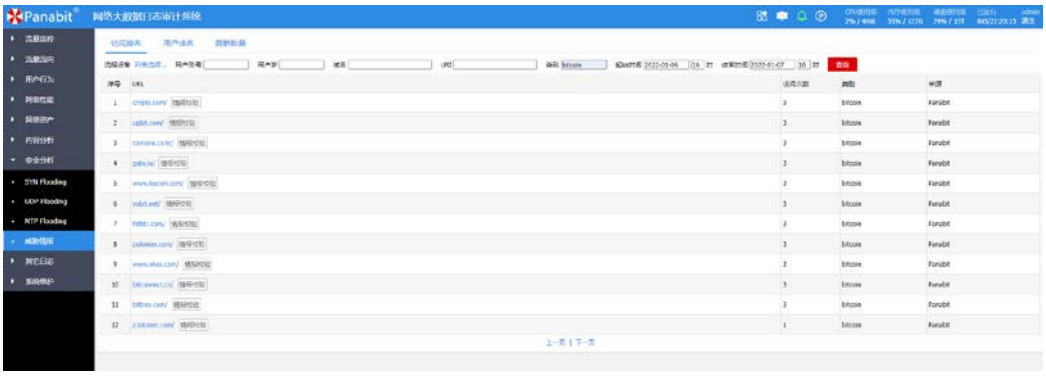


（2）在“会话日志”模块中根据步骤 1 排查的 IP 地址作为源 IP，协议选择“虚拟货币”，查询此 IP 地址访问信息详情。



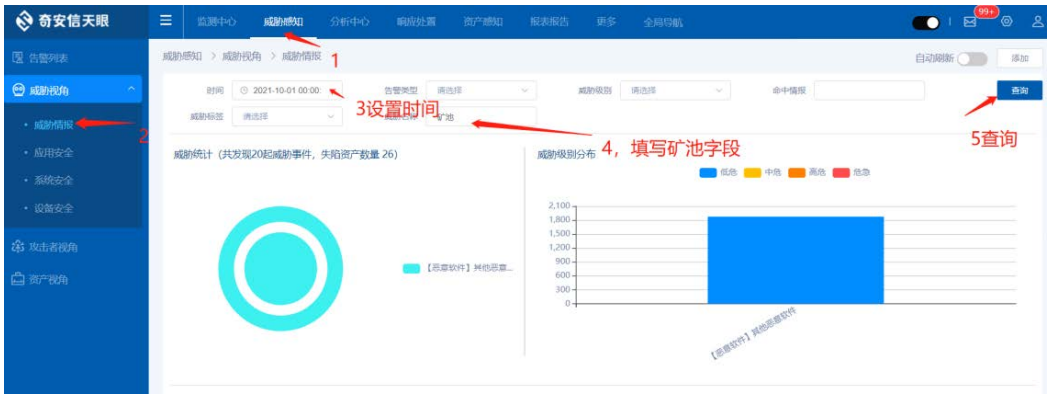
方式二：

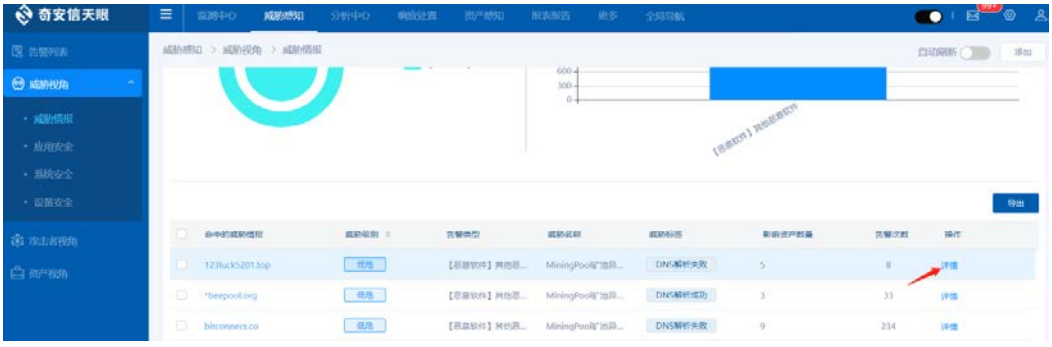
在 IDC 流量日志分析系统“安全分析”-“威胁情报”模块中查询，类别中输入挖矿应用类别“bitcoin”，先定位威胁情报中挖矿域名或者 IP，然后再查询内网 IP 用户。



2.通过网络威胁感知系统进行“挖矿”行为查询如下：

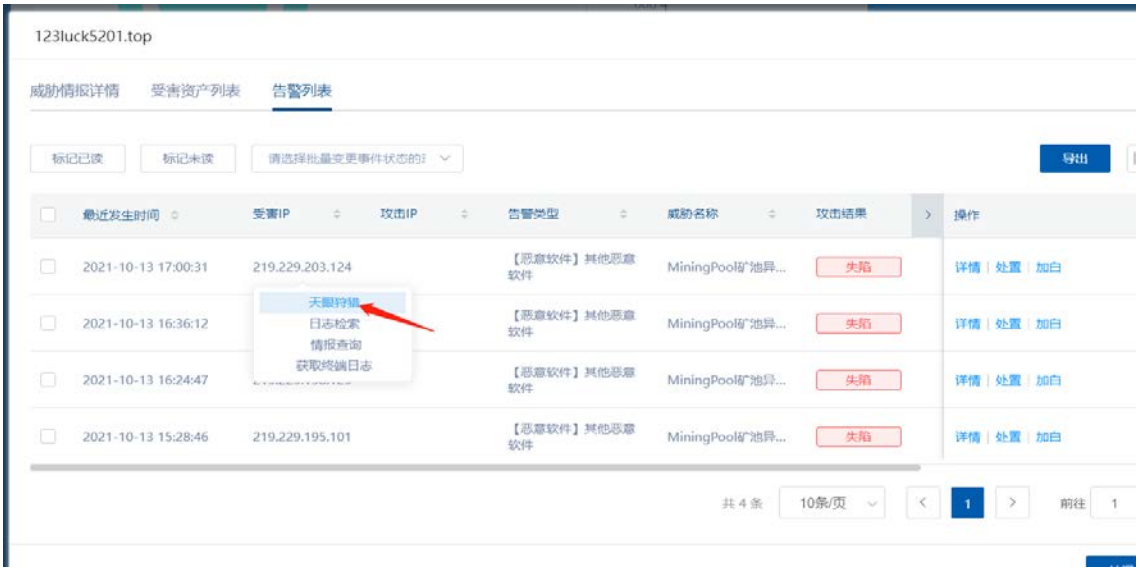
（1）在网络威胁感知系统的“威胁感知”-“威胁视角”-“威胁情报”模块中查询，失陷的威胁为主要排查对象。



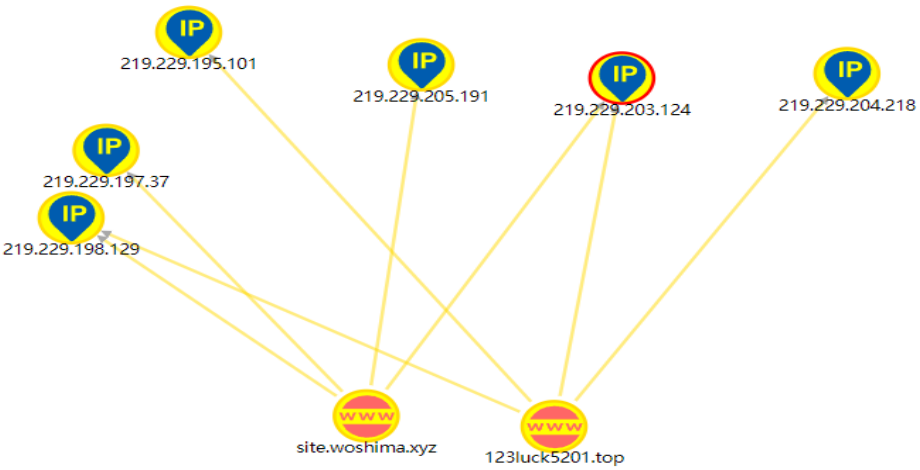


（2）查看涉及此威胁情报的详情，确认哪些是受害资产。

（3）通过告警列表中的受害 IP，查看受害资产。



（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。

（6）针对 IOC 和“挖矿”这种 DGA 域名威胁，存在两种情况：

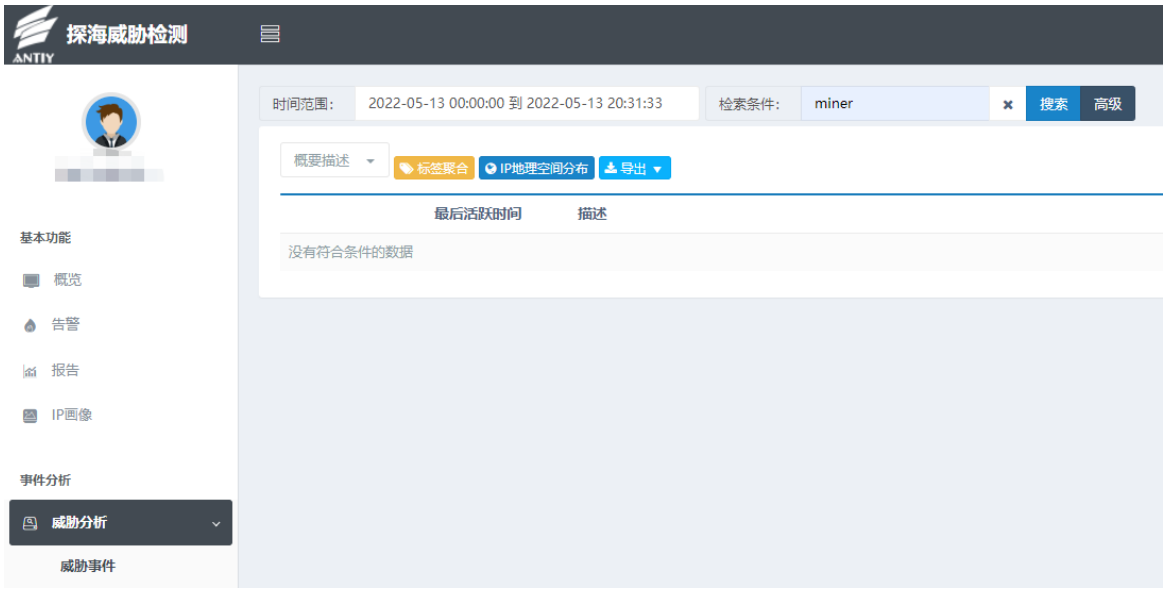
第一种是只有解析行为，但是没有解析成功，这种情况应高级关注，有可能是资产已经存在恶意软件，但是 IOC 威胁告警的

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 || Minepool，多条件聚合检索。



（二）校园网“挖矿”行为监测

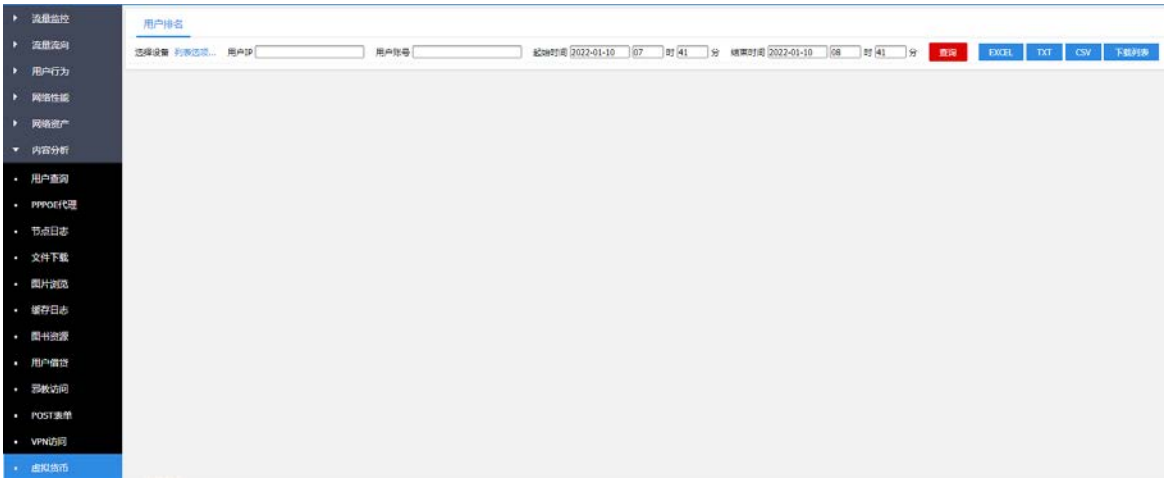
我校所有校园网用户上网行为都经过流控设备(Panabit)，

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：

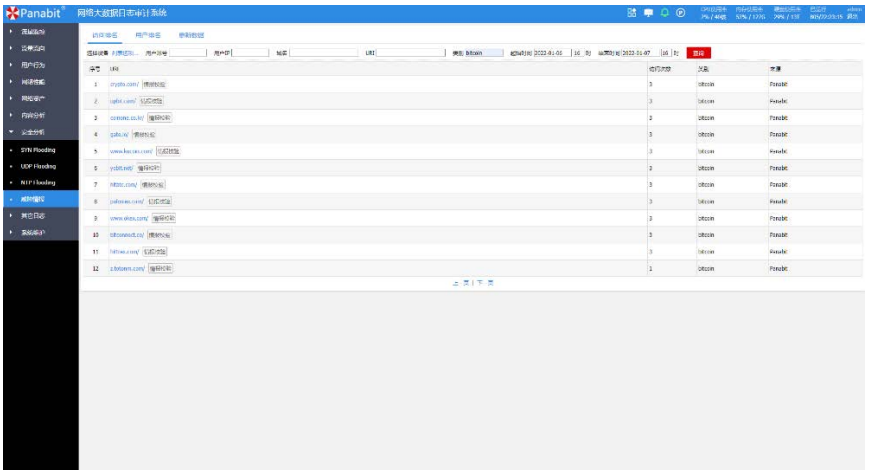
（1）在校园网流量日志分析系统的“内容分析”-“虚拟货币”模块中查询，排名靠前、上行流量明显高于下行流量、上行流量速率超过 1M 的 IP 地址为主要排查对象，查询疑似使用虚拟货币应用的 IP 地址。



（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。

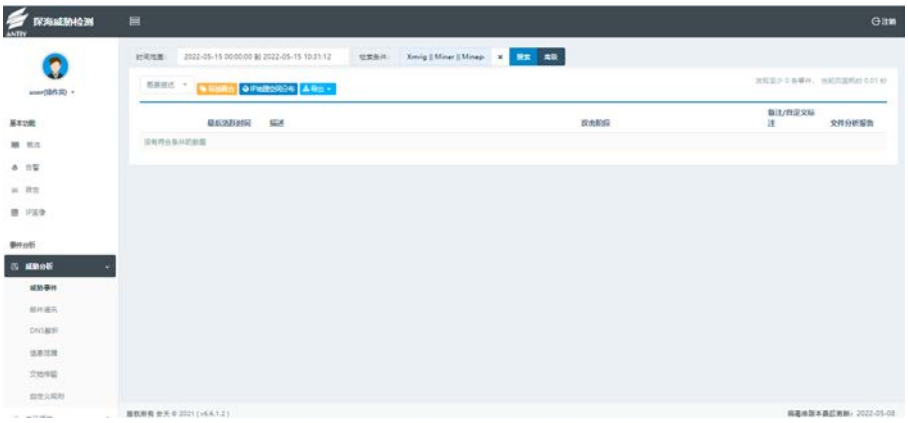
方式二:

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: Xmrig || Miner || Minepool，多条件聚合检索。

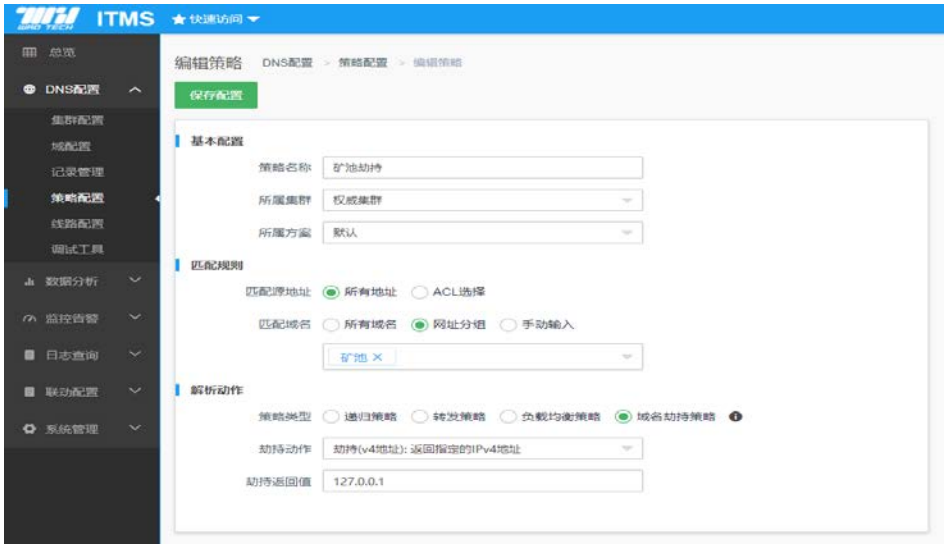


第四章　虚拟货币“挖矿”行为阻断

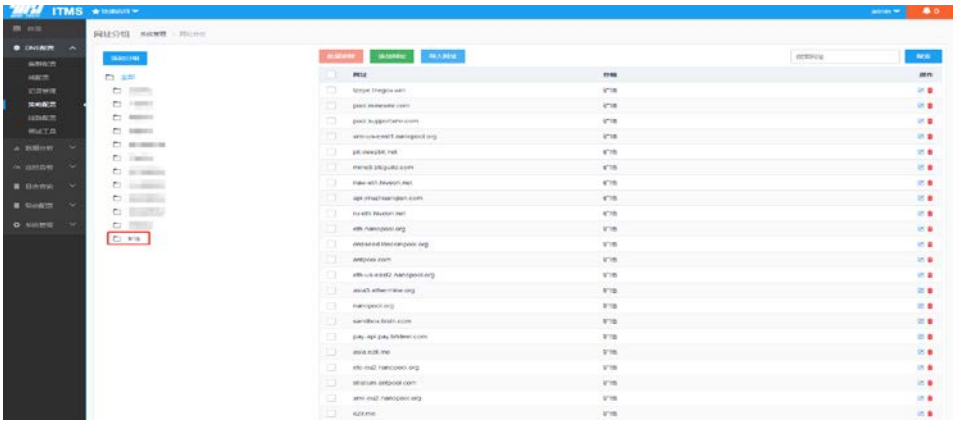
（一）IDC 数据中心“挖矿”行为阻断

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。

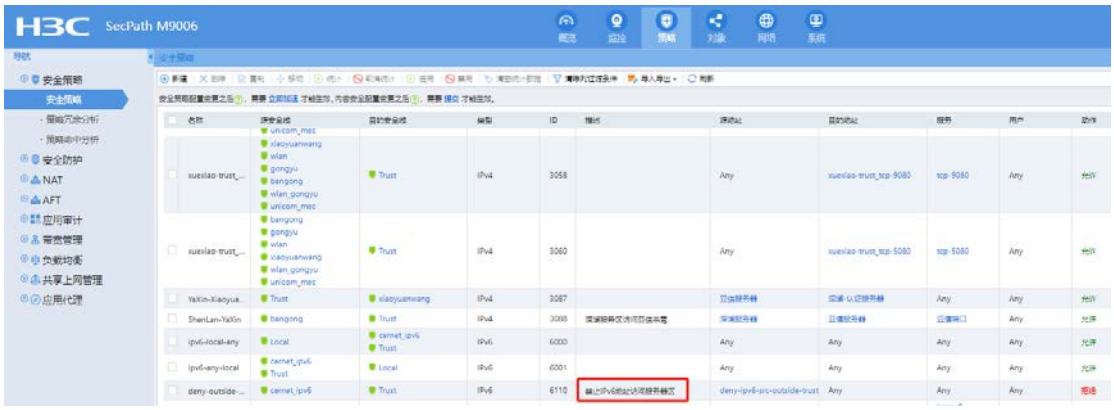


（2）对于新增“挖矿”域名同步更新至矿池劫持策略，保证进一步预防“挖矿”行为的发生。



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。



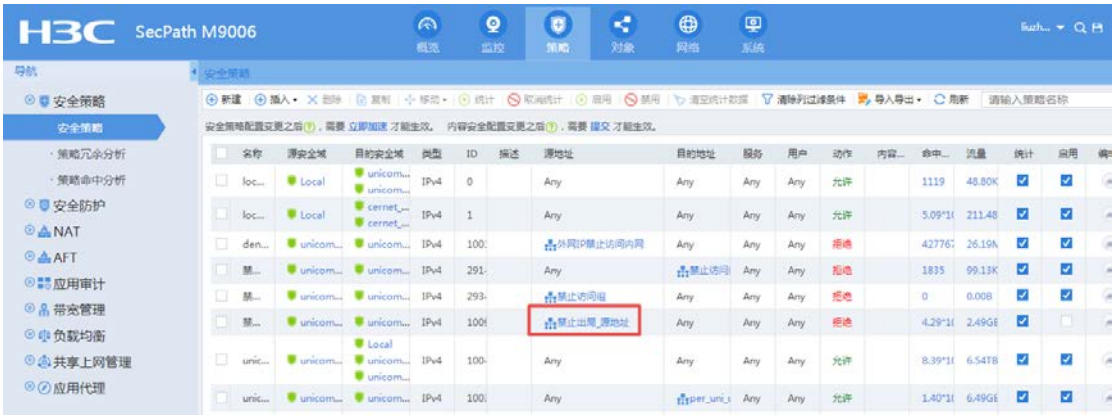
（二）校园网“挖矿”行为阻断

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，直接在校园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:

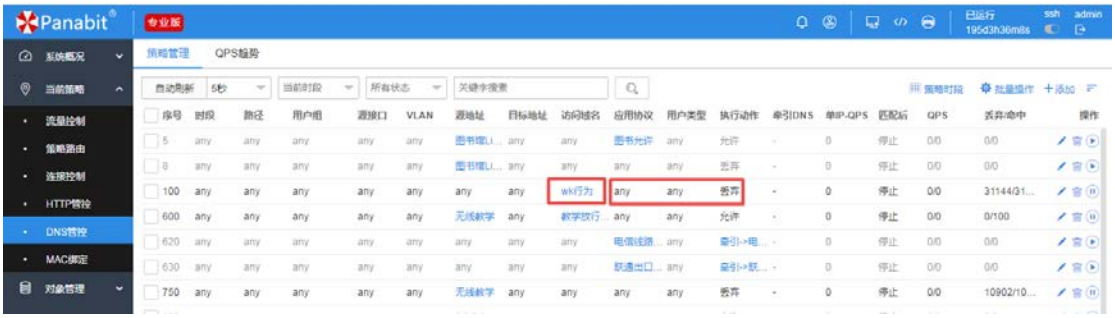
根据查询，IT 安全部现场排查进行确认，确认用户确实存在违规行为之后，针对固定 IP 用户，直接在防火墙禁止 IP 出校园网，待 IT 安全部检查用户整改完成后，通知可以开通时，再放行。



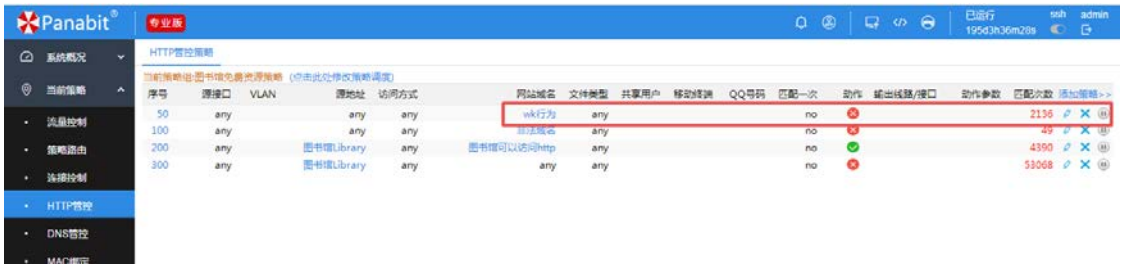
方式三:

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。



通过流控系统动态获得“挖矿”域名，进行“挖矿”域名 HTTP 管控。

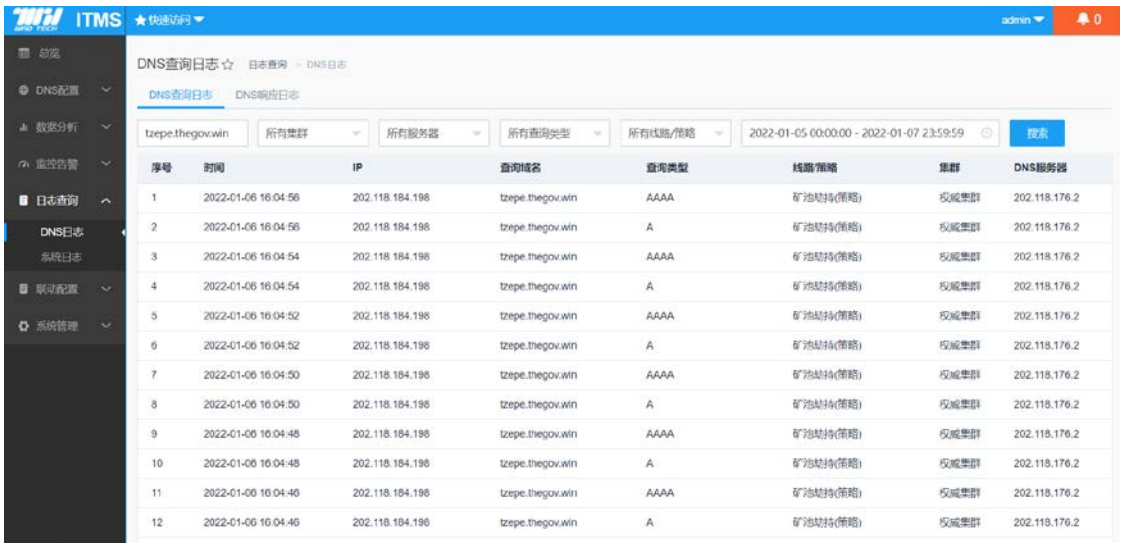


通过流控系统管控规则，阻断用户访问“虚拟货币”应用。

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。

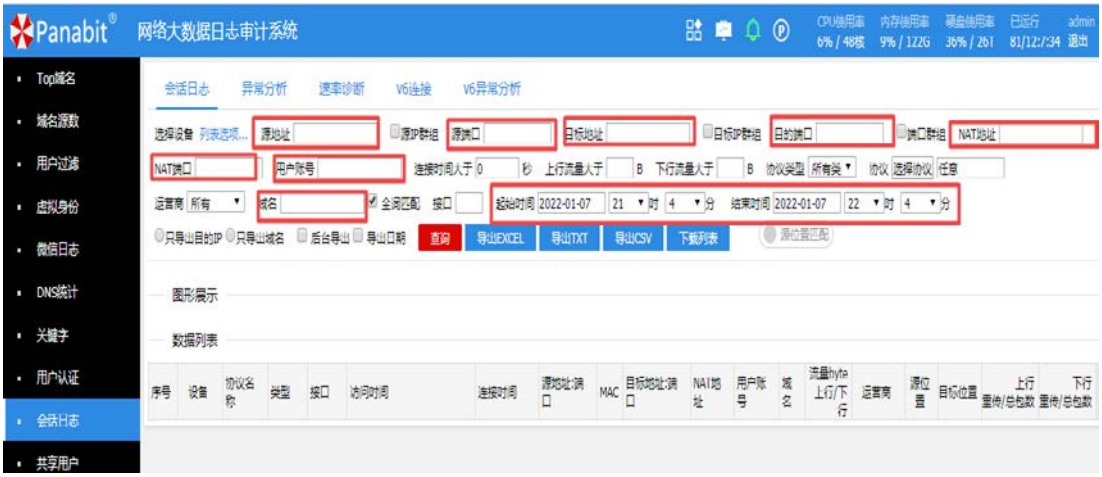


（二）校园网“挖矿”行为终端及用户溯源

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



（2）校园网流量用户会话日志分析监测系统

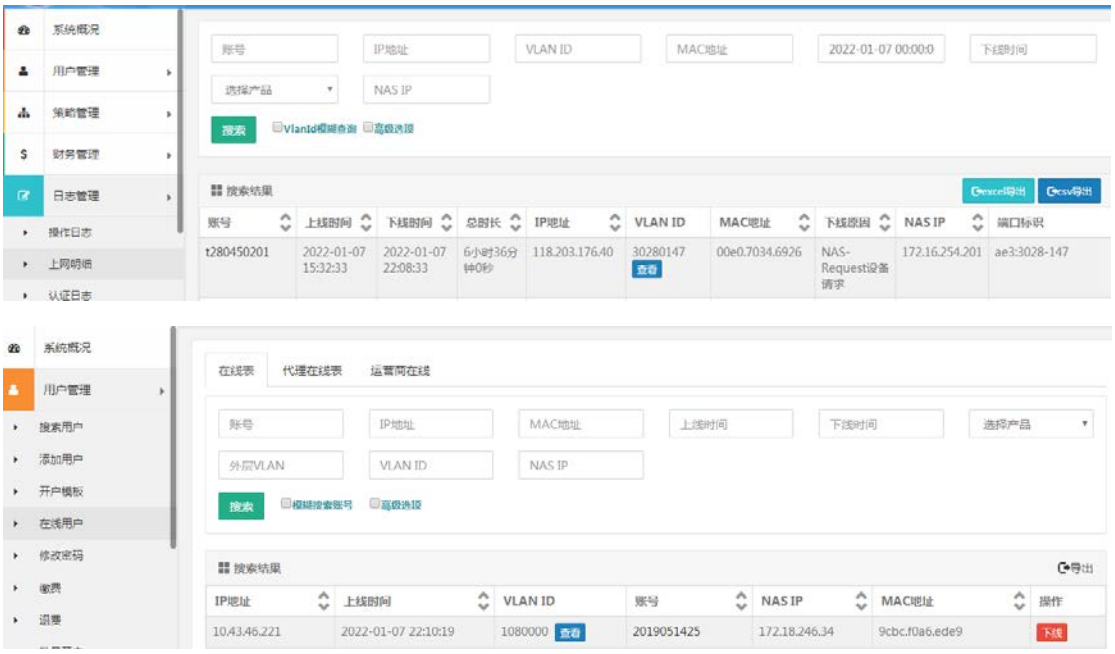
2. IP 相关信息是校园网用户真实 IP 的情况

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

（2）校园网流量用户会话日志分析监测系统

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。



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。