·实验技术·

基于深度流量分析的挖矿行为检测与实践

刘仁婷[1]，郑雅洪[2]，张映敏[1]，侯孟书[2]，孙朝晖[3]

（1. 电子科技大学 信息中心 成都 611730；2. 电子科技大学 计算机科学与工程学院 成都 611730；3. 北京派网软件有限公司，北京 100094）

摘要：为密织防范网络，清理挖矿木马病毒，有效治理校园网虚拟货币挖矿行为，提出了一种校园网恶意挖矿行为的检测与阻断模型。该模型采用基于签名的深度包检测技术，结合动态威胁情报，建立了挖矿协议的状态机模型，对报文进行深度包分析，以识别挖矿协议，在校园网出口实现挖矿流量的检测、识别与阻断。实践证明，该模型能够实时检测出虚拟货币相关流量，动态拦截受害矿机与矿池的通信流量，并实时定位受感染主机，有效地遏制校园网的恶意挖矿行为。

关　键　词：加密货币挖矿检测；挖矿木马；深度包检测；协议识别；网络流量监测

中图分类号：TP915.08　　**文献标志码：**A　　DOI: 10.12179/1672-4550.20230414

Detection and Practice of Cryptomining Behavior Based on Deep Packet Inspection

LIU Renting[1], ZHENG Yahong[2], ZHANG Yingmin[1], HOU Mengshu[2], SUN Chaohui[3]

（1. Information Center, University of Electronic Science and Technology of China, Chengdu 611730, China;
2. Department of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611730, China;
3. Beijing Panabit Software Co. Ltd., Beijing 100094, China）

Abstract: To strengthen the network protection, clean up the mining Trojan virus, and effectively control the cryptomining behavior of the campus network, a detection and blocking model of mining behavior is proposed. The model adopts the signature-based deep packet inspection technology, which is combined with dynamic threat intelligence, establishes a state machine model of mining protocols, conducts in-depth packet analysis, identifies mining protocols, and realizes the detection, identification and blocking of mining traffic at the campus network egress. Practice has proved that the model can detect the cryptomining-related traffic in real time, dynamically intercept the communication traffic between the victim miner and the mining pool, and locate the infected host in real time, which effectively curbs the malicious cryptomining behavior of the campus network.

Key words: cryptomining detection; mining trojans; deep packet inspection; protocol identification; network flow inspection

虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程。受利益驱动，攻击者利用系统漏洞获取系统的控制权限，进而在受害者电脑中，非法植入挖矿木马程序（挖矿木马），利用挖矿木马进行挖矿获利[1]。挖矿木马严重消耗主机算力资源，干扰正常业务运行，危害性大。校园网具有开放性，由于终端用户数量大、公网 IP 众多，且接入端口多，面临的被攻击风险大大增加[2−3]，许多高校深受其害。

针对虚拟货币挖矿，国家发展改革委等部门在 2021 年 9 月联合发布《关于整治虚拟货币“挖矿”活动的通知》[4]，对虚拟货币“挖矿”活动提出明确的监管整治要求。作为高校信息化安全管理部门，如何有效地全面清理校园网内虚拟货币挖矿行为，缓解高校挖矿木马病毒频发成为一个必须直面的焦点问题。

针对这一问题，各高校及众多安全企业对挖矿木马的防范进行了探索[5]。由于挖矿病毒特征变化快，通过单套产品很难实现有效的防范，通常需要构建纵深式防护体系，建立多重防护机制，

收稿日期：2023−09−08；**修回日期：**2024−01−02

基金项目：四川省重大科技专项课题 (2019YFG0399)。

作者简介：刘仁婷（1982−），女，硕士，工程师，主要从事网络安全、人工智能方面的研究。E-mail: liurt@uestc.edu.cn

结合病毒特性，进行有针对性的多重检测，以有效防范挖矿木马。从已公布的安全企业的治理方案来看，一般从“挖矿”病毒的监测、分析、处置、溯源的闭环处置等，进行规划和设计，部署多套安全产品，才能形成有针对性的挖矿木马整治。相关安全产品主要包括安全态势感知系统、服务器安全管理系统、终端安全管理系统以及安全专家服务等[6]。

然而，安全企业的挖矿木马治理方案主要依赖于完整的安全防护体系架构，对于校园网环境并不完全适用，主要有以下 3 点原因。

1）校园网终端以及部分服务器由师生自行维护和管理，信息化管理部门通常不会强制推行安装终端安全管理系统。师生下载和安装带病毒文件或被感染病毒的过程，通常无法第一时间被监控、告警乃至处置。

2）部分高校的安全部署重心在服务器侧，并未在校园网出口部署态势感知类安全设备，因为校园网出口流量大，超过 20 Gbps 的带宽对于态势感知类设备的部署难度高投资大，串接阻断风险高，实现校内用户侧和外网的通信流量进行实时威胁监测困难。

3）部分挖矿木马具备蠕虫化特点，在校园大局域网环境下横向扩散快，从排查定位到完成清理的根除治理周期较长。

目前的恶意挖矿行为识别的研究成果主要集中在基于终端管控或浏览器内的挖矿行为发现，而基于流量监听对挖矿协议识别的研究较少。在校园网出口部署流量探针，通过挖矿行为的流量特征等方式进行协议识别，可以在用户无感知情况下，获取矿机与矿池间的通信数据，实时告警或阻断相关流量，实现对挖矿行为精准定位。文献 [7] 采用了基于自动状态机进行多类别的协议识别，该方法可有效辨别网页浏览、即时聊天、P2P、邮件等协议，已被运用于流量控制和上网行为管理功能的商业产品中。在明文传输的挖矿行为检测中，文献 [8] 通过对挖矿行为的特征提取，使用网络威胁检测引擎 suricata[9] 建立流量检测规则，通过协议自身特有字符串即可对明文传输的挖矿行为触发相关规则告警。文献 [10] 提取了矿池协议通信特征，对明文报文基于行为规则库匹配可以达到 91.73% 的准确性，并对报文进行进一步的信息提取分类和预测，包括币种、矿工账号、算力和能耗预测等。文献 [11] 采用了基于 NetFlow/IFPIX 协议的网络测量方式，提取了 8 个流量特征，对几种常见虚拟货币通过机器学习的方法进行建模与判别，该方法并未考虑挖矿协议报文内容本身的特征。文献 [12] 对流量提取了 51 种特征，在模拟挖矿环境中对比了 5 种机器深度学习的方法用于挖矿流量辨别的性能，并验证了统计特征对加密挖矿流量判别的有效性。

和以上研究成果相比，本文结合了校园网真实场景与现状，对挖矿行为在真实网络流量而非模拟的流量中的行为特征进行深入分析和探索，流量复杂度更大，对模型的实时处理速度要求更高。为此，本文提出了一种在校园网出口部署挖矿行为的检测与阻断模型。基于真实场景验证，该方法能够有效识别出被感染主机与矿池的通信流量并实现动态拦截，对校园恶意挖矿行为的治理手段提出了思考与展望。

1 恶意挖矿行为检测模型

基于深度流量分析的恶意挖矿行为检测模型的拓扑如图 1 所示，通过在校园网出口部署流量分析设备，建立威胁情报库(矿池 IP 库、矿池域名库)、深度包检测(deep packet inspection，DPI)协议模型库以及挖矿协议状态机模型库，实现对挖矿报文的检测与阻断。

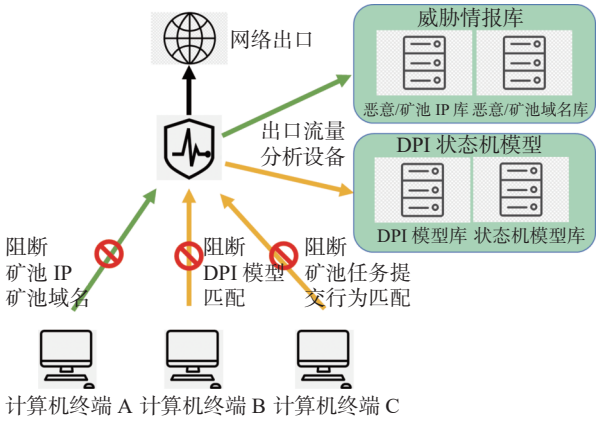

图 1 恶意挖矿行为检测模型

数据报文处理的主要工作流程如图 2 所示。在校园网出口，对所有流量报文进行实时拆包解析时：第一步，提取报文的目的 IP 地址和矿池 IP 库进行匹配，可以将内网与矿池 IP 的通信流量直接阻断或告警；第二步，对于域名系统(domain name system，DNS)请求协议进行筛选，将请求域

名与恶意域名库进行匹配，可以直接在挖矿主机进行 DNS 请求的过程中拦截恶意流量；第三步，对报文进行协议识别，可以使用 DPI 挖矿协议状态机模型，对每一个会话流量的协议行为进行识别。针对加密的挖矿协议流量，该模型也具有一定的识别能力。下面针对该模型中的每一步进行详细介绍。

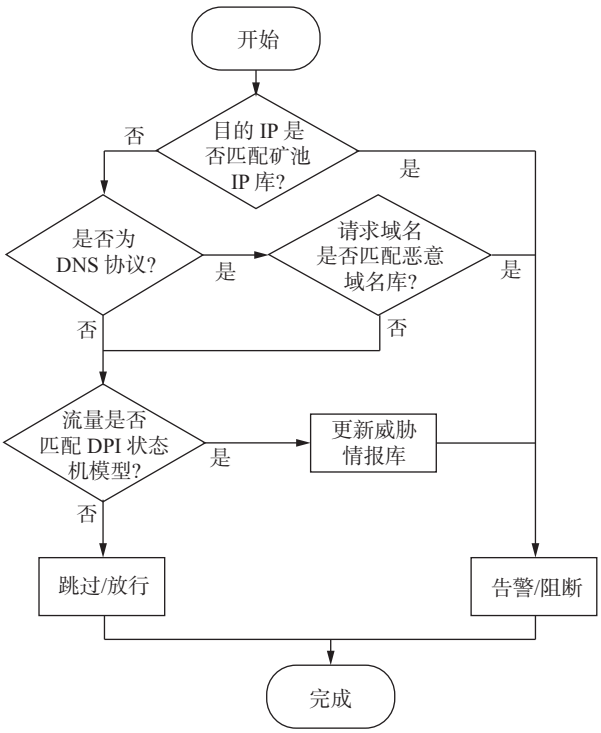

图 2　数据报文处理工作流程图

2　威胁情报库

恶意挖矿行为检测模型的第一步和第二步需要匹配的矿池 IP 库与矿池域名库，可以通过各大安全企业维护的安全情报及威胁情报库处获得。对于威胁情报库需要考虑以下 3 个方面问题。

1）威胁情报的来源

可同时选用多个威胁情报库作为本地库的来源，对于威胁情报库的可靠性需要谨慎选择，否则可能严重影响检测模型的有效性和用户上网体验。例如，某些境外情报库来源可能包含一些境内的非恶意的 IP 或域名，如果不加筛选直接同步，可能影响校园正常业务访问。因此，除了严格控制威胁情报库的入选范围外，还需要在同步威胁情报的过程中，进一步筛选非恶意的 IP 或域名，同时在日志系统中保留阻断日志，以便在出现错误识别时进行排查。

2）威胁情报的时效性

除了少量公共矿池域名与对应的 IP 地址相对固定外，大部分的矿池 IP 与矿池域名都呈现动态变化的趋势。在一段时间后，失效的矿池 IP 可能被分配给正常用户，甚至是校外个人用户终端使用。因此在维护本地威胁情报库时，需要对每一条情报设置有效时限。

3）建立内部情报机制

除外部的专业情报库外，内部情报的准确性较高，主要来源于内部已发现的挖矿终端上配置的矿池地址。其配置文件示例如下：

wallet = 0x6172e1aad41e353d08adc22250af582682851877

coin = ETH

rigName = A4

pool1=103.11.222.206:2049

进一步关联分析，可直接将内网挖矿终端上获取的矿池 IP 或域名作为查询条件，进行流量日志匹配，进而排查到更多与该矿池有连接关系的受害主机。如图 3 所示，与配置文件示例中矿池 IP（103.11.222.206）通信的有 2 台受害主机，因为使用了 TCP2049 端口和加密流量传输，日志系统的协议识别显示为 NFS 协议。

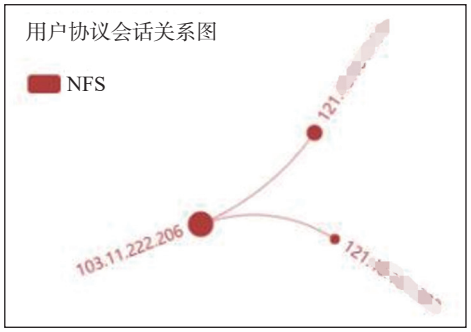

图 3　通过矿池 IP 反向定位内网受害主机

3　DPI 状态机模型

通过将基于签名的 DPI 技术和状态机模型相结合，可以实现对报文的深度分析和协议识别，增加报文识别的准确性。

3.1　基于签名的 DPI 模型库

对于明文传输的挖矿报文采用基于签名的 DPI 技术，通过深入读取 IP 包载荷的内容来对开放系统互连（open system interconnect，OSI）参考模型七层协议中的应用层信息进行重组，从而得到

整个应用程序的内容，再基于应用的指纹特征进行协议的匹配和分类。

以以太币(ETH)[13]挖矿协议为示例，该协议在明文传输以及矿机与矿池通信时，均具备一些有明显特征的字符串，例如:

1）登录操作"*method* ": "*eth_submitLogin*"

2）获取任务"*method* ": "*eth_getWork*"

3）提交任务"*method* ": "*eth_submitWork*"

通过 wireshark 查看 ETH 挖矿协议报文，可以看到明显的特征字符串，如图 4 所示。

基于签名的检测过程可以抽象为包含两个状态的状态机，跳转条件为命中一个较长的连续字符串。例如，当触发条件满足以太币的 3 类特征字符串时，将未知协议的数据报文及相关会话流标记为以太币挖矿协议。以太币挖矿协议状态机模型如图 5 所示。

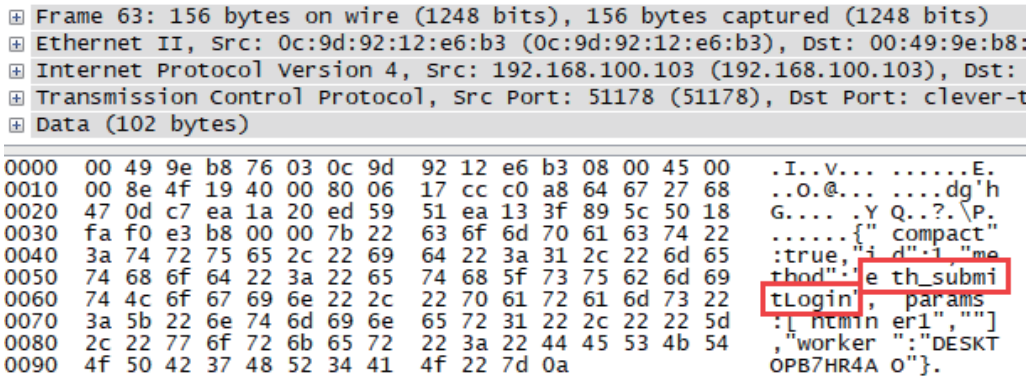

图 4 以太币挖矿协议特征字符串“*eth_submitLogin*”示例

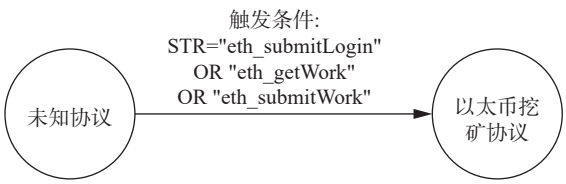

图 5 以太币挖矿协议状态机模型

如果跳转条件或特征字符串为一个较长的连续字符串，那么需要进一步考虑同一个会话流内的特征字符串跨数据包的情况。此时需要涉及会话注册，在注册的一个会话过程中进行跨数据报文的签名信息提取与匹配。

3.2 状态机模型

加密应用的引入会造成提取明文长字符串的 DPI 执行困难。为解决这一问题，需要将一个协议的验证过程设计为多个状态的状态机，状态机的跳转条件包括：短字符串、端口、包长和频率等。通过将这种多个状态的协议状态机进行宏语言描述后转换为相应的 C 语言代码，再链接其他代码之后，加载到出口流量分析设备的操作系统对应接口中，就能形成高速的二进制代码，以提高协议识别的性能。

对于所有新的协议数据包和可能的识别错误数据，首先进入用宏语言描述的全协议状态机库的机器人程序；自动提取其中的关键信息，建立初步的状态机；最后经由人工干预修正，形成符合识别结果的宏语言描述，加入协议识别库中。

以当前主流的池化挖矿协议 stratum[14]为例，矿机与矿池之间需要经历任务订阅、任务下发、账号登录、结果提交和难度调整等几个通信过程。对这样的挖矿协议和行为，可以使用基于流的自动机形式进行建模，也就是使用基于统计属性的有限状态机。状态的转换由特定的输入事件触发，转换的条件由分析方法评估。在本文的设计中，分析方法包括指纹匹配、协议分析和流统计特征等。在检测特定通信流量时，流统计属性可以增强有限状态机的灵活性。触发状态转换的事件首先由分析方法检测到，例如指纹匹配，再依据统计特性进行验证。状态转换中的统计主要包括以下 3 种参数。

1）脉冲重复率：在给定时间段内的特定状态转换条件满足率。

2）间隔时间：两次事件之间的时间间隔。

3）当前流统计指标：一些持续更新的统计值，包括总包数、总字节数和流上线时间。

总的来说，每一个状态机勾画了一个随着应

用报文流的状态转换序列，来描述每一种协议行为。转换的条件可以基于指纹、协议识别和统计属性来评估。这样对于协议的识别，就不仅仅是基于一个单一的报文，而是跟踪整个报文的关联性、流状态以及应用。

以 stratum 协议为例的状态机模型如图 6 所示。其中步骤(1)~步骤(4)代表了矿机(客户端)与矿池(服务端)的注册认证过程，包括客户端发送订阅指令、服务端返回信息、客户端发送认证信息、服务端返回认证结果。步骤(5)由矿池下发难度调整指令给矿机，该步骤可以在认证阶段发生，也可以在后期的挖矿任务执行期发生。图中用“*”标识其可重复执行。而步骤(6)~步骤(8)代表了矿机和矿池之间任务执行与提交的交互过程，包括服务端发送任务分配消息、客户端向矿池提交任务、服务端向客户端反馈任务接受结果。

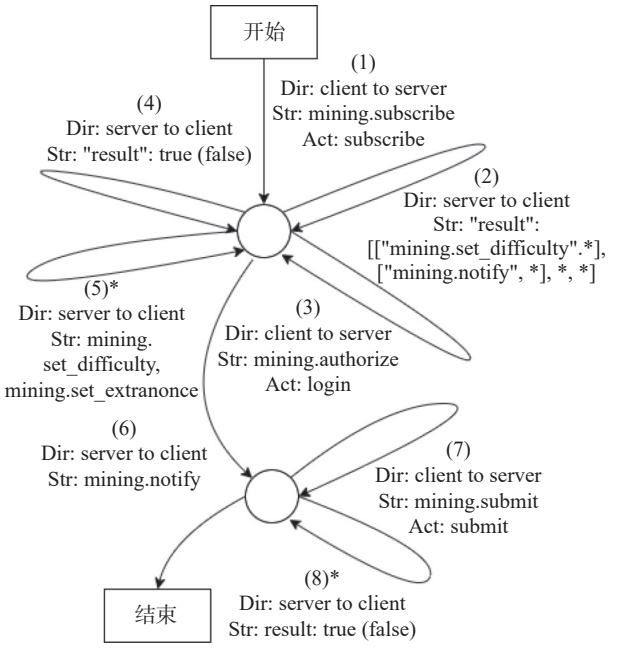

图 6　stratum 挖矿协议状态机模型

4　系统运行结果分析

为了验证所构建系统对恶意挖矿行为和挖矿协议识别的准确性和有效性，针对某高校真实的校园网络出口数据开展了测试和验证，流经校园网出口的实时流量约 20 Gbps，并发用户数约 50 000 人，并发连接数超过 8×10^5 次/秒。将所提的恶意挖矿行为检测模型部署在某高校校园网出口，对虚拟货币协议流量进行识别。在安全防护的需求下，本研究的测试采用串联阻断模式，即发现相关流量后无需人工干预直接阻断。接下来是对系统运行结果进行统计和分析。

4.1　本地威胁情报库

目前外部威胁情报来源主要是基于第三方安全厂商包括天际友盟、深信服、兄弟高校的数据共享，通过情报收集、数据交换，以及沙箱分析进行威胁情报的生产加工，累计超过十万余条活跃的情报数据。校内通过挖矿协议识别和安全检查，也可同步建立内部情报机制。本次实验使用的本地威胁情报库情况如表 1 所示。

表 1　本地威胁情报库统计数据

情报类型	来源	数量	单位
数字货币域名	天际友盟	134 825	条
矿池域名	深信服	26 883	条
矿池域名	校内	214	条
其他恶意域名	天际友盟	8 245	条
其他恶意IP/IP段	中科大	5 520	个
矿池IP	校内	78	个

4.2　基于矿池 IP 与矿池域名的阻断

从对矿池 IP 的阻断情况分析，被阻断的流量主要分类两类：一类是访问矿池 IP 地址的 80 或 443 端口的 TCP-SYN 请求报文；另一类是发给矿池 IP 的 ICMP 报文。单个受害主机会呈现在 5 分钟内连续发送 20 次以上同样请求的现象。

在基于 DNS 请求信息对矿池域名进行阻断的实验过程中，3 个月总计命中并丢弃的 DNS 请求数量接近 8×10^5 次，其中匹配挖矿域名占比 32.5%，其他恶意域名占比 67.5%。对 DNS 阻断模式进行进一步分析发现以下问题。

1）已阻断的对矿池发起 DNS 请求来源于两部分：第一部分是校外受害主机与校外 DNS 之间的矿池域名解析请求，可以初步判定校内终端遭受挖矿病毒侵害，并第一时间进行定位、通报和处置；另一部分是校内的 DNS 服务器与校外 DNS 之间矿池域名递归解析请求，这类请求需要进一步排查校内 DNS 服务器的日志，获得发起 DNS 请求的源 IP，从而完成溯源、定位与处置。

2）校内的 DNS 服务器也可以同步矿池域名或云 DNS，对收到的恶意域名请求拒绝（rcode=5-Refused）。然而单一部署本地 DNS 服务器阻断挖矿，也需要与校园网出口的 DNS 重定向配合。在具体实践过程中，如果简单地在校园网出口采用

目标地址网络转换(destination network address translation，DNAT)方式重定向，会把 DNS 蠕虫流量引流到本地 DNS，对校内 DNS 服务器的性能带来压力。为避免该情况干扰正常网络解析的性能，可以在校园网出口对 DNS 请求部分采用同步威胁情报直接阻断的方式。

3) 因为 DNS 请求被拦截，受害主机会持续对矿池域名发起 DNS 请求。如果未及时对受害主机进行挖矿木马的排查与清理，被阻断的 DNS 请求总数量会呈持续上升趋势。如表 2 所示，源 IP 地址 a.a.a.a 会持续不断向矿池发起域名请求，请求的域名有前缀变化。虽然受害主机并未开始执行挖矿任务，不会表现出 CPU/GPU 等性能异常现象，但是仍应及时处置，对主机进行全面安全检查与查杀。

表 2 内部受害主机某日与矿池域名通信阻断日志(节选)

时间	矿池域名
10:00:35	srv1.trex-miner.com
10:04:15	srv1.trex-miner.com
10:05:26	srv3.trex-miner.com
10:06:05	srv1.trex-miner.com
10:07:16	srv3.trex-miner.com
10:07:55	srv1.trex-miner.com
10:09:06	srv3.trex-miner.com
10:12:06	srv2.trex-miner.com
10:12:46	srv3.trex-miner.com
10:13:26	srv1.trex-miner.com
10:13:56	srv2.trex-miner.com

4) 本地威胁情报库需要进行人工调试，防止误拦截。在对 DNS 阻断日志的跟踪中，出现了 xxx.yahoo.com 记录，这显然是误拦截。经排查发现是恶意域名库中存在一条“hoo.com”记录，因为在 DNS 阻断过程中采用了后缀匹配算法，比如 hoo.com 相当于*hoo.com。这种后缀匹配算法对于表 2 中矿池域名变种有效，但是会造成误伤。因此在针对 hoo.com 这类长度较短且易混淆的恶意域名，可考虑采用精准匹配算法，用“^hoo.com”加以标识。

4.3 挖矿协议识别

基于连续 24 小时对 DPI 状态机模型判定为挖矿协议的流量进行分析，识别到的挖矿协议流量统计如表 3 所示。

表 3 24 小时虚拟货币流量统计

协议模型	连接数	上行流量/byte	下行流量/byte	总流量/byte
挖矿	56 673	3 300	3 000	6 300

和接近 20 Gbps 吞吐量的校园网出口正常流量相比，基于 DPI 状态机模型识别到的挖矿流量仅占总流量的亿万分之一，经过流量统计与报文分析发现以下规律。

1) 挖矿协议流量没有呈现出理想中挖矿协议流量的统计特性，如上行流量明显高于下行流量。经分析发现，因为设置了阻断模式，在算法判定为挖矿协议后直接阻断了后续任务的执行与提交的交互过程。而对于明文的挖矿流量来说，这个阻断过程可能发生在传输控制协议(transmission control protocol，TCP)三次握手连接建立后的矿池注册阶段或难度调整指令阶段，因此上行流量并没有因为任务报文的频繁提交而增多。

2) 识别到的矿池 IP 主要为私有矿池 IP。因为威胁情报库已基本涵盖所有已知的公共矿池 IP，这一步骤识别到的矿池 IP 无法直接利用公开的威胁情报库(如微步在线等)进行查询和验证。

3) 因为采用真实数据流，缺乏训练数据集和验证数据集，DPI 状态机模型的准确性和误报率，尤其是加密流量部分，无法直接计算得出。因此，挖矿协议识别的实验数据并不适用于与文献 [11] 等可控网络环境下的结果直接进行有效性对比和判别。挖矿协议识别流量的有效性验证(模拟数据场景除外)主要依赖于对校内 IP 的溯源与终端排查，在校内终端发现了挖矿进程计为正确(positive)。而终端排查验证工作的不确定因素，如挖矿程序在检查时已被删除、路由器代理导致终端定位失败等，导致可被验证有效的挖矿流量过低，协议识别的准确率不到 40%。因此，为了进一步验证 DPI 状态机及所提恶意挖矿行为检测模型的有效性，需要设计相应的模拟数据场景。

4.4 模拟挖矿场景识别

模拟挖坑场景识别选择门罗币(XMR)[15] 模拟校内存在的主动挖矿行为。因为门罗币是“最受犯罪分子欢迎”的加密货币之一，其挖矿算法利用中央处理器(central processing unit，CPU)的挖矿效率更高，利用没有 GPU 等高性能显卡的“肉鸡”也能获得收益。实验设计了以下 3 种场景。

1) 场景 1

在校内终端部署 XMRig[16] 挖矿客户端用于模

拟矿工与门罗币矿池（pool.minexmr.com:4 444）间的通信，并切换不同的互联网出口链路，测试阻断的有效性。本次实验的恶意挖矿行为检测与阻断模型仅部署于教育网出口。

2）场景 2

模拟挖矿的校内终端部署 xmr-stak[17] 挖矿客户端，采用 TSLv1.3 连接加密方式通信，用于模拟矿工与门罗币矿池间的 443 端口加密通信。

3）场景 3

模拟挖矿的校内终端部署 xmrig，使用校外云端虚拟专用服务器（VPS）代理所有通信流量，采用 SOCKET5 加密方式通信，用于模拟矿工与门罗币矿池间的以流量代理方式加密通信。

所有挖矿客户端均使用默认设置连接矿池。为了避免挖矿测试实验引发安全误报，本实验仅验证了矿机访问矿池是否成功。如果阻断失败，成功进入了挖矿任务执行与提交阶段，将手动中止测试。模拟场景下矿机访问 XMR 矿池成功与否的结果统计如表 4 所示。由于运营商网络拦截策略问题，3 种场景下矿机均能成功连接矿池并执行挖矿任务。而校园网出口通过恶意挖矿行为检测与阻断策略，可以成功对场景 1 和场景 2 的流量进行实时拦截，但不能有效识别加密代理方式。

表 4　模拟场景下矿机访问矿池结果统计表

场景	校园网出口	某运营商网络出口
场景1	失败	成功
场景2	失败	成功
场景3	成功	成功

5　结束语

针对校园网虚拟货币挖矿频发的问题，提出了基于深度流量分析的挖矿流量检测方法，通过建立威胁情报库、DPI 挖矿协议模型库以及状态机模型库，在校园网出口建立了恶意挖矿行为检测模型。经实验验证，该模型能对常见的挖矿协议进行有效的检测与拦截。然而，从挖矿问题产生的源头来看，攻击者受利益驱动的外因固然存在，校内终端安全防护手段缺失以及个人安全意识的薄弱这些内因也不能忽视。结合校内终端安全感知和流量探针进行多维度的挖矿行为检测可以成为下一步的研究探索方向。

参 考 文 献

[1] PASTRANA S, SUAREZ-TANGIL G. A first look at the crypto-mining malware ecosystem: a decade of unrestricted wealth[C]//Proceedings of the Internet Measurement Conference. Amsterdam: ACM, 2019: 73–86.

[2] 郑先伟. 警惕挖矿木马攻击!高校超算系统应密切注意[J]. 中国教育网络, 2020(6): 57.

[3] 郑先伟. 高校需警惕挖矿木马病毒入侵[J]. 中国教育网络, 2021(12): 43.

[4] 中华人民共和国中央人民政府. 国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知: 发改运行〔2021〕1283 号[A/OL]. (2021-09-03)[2021-09-03]. http://www.gov.cn/zhengce/zhengceku/2021-09/25/content_5639225.htm.

[5] 王宽锋, 江魁, 余志航, 等. 网络安全运营体系下的挖矿治理[J].中国教育网络, 2021(12): 62−64.

[6] 金睿. 国家发改委全面整治“挖矿”[J]. 计算机与网络, 2021, 47(22): 8.

[7] HUANG N F, FENG Y H. Application behavior analysis by stateful automata mechanism[J]. Journal of Computers, 2008, 18(4): 3−14.

[8] FREEBUF. suricata 下的挖矿行为检测[EB/OL]. (2019-02-07)[2019-02-07]. https://www.freebuf.com/articles/network/195171.html.

[9] The Open Information Security Foundation. Suricata [EB/OL].(2020-03-01)[2021-03-25].https://suricata.io/.

[10] 史博轩, 林绅文, 毛洪亮. 基于网络流量的挖矿行为检测识别技术研究[J]. 计算机应用研究, 2022, 39(7): 1956−1960.

[11] MUNOZ J Z I, SUAREZ-VARELA J, BARLET-ROS P. Detecting cryptocurrency miners with NetFlow/IPFIX network measurements[C]//2019 IEEE International Symposium on Measurements & Networking (M&N), Catania: IEEE, 2019: 1−6.

[12] PASTOR A, MOZO A, VAKARUK S, et al. Detection of encrypted cryptomining malware connections with machine and deep learning[J]. IEEE Access, 2020, 8: 158036−158055.

[13] ethereum. org. WHAT IS ETHER (ETH)? Currency for our digital future[EB/OL]. (2020-03-01)[2023-08-31]. https://ethereum.org/en/eth/.

[14] Open-source Bitcoin Community. Stratum V2 (SRI) roadmap-to infinity and beyond[EB/OL]. [2023-04-08]. https://stratumprotocol.org/.

[15] The Monero Project. About Monero[EB/OL]. [2020-02-23]. https://www.getmonero.org/.

[16] Xmrig Team. XMRig[EB/OL]. [2021-12-3]. https://xmrig.com/docs/miner .

[17] FIREICE-UK. XMR-STAK: Free Monero RandomX miner and unified CryptoNight miner[EB/OL]. [2020-05-07]. https://github.com/fireice-uk/xmr-stak/.

编辑　王燕