恶意样本和威胁情报资源的分享

小道安全 2023-04-14 07:30 本文共 1173 字 阅读完需 5.5 分钟

> 于威胁情报的分析很大部分都是需要基于恶意样本为载体进行展开分析的。

公众号

背景

对于威胁情报的分析很大部分都是需要基于恶意样本为载体进行展开分析的，白帽研究员、二进制分析以及逆向研究员在学习和研究过程中，也需要各种类型的恶意样本进行研究分析。想要获取各种类型恶意样本的搜索时间成本相对会比较高。

下面是我平时研究学习恶意样本中的威胁情报的主要来源地方，国外国内的恶意样本分析平台还有很多很优秀的平台以及其他网络渠道(例如github)，可以根据自己需要进行恶意样本的获取。

国外恶意样本源

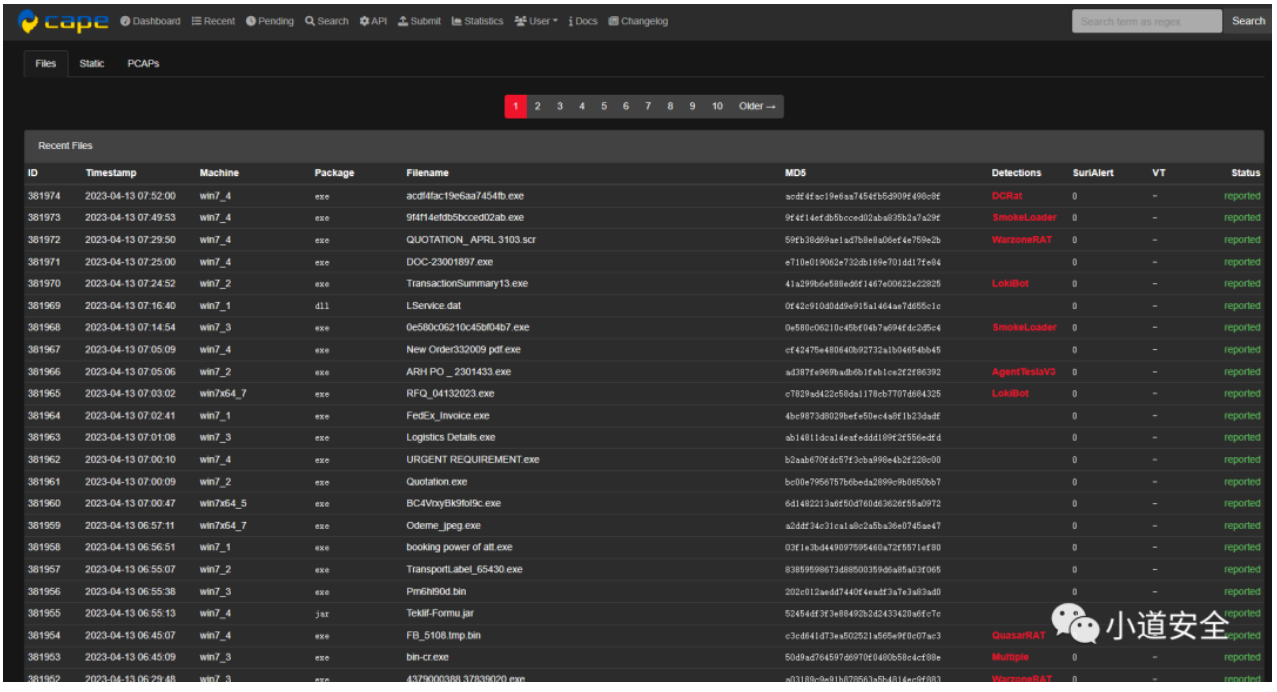
目前很多新的威胁情报都是来源于国外，因此对于各种新攻击手法，可以重点关注国外的恶意样本源，通过下面的6个平台可以获取到恶意样本。

1、https://app.any.run/submissions/

该平台上有各种不同类型的恶意样本，并且对于恶意样本也有比较详细的分析报告可以参考进行恶意样本功能的解析。

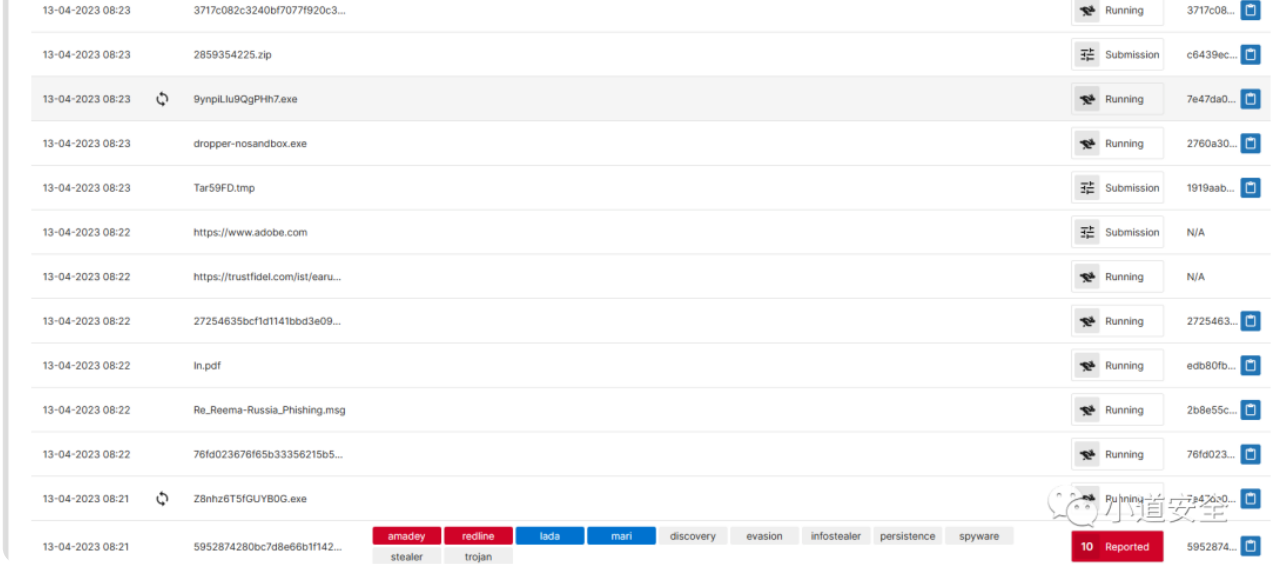
2、https://capesandbox.com/analysis/

这个平台有各种类型的外挂样本，因为样本更新率很高，样本量也非常多，可以通过关注下载最新的一些恶意样本进行最新攻防方法分析和挖掘最新威胁情报。



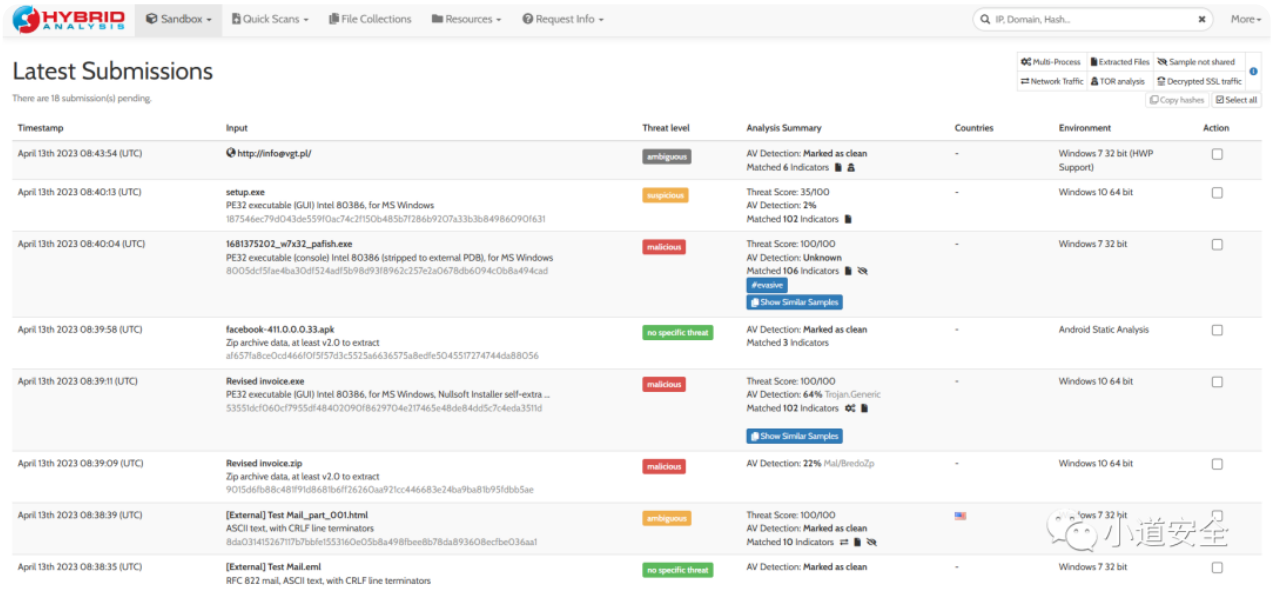
3、https://tria.ge/reports/public

该平台的恶意样本量还有恶意样本的种类还是比较丰富的，同时也有对应的恶意样本的分析报告，可以结合需要进行获取恶意样本。



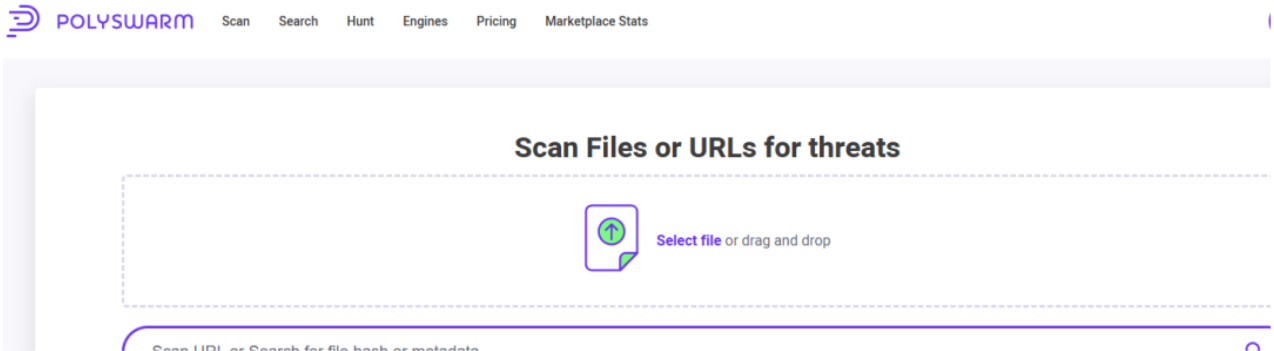
4、https://www.hybrid-analysis.com/

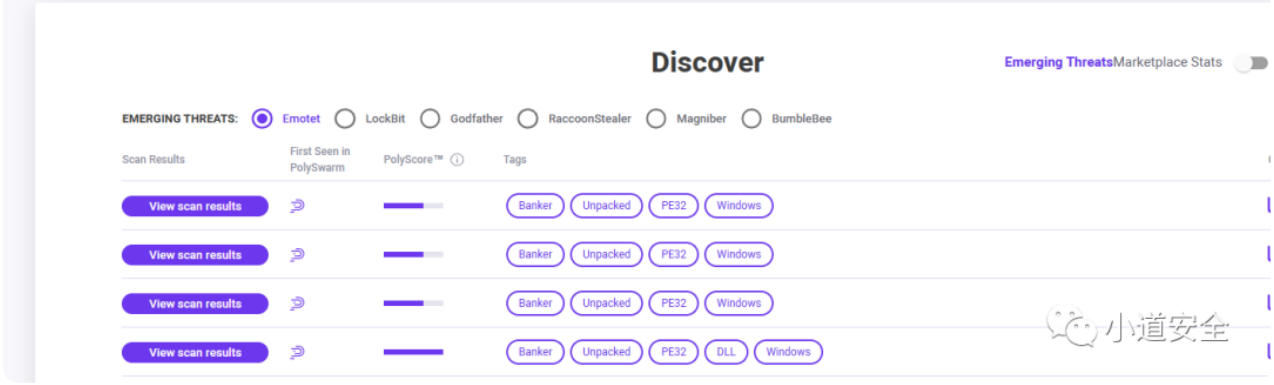
该平台对样本分析识别是否为恶意样本，采用AV的检测方案，同时检测的指标还很多，也对恶意样本进行风险评估，并且将样本里面的攻击方案和防护方案都做分析。



5、https://polyswarm.network/

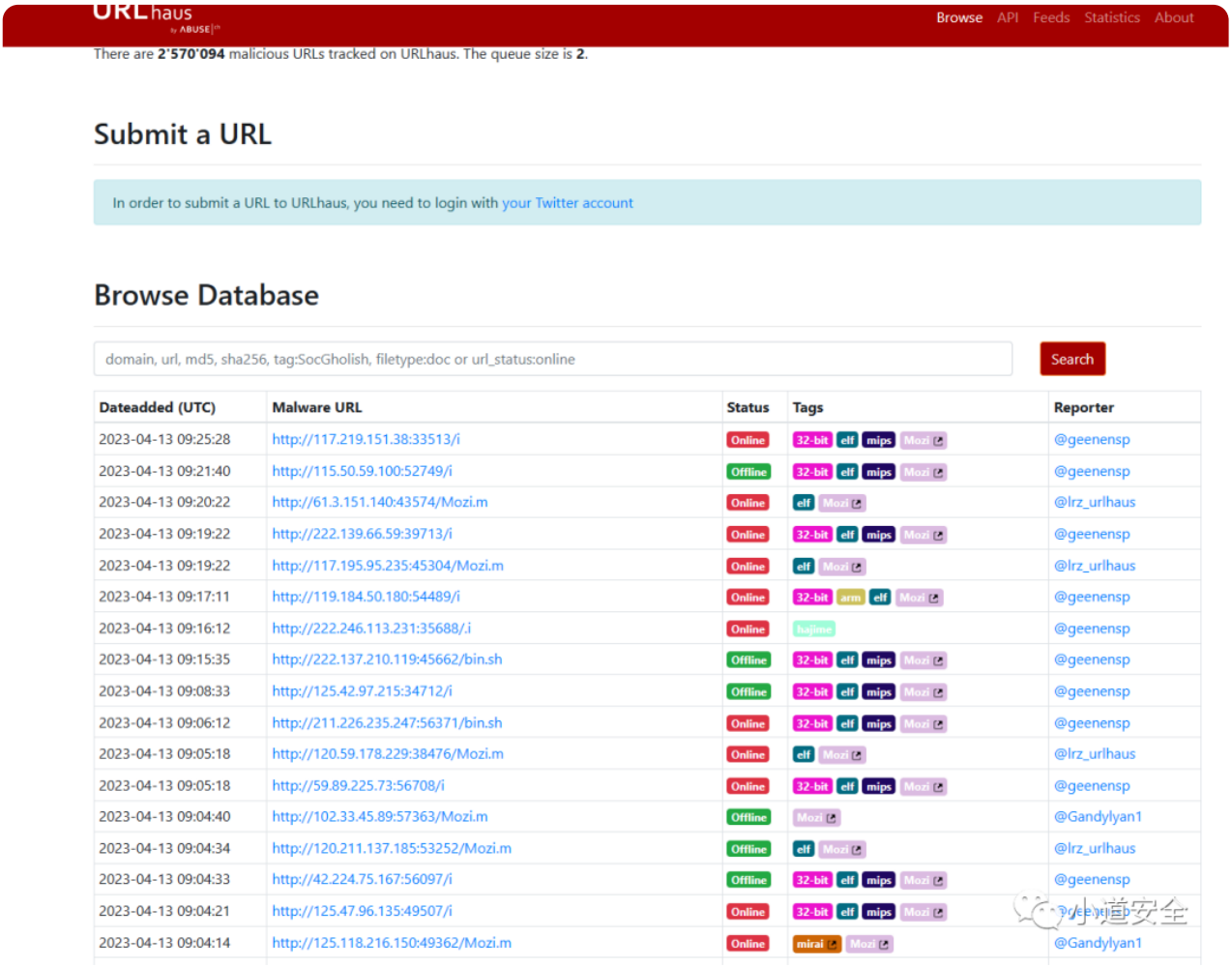
该平台的主要可以用于重点在于区块链和威胁情报这两块，在区块链这块是相对比较不错的。





6、https://urlhaus.abuse.ch/

这个平台主要是用于查验URL、md5、sha256等相关的恶意数据。



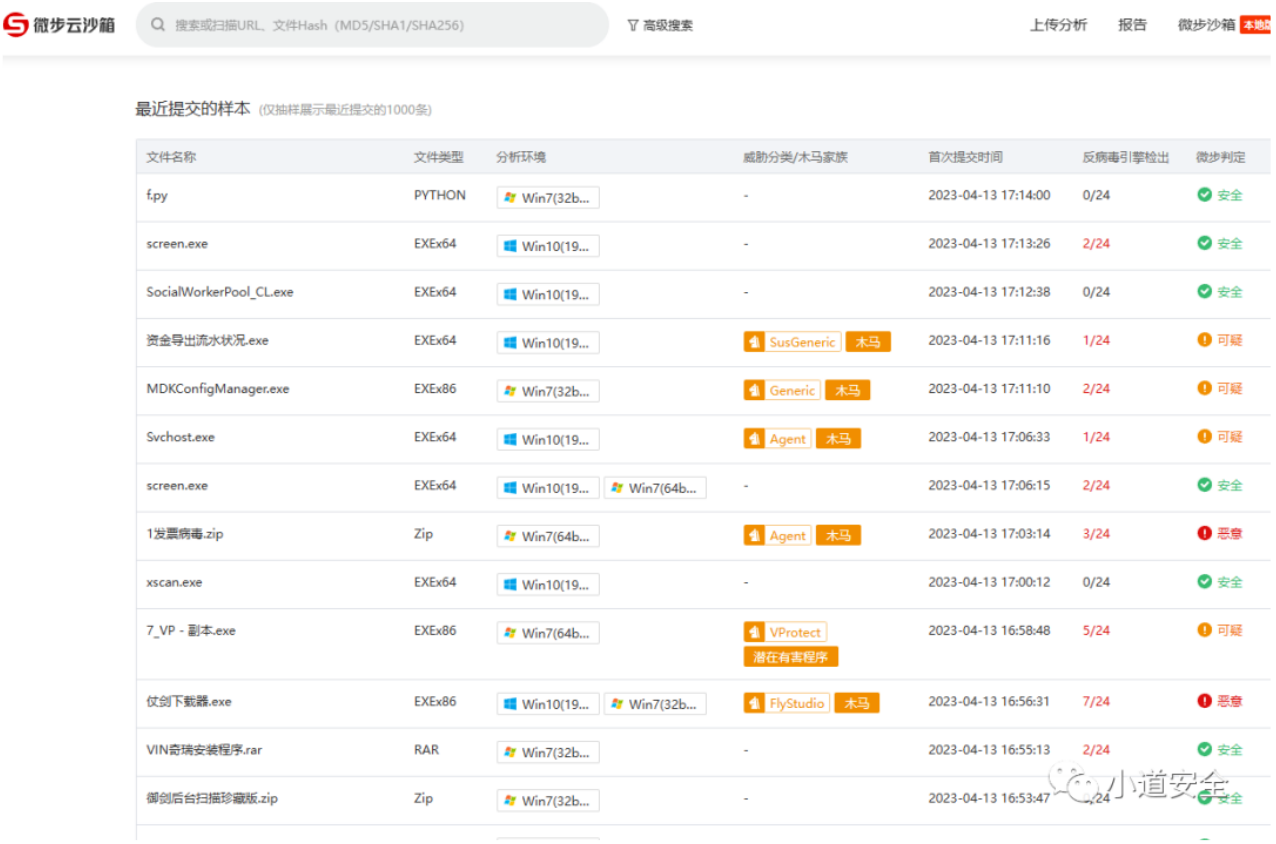
国内恶意样本源

1、微步在线云沙箱：

https://s.threatbook.com/

这个微步云沙箱平台的恶意样本也是各种类型都有并且样本量也很多，

对恶意样本分析也很详细的。国内的样本我基本都是在这里去挖掘的。



2、奇安信威胁情报中心:

https://ti.qianxin.com/

这个平台的恶意样本和威胁情报分析还是很不错，对于威胁情报分析奇安信还是很专业的，可以结合前面平台进行分析和恶意样本获取。

3、腾讯哈勃分析系统：

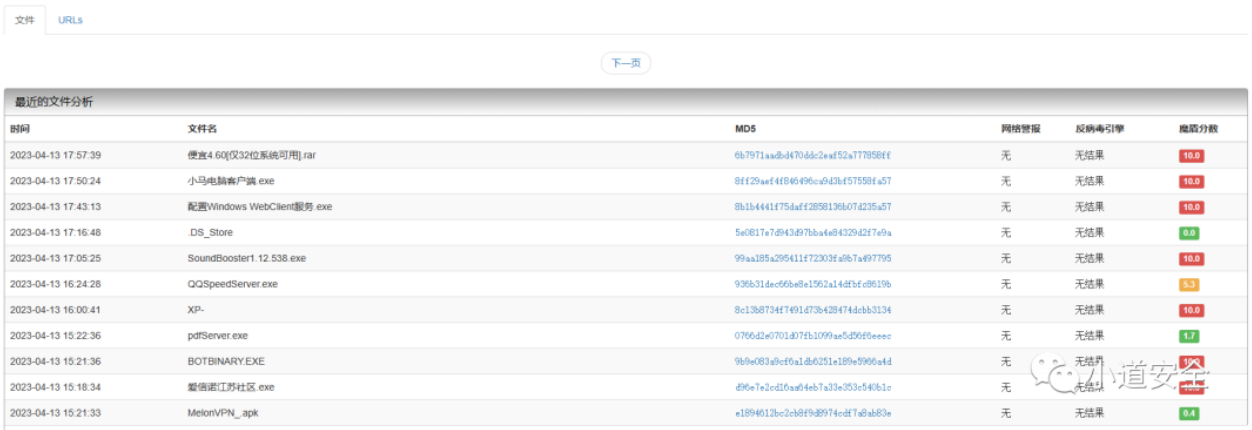
https://habo.qq.com

这个平台也是个很成熟的恶意样本自动化分析平台，同时上传样本的量也还可以。

4、魔盾安全分析：

https://www.maldun.com/analysis/

这个平台的检测分析是基于Yara规则进行对样本分析的，恶意样本的量也还可以。



推荐阅读

一起来逆向分析某黑产APP

这个假微信软件有点套路

对吃鸡APP的分析