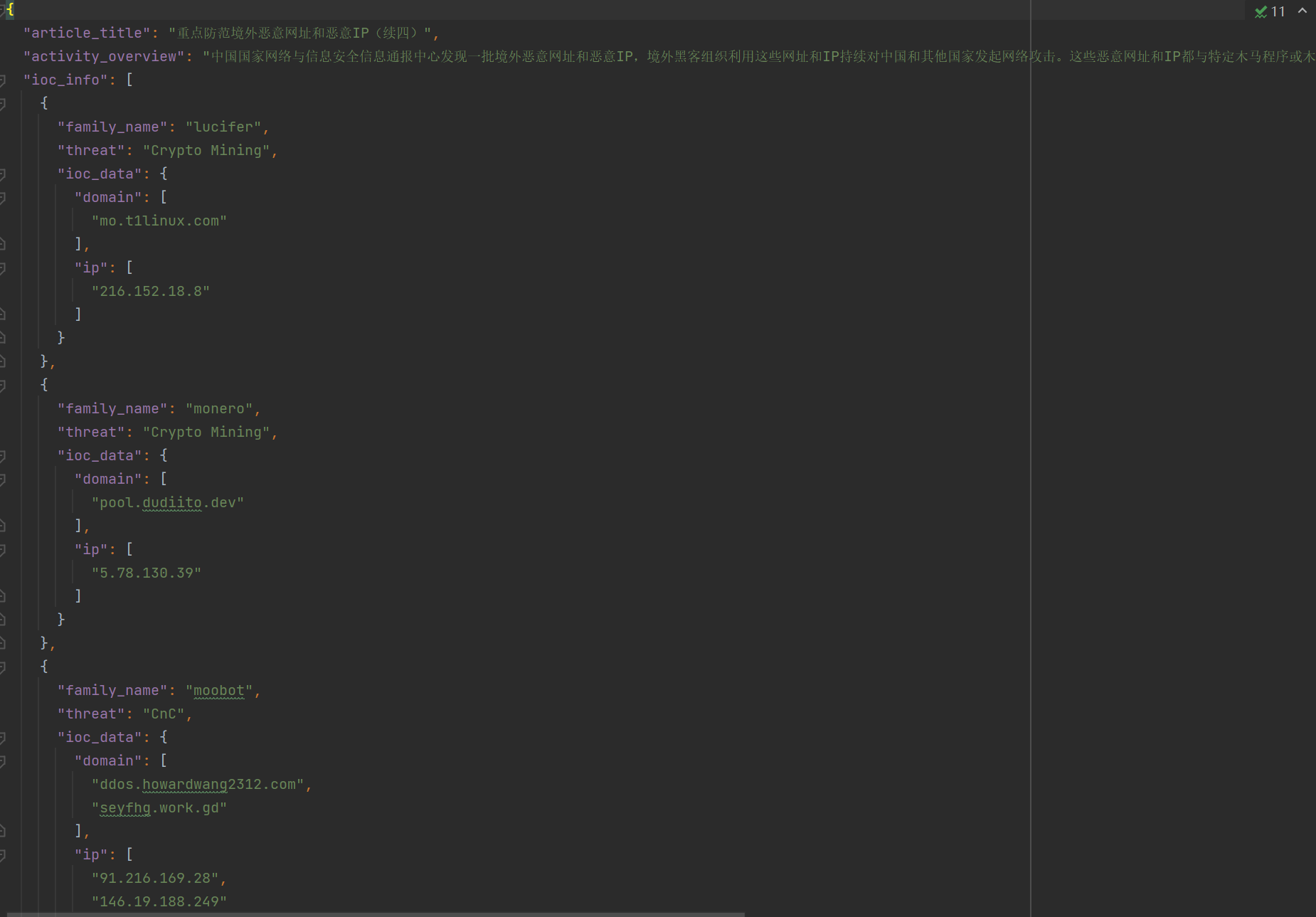
1. 利用大模型从威胁情报的html中提取IOC信息，对html页面清洗删除标签，保留纯文本，模型返回的 JSON 格式的结果，包括：IOC信息，文章威胁内容概括。在本地测试了提取效果。

测试文章和提取结果如下：





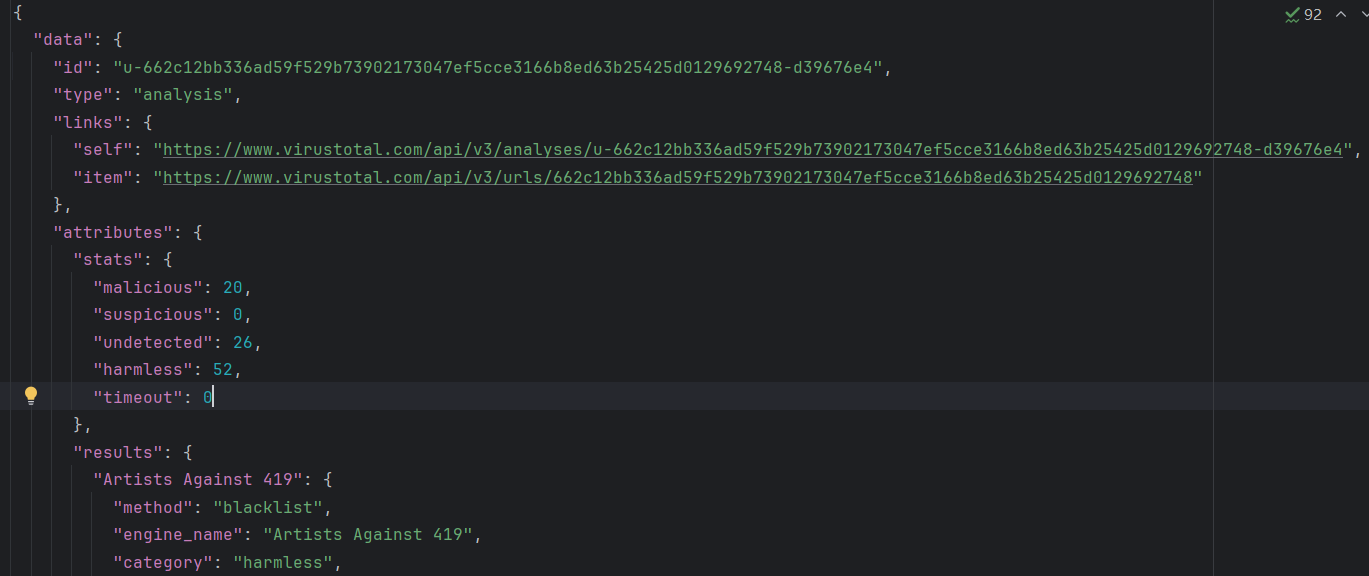
曾家豪

1. virustotal api调研

分析URL ip domai的api使用都类似，无非是需要修改请求的地址某个部分，这三类api的种类都一样，返回的结构也一样，因此以url举例：

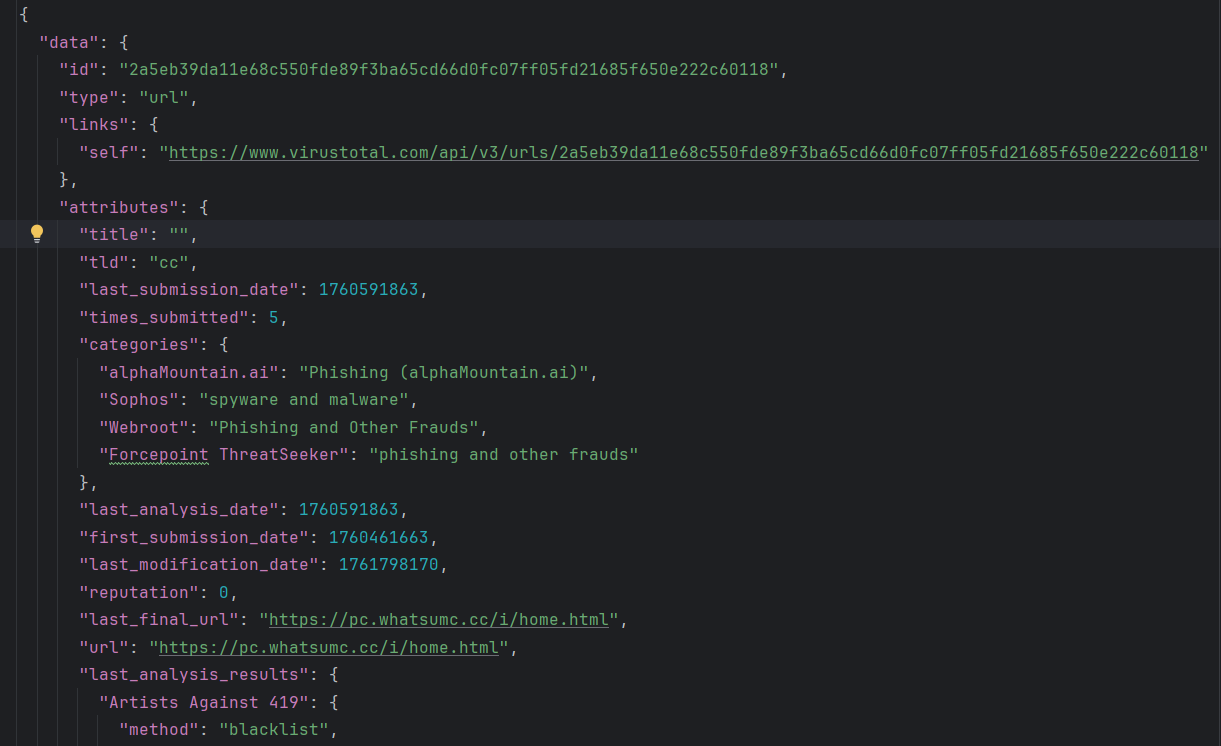
**Scan URL**

这个api的话，会返回分析id。需要进一步用这个分析id去查扫描结果，如下：



**Get a URL report**

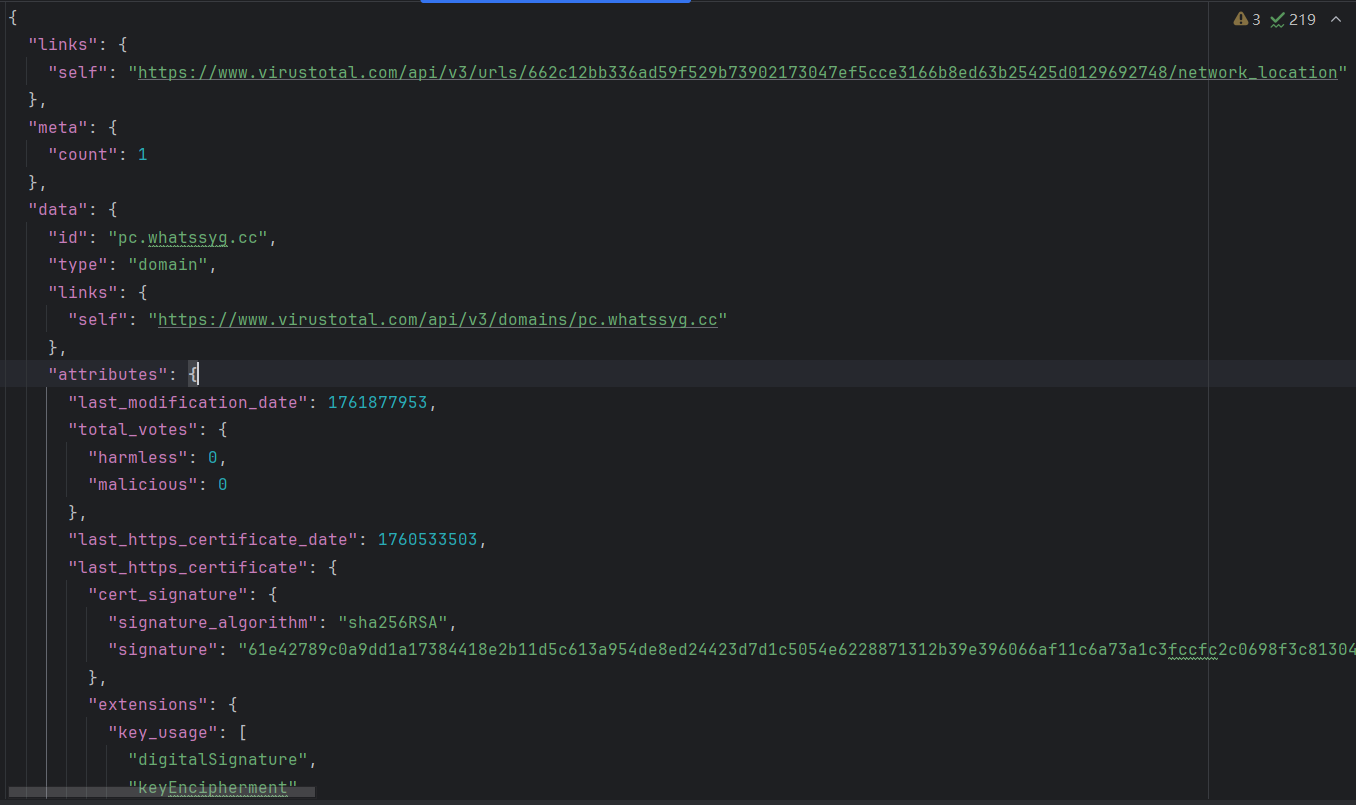
该api直接返回url object，结果如下：

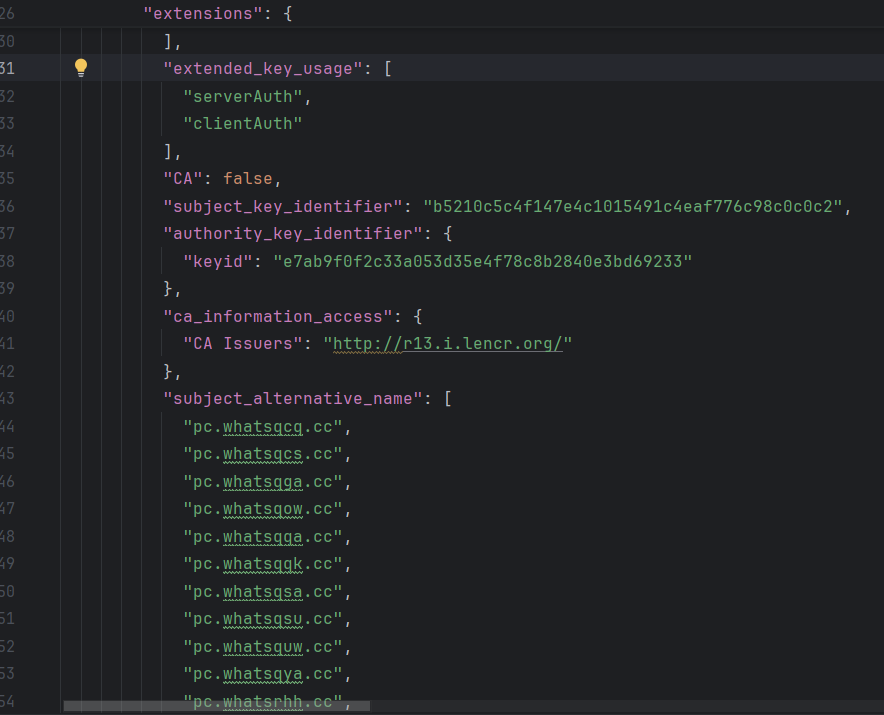


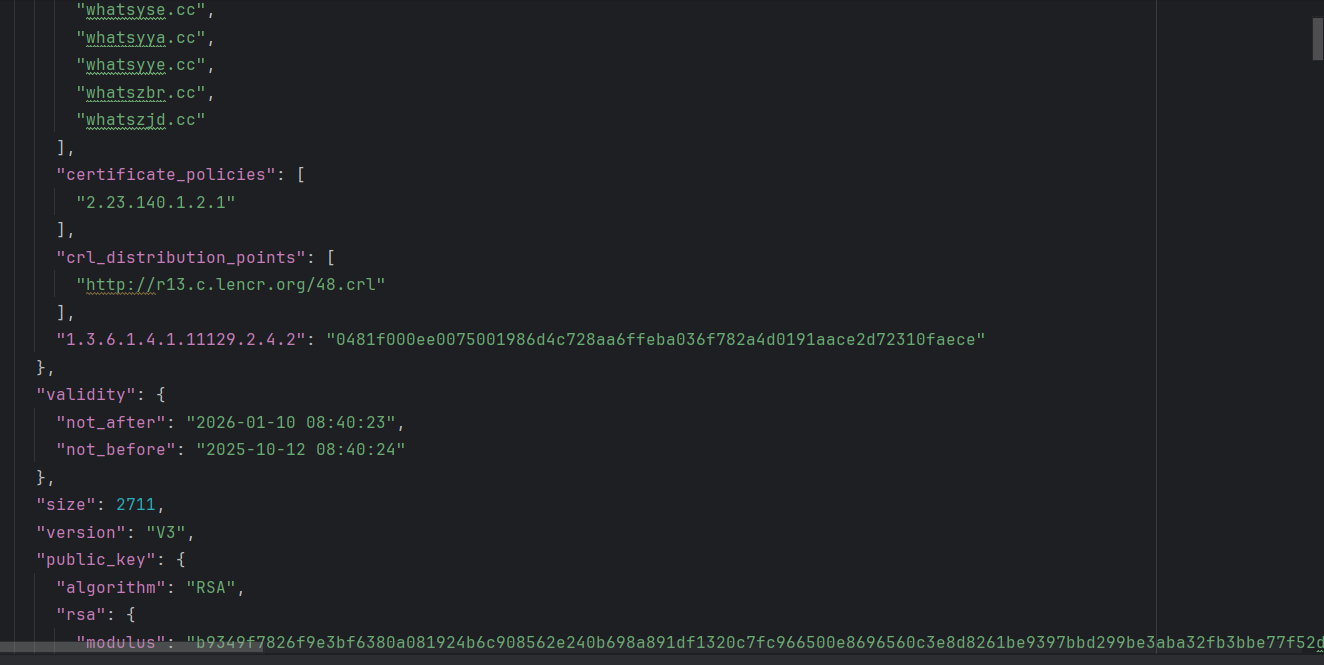
**Get objects related to a URL**（最有效的api）

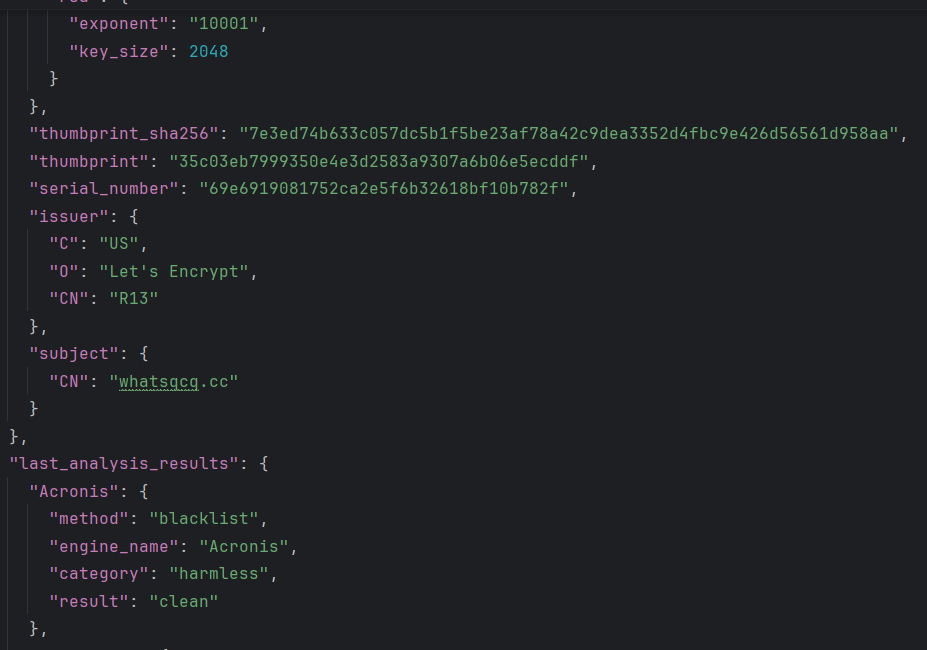
能获取复数个和该url相关的object，其中包含我们需要的信息，如解析出来的ip whois甚至还有其他关联的子域名等等，其api的使用见：<https://docs.virustotal.com/reference/urls-relationships>，Object中对应的字段含义和该api所需要的参数relationship的种类见<https://docs.virustotal.com/reference/url-object>

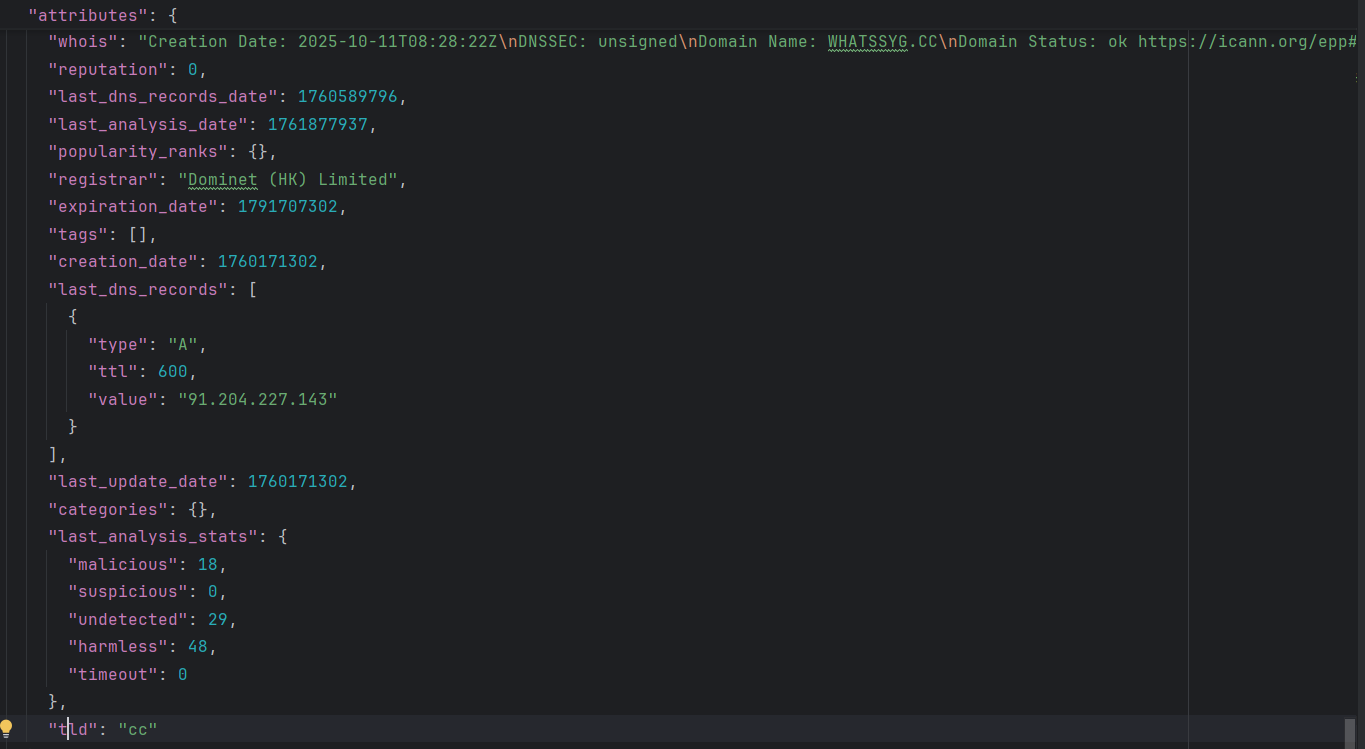
返回结果如下：





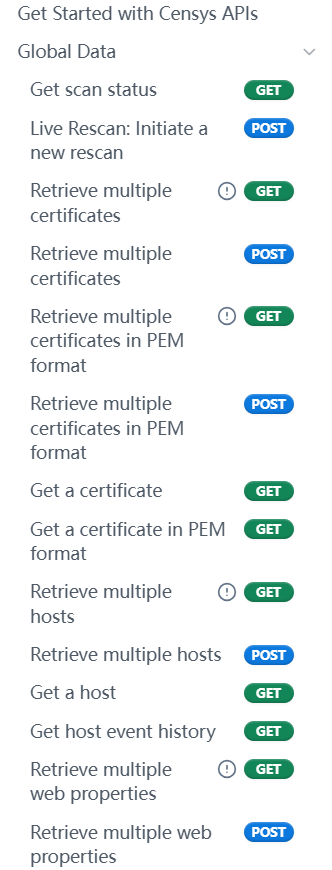
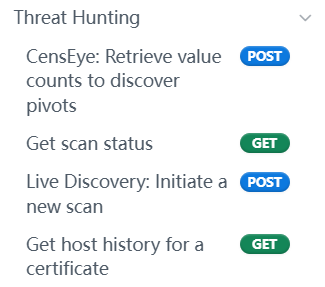






1. Censys api

免费，但是很多功能需要付费，且未找到适用于我们查询的api类。

1. AbuseIPDB api

Api使用文档：<https://docs.abuseipdb.com/?python#check-endpoint>

只能用于ip解析。

Check：可以在这里查看有关所查询 IP 地址的详细信息，例如版本、来源国家/地区、使用类型、ISP 和域名。当然，还有非常有价值的滥用报告。

