

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。

13-04-2023 08:23	3717c082c3240bf7077f920c3...	Running	3717c08...
13-04-2023 08:23	2859354225.zip	Submission	c6439ec...
13-04-2023 08:23	9ynpILu9GgPHh7.exe	Running	7e47da0...
13-04-2023 08:23	dropper-nosandbox.exe	Running	2760a30...
13-04-2023 08:23	Tar59FD.tmp	Submission	1919aab...
13-04-2023 08:22	https://www.adobe.com	Submission	N/A
13-04-2023 08:22	https://trustfidel.com/ist/earu...	Running	N/A
13-04-2023 08:22	27254635bcf1d1141bbd3e09...	Running	2725463...
13-04-2023 08:22	ln.pdf	Running	edb80fb...
13-04-2023 08:22	Re_Reema-Russia_Phishing.msg	Running	2b8e55c...
13-04-2023 08:22	76fd023676f65b33356215b5...	Running	76fd023...
13-04-2023 08:21	Z8nhz6T5fGUYBOG.exe	Running	794526c...
13-04-2023 08:21	5952874280bc7d8e66b1f142...	10 Reported	5952874...

amadey redline lada mari discovery evasion infostealer persistence spyware stealer trojan

小道安全

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。

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
April 13th 2023 08:43:54 (UTC)	http://infoevgt.pl/	ambiguous	AV Detection: Marked as clean Matched 6 Indicators	-	Windows 7 32 bit (HWP Support)	<input type="checkbox"/>
April 13th 2023 08:40:13 (UTC)	setup.exe PE32 executable (GUI) Intel 80386, for MS Windows 187546ec79d043de539f0ac74c21f50e485b72868f207a33b3b84986090f631	suspicious	Threat Score: 35/100 AV Detection: 2% Matched 102 Indicators	-	Windows 10 64 bit	<input type="checkbox"/>
April 13th 2023 08:40:04 (UTC)	1681375202_wx32_pafish.exe PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows 8005d5f5fae4ba30d1514ad15b9b9d9318962c57e2a0678db6094c0b8a494cad	malicious	Threat Score: 100/100 AV Detection: Unknown Matched 106 Indicators	-	Windows 7 32 bit	<input type="checkbox"/>
April 13th 2023 08:39:58 (UTC)	facebook-411.0.0.0.33.apk Zip archive data, at least v2.0 to extract af6571a8ce0cd466f0f9f5f3c5525a6636575a8edfe50455f7274744da88056	no specific threat	AV Detection: Marked as clean Matched 3 Indicators	-	Android Static Analysis	<input type="checkbox"/>
April 13th 2023 08:39:11 (UTC)	Revised Invoice.exe PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extra ... 5355fda1060c77935df4840209f0f8629704c217465e48de84d65c7c4eda351fd	malicious	Threat Score: 100/100 AV Detection: 64% Trojan.Generic Matched 102 Indicators	-	Windows 10 64 bit	<input type="checkbox"/>
April 13th 2023 08:39:09 (UTC)	Revised Invoice.zip Zip archive data, at least v2.0 to extract 90f5d6fbb8c48f9f9d868f0f726260a921cc446683c24ba9ba8fb9f5fbb5aee	malicious	AV Detection: 22% Mal/BredoZp	-	Windows 10 64 bit	<input type="checkbox"/>
April 13th 2023 08:38:39 (UTC)	[External] Test Mail_part_001.html ASCII text, with CRLF line terminators 8da0314f526717f7b6fe15316e0e05b8a498fbee8b78da893608ecfbc036aa1	ambiguous	Threat Score: 100/100 AV Detection: Marked as clean Matched 10 Indicators	-	Windows 7 32 bit	<input type="checkbox"/>
April 13th 2023 08:38:35 (UTC)	[External] Test Mail.html RFC 822 mail, ASCII text, with CRLF line terminators	no specific threat	AV Detection: Marked as clean	-	Windows 7 32 bit	<input type="checkbox"/>

5、https://polyswarm.network/

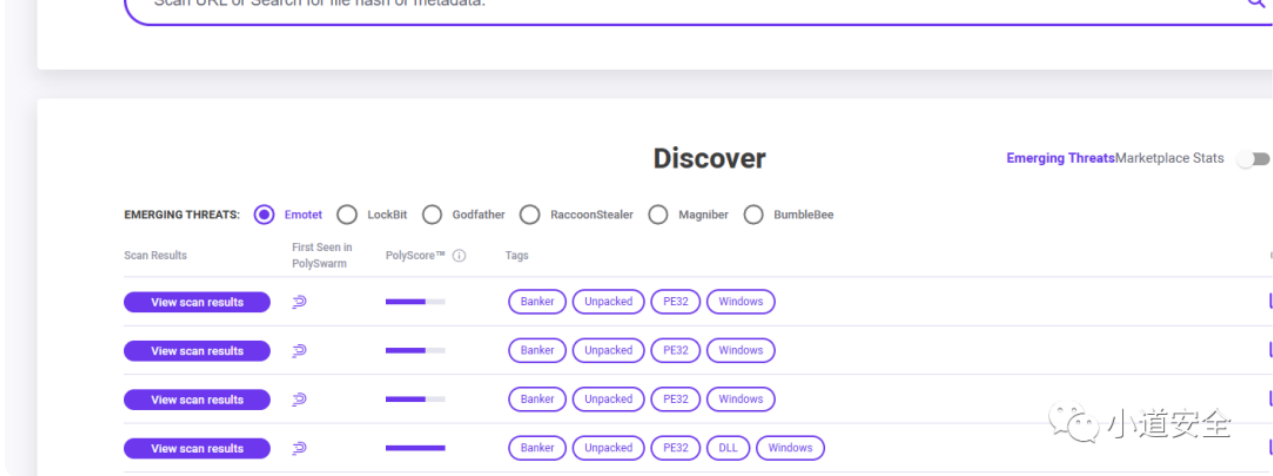
该平台的主要可以用于重点在于区块链和威胁情报这两块，在区块链这块是相对比较不错的。

POLYSWARM Scan Search Hunt Engines Pricing Marketplace Stats

Scan Files or URLs for threats



Select file or drag and drop



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。

URLhaus

ABUSE™

Browse API Feeds Statistics About

There are 2'570'094 malicious URLs tracked on URLhaus. The queue size is 2.

Submit a URL

In order to submit a URL to URLhaus, you need to login with your Twitter account

Browse Database

domain, url, md5, sha256, tag:SocGhoshish, filetype:doc or url_status:online

Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2023-04-13 09:25:28	http://117.219.151.38:33513/i	Online	32-bit elf mips Mozi	@geenensp
2023-04-13 09:21:40	http://115.50.59.100:52749/i	Offline	32-bit elf mips Mozi	@geenensp
2023-04-13 09:20:22	http://61.3.151.140:43574/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2023-04-13 09:19:22	http://222.139.66.59:39713/i	Online	32-bit elf mips Mozi	@geenensp
2023-04-13 09:19:22	http://117.195.95.235:45304/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2023-04-13 09:17:11	http://119.184.50.180:54489/i	Online	32-bit arm elf Mozi	@geenensp
2023-04-13 09:16:12	http://222.246.113.231:35688/i	Online	haxme	@geenensp
2023-04-13 09:15:35	http://222.137.210.119:45662/bin.sh	Offline	32-bit elf mips Mozi	@geenensp
2023-04-13 09:08:33	http://125.42.97.215:34712/i	Offline	32-bit elf mips Mozi	@geenensp
2023-04-13 09:06:12	http://211.226.235.247:56371/bin.sh	Online	32-bit elf mips Mozi	@geenensp
2023-04-13 09:05:18	http://120.59.178.229:38476/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2023-04-13 09:05:18	http://59.89.225.73:56708/i	Online	32-bit elf mips Mozi	@geenensp
2023-04-13 09:04:40	http://102.33.45.89:57363/Mozi.m	Offline	Mozi	@Gandylyan1
2023-04-13 09:04:34	http://120.211.137.185:53252/Mozi.m	Offline	elf Mozi	@lrz_urlhaus
2023-04-13 09:04:33	http://42.224.75.167:56097/i	Offline	32-bit elf mips Mozi	@geenensp
2023-04-13 09:04:21	http://125.47.96.135:49507/i	Online	32-bit elf mips Mozi	@geenensp
2023-04-13 09:04:14	http://125.118.216.150:49362/Mozi.m	Online	mirai Mozi	@Gandylyan1

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。

文件名称	文件类型	分析环境	威胁分类/木马家族	首次提交时间	反病毒引擎检出	微步判定
f.py	PYTHON	Win7(32b...	-	2023-04-13 17:14:00	0/24	安全
screen.exe	EXEx64	Win10(19...	-	2023-04-13 17:13:26	2/24	安全
SocialWorkerPool_CL.exe	EXEx64	Win10(19...	-	2023-04-13 17:12:38	0/24	安全
资金导出流水状况.exe	EXEx64	Win10(19...	SusGeneric 木马	2023-04-13 17:11:16	1/24	可疑
MDKConfigManager.exe	EXEx86	Win7(32b...	Generic 木马	2023-04-13 17:11:10	2/24	可疑
Svchost.exe	EXEx64	Win10(19...	Agent 木马	2023-04-13 17:06:33	1/24	可疑
screen.exe	EXEx64	Win10(19... Win7(64b...	-	2023-04-13 17:06:15	2/24	安全
1发震病毒.zip	Zip	Win7(64b...	Agent 木马	2023-04-13 17:03:14	3/24	恶意
xscan.exe	EXEx64	Win10(19...	-	2023-04-13 17:00:12	0/24	安全
7_VP - 副本.exe	EXEx86	Win7(64b...	VProtect 潜在有害程序	2023-04-13 16:58:48	5/24	可疑
仗剑下载器.exe	EXEx86	Win10(19... Win7(32b...	FlyStudio 木马	2023-04-13 16:56:31	7/24	恶意
VIN寄瑞安装程序.rar	RAR	Win7(32b...	-	2023-04-13 16:55:13	2/24	安全
御剑后台扫描珍藏版.zip	Zip	Win7(32b...	-	2023-04-13 16:53:47	0/24	安全

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。



最近的文件分析					
时间	文件名	MDS	网络警报	反病毒引擎	魔盾分数
2023-04-13 17:57:39	便宜4.60[仅32位系统可用].rar	6b7971aa8b4470ddc2aaf52a777858ff	无	无结果	10.0
2023-04-13 17:50:24	小马电脑客户端.exe	8ff29aaf44849496ca943bf57559fa57	无	无结果	10.0
2023-04-13 17:43:13	配置Windows WebClient服务.exe	8b1b4441f75daf2858136a074235a57	无	无结果	10.0
2023-04-13 17:16:48	DS_Store	5e0817e7d943d97bba4e8432942f7e9a	无	无结果	9.9
2023-04-13 17:05:25	SoundBooster1.12.538.exe	9f9aa185a295411f72303fa0b7a497795	无	无结果	10.0
2023-04-13 16:24:28	QQSpeedServer.exe	936b314dc066a8e1562a14d4bfcb619b	无	无结果	5.3
2023-04-13 16:00:41	XP-	8c1368734f7491d73b428474dcb3134	无	无结果	10.0
2023-04-13 15:22:36	pdfServer.exe	0766d2a0701d0761099ae5d96f0eeec	无	无结果	1.7
2023-04-13 15:21:36	BOTBINARY.EXE	9b9e083a0cf0a1db0201e189e5996a4d	无	无结果	10.0
2023-04-13 15:18:34	微信诺江苏社区.exe	d96e7e2cd26aad4eb7a33c00c04b61c	无	无结果	10.0
2023-04-13 15:21:33	MelonVPN_.apk	e1894012b-c0cb8f5-8974c-df7a8ab83e	无	无结果	9.4

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

[官方主页](#) [下载新版](#) [问题反馈](#) [捐赠支持](#) 

浏览器扩展 Circle 阅读助手排版，版权归 mp.weixin.qq.com 所有