从大数据看境外黑客对我国互联网威胁

秦波@知道创宇

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- 姓名：秦波
- 公司：北京知道创宇信息技术有限公司
- 主要研究成果有：协编国家标准《Web 过滤防护产品标准》，OWASP《WAF 测试基准项目》；主编电信标准《Web 应用防火墙标准》，军方标准《军方web安全》等；专利联合发明《一种网络安全防护方法、设备和系统》，《通过自学习生成白名单防护规则》

KNOWNSEC
知 道 创 宇

目录

OWASP 中国
The Open Web Application Security Project

1.Web安全数据组成部分（每天4T）

- 收集20亿域名的漏洞信息
- 收集网络空间的组件指纹
- 收集60万+网站的被攻击数据

2.如何处理大数据

数据同步和查询机制

数据监控和分析

3.境外攻击情况

- 攻击数量统计
- 攻击方法统计
- 各国攻击例子

4.总结

大数据下的防护思路

研究安全大数据的意义

目录

OWASP 中国
The Open Web Application Security Project

1.Web安全数据组成部分（每天4T）

- 收集20亿域名的漏洞信息
- 收集网络空间的组件指纹
- 收集60万+网站的被攻击数据

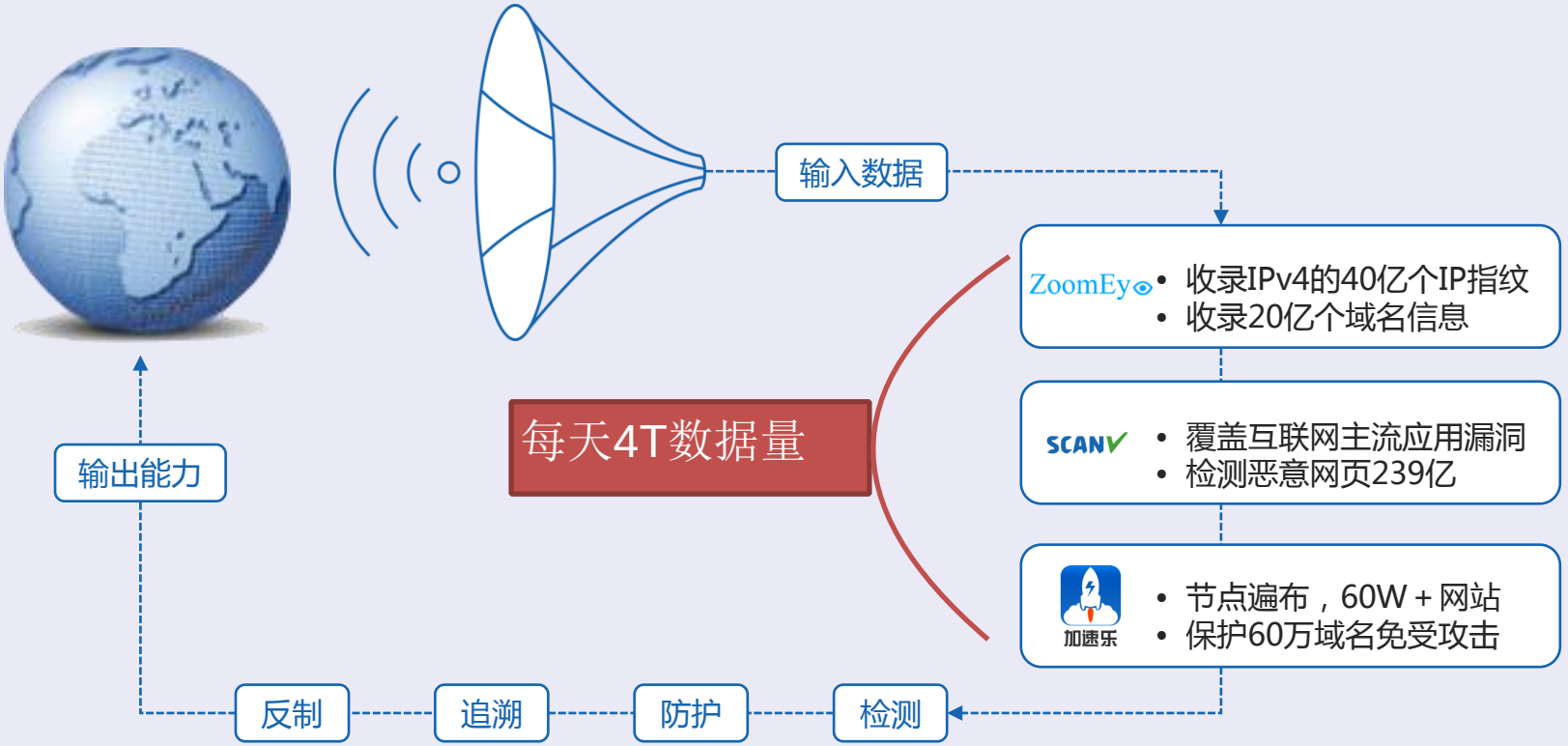
2.如何处理大数据
数据同步和查询机制
数据监控和分析

3.境外攻击情况
- 攻击数量统计
- 攻击方法统计
- 各国攻击例子

4.总结
大数据下的防护思路
研究安全大数据的意义

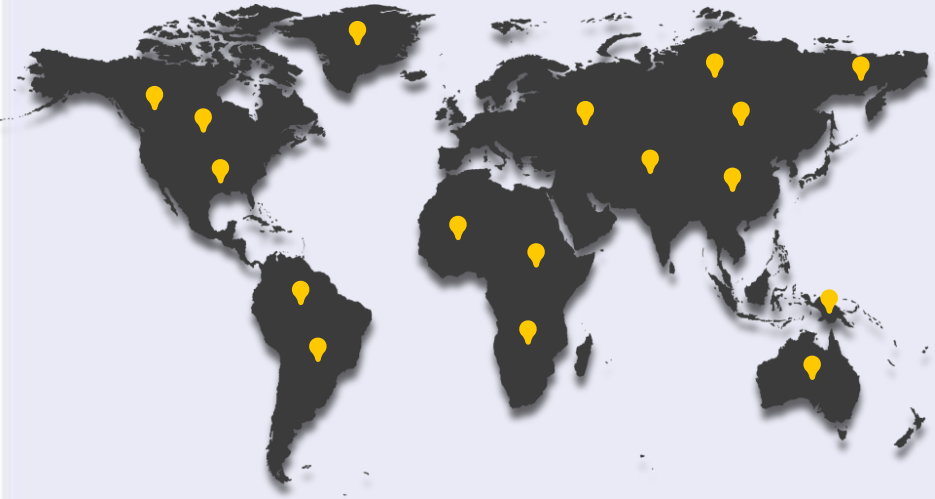
我们的数据来源是什么

OWASP 中国
The Open Web Application Security Project



监控节点、数据中心

OWASP 中国
The Open Web Application Security Project



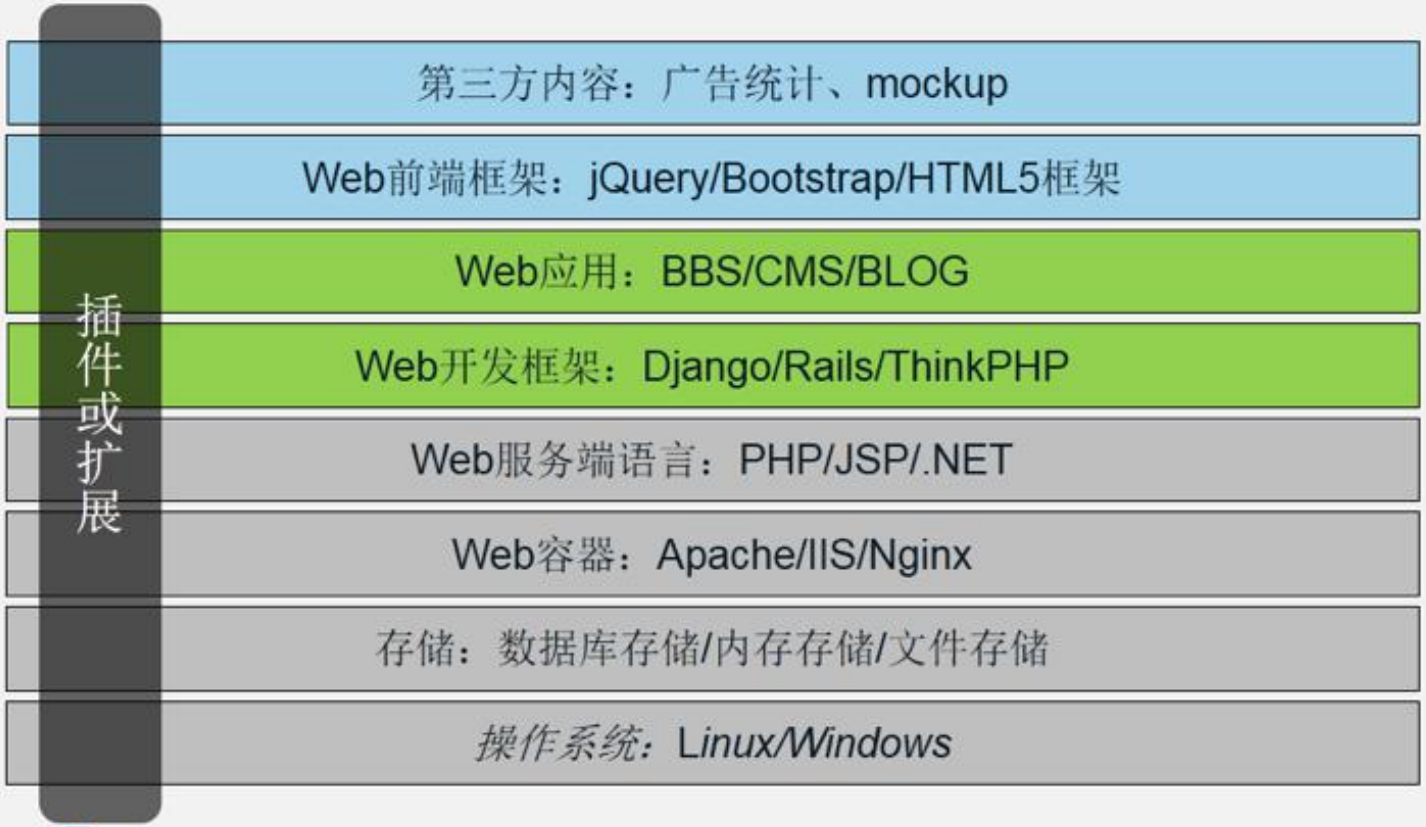
遍布全球的监控节点
40亿IP和20亿域名
数百亿递增的恶意URL
每天100T的日志数据

实时统计漏洞、攻击手法
分析行业、区域的安全Index变化值
溯源黑客形迹（无视代理）
锁定IP攻击信息总汇：
- 在哪天的哪个时间段发起过攻击
- 攻击过哪些网站、攻击过多少次
- 用过哪些工具
- 用过哪些已知漏洞

网络空间的组件层次

OWASP 中国
The Open Web Application Security Project

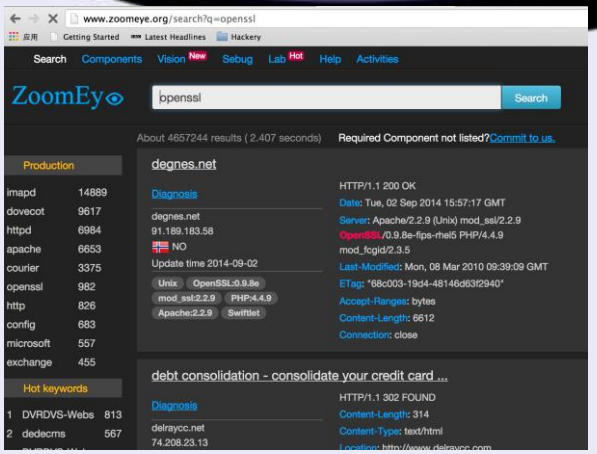
Web服务组件



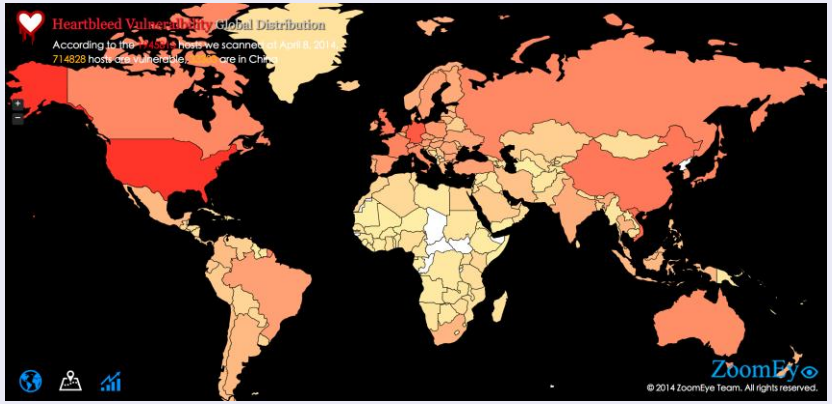
KNOWNSEC
知 道 安 全

ZoomEye—全球网络组件指纹库

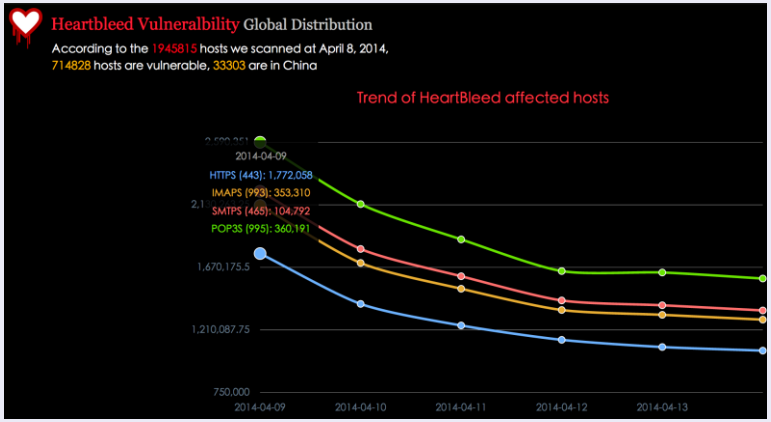
1.输入任何网络组件，比如openssl



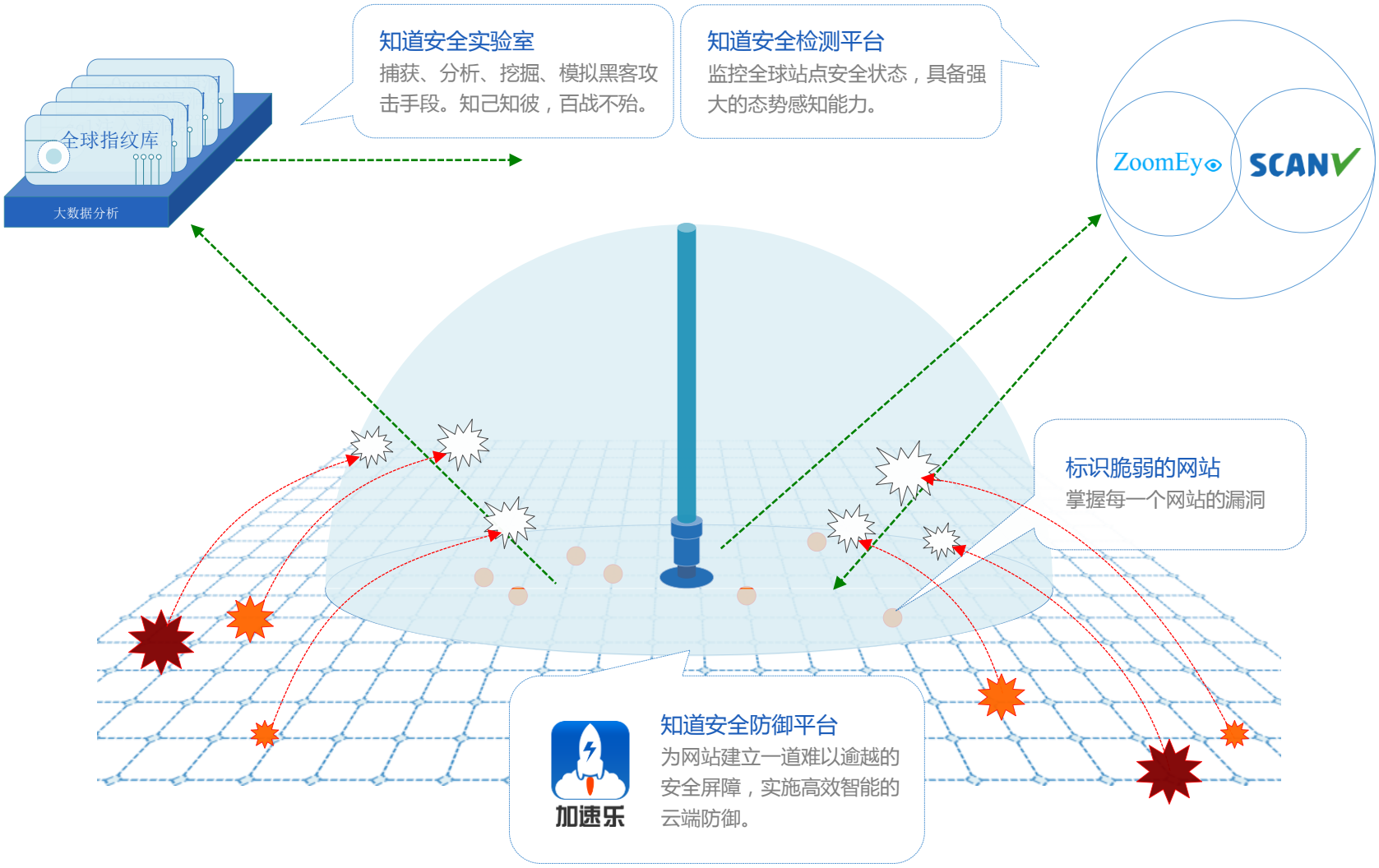
2.得到搜索结果详情



3.全球受影响的Openssl组件分布



4.每天修复情况统计分析


知道安全实验室
捕获、分析、挖掘、模拟黑客攻击手段。知己知彼，百战不殆。
知道安全检测平台
监控全球站点安全状态，具备强大的态势感知能力。
全球指纹库
大数据分析
ZoomEye
SCANV
标识脆弱的网站
掌握每一个网站的漏洞
加速乐
知道安全防御平台
为网站建立一道难以逾越的安全屏障，实施高效智能的云端防御。

目录

OWASP 中国
The Open Web Application Security Project

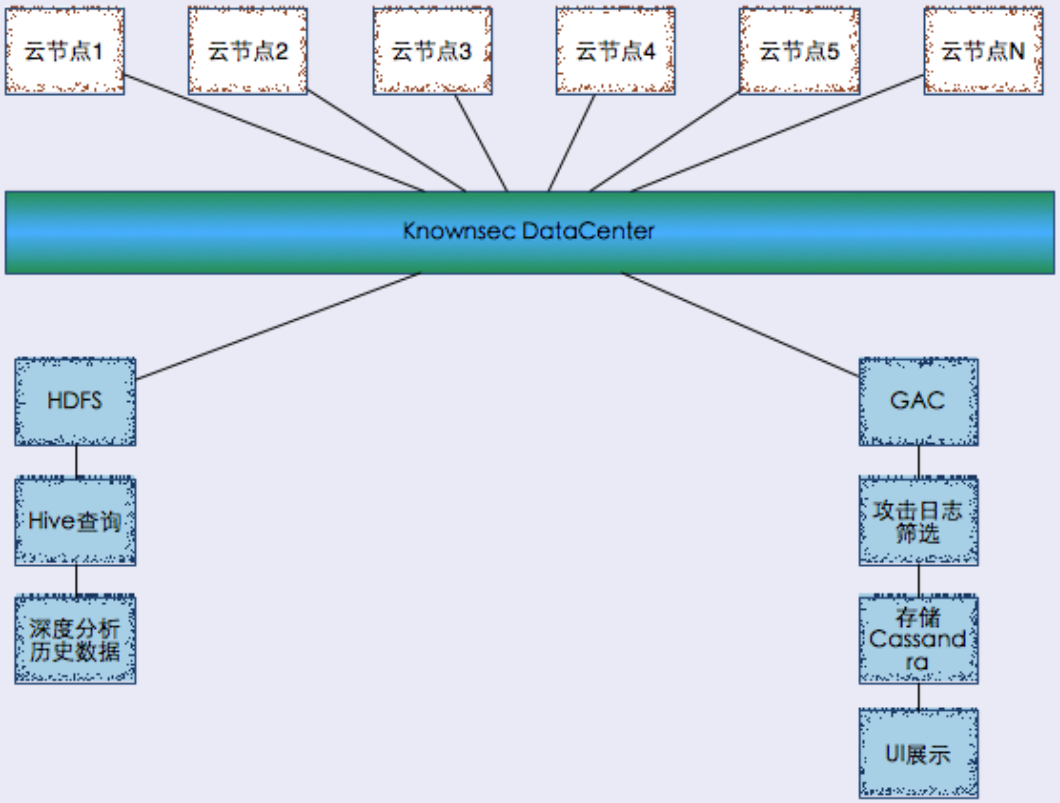
1.Web安全数据组成部分（每天4T）
- 收集20亿域名的漏洞信息
- 收集网络空间的组件指纹
- 收集60万+网站的被攻击数据

2.如何处理大数据
数据同步和查询机制
数据监控和分析

3.境外攻击情况
- 攻击数量统计
- 攻击方法统计
- 各国攻击例子

4.总结
大数据下的防护思路
研究安全大数据的意义

如何处理安全数据机制



云节点日志定期同步到数据中心，每小时通过UI自动展示；所有数据可通过Hive历史查询不同唯独的结果。

Hive查询实例

OWASP 中国
The Open Web Application Security Project

Hive例子：统计2014年9月8日攻击政府网站最多的IP Top 10

```
select client_ip, count(1) as times from rcfiles_2014 where
logdate='2014-09-08' and tag='attack' and host like '%.gov.cn'
group by client_ip
sort by times desc
limit 10;
```

```
hive> select client_ip, count(1) as times from [redacted] where
    > logdate='2014-09-08' and tag='attack' and host like '%.gov.cn'
    > group by client_ip
    > sort by times desc
    > limit 10;
Total MapReduce jobs = 3
Launching Job 1 out of 3
Number of reduce tasks not specified. Estimated from input data size: 1
In order to change the average load for a reducer (in bytes):
  set hive.exec.reducers.bytes.per.reducer=<number>
In order to limit the maximum number of reducers:
  set hive.exec.reducers.max=<number>
In order to set a constant number of reducers:
  set mapred.reduce.tasks=<number>
Starting Job = job_1409580006455_1407, Tracking URL = http://[redacted]/prox
Kill Command = [redacted] job  -kill job_140
Hadoop job information for Stage-1: number of mappers: 18; number of reducers: 1
2014-09-10 15:26:56,896 Stage-1 map = 0%,  reduce = 0%
2014-09-10 15:27:04,197 Stage-1 map = 6%,  reduce = 0%, Cumulative CPU 3.34 sec
2014-09-10 15:27:05,232 Stage-1 map = 22%,  reduce = 0%, Cumulative CPU 13.51 sec
2014-09-10 15:27:06,270 Stage-1 map = 28%,  reduce = 0%, Cumulative CPU 17.54 sec
2014-09-10 15:27:07,302 Stage-1 map = 28%,  reduce = 0%, Cumulative CPU 17.54 sec
2014-09-10 15:27:08,341 Stage-1 map = 46%,  reduce = 0%, Cumulative CPU 32.99 sec
2014-09-10 15:27:09,378 Stage-1 map = 56%,  reduce = 0%, Cumulative CPU 50.29 sec
2014-09-10 15:27:10,411 Stage-1 map = 67%,  reduce = 0%, Cumulative CPU 62.04 sec
2014-09-10 15:27:11,445 Stage-1 map = 81%,  reduce = 0%, Cumulative CPU 81.74 sec
2014-09-10 15:27:12,487 Stage-1 map = 81%,  reduce = 0%, Cumulative CPU 81.74 sec
2014-09-10 15:27:13,521 Stage-1 map = 84%,  reduce = 0%, Cumulative CPU 82.42 sec
```

建立查询任务的截图

```
MapReduce Jobs Launched:
Job 0: Map: 18  Reduce: 1   Cumulative CPU: 100.39 sec   HDFS Read: 243417615 HDFS Write: 77825 SUCCESS
Job 1: Map: 1  Reduce: 1   Cumulative CPU: 5.21 sec   HDFS Read: 78255 HDFS Write: 380 SUCCESS
Job 2: Map: 1  Reduce: 1   Cumulative CPU: 2.48 sec   HDFS Read: 810 HDFS Write: 210 SUCCESS
Total MapReduce CPU Time Spent: 1 minutes 48 seconds 80 msec
OK
139.210.[redacted]  432673
112.65.2[redacted]  186941
202.106.2[redacted] 119697
116.213.1[redacted]  24847
209.132.1[redacted]  20842
103.230.1[redacted]  20277
125.46.5[redacted]   19325
211.95.7[redacted]   17352
202.102.[redacted]   16146
59.63.1[redacted]    15539
Time taken: 207.055 seconds, Fetched: 10 row(s)
hive>
```

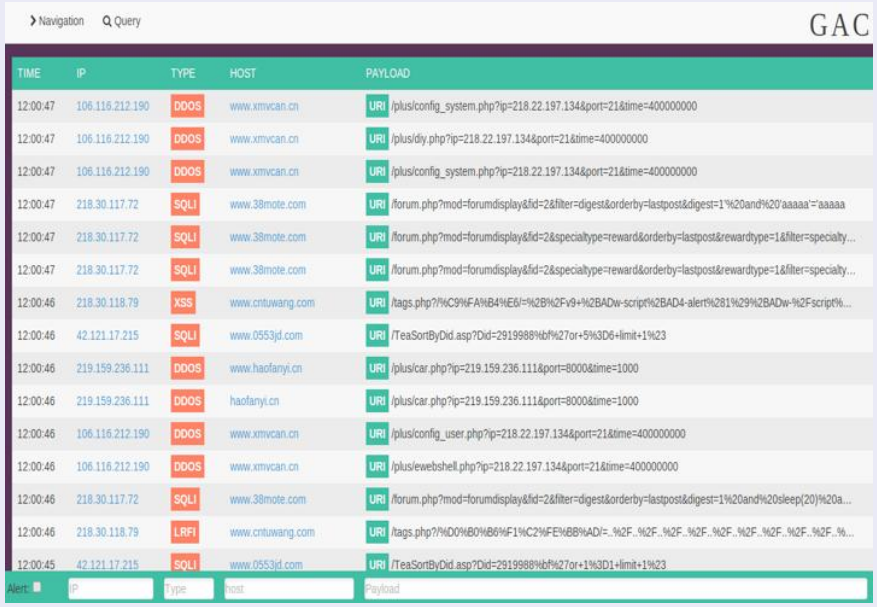
任务结束的结果显示截图

实时监控

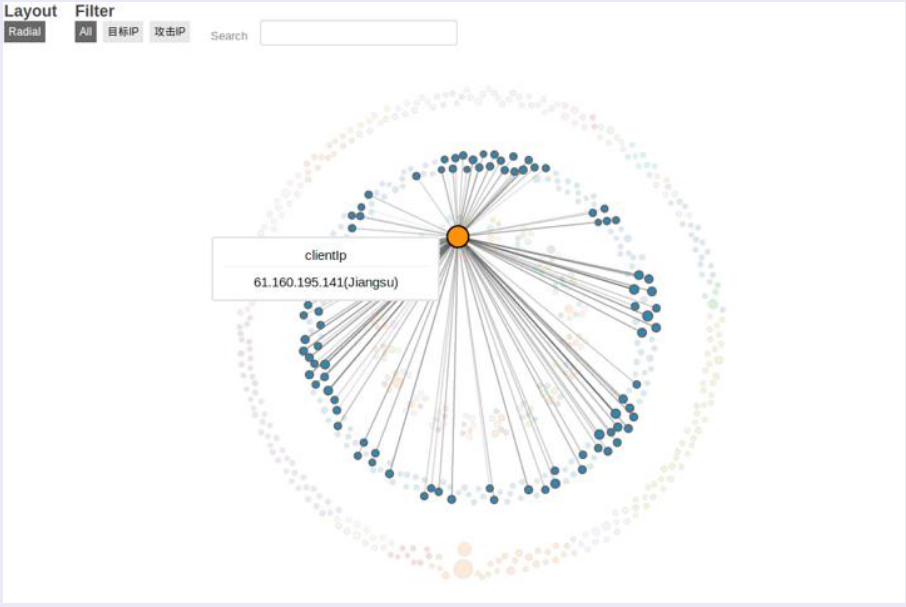
OWASP 中国
The Open Web Application Security Project

展示攻击流

OWASP 中国
The Open Web Application Security Project



攻击IP和目标HOST以及PAYLOAD（攻击字符串）

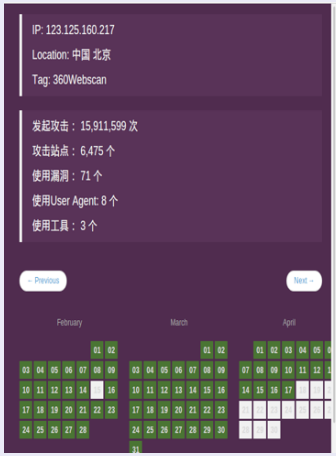


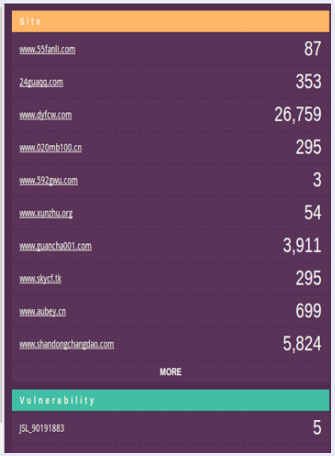
Ddos攻击源

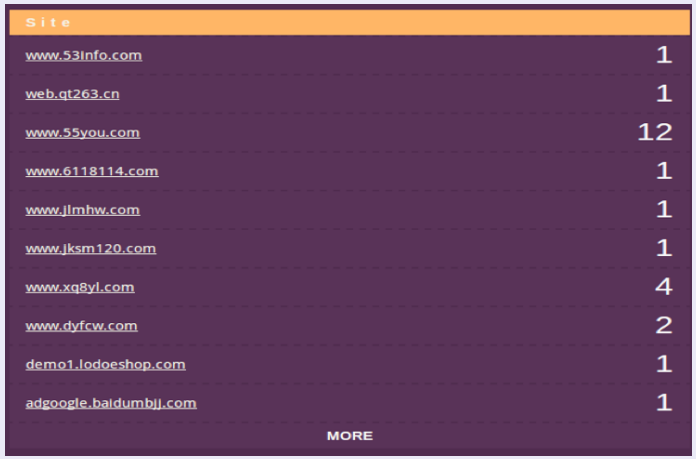
攻击IP详细信息

OWASP 中国
The Open Web Application Security Project

分析攻击IP的时间、攻击对象、Useragent、所用工具等







目录

OWASP 中国
The Open Web Application Security Project

1.Web安全数据组成部分（每天4T）
- 收集20亿域名的漏洞信息
- 收集网络空间的组件指纹
- 收集60万+网站的被攻击数据

2.如何处理大数据
数据同步和查询机制
数据监控和分析

3.境外攻击情况
- 攻击数量统计
- 攻击方法统计
- 各国攻击例子

4.总结
大数据下的防护思路
研究安全大数据的意义

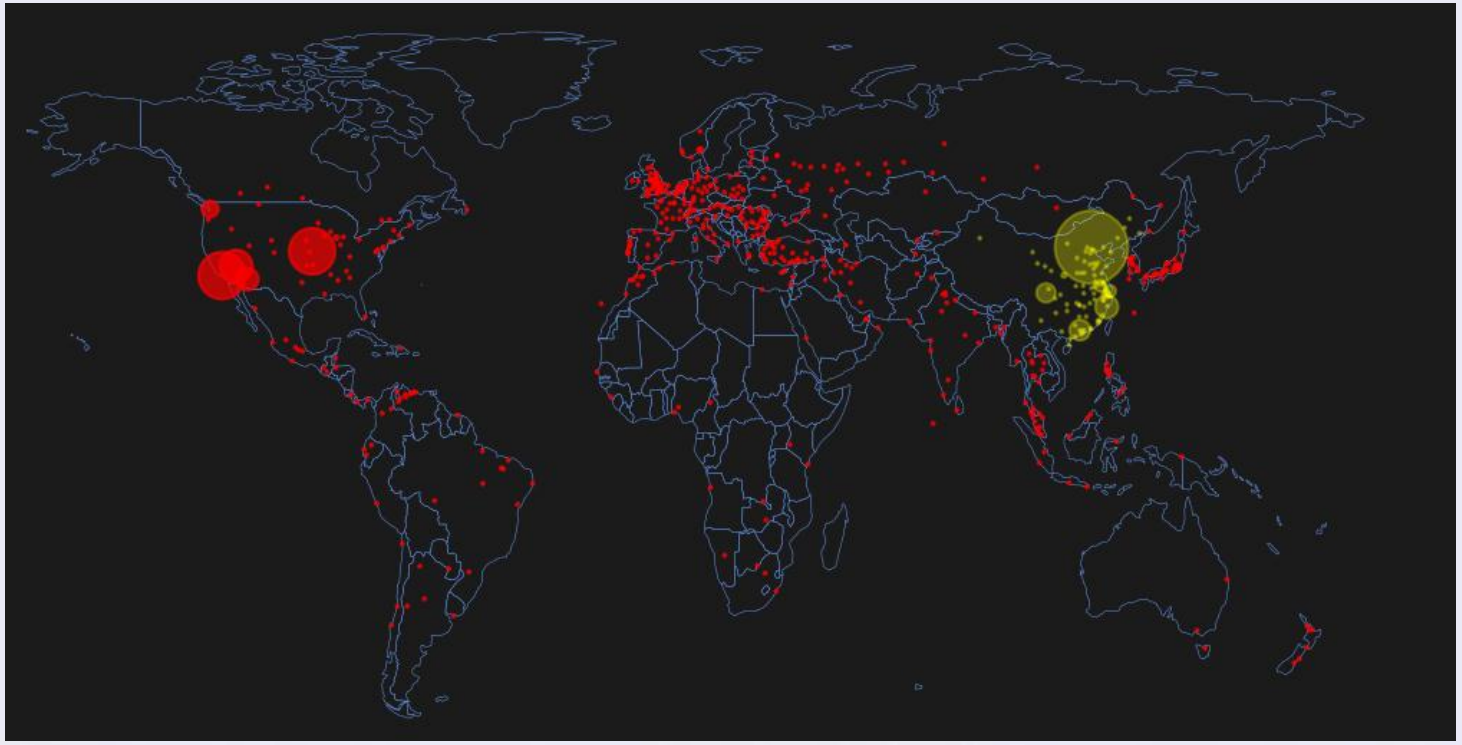
2014年7月攻击趋势

OWASP 中国
The Open Web Application Security Project

全球攻击分布情况

OWASP 中国
The Open Web Application Security Project

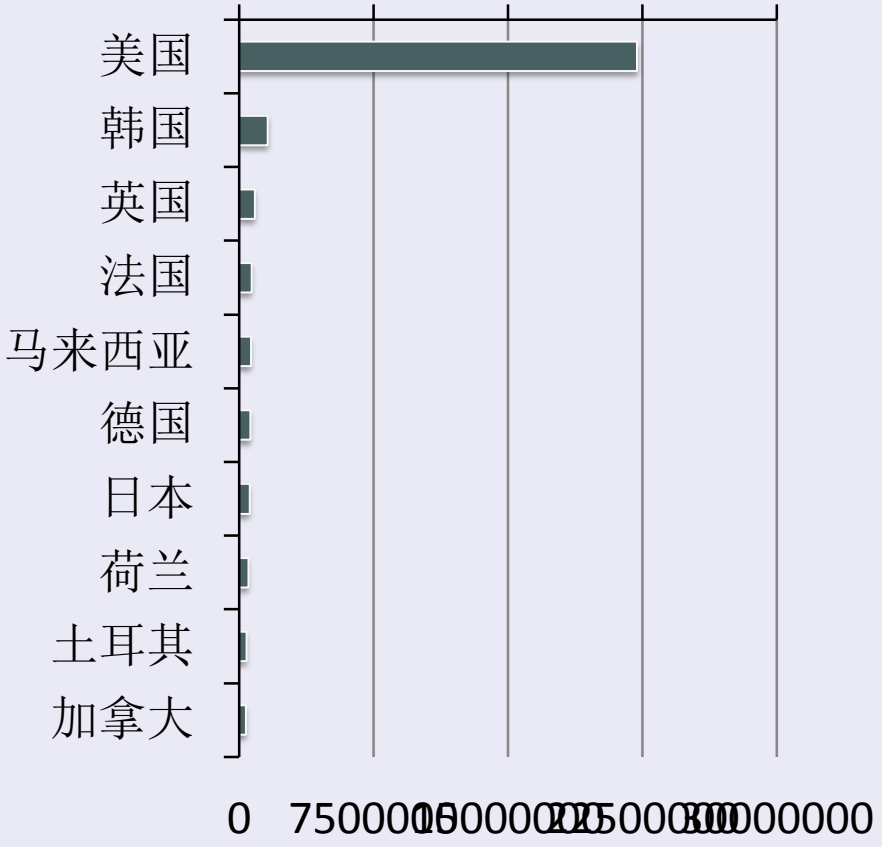
红色的点：境外攻击源
黄色的点：中国被攻击目标
平均每日拦截110万次国外的攻击
来自美国的攻击最多；来自德国、法国、英国的攻击比较密集；
受攻击最多的是北京的网站。



各国攻击次数统计

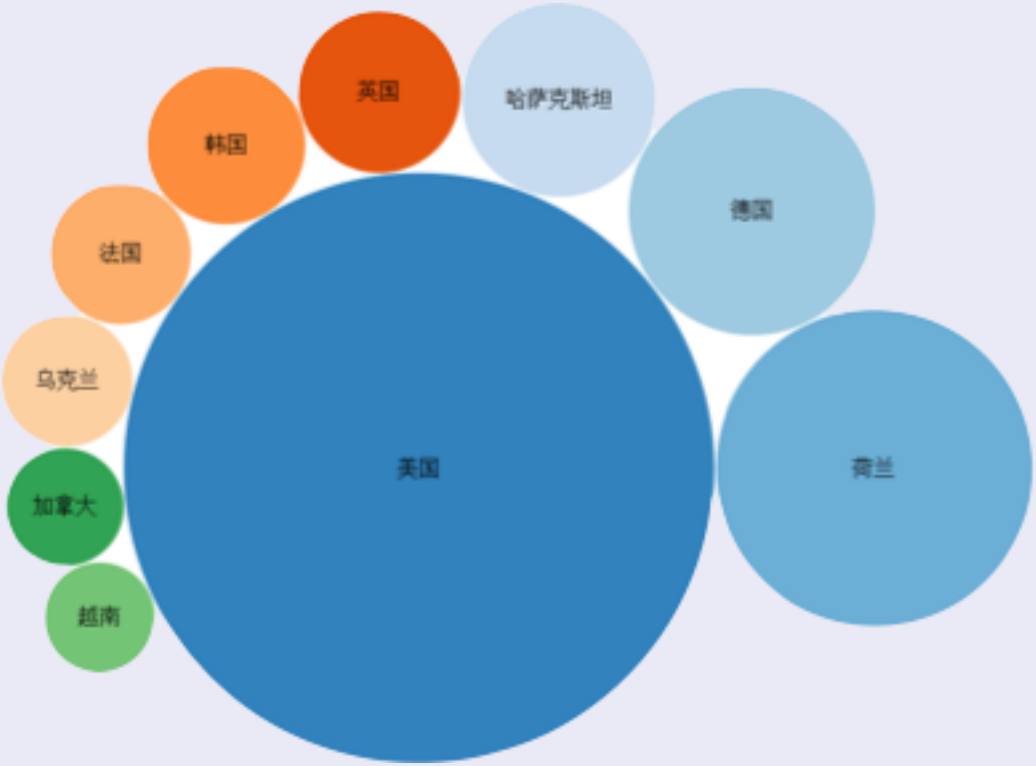
OWASP 中国
The Open Web Application Security Project

国家	攻击次数
美国	22202705
韩国	1630804
英国	903697
法国	715994
马来西亚	675797
德国	647342
日本	597941
荷兰	526643
土耳其	420877
加拿大	395771



SQL注入攻击各国排名

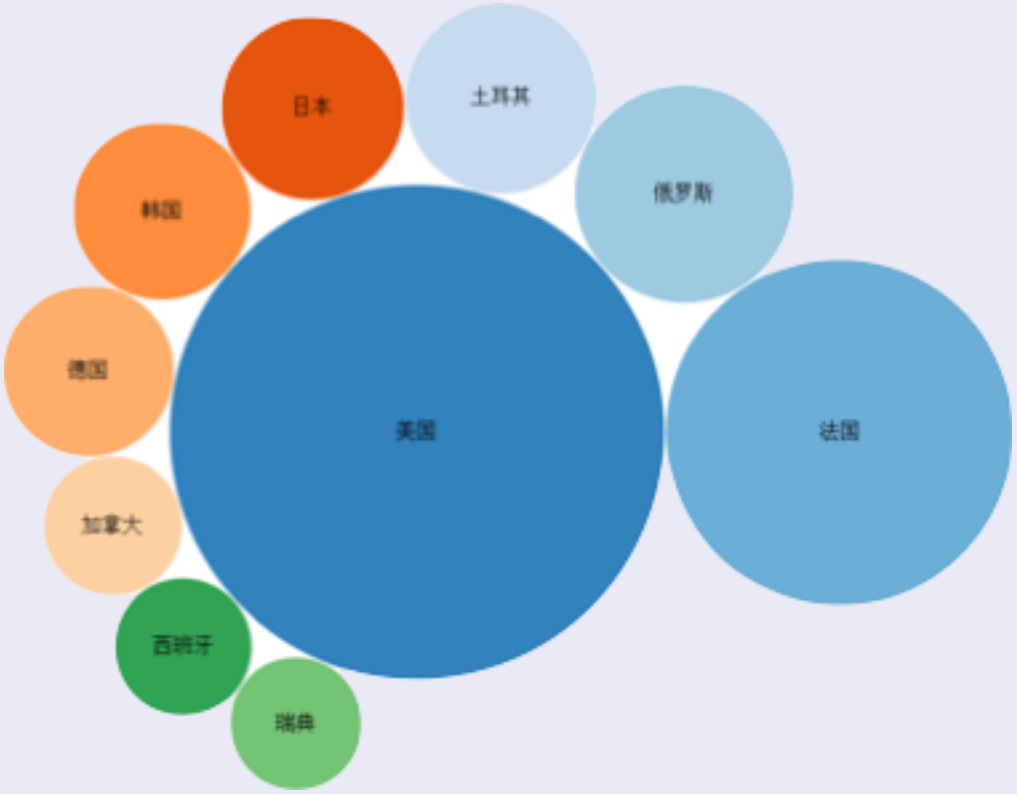
OWASP 中国
The Open Web Application Security Project



国家	攻击次数
美国	149947
荷兰	43390
德国	26481
哈萨克斯坦	16188
英国	11294
韩国	10813
法国	8479
乌克兰	7367
加拿大	5919
越南	5233

文件包含攻击各国排名

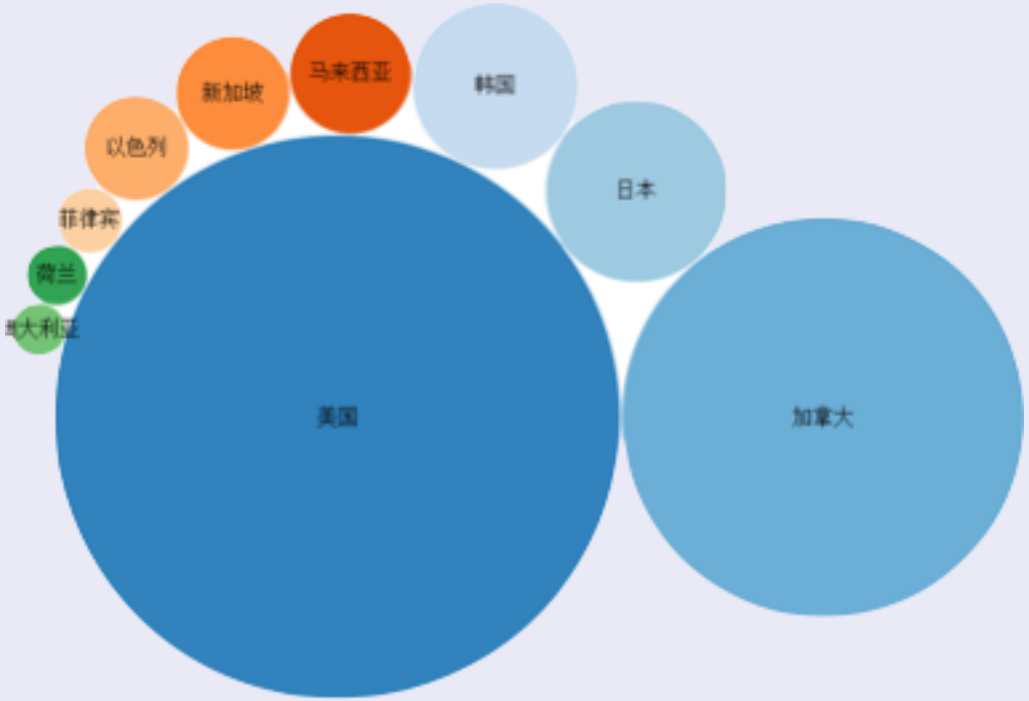
OWASP 中国
The Open Web Application Security Project



国家	攻击次数
美国	23132
法国	11370
俄罗斯	4516
土耳其	3456
日本	3189
韩国	2991
德国	2759
加拿大	1823
西班牙	1780
瑞典	1670

上传后门攻击各国排名

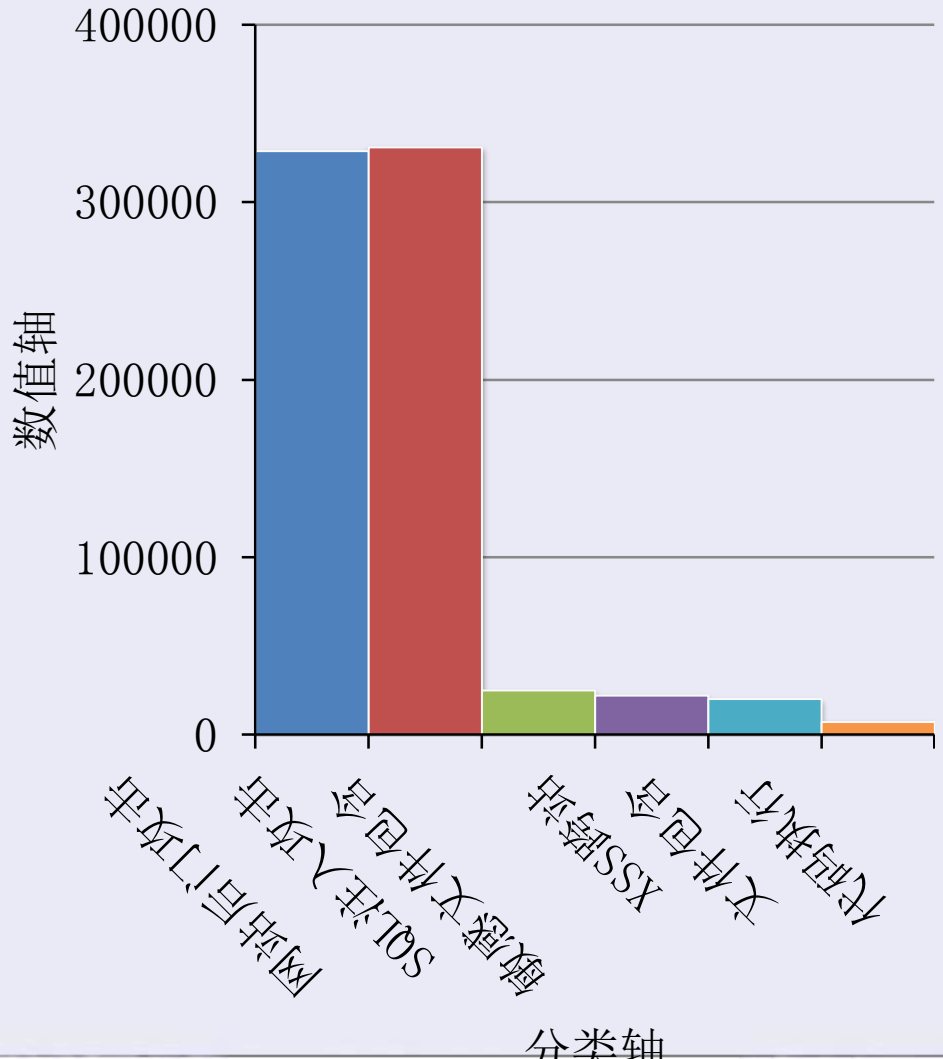
OWASP 中国
The Open Web Application Security Project

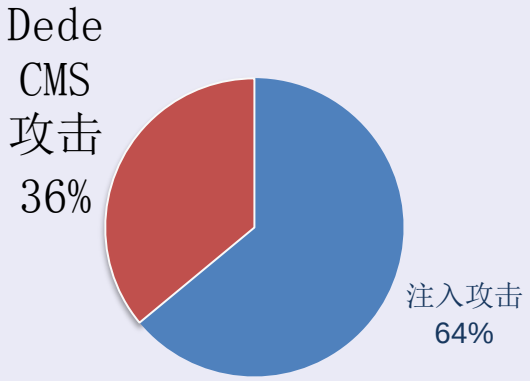


国家	攻击次数
美国	3323610
加拿大	167545
日本	34371
韩国	28823
马来西亚	15245
新加坡	13436
以色列	11284
菲律宾	4288
荷兰	3724
澳大利亚	2836

美国黑客攻击类型

OWASP 中国
The Open Web Application Security Project





- 注入攻击中，有36%的都是针对DedeCMS

巴西黑客对中国网站频繁攻击

- 名为team-defacers的黑客组织巴西服务器后当作“肉鸡”进而攻击其它网站。
- 图为team-defacers入侵服务器之后放出cPanel的帐号和密码。
- 经过对该组织的追踪，发现他们大量使用SQL注入攻击。

阿尔及利亚黑客Barbaros-DZ 频繁攻击中国政府网站

OWASP 中国
The Open Web Application Security Project

Notifier	H	M	R	L	Domain	OS
Barbaros-DZ	H		R		balinzuoqi.cfjcy.gov.cn	Win 2003
Barbaros-DZ	H				whmt.ahxf.gov.cn	Win 2008
Barbaros-DZ					www.renda.gov.cn/dz.htm	Win 2003
Barbaros-DZ					jinrong.wangqing.gov.cn/x.txt	Win 2003
Barbaros-DZ	H				jkxd.wz.gov.cn	Win 2003
Barbaros-DZ	H				www.scrm.gov.cn	Win 2000
Barbaros-DZ		M	R		3g.hsrk.gov.cn/dz.htm	Win 2003
Barbaros-DZ	H				www.xazx.gov.cn	Win 2003
Barbaros-DZ	H	M			www.qjdj.zt.gov.cn	Unknown
Barbaros-DZ	H	M			tq.yasgtzy.gov.cn	Win 2003
Barbaros-DZ					www.zkinvest.gov.cn/dz.htm	Win 2003
Barbaros-DZ	H				www.yjjw.gov.cn	Unknown
Barbaros-DZ	H		R		snfgw.gssn.gov.cn	Win 2008
Barbaros-DZ	H	M			lyzx.zmdly.gov.cn	Win 2008
Barbaros-DZ	H				foodsafe.tx.gov.cn	Win 2003
Barbaros-DZ	H		R		whj.luzhou.gov.cn	Win 2003
Barbaros-DZ	H				shangzhuang.yandu.gov.cn	Win 2003
Barbaros-DZ	H		R		ly.lnzxw.gov.cn	Win 2003
Barbaros-DZ	H				www.gxbldj.gov.cn	Win 2003
Barbaros-DZ	H				jljiangyuan.lss.gov.cn	Win 2003
Barbaros-DZ			R		dycl.dongying.gov.cn/lix/x.htm	Win 2003

从2012年7月12日至2013年3月，Barbaros-DZ利用文件包含漏洞使超过4000个中国政府网站被其入侵，并留下了黑页示威。

俄罗斯的MSSQL广告僵尸

OWASP 中国
The Open Web Application Security Project

2013年4月及2014年7月，监测到来自俄罗斯两个IP针对ASP/ASPX+MSSQL架构的网站，利用注入漏洞来插入广告，中国上万个网站受到影响（右上图），平均每日为800个网站拦截此攻击。从Update语句中有两个网址分别corypaydayloans.com和maxxpaydayloans.com，从whois里获取到注册者信息，并访问最新注册的willpaydayloans.com是一个贷款的网站（右下图）。

搜索被攻击的网站

攻击者的广告网站

土耳其黑客组织1923Turk大规模攻击中国网站

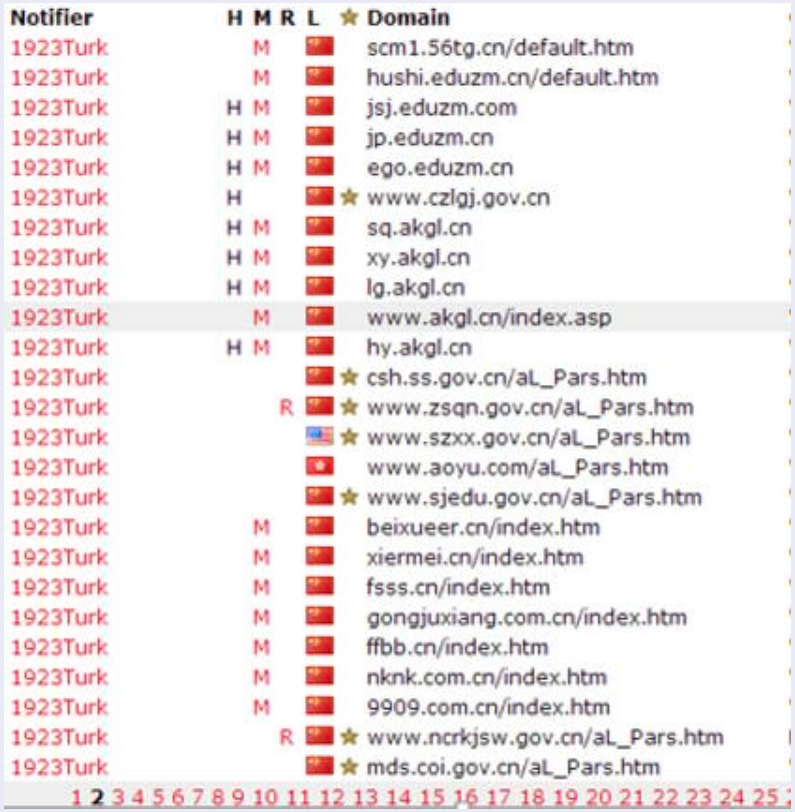
OWASP 中国
The Open Web Application Security Project

- 2014年1月22日，中央民族大学网站某个子站页面被篡改
- 根据被篡改的页面显示，攻击来自土耳其黑客组织1923Turk

土耳其黑客组织1923Turk大规模攻击中国网站 2

OWASP 中国
The Open Web Application Security Project

- 事件背景源于新疆暴力事件
- 超过2000个中国网站被攻击，政府400个、学校网站200个。只攻击.cn域名。
- 利用IIS解析漏洞，试图上传Webshell “/trl.asp;txt”
- 通过Webshell手工篡改网站主页



Notifier	H	M	R	L	★	Domain
1923Turk		M				scm1.56tg.cn/default.htm
1923Turk		M				hushi.eduzm.cn/default.htm
1923Turk	H	M				jsj.eduzm.com
1923Turk	H	M				jp.eduzm.cn
1923Turk	H	M				ego.eduzm.cn
1923Turk	H				★	www.czlgj.gov.cn
1923Turk	H	M				sq.akgl.cn
1923Turk	H	M				xy.akgl.cn
1923Turk	H	M				lg.akgl.cn
1923Turk		M				www.akgl.cn/index.asp
1923Turk	H	M				hy.akgl.cn
1923Turk					★	csh.ss.gov.cn/aL_Pars.htm
1923Turk			R		★	www.zsqn.gov.cn/aL_Pars.htm
1923Turk					★	www.szxx.gov.cn/aL_Pars.htm
1923Turk						www.aoyu.com/aL_Pars.htm
1923Turk					★	www.sjedu.gov.cn/aL_Pars.htm
1923Turk		M				beixueer.cn/index.htm
1923Turk		M				xiermei.cn/index.htm
1923Turk		M				fsss.cn/index.htm
1923Turk		M				gongjuxiang.com.cn/index.htm
1923Turk		M				ffbb.cn/index.htm
1923Turk		M				nknk.com.cn/index.htm
1923Turk		M				9909.com.cn/index.htm
1923Turk			R		★	www.ncrkjsw.gov.cn/aL_Pars.htm
1923Turk					★	mds.coi.gov.cn/aL_Pars.htm

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

我们研究的结论

OWASP 中国
The Open Web Application Security Project

- 1. 中国网站正受着来自世界各国的安全威胁。
- 全国每年有24万网站被黑，其中政府网站2万（总数10万）
- 全国超过 17% 的站点存在明显的高危漏洞
- 中国目前大约240万个网站使用了.cn的域名，是主要的攻击目标
- 接近 10% 的网站引用了第三方组件
- 超过 3.3% 的网站所安装的组件是在无补丁状态下使用
- 每天全网针对Web站点的攻击超过 3 亿 次
- 2.以美国、俄罗斯为首的各国通过网络攻击，控制大量服务器建立起“僵尸网络群”，留到网络战争爆发时将导致不可估量的严重后果。

目录

OWASP 中国
The Open Web Application Security Project

1.Web安全数据组成部分（每天4T）
- 收集20亿域名的漏洞信息
- 收集网络空间的组件指纹
- 收集60万+网站的被攻击数据

2.如何处理大数据
数据同步和查询机制
数据监控和分析

3.境外攻击情况
- 攻击数量统计
- 攻击方法统计
- 各国攻击例子

4.总结
大数据下的防护思路
研究安全大数据的意义

如何有效防护

OWASP 中国
The Open Web Application Security Project

1.协同防御：利用云的大样本威力识别恶意来源建立黑名单封堵（发现高危0day的利用，在大面积攻击爆发之前遏制）；
3.日常防护：WAF引擎建立一个精简有效的防护集，
2.大规模攻击：被攻击后抓取所有playload分析并转化防护规则，通过云分发给防护引擎；

```
358 --add
359 --! @brief discuz检测函数
360 --! @param self 私有成员
361 --! @return boolean，是否检测到攻击
362 local function [redacted](self)
363 |   local uri_raw = [redacted]
364 |   local request_body = [redacted]
365     local method = self.method
366 |   return (method == "POST"
367 |   |   |   and request_body
368 |   |   |   and match(uri_raw,"\\butility[/\\x5c]+convert[/\\x5c]+index\\.php","ioj")-
369 |   |   |   and match(request_body,"newconfig","ioj")
370 |   |   |   and match(unescape_uri(request_body),"\\[[^&]*\\W[^&]*\\]","oj"))
371 end-
```

云WAF规则里针对Discuz某个漏洞响应的规则截图

研究安全大数据的意义

OWASP 中国
The Open Web Application Security Project

1. 为我国信息安全发展的重大战略提供理论和事实数据支撑，为网络空间战的部署做提前方案；

2. 任何个体都是整体的一个环节，从宏观到微观的全局视野更有利于正确地理解当前和将来地安全态势；

3. 从数据中寻找规律：
对某地域、行业的共同点可以统一进行防御，对总共百个的攻击来源可批量封堵拦截，对有代表性，广泛应用的第三方组件漏洞提前预警修复；

4. 从源头遏制攻击者三大目的：反动言论传播、地下黑产、APT攻击的前奏。

谢谢！

OWASP 中国
The Open Web Application Security Project

请关注我的微信：bobkey
分享最新安全动态和攻防数据

希望开放安全大数据与合作