DTCC

2017第八届中国数据库技术大会

DATABASE TECHNOLOGY CONFERENCE CHINA 2017

大数据在安全行业的应用
网络空间测绘

白帽汇-龙专
longzhuan@baimaohui.net

目录

背景

Fofa应用

漏洞扫描结合

技术实践

安全漏洞越来越多

- Shadow Brokers公布NSA黑客工具，包含众多Windows 0day漏洞
- Struts2命令执行漏洞
- IOT设备弱口令
- PHPMailer命令执行漏洞
- ImageMagic命令执行漏洞
- Redis未开启验证导致数据泄露
- Elasticsearch、CauchDB等系统勒索事件

……

一个无法规避也不好解决的场景

当某个安全漏洞突发的时候，需要统计和分析：

- 有多少联网设备使用这个系统？
- 哪些受影响？

网络空间测绘+全网扫描

什么是网络空间测绘

网络空间测绘是运用一些技术方法，来探测全球互联网空间上的资产业务应用和分布情况，并用搜索引擎的方式提供服务，可供搜索的范围包括所有联网的资产。

网络空间测绘与资产管理的区别

	传统意义的资产管理	网络空间测绘
侧重点	**硬件和IP资产** 如：投影仪，上网卡	**IP上承载的业务系统** 如：docker系统，金蝶财务，用友OA管理软件
实时性	**慢** 依赖管理手段	**快** 技术手段实时更新
覆盖度	**少** 很多私搭服务器	**全** 全网段，多端口，多协议
准确度	**低** 业务切换，导致大量信息失真	**高** 应用层识别

网络空间测绘是对资产进行安全管理的更为有效的形式

目录

背景

Fofa应用

漏洞扫描结合

技术实践

白帽汇网络空间测绘的实践

http://www.fofa.so

是一款网络空间资产搜索引擎。

能够帮助大家迅速进行网络资产匹配，快速开展应用分布统计、漏洞影响范围分析等工作。

运营现状

覆盖服务数量 247400000+

覆盖网站数量 237200000+

覆盖规则数量 5550+

什么时候需要用到FOFA

- 如何获取某个系统的分布情况？
- 如何知道哪些网站用了某套系统？
- 如何获取一个根域名下所有子域名网站？
- 如何根据一个子域名网站找到跟他在一个IP的其他网站？
- 全网漏洞扫描：一个新的漏洞在全网的影响范围。

……

每类资产，都有自己的指纹

单个资产，也有自己的指纹

资产指纹

- 梭子鱼安全设备：

  body="http://www.barracudanetworks.com?a=bsf_product"

  header="BarracudaHTTP"

- 锐捷路由器：

  body="free_nbr_login_form.png"

- Jenkins：

  header="X-Jenkins-Session" || body="translation.bundles"

- F5：

  header="BIGipServer"

FOFA Pro

规则列表 规则专题 企业版 edison

header="BarracudaHTTP"

收藏规则

安全设备指纹

•梭子鱼：

通过header查找: header="BarracudaHTTP"

="BarracudaHTTP" 获得 15187 条匹配结果，用时 3009 毫秒，模式: extended。

网站 15187

国家排名

美国 9211

加拿大 835

中国 778

荷兰 334

英国 333

端口排名

443 23

8000 9

81 5

8080 4

80 2

Server排名

BarracudaHTTP 4.0 11

BarracudaHTTP 3.0 3

← 上一页 1 2 3 4 5 6 7 8 9 1518 1519 下一页 →

https://216.7.226.25 443

216.7.226.25
2016-10-11
United States / Spring
216.7.226.25
BarracudaHTTP 4.0

HTTP/1.1 200 OK
Server: BarracudaHTTP 4.0
Date: Tue, 11 Oct 2016 12:31:55 GMT
Content-Type: text/html
Content-Length: 95
Last-Modified: Wed, 05 Nov 2014 18:44:37 GMT
Connection: keep-alive

https://74.219.212.166 443

74.219.212.166
2016-10-11
United States / Cincinnati
74.219.212.166
BarracudaHTTP 4.0

HTTP/1.1 200 OK
Server: BarracudaHTTP 4.0
Date: Tue, 11 Oct 2016 12:31:21 GMT
Content-Type: text/html
Last-Modified: Sat, 23 Jul 2016 00:55:23 GMT
Transfer-Encoding: chunked

搜索 **header="BarracudaHTTP"** 获得 15187 条匹配结果， 用时 3009 毫秒，模式: extended。

类型分布

网站	15187

国家排名

美国	9211
加拿大	835
中国	778
荷兰	334
英国	333

端口排名

443	23
8000	9
81	5
8080	4
80	2

Server排名

BarracudaHTTP 4.0	11
BarracudaHTTP 3.0	3

状态

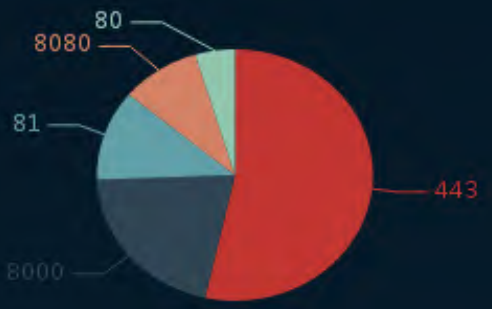
查询耗时: 2257ms

安全设备指纹

- 梭子鱼：

设备分布情况统计

端口信息统计



搜索 **body="free_nbr_login_form.png"** 获得 2657 条匹配结果， 用时 2569 毫秒，模式: extended。

路由器指纹

- 锐捷路由器：

通过body查找:

body="free_nbr_login_form.png"

类型分布

网站 2657

国家排名

中国 2653
澳大利亚 1
香港特别行政区 1
意大利 1
美国 1

端口排名

8080 369
8082 140
80 28
443 1
8081 1

Server排名

Start HTTP-Server/1.1 1

状态

查询耗时: 3470ms

---

https://218.64.115.106 443

锐捷网络 --NBR路由器--登录界面
218.64.115.106
2016-10-11
China / Nanchang
218.64.115.106
Start HTTP-Server/1.1

HTTP/1.1 200 OK
Date: Mon, 01 Mar 1993 00:26:11 UTC
Server: Start HTTP-Server/1.1
Content-Type: text/html
Content-Length: 9570
Last-Modified: Sun, 29 Sep 2013 01:58:02 GMT
Expires: Thu, 16 Feb 1989 00:00:00 GMT

110.186.73.88:8082 8082

锐捷网络 --NBR路由器--登录界面
110.186.73.88
2016-09-20
China / Chengdu
110.186.73.88

HTTP/1.1 200 OK
Date: Mon, 01 Mar 1993 00:26:11 UTC
Server: Start HTTP-Server/1.1
Content-Type: text/html
Content-Encoding: gzip
Content-Length: 4090
Last-Modified: Thu, 01 Jan 1970 00:02:40 GMT
Expires: Thu, 16 Feb 1989 00:00:00 GMT

110.186.73.102:8082 8082

锐捷网络 --NBR路由器--登录界面
110.186.73.102
2016-09-20
China / Chengdu

HTTP/1.1 200 OK
Date: Mon, 01 Mar 1993 00:26:11 UTC
Server: Start HTTP-Server/1.1
Content-Type: text/html

app="Jenkins"

收藏规则　下载数据

业务支撑系统

- Jenkins：

app= “jenkins"

搜索 app="Jenkins" 获得 44441 条匹配结果，用时 39 毫秒，模式: extended。

← 上一页　1　2　3　4　5　6　7　4445　下一页 →

国家排名

美国	20641
德国	3760
中国	3315
爱尔兰	2847
法国	1896

端口排名

8080	26220
80	7586
443	7469
8081	1829
8443	374

https://jenkins.zxda.net　443

Dashboard [Jenkins]
60.211.209.115
2017-05-11
China / Jining
zxda.net
openresty/1.11.2.2

HTTP/1.1 200 OK
Server: openresty/1.11.2.2
Date: Thu, 11 May 2017 14:01:34 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 4092
Connection: keep-alive
X-Content-Type-Options: nosniff

ci.lightbend.com　80

Dashboard [Jenkins]

可供查询的字段

基础字段：

port

protocol

banner

title

header

body

cert

过滤器：

domain

host

ip

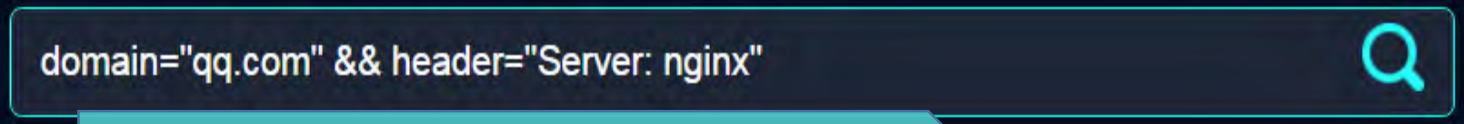
country

city

region

……

支持单个和组合搜索



过滤器

- 域名是qq.com且使用Nginx服务器的：

domain="qq.com" && header="Server: nginx"

类型分布

网站

&& header="Server: nginx" 获得 2670 条匹配结果，用

时 104 毫秒，模式: extended。

国家排名

中国 2670

端口排名

80	2602
443	53
8080	8
3000	1
8000	1

Server排名

nginx	432
nginx/1.4.3	358

← 上一页 1 2 3 4 5 6 7 ... 267 下一页 →

v.t.qq.com

Test Page for the Nginx HTTP Server on EPEL

58.251.139.142

2017-03-03

China / Guangzhou

qq.com

nginx/1.5.7

HTTP/1.1 200 OK
Server: nginx/1.5.7
Date: Fri, 03 Mar 2017 14:14:09 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1161
Connection: keep-alive
Accept-Ranges: bytes

ur.qq.com

搜索 ip="121.42.202.130" 获得 15 条匹配结果， 用时 12 毫秒， 模式: extended。

← 上一页 1 2 下一页 →

过滤器

- 获取某个IP上绑定的host： ip="121.42.202.130"

baimaohui.cn

白帽汇官网-专注于安全大数据 企业威胁情报
121.42.202.130
2017-03-30
China / Hangzhou
baimaohui.cn
nginx/1.8.0

```
HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Thu, 30 Mar 2017 07:24:27 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
```

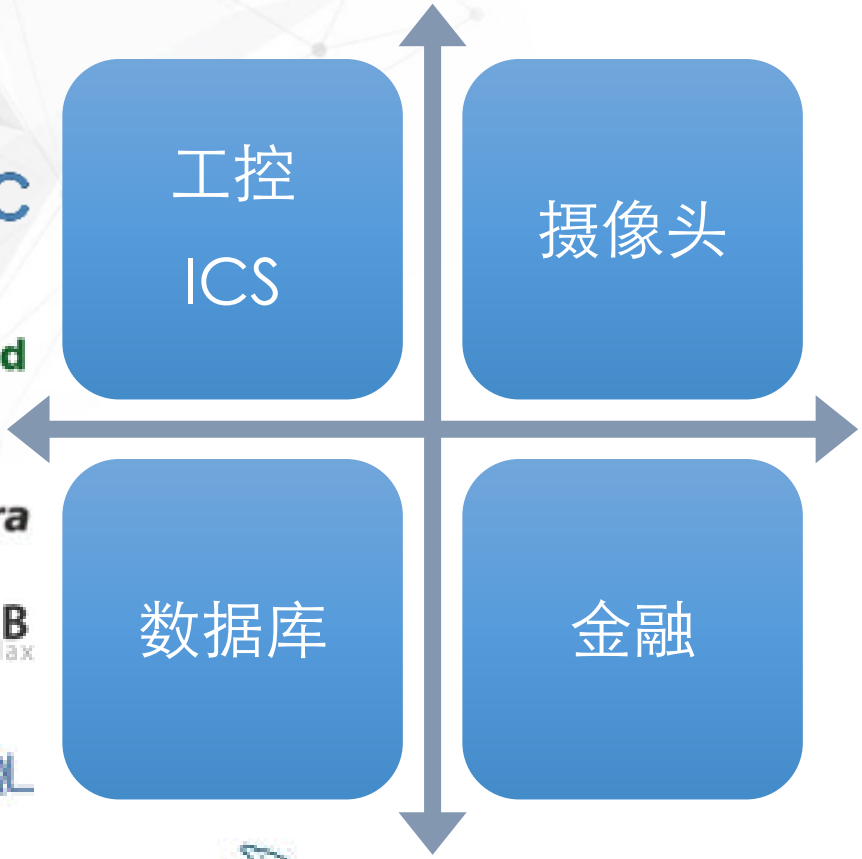
i.nosec.org 80

NOSEC用户中心
121.42.202.130
2017-03-28
China / Hangzhou
nosec.org
nginx/1.8.0

```
HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Tue, 28 Mar 2017 03:19:01 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 5802
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
```


header="server: apache" && country="CN"
收藏规则
下载数据
过滤器
• 获取某个国家的Apache使用情况：
header="server: apache" && country="CN"
apache" && country="CN" 获得 3582859 条匹配结果，
extended。
国家排名
中国 3582859
端口排名
80 2866051
8080 230670
443 180610
8081 64974
81 34129
Server排名
Apache 607065
Apache-Coyote/1.1 369719
Apache/2.2.15 (CentOS) 59915
Apache/2.2.3 (CentOS) 47480
← 上一页 1 2 3 4 5 6 7 358286 下一页 →
120.27.92.224
Decentralized Exchange
ubuntu
120.27.92.224
2017-04-16
China / Hangzhou
120.27.92.224
Apache/2.4.7 (Ubuntu)
HTTP/1.1 200 OK
Date: Sun, 16 Apr 2017 04:59:20 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Mon, 27 Mar 2017 13:48:05 GMT
Etag: "11ea-54bb697ba0221-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
180.153.59.145:8087
180.153.59.145
2017-04-16
China / Shanghai
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1

针对特定系统的检索



mongoDB
riak
MITSUBISHI ELECTRIC
redis
elastic
memCached
Cassandra
Apache CouchDB relax
PostgreSQL
MySQL
PHOENIX CONTACT
EtherNet/IP
SIEMENS
dnp
Modbus
TRIDIUM Connecting minds and machines
BACnet
GE Industrial Solutions
HART IP
CoDeSys
red lion
OMRON

FOFA的特点

如下几点特色：

- 能够针对HTML正文进行代码级别的全文检索
- 聚焦网站资产，数据量更大，覆盖更全
- 指纹识别后置，自定义规则库，随时应对新系统，无需重新爬虫或重新分析
- 支持非标准端口

这些你们能做到吗？

目录

背景

Fofa应用

漏洞扫描结合

技术实践

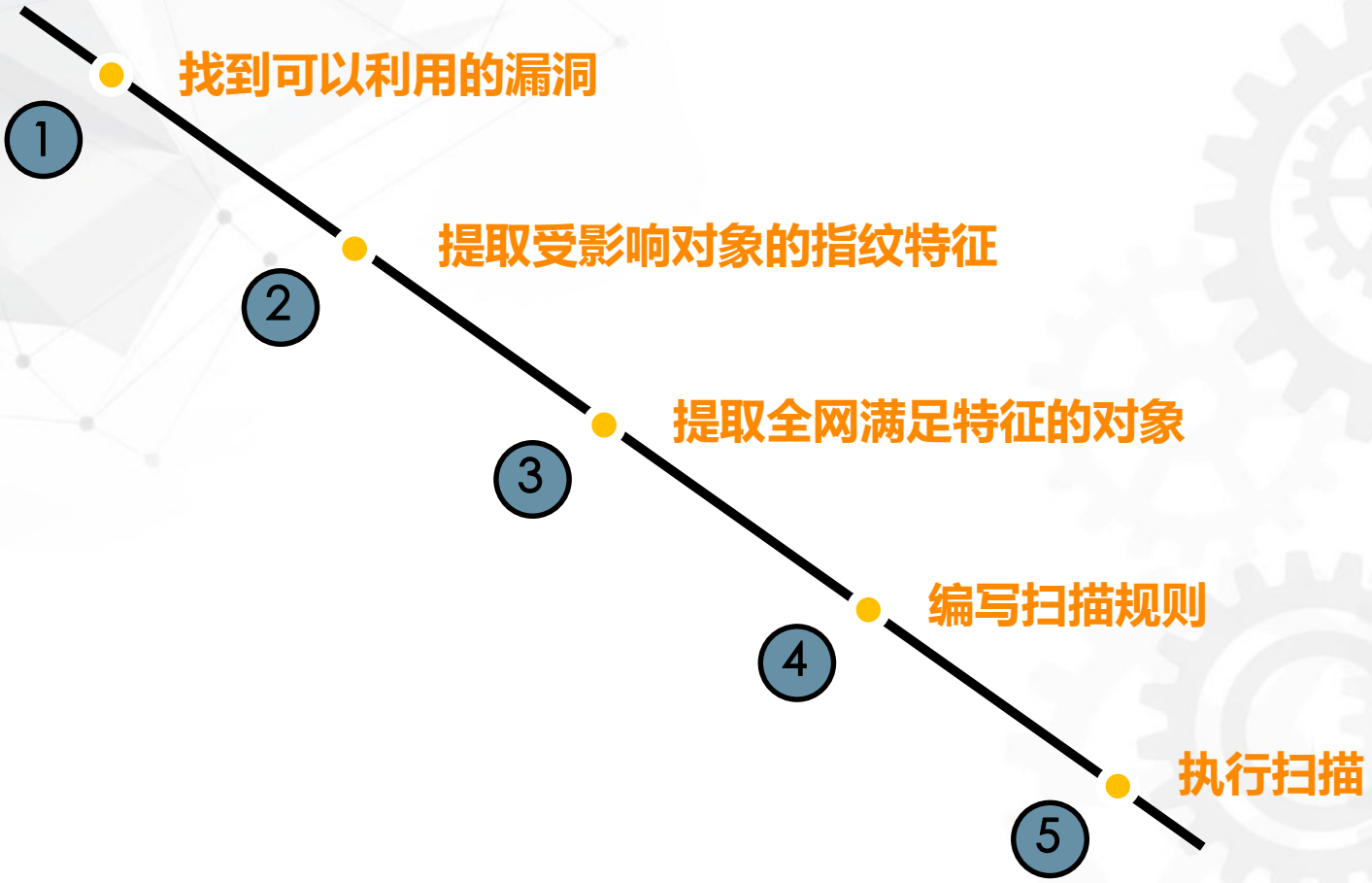
Fofa全网漏洞扫描的实践

全网漏洞扫描与传统Web漏洞扫描的区别

	传统扫描	全网扫描
触发方式	扫描对象	漏洞
扫描方式	全漏洞集合	一个漏洞
依赖方式	漏洞库的完整度	全球网站覆盖度
速度	慢	快

全网漏洞扫描不是为了替换现有的漏洞扫描器，而是作为其的补充。
它解决的是在某个漏洞突发时，把扫描时间从几天减少到几分钟。

一次完整的全网漏洞扫描的过程



一个典型的漏洞

漏洞概要

缺陷编号：

漏洞标题：用友CRM系统任意文件读取/任意文件上传getshell（附众多案例）

相关厂商：用友软件

漏洞作者：路人甲

提交时间：2015-08-31 11:19

公开时间：2015-12-04 11:20

漏洞类型：SQL注射漏洞

危害等级：高

自评Rank：15

漏洞状态：漏洞已经通知厂商但是厂商忽略漏洞

Tags标签：安全意识不足 php源码审核 安全意识不足

0x2 任意文件上传getshell

同样保存如下内容为upload.htm

```
<html>
<form action="http://180.169.30.13:2046/ajax/getemaildata.php?DontCheckLogin=1" method="post" enctype ="multipar
t/form-data">
  <input type="file" name="file" />
  <input type="submit" name="upload" value="upload"/>
</form>
</html>
```

然后上传任意文件，用burpsuite抓包修改，在文件名后面加一空格，如图所示

可以看见成功上传了文件，但这里注意文件名的获取：

上传的文件名为：

mht2135.tmp.mht 将前面的mht更改为upd 后面的数字减1，再将最后的mht更改为php

即文件名为：upd2134.tmp.php 路径依然在/tmpfile/

```
http://180.169.30.13:2046/tmpfile/upd2134.tmp.php
```

20分钟完成一次全网漏洞扫描

17分钟写POC

http交互流程

3分钟完成全网漏洞扫描

依赖网络空间测绘


FOFA
三分钟完成
全网漏洞报告
白帽汇
BAIMAOHUI.NET
https://fofa.so/

重大行业应用

配合企业进行多次行业快速预警

- 《ShadowBroker放大招-多种Windows 0day利用工具公布》
- 《威胁情报预警：Elasticsearch勒索事件》
- 《Joomla!用户特权提升漏洞影响范围分析：涉及全球超15000网站》
- 《飞塔后门？FortiGate 疑似存在SSH后门》
- 《Redis Crackit入侵事件分析》

……

目录

背景

Fofa应用

漏洞扫描结合

技术实践

网络空间测绘的基础：端口扫描

- 传统的nmap端口扫描虽然全，但是速度太慢
- 快速端口扫描存在丢包的问题
- 存在防火墙误报问题

针对协议识别速度慢和防火墙误报问题

开发了一套协议识别程序

覆盖240+端口，110+协议的深度解析，包括主流的网络服务、数据库、IOT，甚至是工控协议

为了识别各个组件上的具体应用

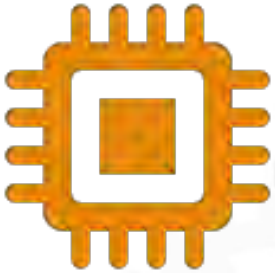
收集和整理了一套指纹识别库

目前有超过5500+的识别规则

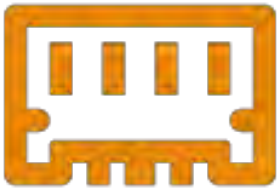

FOFA Pro
规则列表
规则专题
API
企业版
客户端
Heroes
机房监控 (3条)
iMonitor-DND 监控系统 计通机房环境监控系统
户外广告 (1条)
DSIS多媒体信息发布系统
UPS监控 (2条)
PowerAlert UPS监控
协作产品 (2条)
其他服务器产品 (7条)
TCExam TBDev-YSE Biamp-Server Tickets-CAD-System Tiger-Netcom-Device X10media-Torrent-Search-Engine X10media-MP3-Search-Engine
DNS服务器 (2条)
DDNS PowerDNS
docker项目管理 (1条)
harbor
公安行业 (3条)
辰锐单向传输系统 金万码巡更产品 移动执法终端
文件管理产品 (2条)
QuiXplorer 国迈电子安全文档管理系统
即插即用设备 (5条)
M2M-Server PnPSCADA TI-DM385 TI-DM8127 TI-DM812x
房地产行业 (4条)

核心

ES使用总结



- 集群分散部署
- 高性能CPU
- 大内存
- SSD



ES调优

- 我们团队翻译的《http://t.cn/RXqswOq》
- 参数优化
- 分片优化

调优前一次搜索查询30s以上；调优后，1s以内

数据迁移

任意表、任意字段均可一键迁移

数据快速更新带来如下问题

1. 更新的数据量很大
2. 插入缓冲区（Redis）积压严重，导致其不稳定
3. 全文搜索速度慢

白帽汇微信

龙专

THANKS

SequeMedia 盛拓传媒 ITPUB ChinaUnix