Web扫描器的架构变迁之路

白帽汇-龙专
longzhuan@baimaohui.net

个人简介

- 2009年之前，软件工程师；
- 2009年，加入诺赛科技，主导全球第一款云端扫描器（iiscan）平台开发；
- 2011年，加入360，担任网站安全部门后端核心研发，360鹰眼产品技术负责人；
- 2015年至今，白帽汇公司联合创始人兼CTO，负责FOFA/FOEYE产品；

目录

- **背景**
  - 初代扫描器
  - Web2.0扫描器
  - 云端扫描器
  - 基于流量分析扫描器
  - 全网漏洞专扫

安全事件（2017）

- 洲际酒店(IHG)信用卡数据泄露；
- Cloudflare流量泄露，200万网站受影响；
- 永恒之蓝勒索病毒；
- 2亿美国选民数据泄露；
- 1.4亿Verizon用户数据泄露；
- 征信机构Equifax数据泄露，超过1.4亿数据泄露；
- 德勤500万邮件信息泄露；
- WPA2协议漏洞；
- 英特尔芯片爆出多个漏洞；
- 苹果MAC系统爆出超低级漏洞，影响所有用户；

……

业务现状

大部分业务以Web方式提供服务，系统多使用CMS系统、开源框架或自主开发。

大多数程序只考虑完成功能，对于安全性考虑不足，导致漏洞频出。

安全风险

被拖库

被挂后门

被内网渗透

风险产生原因

程序缺陷

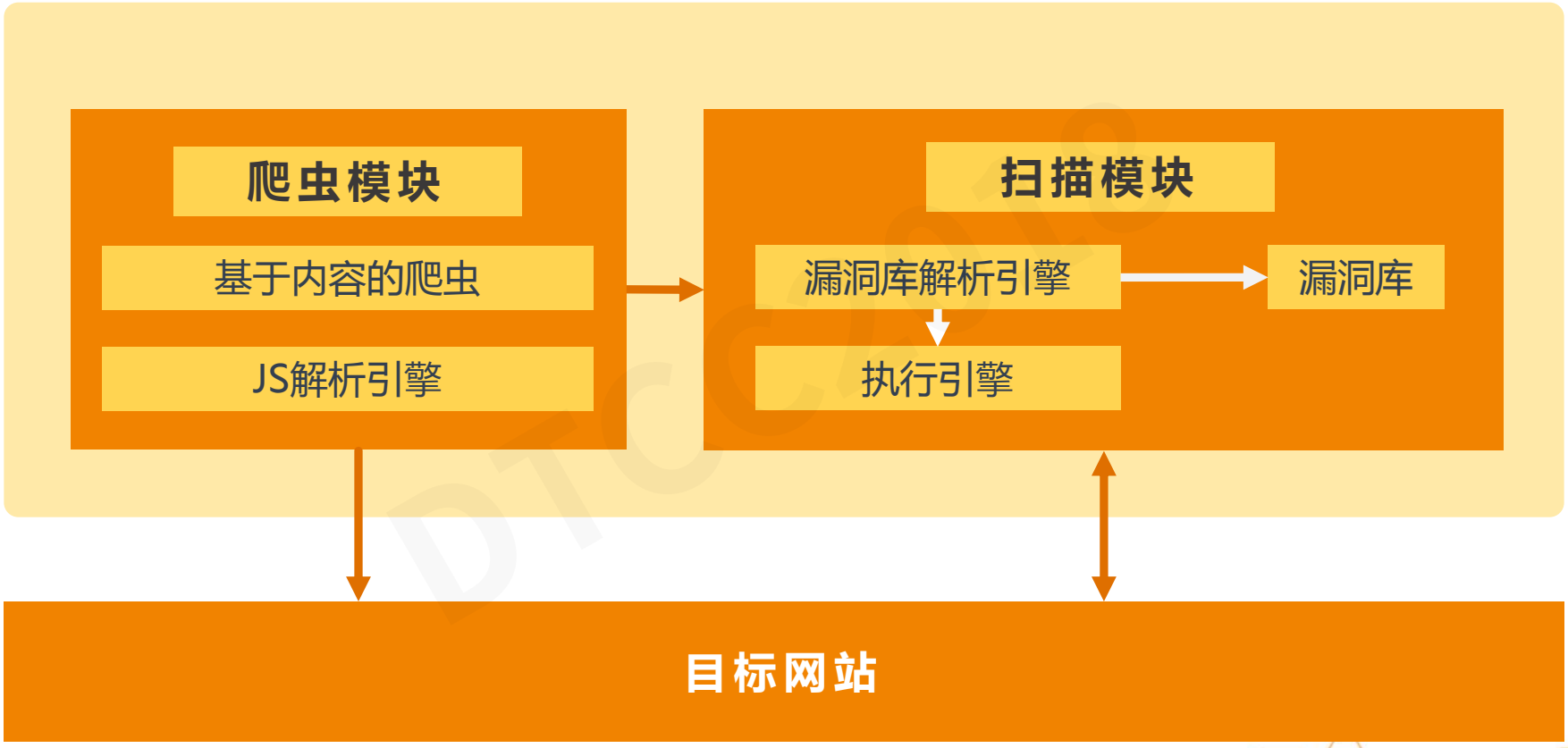
管理缺陷

怎么办？

目录

- 背景
- **初代扫描器**
- Web2.0扫描器
- 云端扫描器
- 基于流量分析扫描器
- 全网漏洞专扫

初代扫描器



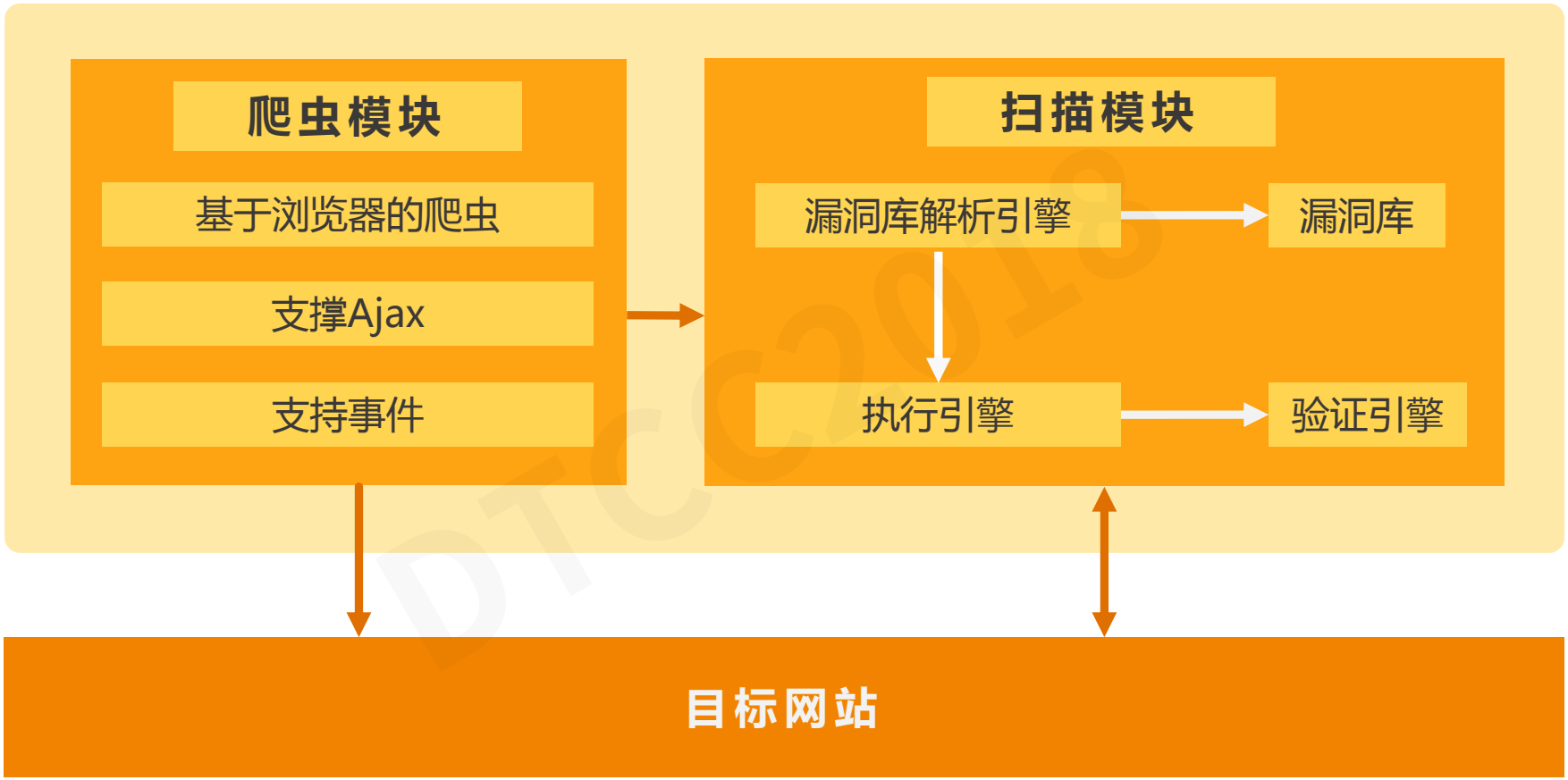
目录

- 背景
- 初代扫描器
- **Web2.0扫描器**
- 云端扫描器
- 基于流量分析扫描器
- 全网漏洞专扫

Web2.0技术

- **Ajax**：异步或局部刷新
- **事件**：某些链接是触发某个动作才出现的
- **表单**：自动填充表单

Web2.0扫描器



问题

- 扫描器不是硬件就是软件
- 人工介入，自动化程度低
- 无法支持大批量网站扫描

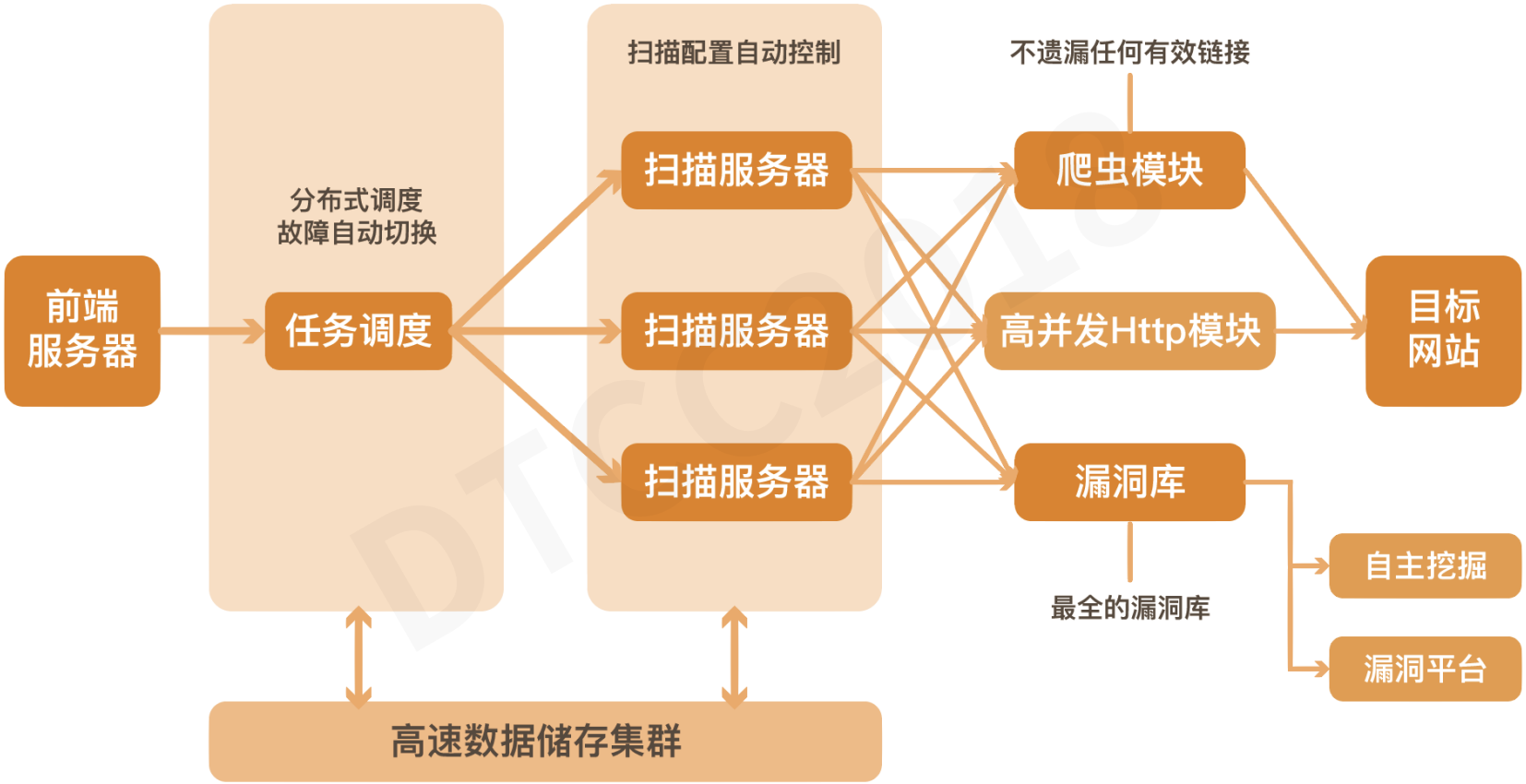
目录

- 背景
- 初代扫描器
- Web2.0扫描器
- **云端扫描器**
- 基于流量分析扫描器
- 全网漏洞专扫

云技术

当云计算火起来之后，扫描器也云平台化了

云端扫描器架构



难点

- 支持百万级用户的扫描架构
- 分布式架构的稳定性
- 自动化运维

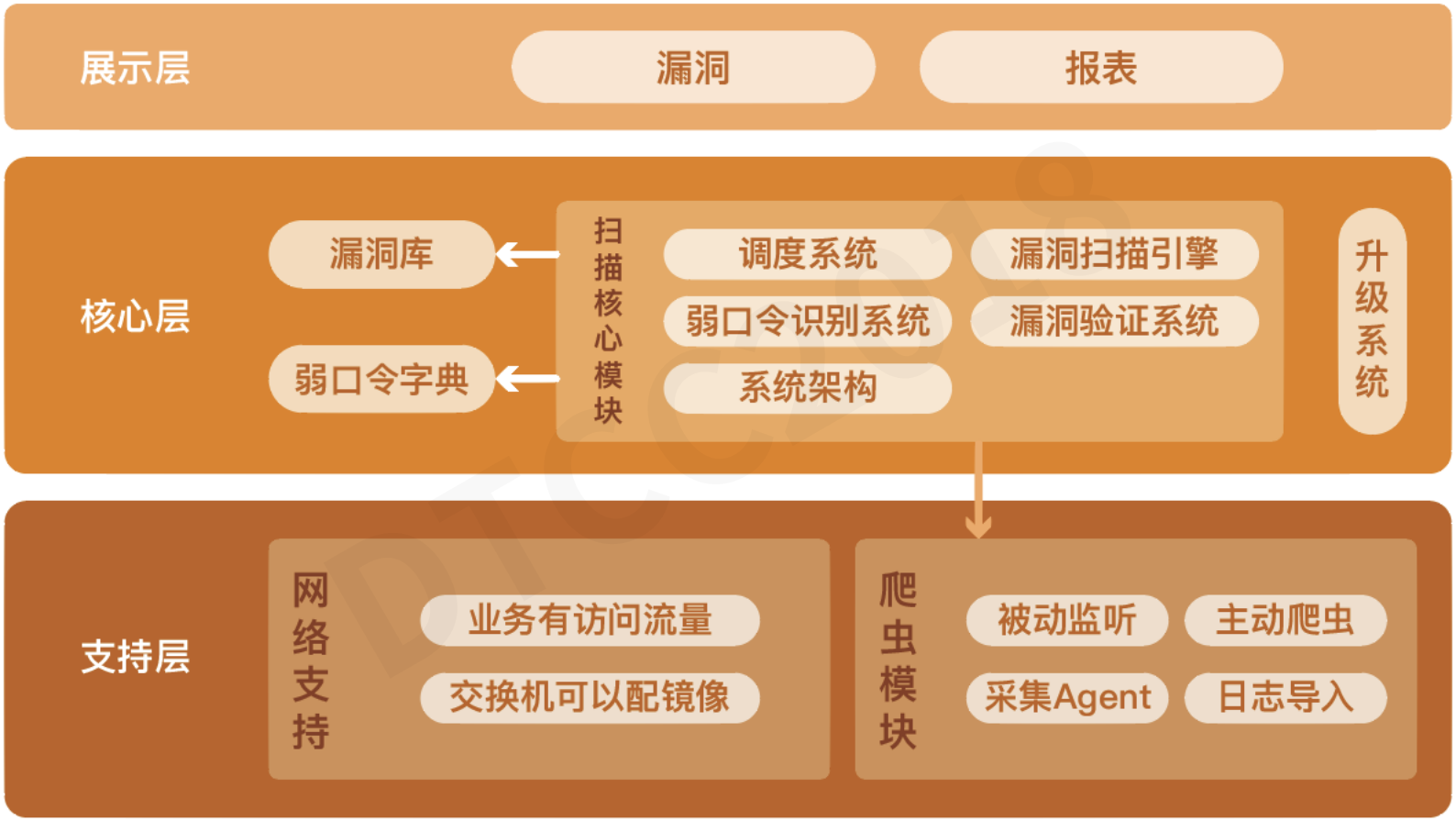
目录

需求背景

- API
- APP后端服务器
- 各种猝不及防的活动

爬虫没有入口

基于流量分析的扫描器



难点

- 如何处理巨大的流量
- https支持
- 排除无效链接
- 循环扫描

目录

- 背景
- 初代扫描器
- Web2.0扫描器
- 云端扫描器
- 基于流量分析扫描器
- **全网漏洞专扫**

需求背景

各种网络空间测绘平台出来后

扫描器

盲扫

特定目标、单个漏洞

准确打击

定义

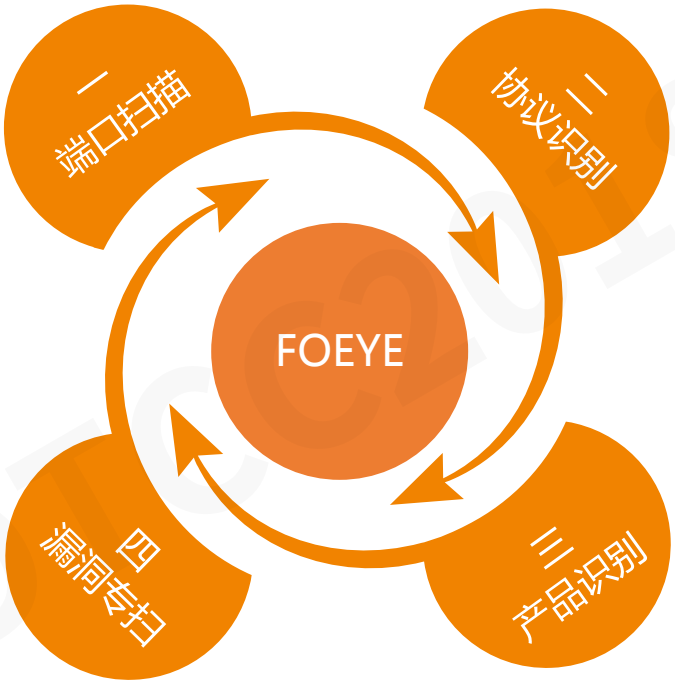
网络空间测绘是通过识别联网的对象，**获取IP、端口、协议和产品信息**，以搜索引擎提供服务的一种**资产建模**技术；并支持快速轻量级漏洞专扫服务。

Cyberspace Mapping

网络空间测绘四要素

异步无状态的端口扫描
识别**260多个端口**
端口可扩展

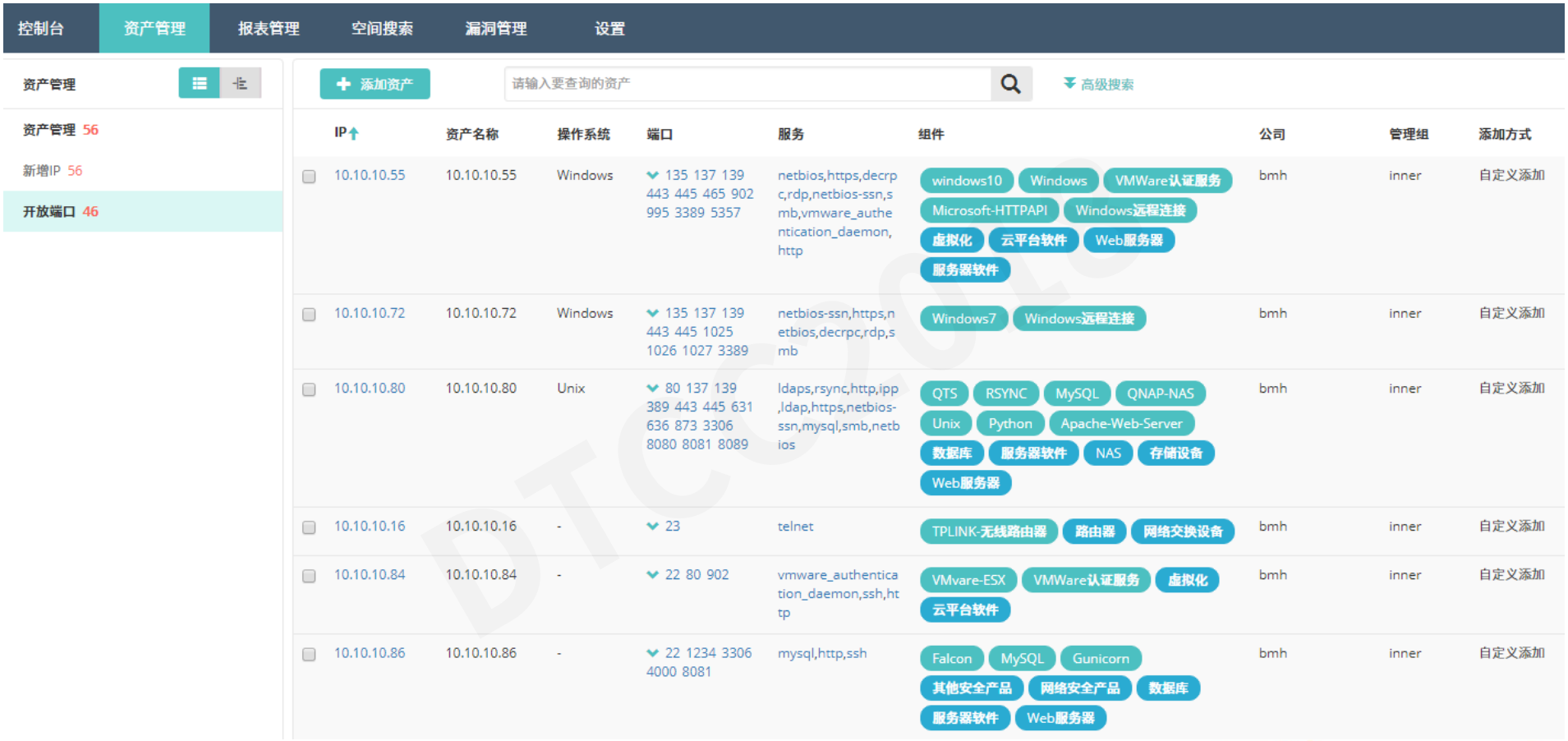
自研协议识别，可扩展
支持**130多种协议**
识别95%以上开放端口



漏洞专扫自有POC
白帽子征集
超过**1000个POC**

产品规则涵盖14个大类，
130多个小类
超过**36000条规则**

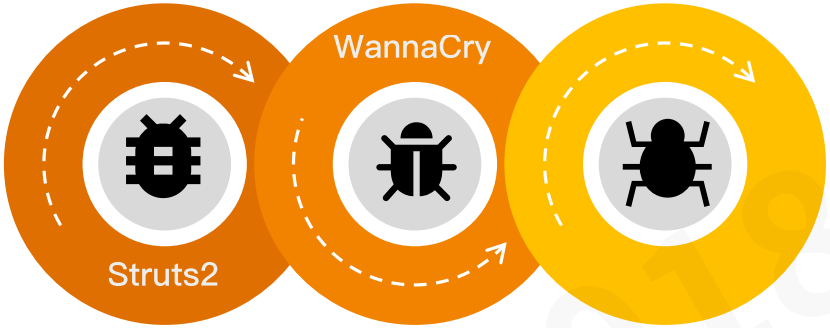
产品实例



网络资产建模


应用系统
[CRM、OA、
邮件系统、CMS系统等]
WEB服务器或中间件
[Apache、Nginx、IIS、
Weblogic、Websphere等]
操作系统
[Windows、Linux、Unix、MAC-OS等]
硬件
[浪潮、华为、DELL等]

漏洞应急



在某个高危漏洞爆发的时候
如果企业资产超过10万，如何在几分钟内扫完？

全网漏洞专扫

一次完整全网漏洞专扫的过程

20分钟完成一次全网漏洞专扫

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

全网漏洞专扫与传统漏扫的区别

	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

全网漏洞专扫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**。

1 摘要

2015年11月10日中午12点左右，我们发现了某不知名团体利用redis设计缺陷，针对国内互联网进行了全网性的入侵事件。这次大规模的攻击事件主要针对Linux服务器，如果redis服务器使用root权限启动，并且没有配置认证，就可能能够导致redis数据丢失，服务器被添加账号用于ssh远程登录。

经过白帽汇安全团队的进一步分析，此次攻击事件已经导致至少10000家暴露redis服务器被成功入侵，我们会在后续持续更新进一步动态。

2 入侵事件

2015年11月10日中午12点左右，我们在公网部署的多台安全探针服务器陆续触发了异常告警，有多台redis数据被突然清空。通过分析发现：

- 执行了flushall清空数据的操作
- 在redis数据中新建了一个名为crackit的key键值，内容为ssh-rsa AAAAB3Nza<此处省略若干字母>mo6BLZV4/ crack@redis.io， 如下图

```
[root@test ~]$ redis-cli -h [redacted] get crackit
"\n\n\nssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCcuHEVMRqY/Co/RJ
5o5RTZmpl6sZ7U6w39WAvM7Scl7nGvr5mS4MRRIDaoAZpw7sPjmBHz2HwVAPY
GCekcIVkBXzc3p31v79fWeLXXyxtsOjFz8YzhYMZiugOgCKvRIs63DFf1gFoM
/OHUyDHosi8E6BOi7ANqupScN8CIxDGsXMFr4EbQn4DoFeRTKLg5fHL9qGama
XXZRECkWHmjFYUZGjgeAlSydzR49x36jQ6nuFBM18cEzeSzkxbbtubnbAOMrB
52tQX4RrOqmuWVE/Z0uCOBlbbG+9sKyY9wyp/aHLnRiyC8G8vbrZqQmyn9Yu1
zBp3tY8Tt6Dwmo6BLZv4/ crack@redis.io\n\n\n\n\n"
```

- 在/root/.ssh文件夹下新建了一个authorized_keys文件，内容很明显是redis生成的db二进制文件，里面清晰的看到crackit对应内容，也就是入侵者尝试通过配置一个ssh的key来进行登录。内容如下图：

```
[root@test ~/.ssh]# ls
appendonly.aof  authorized_keys  id_dsa  id_dsa.pub  known_hosts
[root@test ~/.ssh]#
```

【漏洞预警】Struts2 最新命令执行漏洞S2-053[最新更新，有PoC]

8 个月前 分享到:

情报类型	可信度	情报威胁等级	公开情况	提交人
重大安全漏洞	★★★★★	严重情报		BaCde

详情

补充

北京时间2017年09月7日，Struts2 点官方发布最新一个漏洞公告，官方设定漏洞危害等级为中等。 编号为S2-053。该漏洞可能导致攻击者提升权限，控制服务器。由于Struts2使用广泛，国内政府，大型企业均有使用该框架，请及时升级最新版本或做好防护措施。

Struts2是一个基于MVC设计模式的Web应用框架，目前已经发展成为一个非常成熟的框架。在全球共有2723866个Struts2网站对外开放，全球用大量的网站使用该框架开发。其中许多政府，大型企业均有使用。

根据FOFA系统数据显示，Struts2 全球使用最多的国家是美国，共有913859个；中国第二525319；德国第三，共有132235个；韩国第四，共有74821个；荷兰第五，共有58608个。中国地区中浙江省最多，共有143706个；北京市第二，共有106511个；广东省第三，共有48431个；上海市第四，共有40297个；江苏省第五，共有25527个。

白帽汇-龙专

THANKS


HANA
Hadoop
SQL
MySQL
DB2
BigDate
Spark
SQL Server
NewSQL
Oracle
MPP
NoSQL
OLAP

讲师申请
联系电话（微信号）：18612470168

关注“ITPUB”更多
技术干货等你来拿~

与百度外卖、京东、魅族等先后合作系列分享活动

微学堂

让学习更简单

微学堂是以ChinaUnix、ITPUB所组建的微信群为载体，定期邀请嘉宾对热点话题、技术难题、新产品发布等进行移动端的在线直播活动。

截至目前，累计举办活动期数60+，参与人次40000+。

ITPUB学院

ITPUB学院是盛拓传媒IT168企业事业部（ITPUB）旗下
企业级在线学习咨询平台
历经18年技术社区平台发展
汇聚5000万技术用户
紧随企业一线IT技术需求
打造全方式技术培训与技术咨询服务
提供包括企业应用方案培训咨询（包括企业内训）
个人实战技能培训（包括认证培训）
在内的全方位IT技术培训咨询服务

ITPUB学院讲师均来自于企业
一些工程师、架构师、技术经理和CTO
大会演讲专家1800+
社区版主和博客专家500+

培训特色

无限次免费播放
随时随地在线观看
碎片化时间集中学习
聚焦知识点详细解读
讲师在线答疑
强大的技术人脉圈

八大课程体系

基础架构设计与建设
大数据平台
应用架构设计与开发
系统运维与数据库
传统企业数字化转型
人工智能
区块链
移动开发与SEO

联系我们

联系人：黄老师
电　话：010-59127187
邮　箱：edu@itpub.net
网　址：edu.itpub.net
培训微信号：18500940168