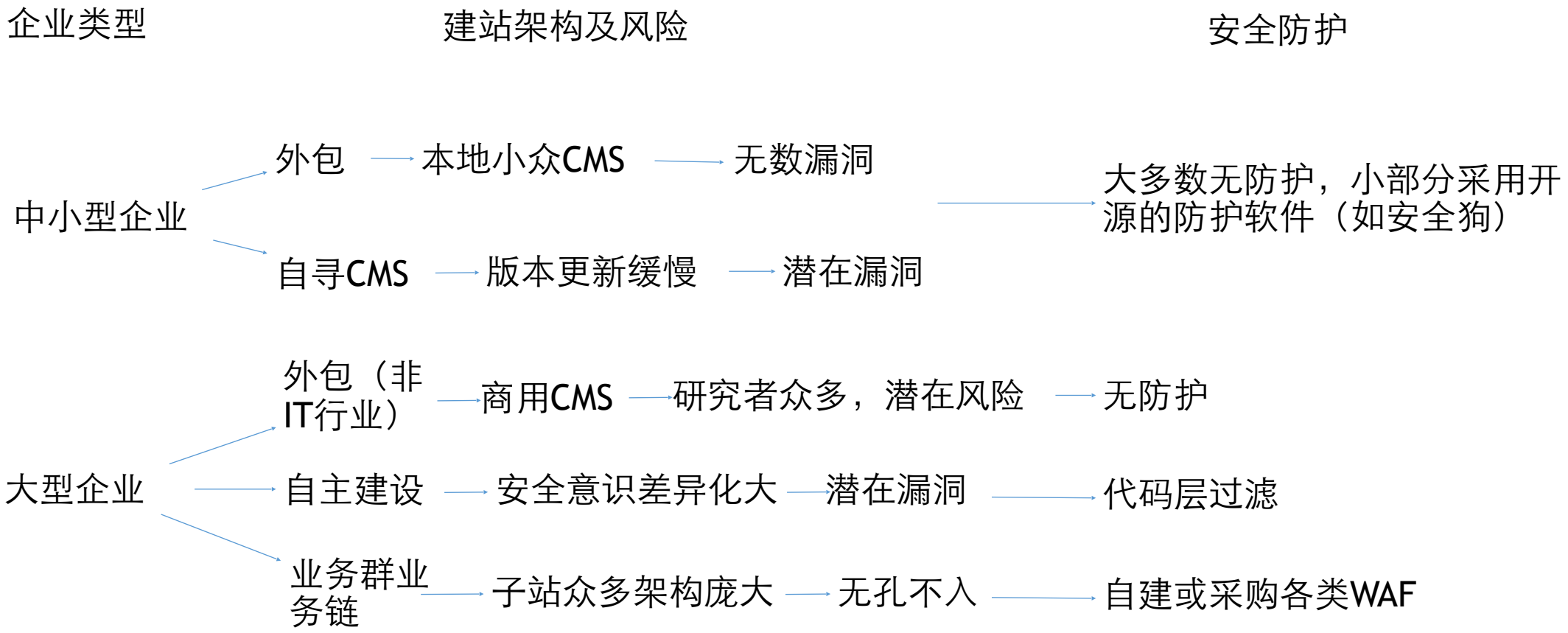
星冕——守护这片星空

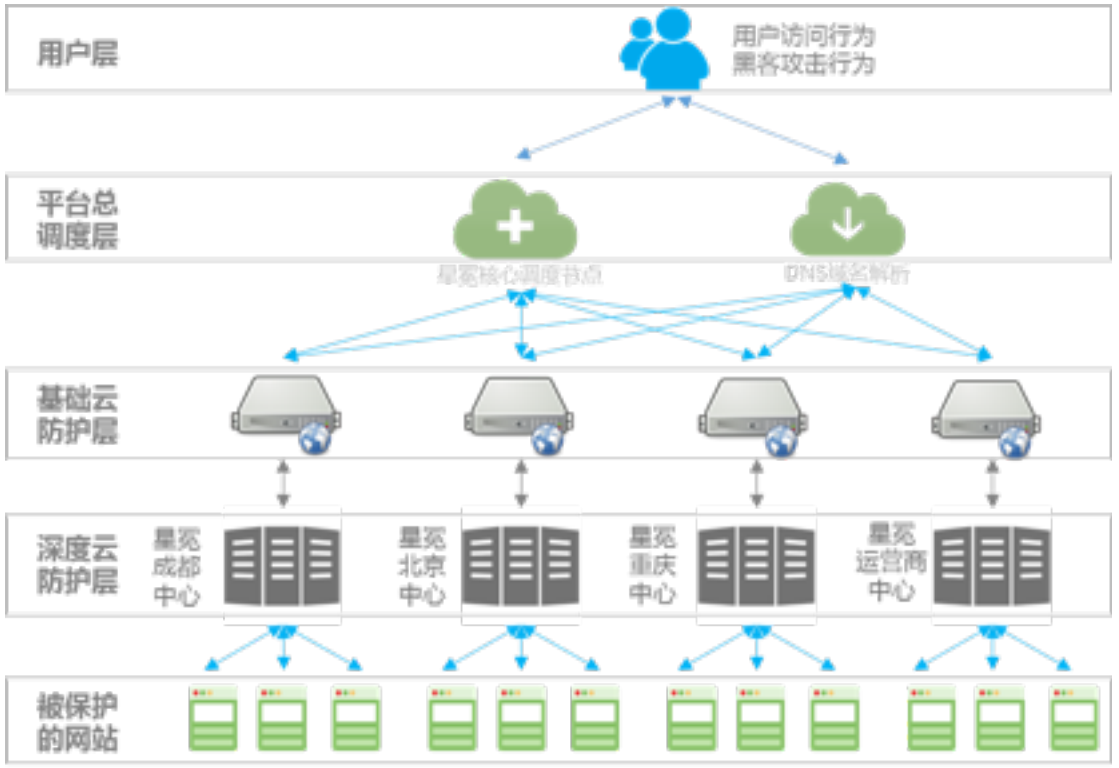
主讲人——PKAV何鹏程(蘑菇)

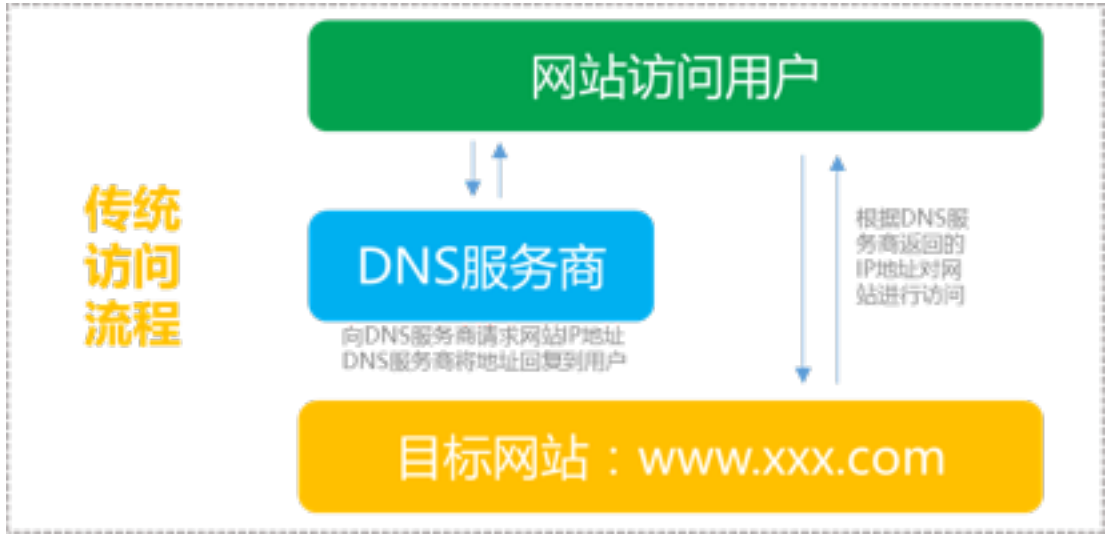
各类型企业面临的安全风险



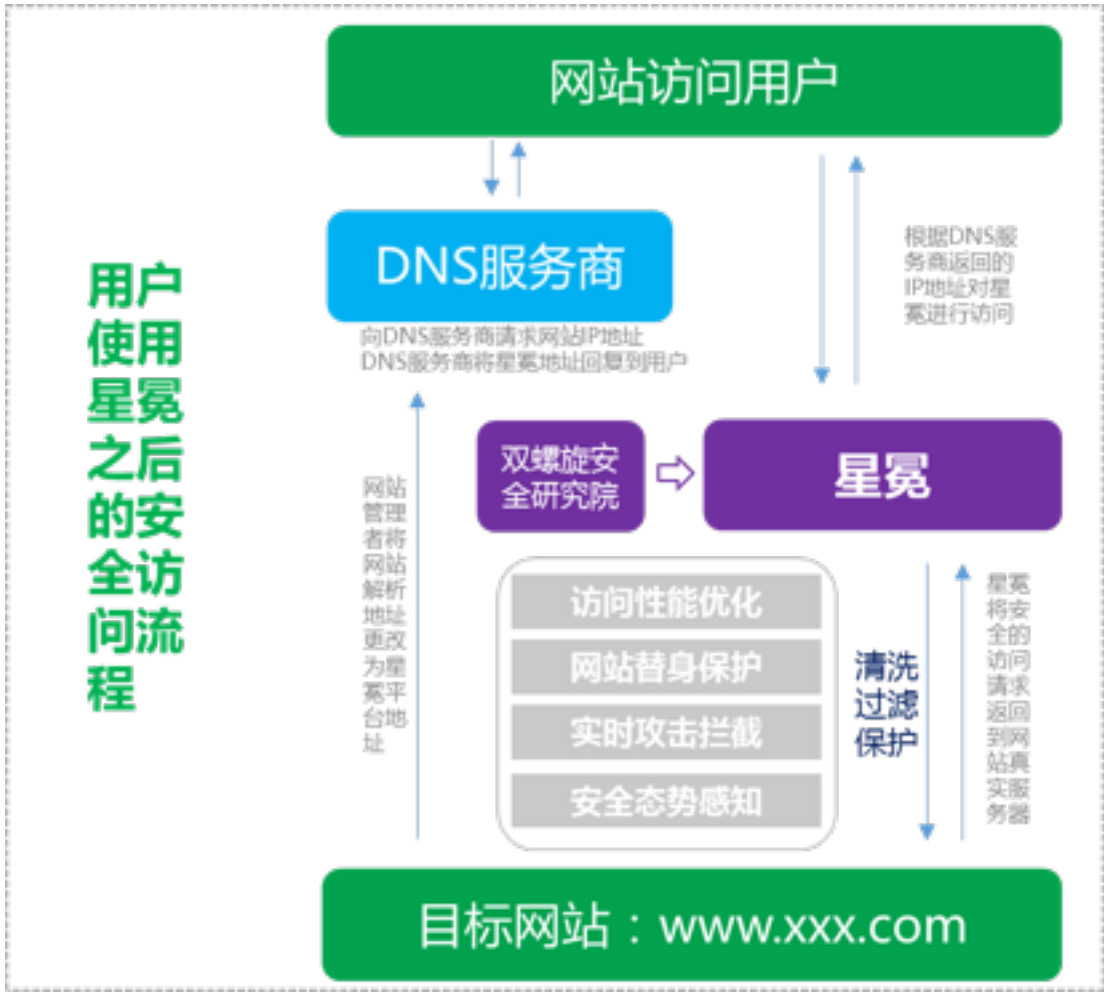
如何在不改变系统原有架构的前提下统一规避风险?

PKAV团队自研的集网站监控、防护与态势感知为一体的系统——星冕





平台功能	功能说明
网站访问加速	对接入设备的网站实现反向代理，反向代理能够帮助用户智能选路并通过静态缓存实现访问加速的功能，与此同时，反向代理能够帮助用户拦截各类攻击请求。
网站日志审计	记录和分析网站的威胁情报日志，以小时为单位对权限范围内的管辖网站进行多维度的日志分析，通过点击日志还可以查看所有网站的安全状态详情，并通过链接定位到安全细节。
全站流量分析	提供实时以及非实时的流量分析统计，用户可以根据自己的需求查看网站的流量负荷并从中提取和发现出异常流量和攻击行为。
多维攻击检测	提供三种维度的攻击检测和积分机制，包括WAF积分、场景积分和固化URL积分三类，用户可以通过该模块来查看网站的安全状态，同时该模块也会智能地拦截非法用户的访问请求。
访问行为还原	当用户选择了指定时间段的指定IP后，可以将该时间段的IP访问行为进行多维度的还原以识别这段时间的用户访问。特别是当确定了攻击者后可以通过该模块来完成入侵行为的还原，并且具有良好的展示效果。
网站篡改检测	通过大数据的手段来识别网站是否遭到了恶意篡改，包括进行网站的源码相似度、图片相似度、词云相似度等多维的数学检测，从而判断网站目前的安全状况。
网站后门检测	通过整站后门检查，检测网站是否被植入后门。
反向落地追踪	提供JS回执功能，对于可疑IP选择性的开启JS回执功能，该模块可以配合指纹系统定位攻击者的虚拟身份信息。
黑白名单添加	提供黑白名单添加的接口，包括IP黑名单、IP白名单以及URL白名单三类，管理员可以自行调节该接口来对特殊页面和特殊IP进行管理。



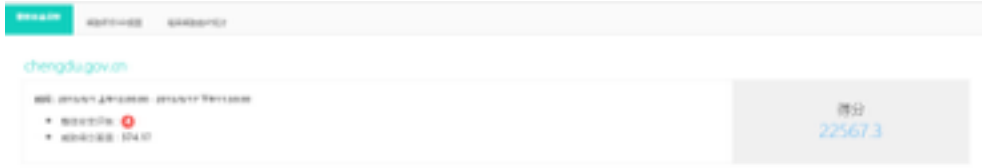
攻击拦截方式

传统的攻击拦截模式 → 基于静态WAF规则

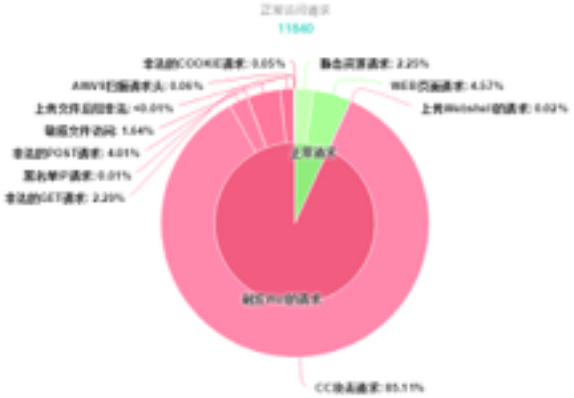
星冕的攻击拦截模式 → 专业团队维护的动态规则
→ 基于行为的场景规则
→ 固化URL规则

威胁情报日志记录

威胁得分与评级



基于规则的访问详情



固化URL监测信息

固化URL监测信息

COUNT	REQUEST_METHOD	PARA	REQUEST_URI
4704	get	id	*
435	get	lanmuid	*
366	get	sublanmuid	*
1	post	aid	/dede/morey/

场景监测信息

场景监测信息

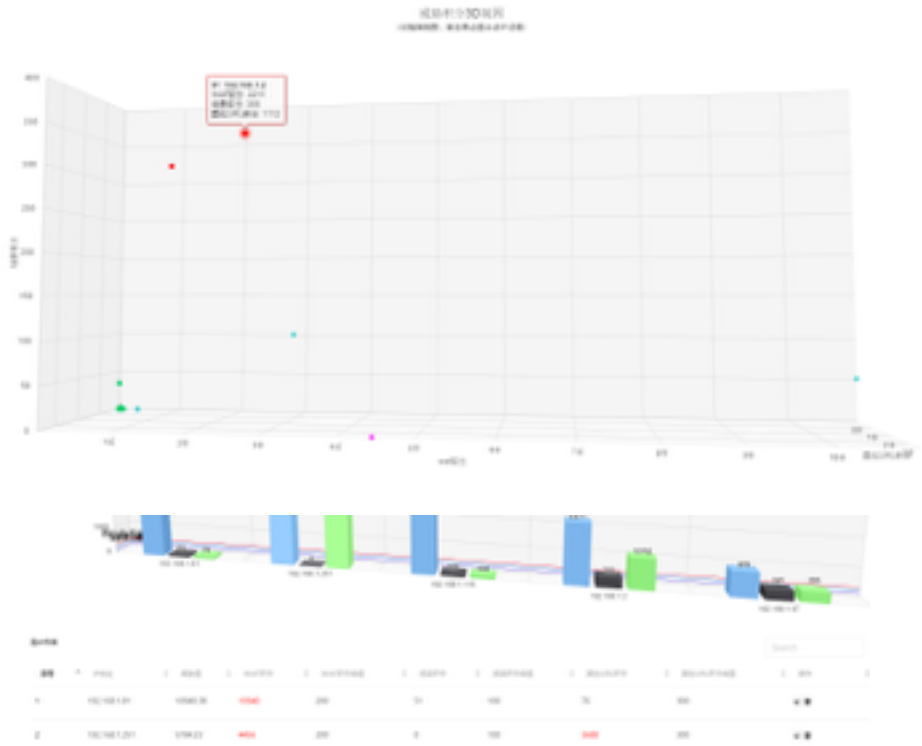
名称	数值
某页面单请求访问21到50次	15
某页面单请求访问100次以上	1
某页面单请求访问10次到20次	44
用户登录后直接执行进程操作（上传图片）	3
当前时间，操作和备份数据库	2
登陆后台后直接访问数据库	7
后台单登陆5次以上	3
某页面单请求访问51次到100次	4
当前时间个人邮件（上传）	2

行为还原方式

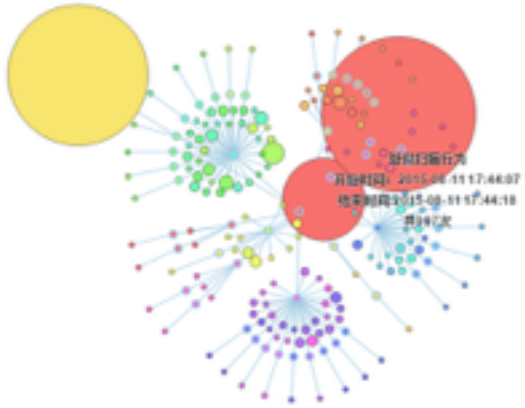
传统的行为还原方式 → 日志分析

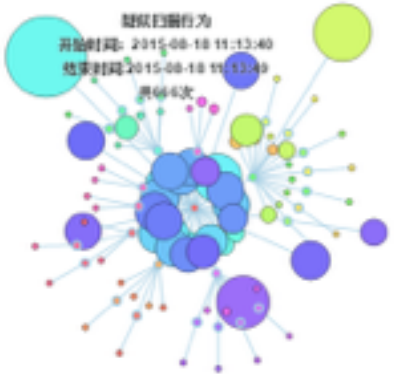
星冕的行为还原方式
- 可视化的访问记录显示
- 可视化的访问时段还原
- 基于算法的扫描行为识别

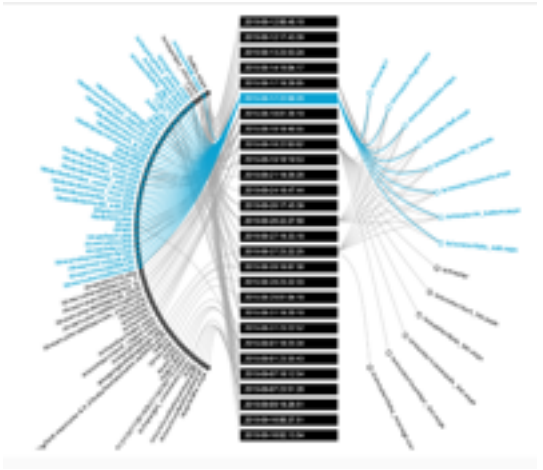
定向的行为还原接口

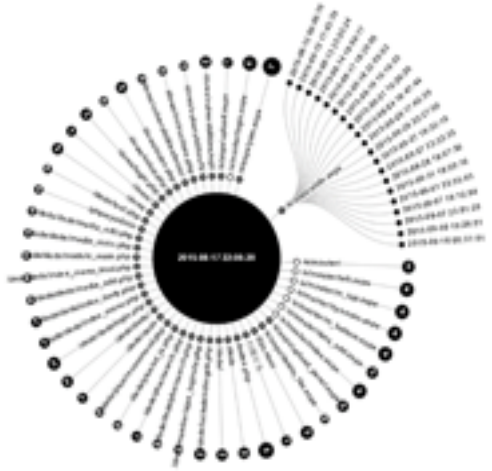


自定义的行为还原接口









网页篡改检测

传统的网页篡改检测 → 源码检测

星冕的网页篡改检测
- 源码检测
- 链接检测
- 分词检测
- 图像检测

反向落地追踪

传统的落地追踪模式 → 落地到IP以及该IP的地理位置

缺点
- 只有IP地址，无法定位到更为相信的信息
- 一旦用户挂上VPN则无法定位到准确信息
- 只能定位到公网地址，内网的用户无法区分

星冕的落地追踪模式 → 指纹识别

回传隐藏JS　　配合指纹系统

获取访客的唯一网络标识，以及该标识所对应的网络身份（包括ID、用户名、昵称等）

- 获取详尽的虚拟身份
- 无视任何VPN
- 无视任何网络环境
- 性能稳定可做长期监控

指纹系统总体技术架构->纯粹依靠漏洞，很难被模仿和被超越

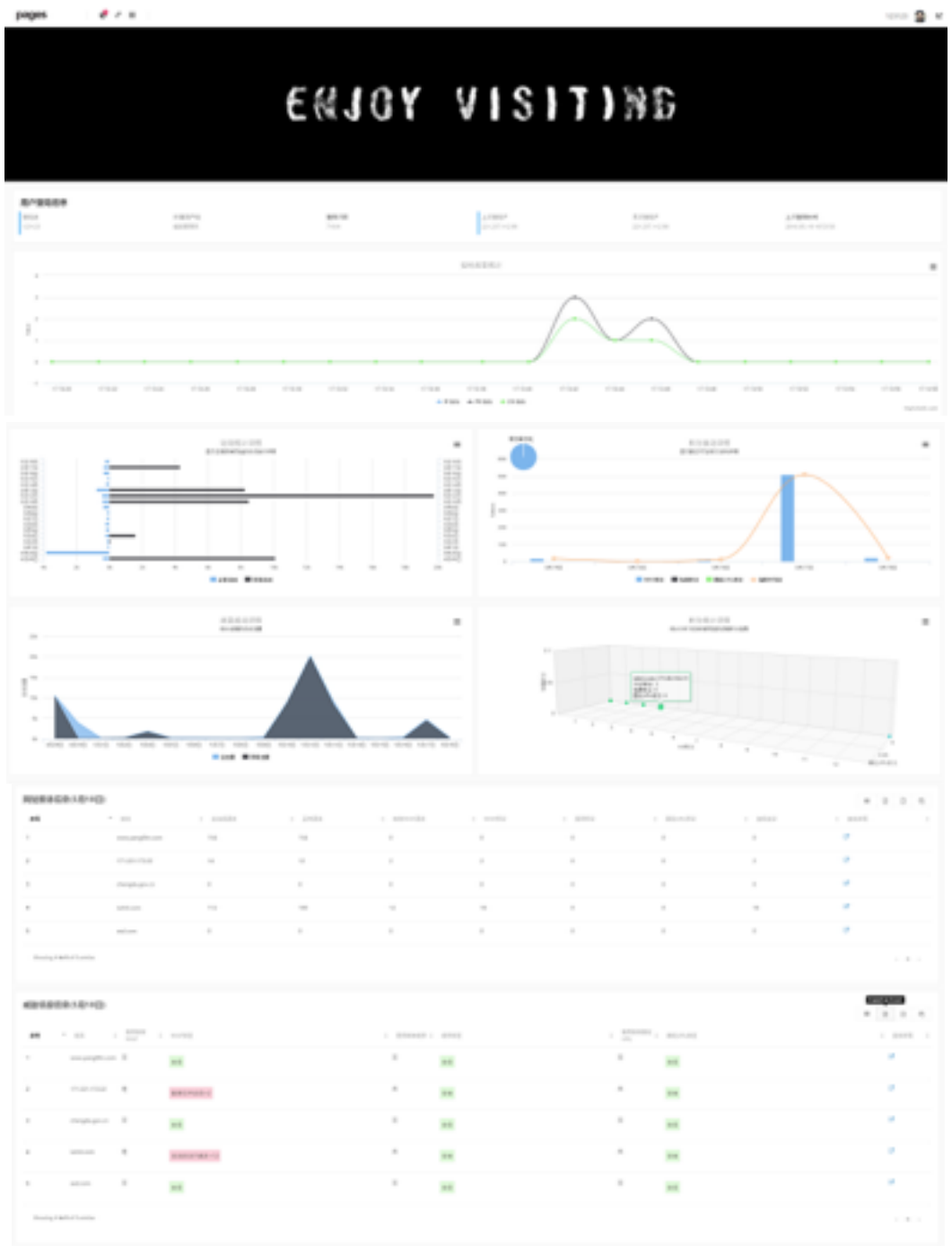
我们能获取到的网站指纹

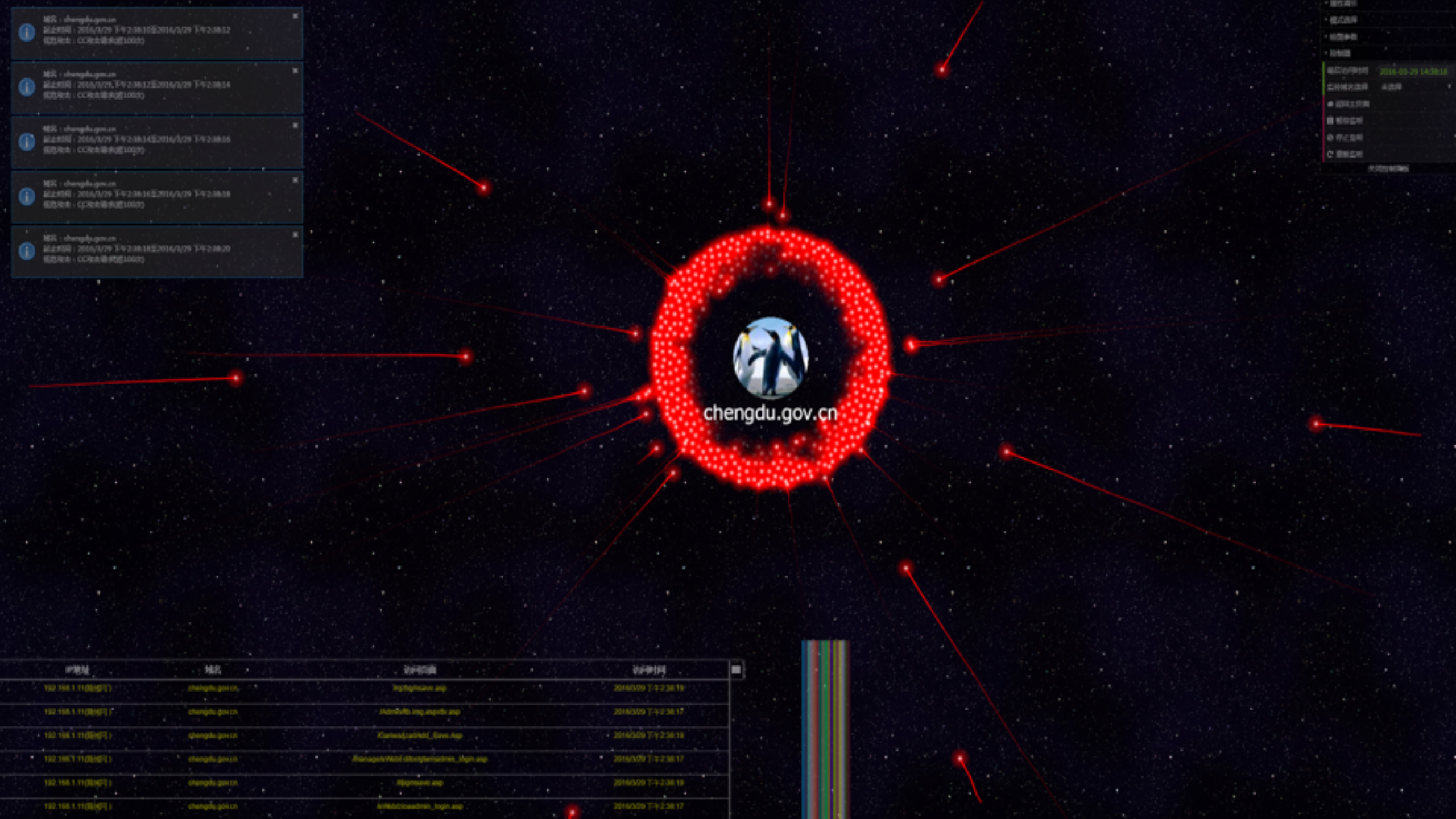
除此之外用户也可以自定义返回JS信息（例如用作推广）

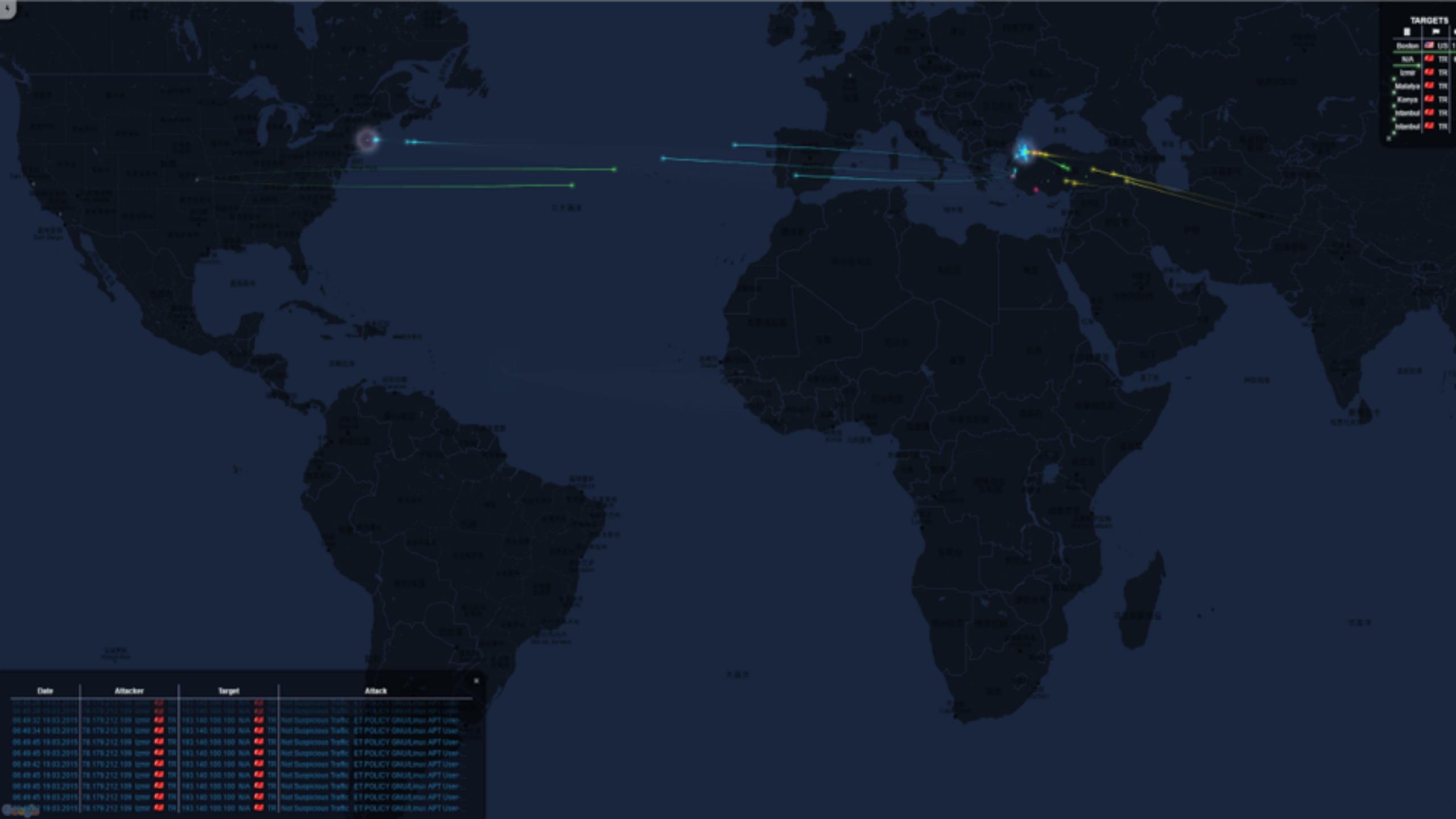
详细监测信息

传统的监测信息记录 → 数据库->表格的单一展示

星冕的监测信息记录
- 图、文、表相结合
- 完善的报告生成体系
- 自定义的攻击预警提示
- 直观的实时监控信息




chengdu.gov.cn



TARGETS

Boston	🇺🇸	US
N/A	🇹🇷	TR
Izmir	🇹🇷	TR
Malatya	🇹🇷	TR
Konya	🇹🇷	TR
Istanbul	🇹🇷	TR
Istanbul	🇹🇷	TR

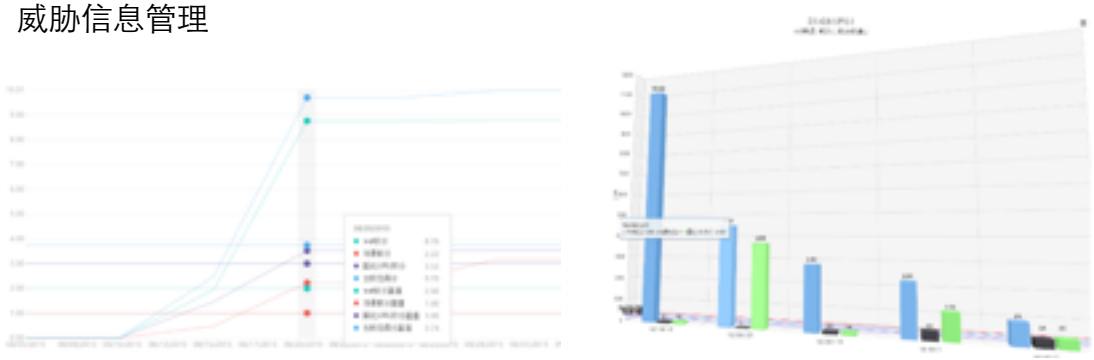
Date	Attacker	Target	Attack
06:49:28 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:28 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:32 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:34 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:45 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:45 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:42 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:45 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:45 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
06:49:45 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...
[illegible] 19.03.2015	78.179.212.109 Izmir 🇹🇷 TR	193.140.100.100 N/A 🇹🇷 TR	Not Suspicious Traffic ET POLICY GNU/Linux APT User-...

除此之外

流量分析

黑白名单添加

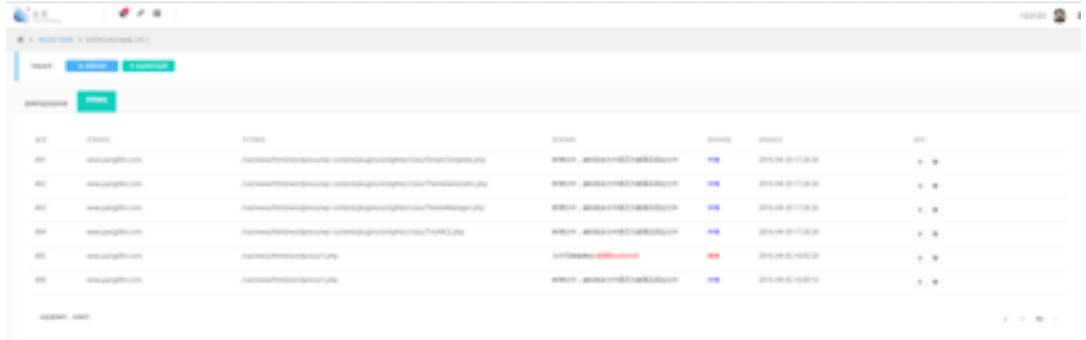
威胁信息管理



域名及用户管理

操作日志管理

后门检测



细节决定成败

品质铸就辉煌