2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

基于威胁情报驱动的云安全实践

陈 奋 安全狗 CEO

目 录
Contents

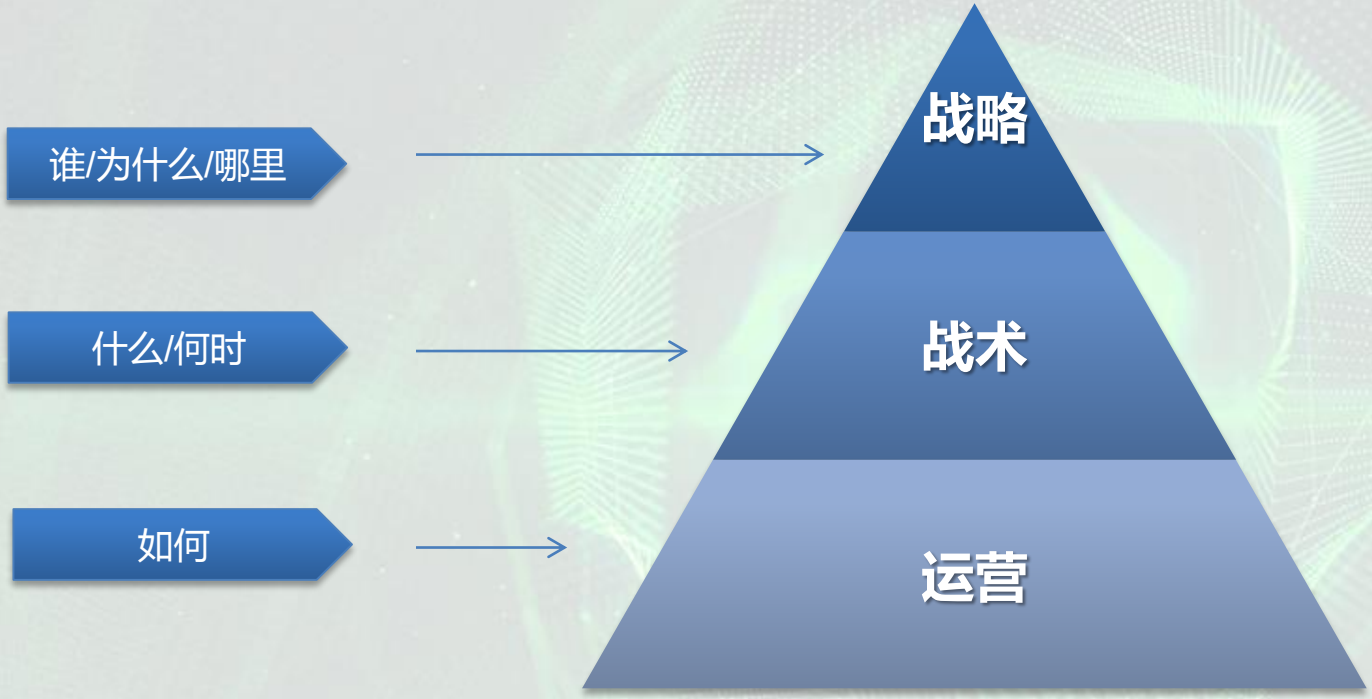
Section. 01

基于威胁情报驱动的云安全平台架构

威胁情报（TI）研究的重要意义

Gartner 对威胁情报的定义：

基于证据、关于资产所面临的现有或新兴威胁及风险的 **认识**，包括环境、机制、指标、可能结果及可付诸行动的建议，可为威胁或风险应对 **决策提供信息。**



基于威胁情报驱动的云安全平台架构

以威胁情报为驱动

漏洞情报 | 威胁情报 | 威胁情报 | 漏洞情报 | 威胁情报

输入 | 输入 | 输入 | 输入

云安全管理平台

风险管理	攻击威胁	持续监测	联动响应
漏洞风险	攻击分析	行为监测	安全加固
配置风险	定向攻击	日志监测	安全策略/规则
基线安全	高级威胁	完整性监测	黑白名单
权限风险	日志分析	流量监测	
人员/资产风险			

产生 | 产生 | 产生

漏洞情报 | 威胁情报 | 威胁情报

公有云用户

阿里云
腾讯云
HUAWEI 华为企业云
金山云 WWW.KSYUN.COM
• • •

私有云平台

vmware
openstack

Section. 02

基于云安全平台攻防数据的威胁情报分析模型

威胁情报研究的基础

数据！

大量的数据！

大量的实时数据！

大量的、实时的有效数据！

深度分析和挖掘

安全狗用户全球分布图

日均拦截超过 2亿 次攻击，涵盖WEB攻击、系统攻击和网络攻击

安全狗

进行威胁情报研究的数据优势

安全狗拥有海量、持续且多维的独有数据

安全狗·服云已覆盖超两百八十万台的（云）服务器，解决了循证观测中单点数据量少与随机性不足的问题

日均拦截超过两亿次攻击，获取的威胁数据和事件实时性强、随机性大、可观测度高、攻击信息和特征丰富，足以支撑对威胁的证据提取，以及对事件（现象）场景的构建

具备实时应对活动数据的采集能力，足以支撑应对活动有效性的判断，指导建立应对活动的经验决策模型和应急式响应的效果观测

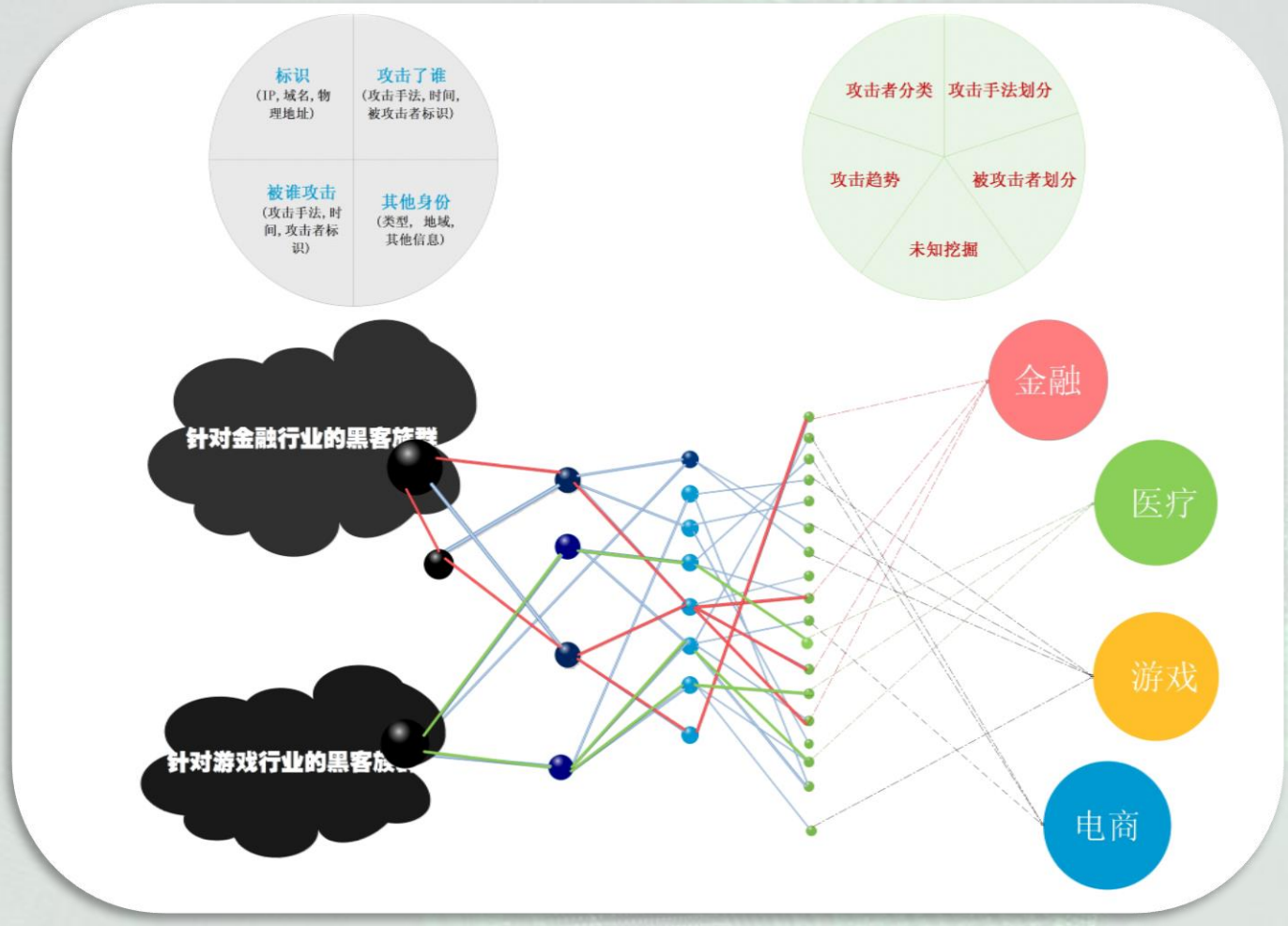
安全元数据


攻击者
攻击频度
攻击广度
攻击时间线
攻击IP，时空属性
服务器信息，业务信息
攻击类型（Payload信息）

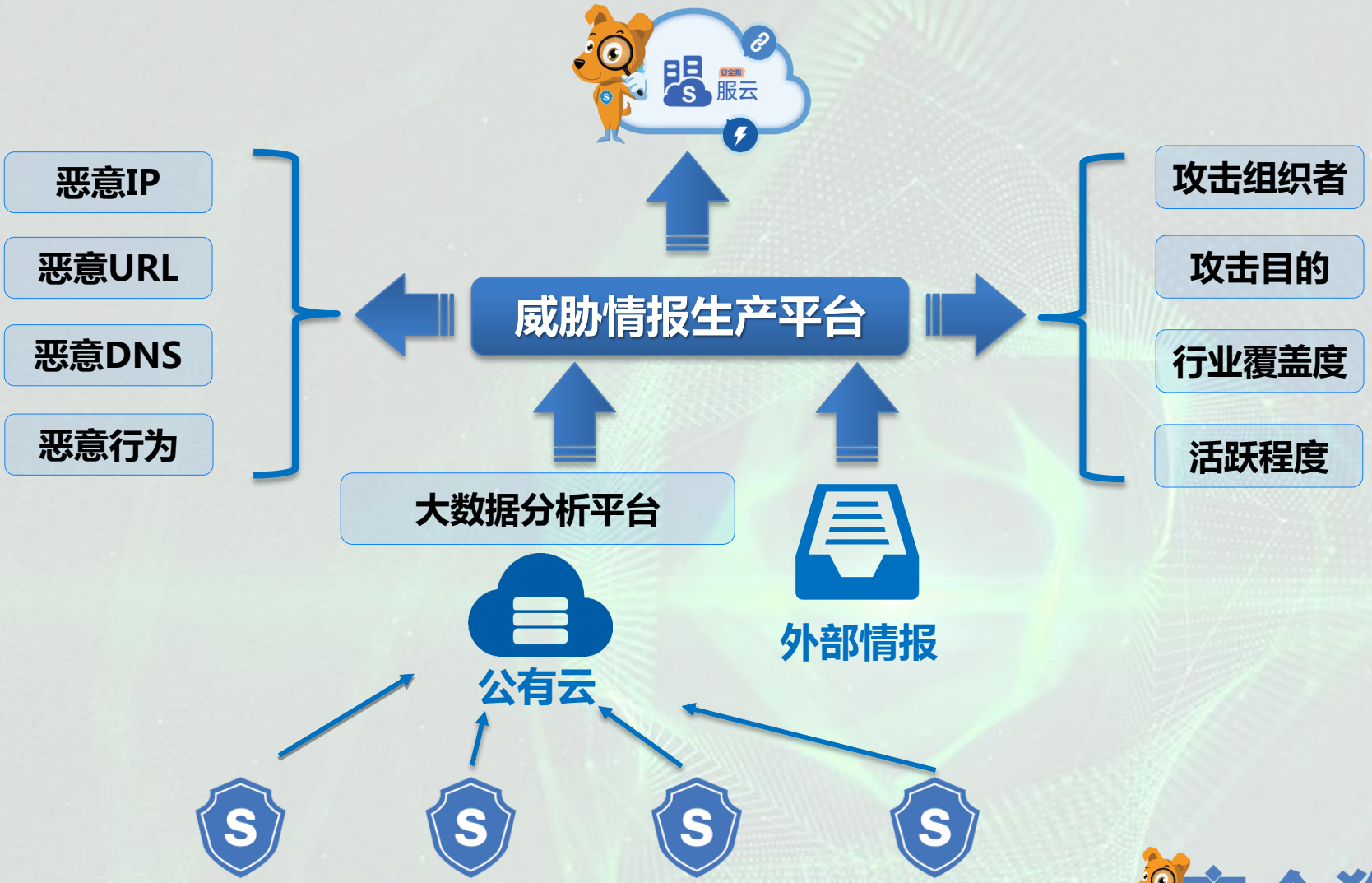

被攻击者
业务类型
业务模型
业务信息
被哪些IP攻击，攻击时间线，攻击结果
被攻击的类型，频率，端口，手法
IP，地域信息，硬件信息
服务器是否发动了攻击，感染情况
服务器类型，网络拓扑，域名，流量

攻防情报推演

黑客族群定位


标识
(IP, 域名, 物理地址)
攻击了谁
(攻击手法, 时间, 被攻击者标识)
被谁攻击
(攻击手法, 时间, 攻击者标识)
其他身份
(类型, 地域, 其他信息)
攻击者分类
攻击手法划分
攻击趋势
被攻击者划分
未知挖掘
针对金融行业的黑客族群
针对游戏行业的黑客族群
金融
医疗
游戏
电商

安全威胁情报产生



- 只有 **经过分析并打上更深层次属性标签的安全数据**，才具备情报价值，否则还只是传统安全规则类型的数据。

- 每家公司都有自己数据的特点和分析的视角，需要 **加强数据共享和碰撞** 才能使数据的情报价值全面提升。

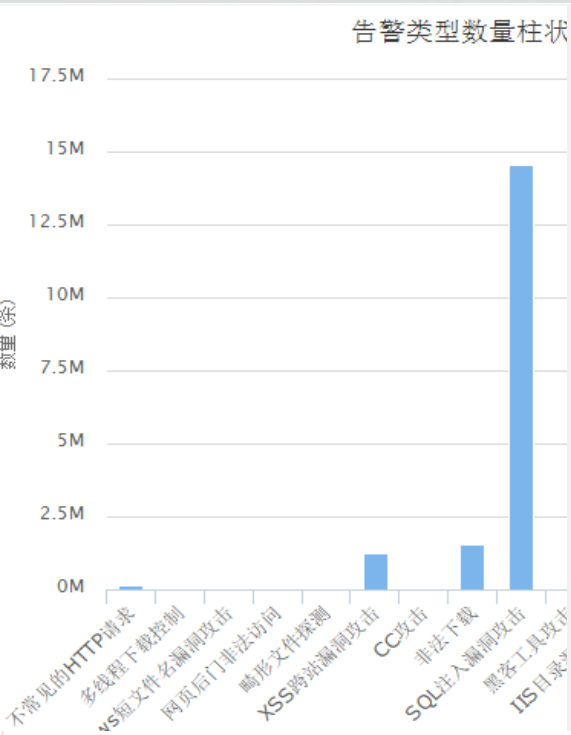
Section. 03

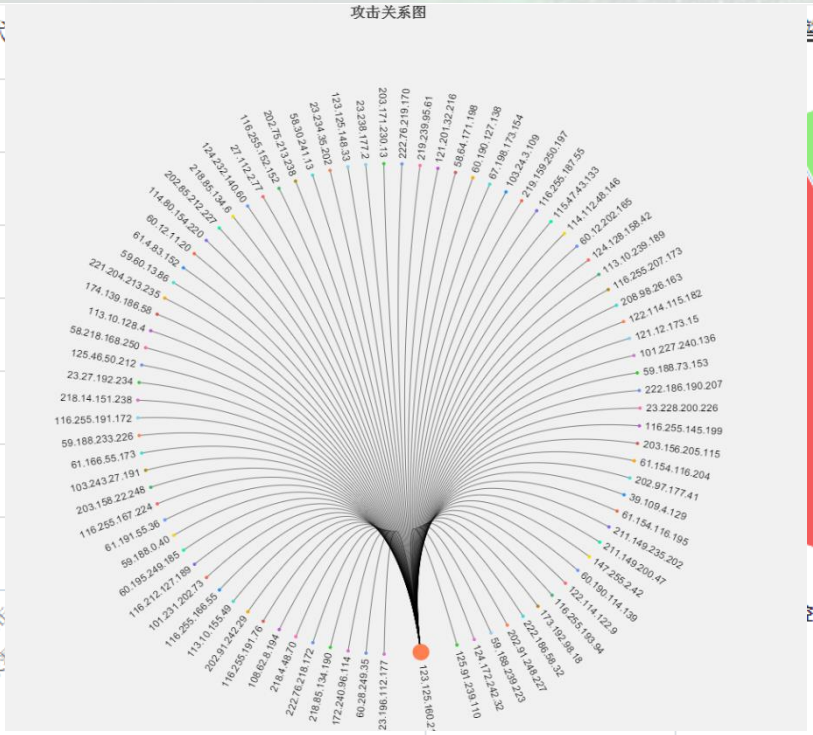
基于云安全平台攻防数据提取到的威胁情报

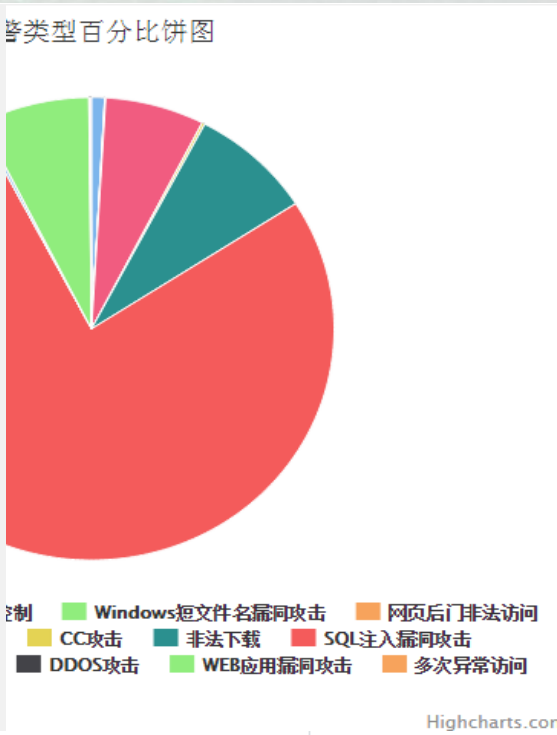
（1）黑IP的故事

举例：关于黑IP趋势的观测

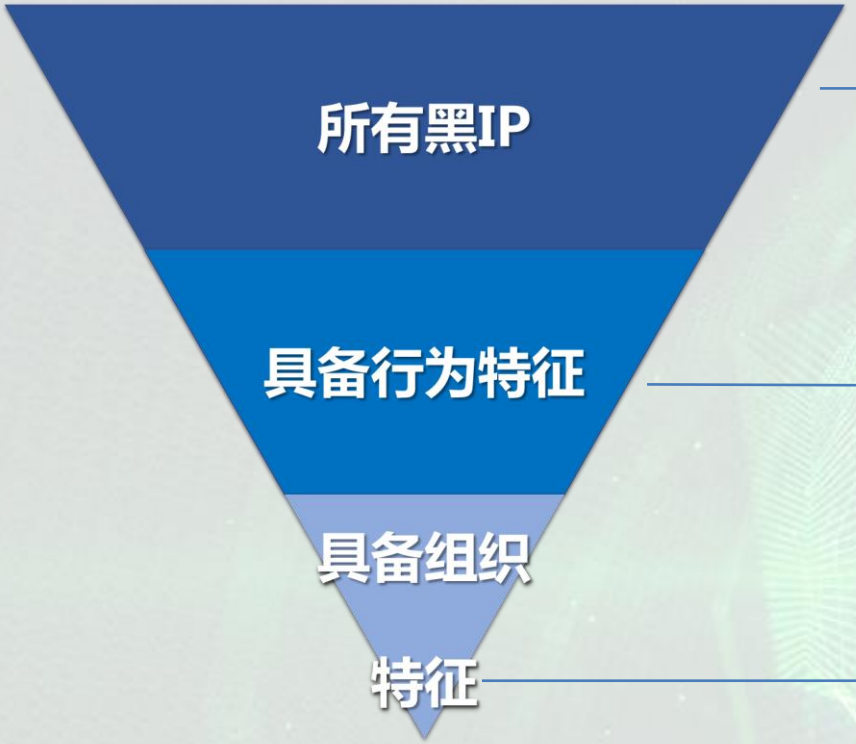
安全狗每天可捕获超过 100,000 个黑IP，并同步给所保护的用户设备







黑IP的价值链



- 长期活跃的
- 短期活跃的
- 基于代理跳板的（WHOIS、机房信息及地理位置）
- 被控制主机
- 其他基础属性

- 扫描器家族
- 暴力破解家族
- 批量扫漏洞家族（扫系统漏洞、WEB漏洞）

- “黑色”SEO组织
- 针对金融等行业目标的渗透组织
- 羊毛党

标签属性越丰富的黑 IP，价值越高

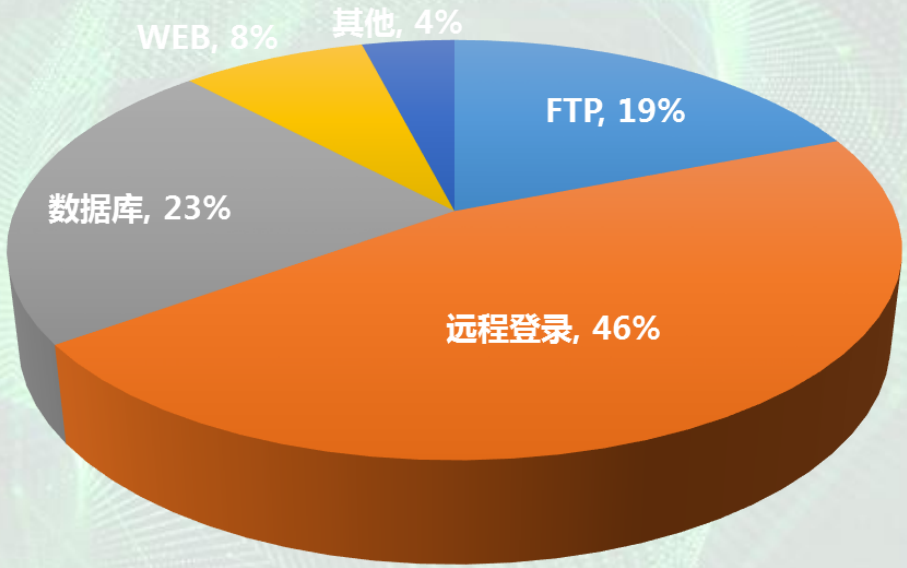
黑IP家族追踪分析：暴力破解党

（1）暴力破解党

- 针对（云）服务器攻击占比最大（相信各大云厂商也是这个结论）
- 控制大量肉鸡进行分布式破解
- 无特定目标分类，全网盲扫

先看一组图

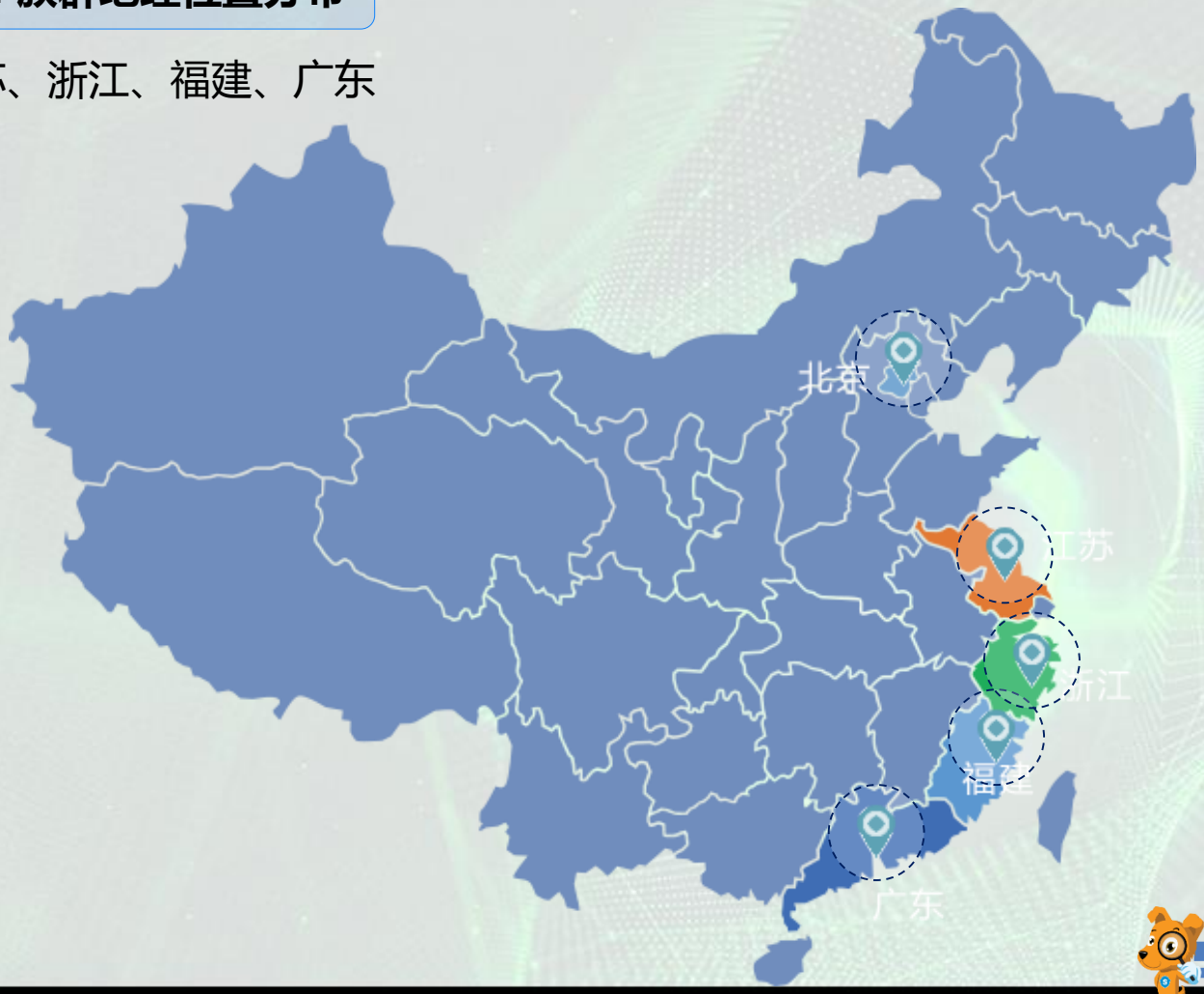
暴力破解类型分布图



黑IP家族追踪分析：暴力破解党

暴力破解IP族群地理位置分布

北京、江苏、浙江、福建、广东



黑IP家族追踪分析：暴力破解党

破解成功后主要行为： 快速上传肉鸡程序、上传攻击后门、制作虚拟化服务器等。

根据攻击特征，我们把这些IP打了8个家族标签，如下以”**VPS党**”为例说明：

黑IP家族追踪分析：VPS党

服务器 | 杭州 | Linux
活跃度高 | 性能高 | 非代理
C&C： 47.88.77.*
暴力破解：系统
风险值：中

服务器 | 广州 | Linux
活跃度高 | 性能高 | 非代理
C&C： 47.88.77.*
暴力破解：系统
风险值：中

服务器 | 北京 | Linux
活跃度高 | 性能中 | 非代理
C&C ： 47.88.77.*
暴力破解：系统
风险值：中

破解成功后1小时内下载国外开源虚拟化软件，把当前机器分割成几台虚拟机

安全狗

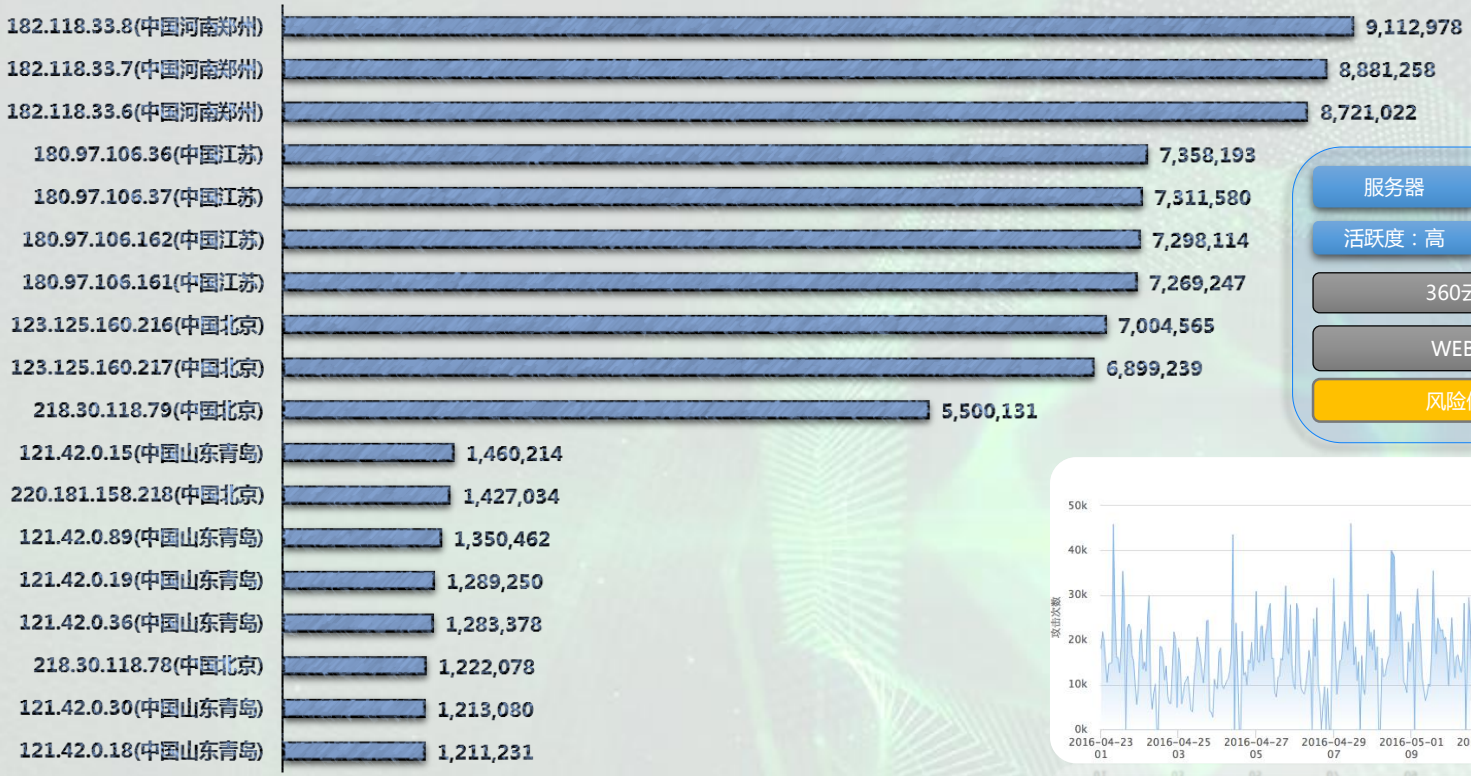
黑IP家族追踪分析：扫描器家族

（2）扫描器家族

扫描器家族标签也分为几类：

- 国内几家做云扫描的安全公司（授权 OR 未授权）
- 专门扫 web 漏洞
- 专门扫 webshell
- 专门扫敏感文件

黑IP家族追踪分析：云扫描器家族



服务器 | 郑州 | Linux

活跃度：高 | 性能：高 | 非代理

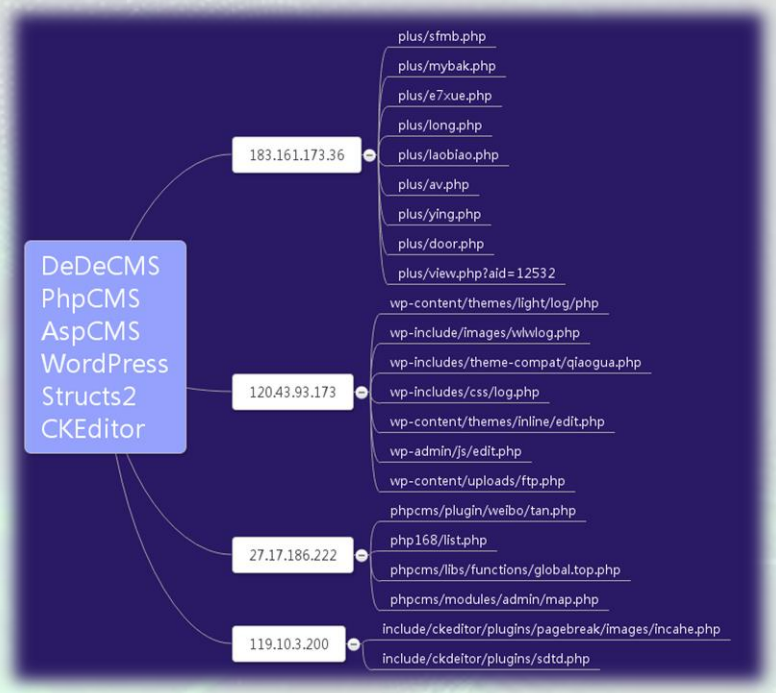
360云扫描

WEB扫描

风险值：低

黑IP家族追踪分析：Webshell扫描家族

- 主要扫描以发现几大流行CMS历史上漏洞常见攻击代码产生的 WebShell；
- 扫描成功后通常由菜刀工具进行批量管理；
- 此类家族目的明确，整体风险值较低；经常给网站带来大量无效访问，对日志分析进行干扰。



黑IP情报价值

黑IP的情报价值：

- 转换成防御规则（常规用途）
- 溯源分析
- 入侵事件的危害定级

（2）Webshell 追踪

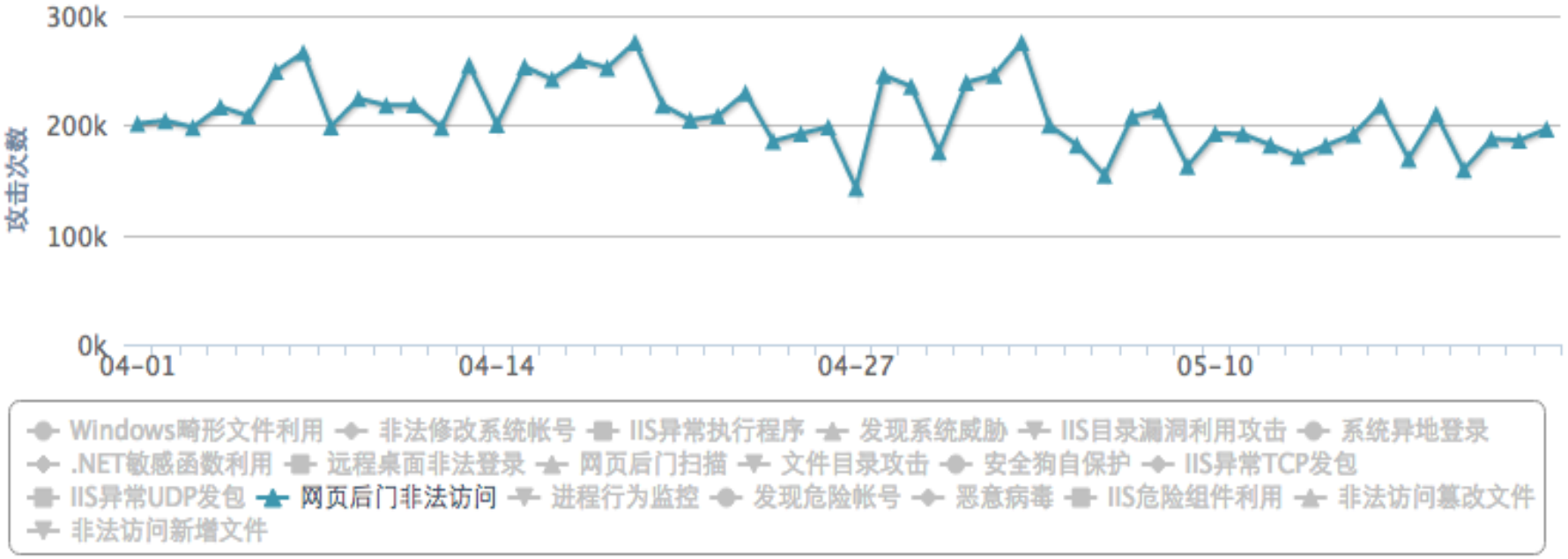
Webshell 情况

累计 WebShell 样本： 近200万个变种

- 覆盖ASP/ASPX/PHP/JSP等多种脚本
- 给 webshell 类型家族打上标签

常规一句话后门	变形一句话后门	DDOS攻击后门	搜索引擎欺骗
全功能型后门	提权型后门	SEO控制后门	其他

Webshell 每日攻击趋势：相对比较平稳



网页后门非法访问	发现51.255.65.80(法国法国)访问网页后门www.bjxgy.com.cn/tops/157/link.asp?=845921_473408，已被安全狗成功阻止	www.bjxgy.com.cn	51.255.65.80	2016-05-23 00:00:15
网页后门非法访问	发现51.255.65.34(法国法国)访问网页后门www.bjxgy.com.cn/tops/104/link.asp?page=/article/597284.html，已被安全狗成功阻止	www.bjxgy.com.cn	51.255.65.34	2016-05-23 00:00:16
网页后门非法访问	发现164.132.161.60(法国法国)访问网页后门www.bjxgy.com.cn/tops/1/link.asp?page=/article/512783.html，已被安全狗成功阻止	www.bjxgy.com.cn	164.132.161.60	2016-05-23 00:00:20
网页后门非法访问	发现51.255.65.76(法国法国)访问网页后门www.bjxgy.com.cn/tops/1/link.asp?page=/article/268625.html，已被安全狗成功阻止	www.bjxgy.com.cn	51.255.65.76	2016-05-23 00:00:21
网页后门非法访问	发现151.80.31.181(法国北部－加来海峡大区鲁贝)访问网页后门www.bjxgy.com.cn/tops/417/link.asp?page=/article/048550.html，已被安全狗成功阻止	www.bjxgy.com.cn	151.80.31.181	2016-05-23 00:00:22
网页后门非法访问	发现51.255.65.67(法国法国)访问网页后门www.reluex.com/en/tmo/56461.asp，已被安全狗成功阻止	www.reluex.com	51.255.65.67	2016-05-23 00:01:56
网页后门非法访问	发现164.132.161.20(法国法国)访问网页后门www.shashiguliao.cn/cjjuey/jint/flGi/2Qs/w04r/index.php，已被安全狗成功阻止	www.shashiguliao.cn	164.132.161.20	2016-05-23 00:02:10
网页后门非法访问	发现148.251.13.51(德国巴伐利亚州纽伦堡)访问网页后门www.sihaijixie.com/rss.php?thread-365722-9.html，已被安全狗成功阻止	www.sihaijixie.com	148.251.13.51	2016-05-23 00:03:05
网页后门非法访问	发现164.132.161.12(法国法国)访问网页后门www.bjxgy.com.cn/tops/107/link.asp?page=/article/978278.html，已被安全狗成功阻止	www.bjxgy.com.cn	164.132.161.12	2016-05-23 00:03:03
网页后门非法访问	发现164.132.161.49(法国法国)访问网页后门www.bjxgy.com.cn/tops/582/link.asp?page=/article/877315.html，已被安全狗成功阻止	www.bjxgy.com.cn	164.132.161.49	2016-05-23 00:03:04
网页后门非法访问	发现151.80.31.168(法国北部－加来海峡大区鲁贝)访问网页后门hyhbsb.cn/images/wwwpj749com.php?2016-03-22.html，已被安全狗成功阻止	hyhbsb.cn	151.80.31.168	2016-05-23 00:02:55
网页后门非法访问	发现164.132.161.78(法国法国)访问网页后门www.sichengjixie.com/images/dd/39469.asp?WebShieldDRSessionVerify=KoV0gDKTbu9Ekrx1z2wm，已被安全狗成功阻止	www.sichengjixie.com	164.132.161.78	2016-05-23 00:03:07
网页后门非法访问	发现151.80.31.157(法国北部－加来海峡大区鲁贝)访问网页后门www.bjxgy.com.cn/tops/100/link.asp?page=/article/553687.html，已被安全狗成功阻止	www.bjxgy.com.cn	151.80.31.157	2016-05-23 00:03:02
网页后门非法访问	发现164.132.161.92(法国法国)访问网页后门www.bjxgy.com.cn/tops/1/link.asp?page=/article/105786.html，已被安全狗成功阻止	www.bjxgy.com.cn	164.132.161.92	2016-05-23 00:03:05

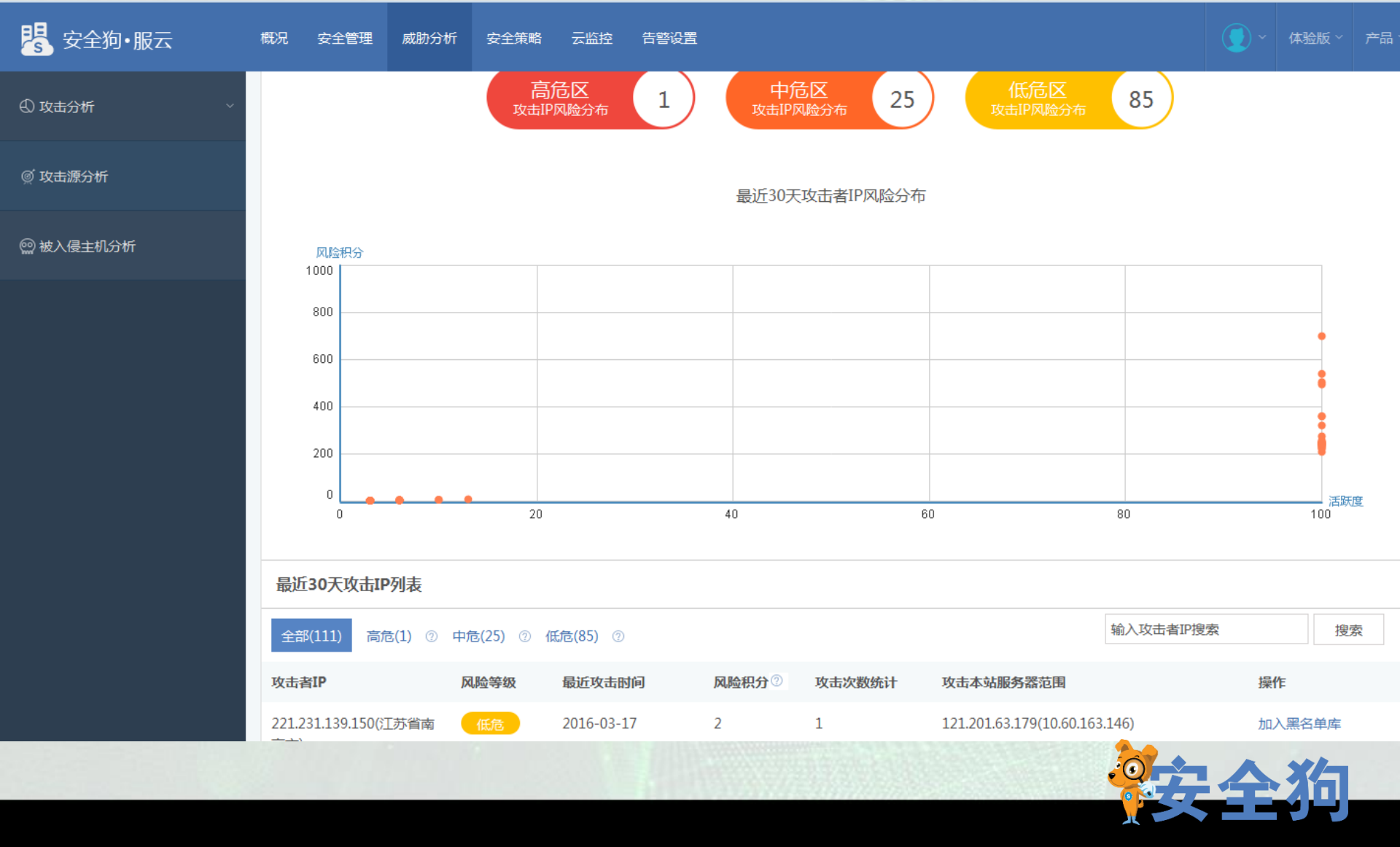
Webshell 攻击分析

WebShell 攻击分析：

- 样本变化灵活，难以聚集族群特性
- 攻击IP分散（寻找有价值的族群性攻击IP群）
- 特种 WebShell 样本挖掘

Section. 04
威胁情报在云安全平台的应用

攻击源分析


安全狗·服云
概况
安全管理
威胁分析
安全策略
云监控
告警设置
体验版
产品
攻击分析
攻击源分析
被入侵主机分析
高危区
攻击IP风险分布
1
中危区
攻击IP风险分布
25
低危区
攻击IP风险分布
85
最近30天攻击者IP风险分布
风险积分
1000
800
600
400
200
0
0
20
40
60
80
100
活跃度
最近30天攻击IP列表
全部(111)
高危(1)
中危(25)
低危(85)
输入攻击者IP搜索
搜索
攻击者IP
风险等级
最近攻击时间
风险积分
攻击次数统计
攻击本站服务器范围
操作
221.231.139.150(江苏省南
低危
2016-03-17
2
1
121.201.63.179(10.60.163.146)
加入黑名单库

安全狗

攻击源分析

攻击者IP：142.163.43.50 返回

基本信息

攻击手法

攻击事件

攻击事件	最近攻击时间	被攻击应用/IP	攻击特征	风险等级
文件包含漏洞攻击 (持续攻击75次)	2016-07-05 12:43:08	218.107.192.67(10.10.1.93;10.10.1.4)	发现120.42.99.154(福建厦门)访问security.safedog.cn/login.html?service=../../../../../../../../../windows/... 复制	中危
SQL注入攻击 (持续攻击74次)	2016-07-05 12:42:15	218.107.192.67(10.10.1.93;10.10.1.4)	发现120.42.99.154(福建厦门)SQL注入攻击security.safedog.cn/login.html?service=invalid../../../../../../../..... 复制	中危
非法下载 (持续攻击24次)	2016-07-05 12:42:15	218.107.192.67(10.10.1.93;10.10.1.4)	发现120.42.99.154(福建厦门)非法下载www.safedog.cn//WEB-INF/jboss-web.xml.bak，已被安全狗成功阻止	中危
XSS注入攻击 (持续攻击16次)	2016-07-05 12:42:15	218.107.192.67(10.10.1.93;10.10.1.4)	发现120.42.99.154(福建厦门)利用XSS跨站漏洞攻击www.safedog.cn/?search=<script>alert(1)</script>，拦截原因: 防... 复制	中危
WEB应用漏洞攻击 (持续攻击60次)	2016-07-05 12:41:09	218.107.192.67(10.10.1.93;10.10.1.4)	发现120.42.99.154(福建厦门)利用WEB应用漏洞攻击www.safedog.cn/cgi-bin/php5-cgi?-d allow_url_include=on -d safe_mode... 复制	中危

联动防御策略


安全狗·服云
概况
安全管理
威胁分析
安全策略
云监控
告警设置
DEMO
专业版
攻击分析
所有攻击事件分析
定向攻击事件分析
攻击源分析
被入侵主机分析
最近30天定向攻击概览
定向攻击事件71个，无高级攻击事件
定向攻击事件趋势
12
10
16/06/19
16/06/23
16/06/27
16/07/01
16/07/05
定向攻击事件
定向渗透攻击-联动防护策略设置
联动策略：已开启
联动规则：近6小时持续攻击 2 次以上则自动下发至客户端IP黑名单库
应用软件：服务器安全狗 网站安全狗
确定
1
2
选择日期：
批量加入IP黑名单库
管理IP黑名单库
联动策略设置： 定向渗透攻击设置 定向web扫描设置 持续暴力破解设置
攻击者IP
搜索
定向攻击类型
最近攻击时间
被攻击应用/IP
攻击者IP
高级攻击特征
操作
定向web扫描
2016-07-05 12:41:09
218.107.192.67 (10.10.1.93;10.10.1.4)
120.42.99.154
最近1小时该攻击IP针对您的网站频繁的进行WEB应用漏洞攻击等深度漏洞扫描，扫描次数达80，扫描类型3种，这意味专业黑客正在定点探测您的网站详情
加入黑名单库
定向黑名单模板

THANKS

ISC 2016 中国互联网安全大会 | 360互联网安全中心

安全狗