



2017 | JSRC安全乌托邦 大数据与威胁情报

北京·奥林匹克公园·水立方3号门2层

2017年7月29日

用安全情报实现威胁检测和响应的闭环

杨大路
天际友盟 CEO

安全情报的范畴

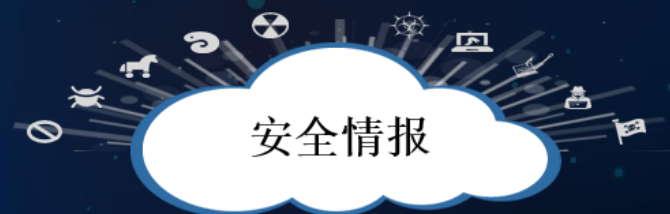
安全情报

- 资产情报
- 威胁情报
- 安全措施情报
- 安全需求情报
- 漏洞情报
- 事件情报
- 业务战略情报

安全情报的作用

I (Intelligence)

安全情报的生产、应用、消费



技术研究、平台产品、API接口、知识共享

E (Ecosystem)

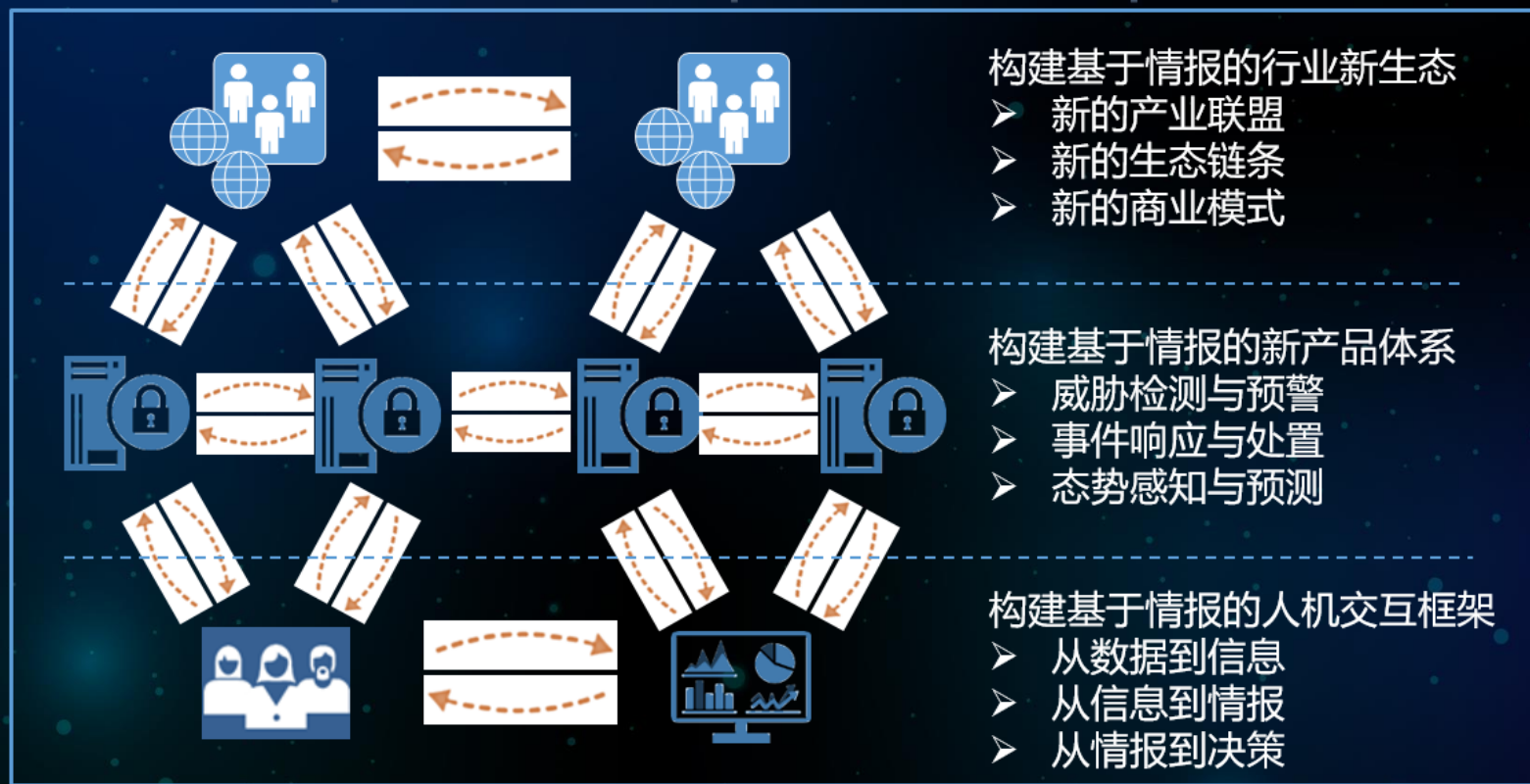
厂商间的行业生态联动

D&A (Data&Ability)

产品间的数据与能力联动

K (Knowledge)

人机间的知识联动



发现接入网有大面积异常活动

分析预警



（原创）2017-05-28 烽火台情报联盟 天际联盟情报站

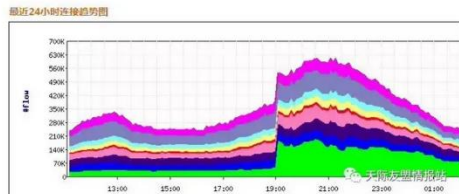
烽火台威胁情报联盟于2017年5月26日19点开始，监测到一次大面积网络攻击活动。本次活动呈现的最明显特点是参与攻击的源地址覆盖度超级广泛，几乎在全国所有省市运营商的骨干网络上均有明显活动。因其罕见的广泛参与性，我们将本次攻击活动命名为：RainbowDay。通过联盟成员Panabit公司的调查，其攻击源覆盖的大多数IP都位于不同运营商上，且攻击源IP地址与Panabit设备覆盖的实时在线IP地址数量呈1:5左右。

1、RainbowDay攻击活动行为

本次攻击活动类型属于UDP连接数和带宽消耗型DDoS攻击；

第一阶段，于5月26日19点全国大量真实IP地址开始攻击地址183.60.111.150，一直持续到28日凌晨3点结束；

第二阶段，于5月28日早晨7点左右开始攻击地址59.153.75.7，至目前仍在继续。



| 序号 | 目标IP | 连接数 | 上行流量 | 下行流量 | 序号 |
|----|----------------|--------|--------|--------|----|
| 1 | 202.96.69.38 | 266130 | 9.66M | 29.76M | 1 |
| 2 | 183.60.111.150 | 211805 | 37.1M | 0 | 2 |
| 3 | 202.96.64.68 | 65642 | 3.99M | 0.09M | 3 |
| 4 | 8.8.8.250 | 31476 | 16.02M | | 4 |

受害证实

超大规模网络攻击时代已来！途隆云遭受650G DDoS攻击

2017-05-29 达闼安全公告 [查看详情](#)

图1 2016年5月25日的降雨

降雨量在12:00至14:00之间达到峰值，约为6500。降雨量在14:00至16:00之间显著下降，约为1500。降雨量在16:00至18:00之间再次上升，约为3500。

| 国家 | 线路条数 | 里程公里 |
|----|------|------|
| 日本 | 284 | 2000 |
| 韩国 | 365 | 2000 |
| 台湾 | 212 | 2000 |
| 香港 | 212 | 2000 |

调查取证

“暗黑流量”超大规模DDoS溯源分析

原创 2017-06-09 云鼎实验室 云鼎实验室

6月9日调查报告

报道例：目前攻击呈现出三个阶段：

1. 5月28日19时美国大屠杀纪念馆地址开始攻击IP地址163.60.111.190，一直持续到凌晨28日凌晨3点结束；
2. 5月28日早晨7点左右开始攻击地址58.153.75.7；
3. 6月9日攻击呈现多样化。

经过对攻击源机器进行分析，腾讯云云鼎实验室工程师在机器中发现暗云虫的变种（暂时命名为暗云IV），通过对流量、内存DUMP数据等内容进行分析，基本确定本次超大规模ddos发出由“暗云”黑客团伙发起。

二、详细分析

我们在对目标机器排查中,发现了MBR中可疑rootkit,在对MBR内容进行分析,我们发现肉鸡机器的MBR与带云 MBR 中InfectedMBR 与 original MBR的相对位置相同,而且病毒均存储在 3,6,3 的60个扇区中。

应急响应

国家互联网应急中心开通暗云木马感染数据免费查询服务

来源: CNCERT 时间: 2017-06-13

2017年6月9日开始，一款名为“暗云”的木马在互联网大范围传播。“暗云”木马具有隐蔽性强、潜伏危害大、传播范围广泛等特点。6月9日至今，国家互联网应急中心监测发现境内有180余万台电脑感染了此木马。为此，国家互联网应急中心首次开通了“暗云”木马感染数据免费查询服务：<http://www.cn-cert.org.cn/interior/index.html>。自即日起接受公众咨询。如果您有意见或建议，欢迎通过电话 010-82959393 或邮箱 cn-cert@cn-cert.org.cn 向国家互联网应急中心反馈。

说明：1. “随云”木马只能感染Windows桌面系统，请您在Windows电脑浏览器中打开查询页面进行查询，地址：
<http://d.cert.org.cn>。

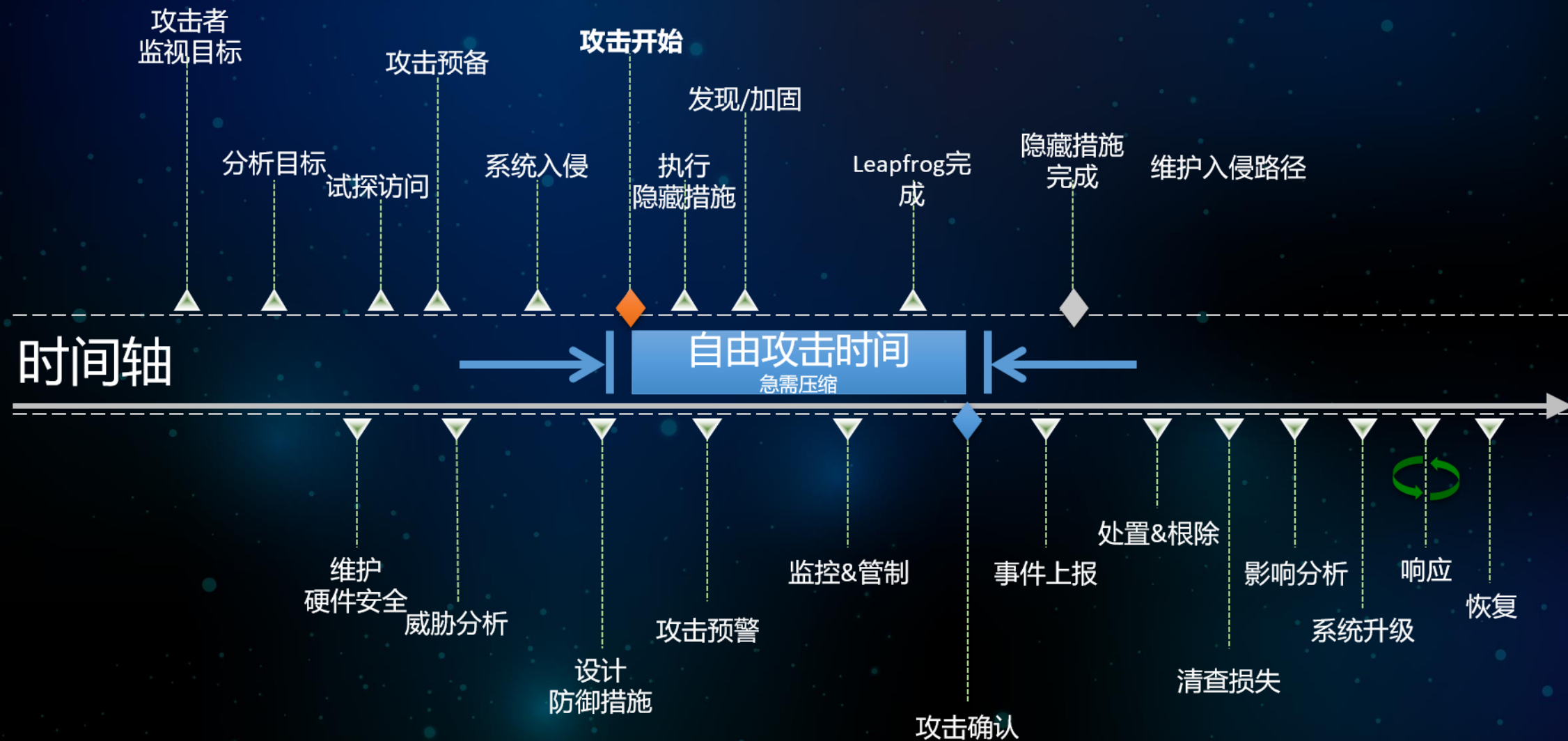
2.如果您使用宽带拨号上网或手机上网,由于IP地址经常变化,会导致查询结果不准确,仅供参考。

攻击、检测&响应的现状



攻击技术飞跃，传统检测&响应手段低效

以缩短“自由攻击时间”为目标



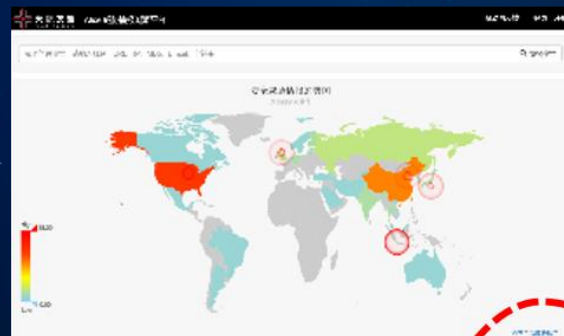
安全情报在检测&响应环节的价值



安全情报辅助网络异常检测

自己的情报
开源的情报
商业的情报

多源整合



威胁情报
信誉Feed
检测规则

API自动获取



用户网络镜像流量

单点登录查询

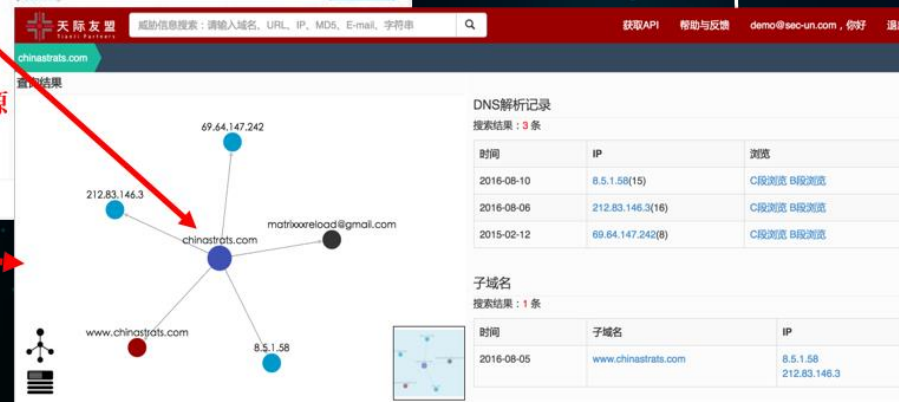
发现异常

黑域名

| 首次发现时间 | 最后发现时间 | IP | 域名/域名/分类 | 域名类型 | 域名IP | 关联IP数量 | 域名IP数量 | 域名IP数量 | 操作 |
|---------------------|---------------------|--------------|----------------------|------|--------------|--------|--------|--------|------|
| 2016-08-24 16:20:02 | 2016-08-24 17:17:06 | 212.83.146.3 | chinastrats.com / 未知 | 未知 | 212.83.146.3 | 4 | 222 | 222 | 查看详情 |
| 2016-08-24 16:20:02 | 2016-08-24 17:17:06 | 212.83.146.3 | chinastrats.com / 未知 | 未知 | 212.83.146.3 | 4 | 222 | 222 | 查看详情 |
| 2016-08-24 16:20:02 | 2016-08-24 17:17:06 | 212.83.146.3 | chinastrats.com / 未知 | 未知 | 212.83.146.3 | 4 | 222 | 222 | 查看详情 |
| 2016-08-24 16:20:02 | 2016-08-24 17:17:06 | 212.83.146.3 | chinastrats.com / 未知 | 未知 | 212.83.146.3 | 4 | 222 | 222 | 查看详情 |
| 2016-08-24 16:20:02 | 2016-08-24 17:17:06 | 212.83.146.3 | chinastrats.com / 未知 | 未知 | 212.83.146.3 | 4 | 222 | 222 | 查看详情 |

点击溯源

结果返回



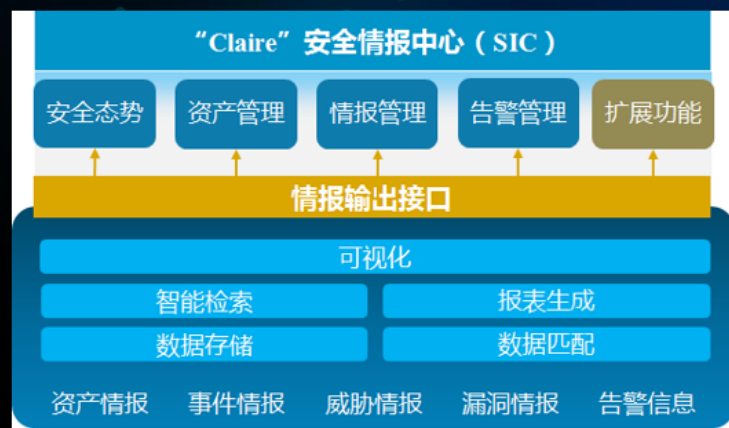
关联情报
关联IOCs

API自动获取

安全情报驱动资产漏洞管理闭环



外部漏洞情报
分发至本地



情报输出

安全漏洞

模块联动

“Helena” 资产与
漏洞管理模块

外网资产监控

- 外网漏洞扫描
- 用户域名监控
- 社交媒体监控

内网资产发现

- 操作系统
- 应用软件
- 通用组件
- 网络设备



漏洞扫描&验证

- 漏洞扫描
- POC/EXP智能调用
- 自动化漏洞验证

漏洞扫描&验证

- 资产漏洞情报推送
- 漏洞修复建议
- 辅助安全决策

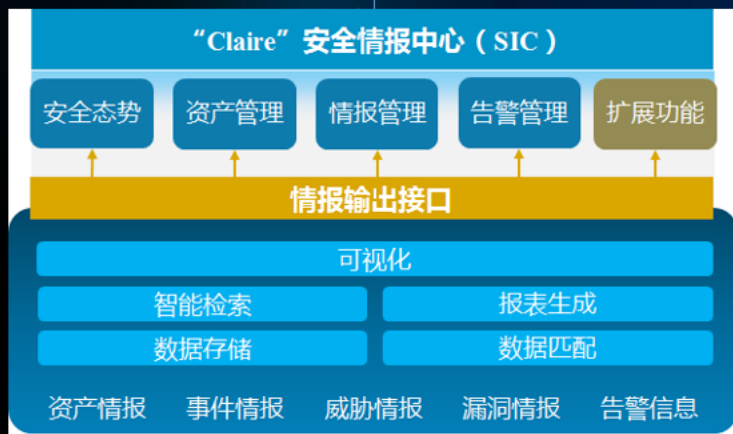
安全情报驱动检测&响应闭环



外部情报
分发至本地

Step2: 情报预警平台对转发的数据进行比对、展现

- 远控域名、ip
- APT
- 僵尸、钓鱼、勒索软件



Step1: 预警网关将被动监听数据
传送给SIC

- IP通信日志
- URL访问记录
- DNS请求日志
- Mail邮件访问

Step3:

- 检测结果进行呈现——失陷主机、严重级别、攻击类型
- 下发策略进行流量过滤



过滤后流量

情报预警网关

原始流量

通过数据管理提升安全情报质量



同源去重：将同一来源不同事件的情报数据进行去重汇总，合并威胁分类与影响范围标签。



去伪降噪：对数据进行验证，去除错误、失效、无效的数据信息。



老化处理：持续监控情报数据，去除信誉值低于输出阈值的数据条目。



多源去重：根据用户订阅需求，按标签筛选对应的情报数据，对结果进行多源聚合，合并情报来源、威胁分类与影响范围标签。



情报封装：基于STIX国际标准进行情报的封装打包。

安全情报提升主动防御能力

每月/季度/
年度品牌事
件汇总报告

钓鱼网站、
仿冒App、冒名
社交媒体帐号

客户授权

事件建立

通报客户初步
分析结果

- IP地址
- 主机所在国家
- 网络服务商
- 域名注册商
- 预计关停时间

调查取证、综合分析，根据攻击类型向以下单位申诉渠道关停，并像客
户汇报事件进展和可用风控信息

综合分析可能发现：

- 深度取证
- 风险IP地址
- 假饵反钓
- 潜在受害客户
- 钓鱼攻击工具包
- 仿冒App 恶意功能
- 社交帐号粉丝交互

站点管理员

网络主机

域名注册商

网络提供商

所属国家CERT

App Store管理员

社交媒体平台管
理员

品牌保护事件解决成功

通报客户关停结果

- 关停成功
- 关停时长

安全情报驱动产业生态协作案例



烽火台安全威胁情报联盟
FengHuoTai CTI Alliance



天际友盟
TianJi Partners



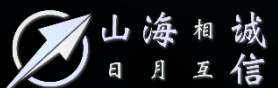
神州网云
SZWY



观星
Data Star Observatory



Panabit®



山海相诚信
日月互信



互信互通
HU XIN HU TONG



cirrus gate 思睿嘉得



WebRAY



云盾科技
CLOUDYSECURITY



ipip .net



SPINFO
世平信息



Watcher LAB

➤ 联盟情况

国内首个威胁情报联盟，2015年10月成立，12家成员企业。

➤ 联盟宗旨

以安全威胁情报为核心，打造平等互惠的新生态圈模式，共谋共策，推进威胁情报的标准制定及应用推广。

➤ 合作理念

“联合”、“共享”与“共赢”。

➤ 合作模式

技术合作：关键基础设施共建，对内情报信息共享，对外产品联动协同。

服务合作：服务支持体系共建，服务人员集中培训，服务内容统一管理。

市场合作：解决方案整体打包，市场推广互通协作，客户资源信息共享。

THANK YOU !