



基于移动威胁情报的安全价值观

马志远

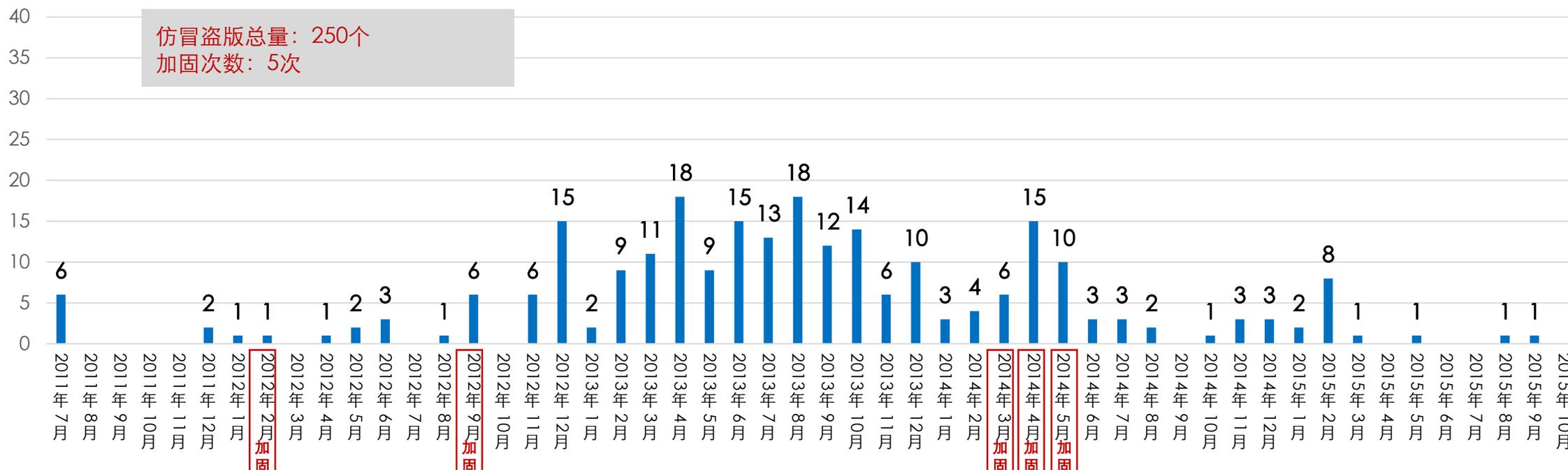
AVK 移动安全·安天

- 各种信息不对称和 “盲” 人摸 “象”
- 基于威胁情报的数据组织和驱动方式
- AVL Insight移动威胁情报的源体系
- AVL Insight移动威胁情报的工程实践
- Talk is Cheap , Show Me !

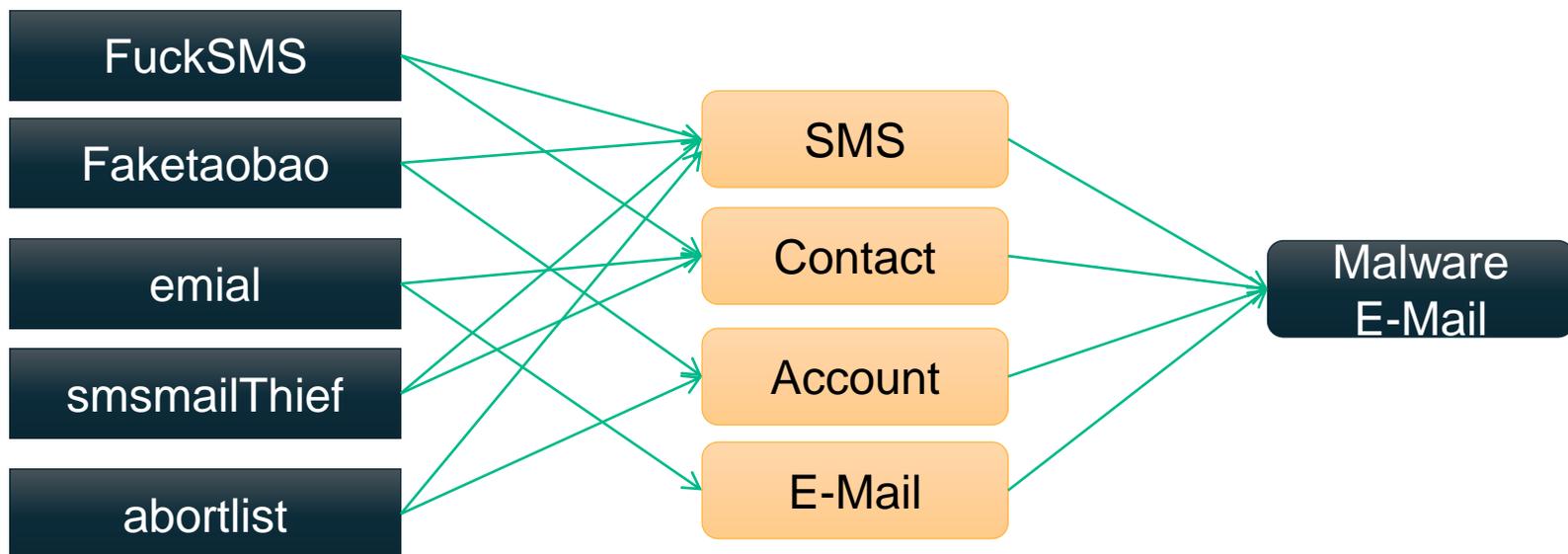


盲人摸象——企业使用安全技术与实际安全威胁的不对称

某游戏应用仿冒盗版样本数量变化趋势



不对称——企业的安全认知与用户威胁场景下的不平衡



[Redacted]

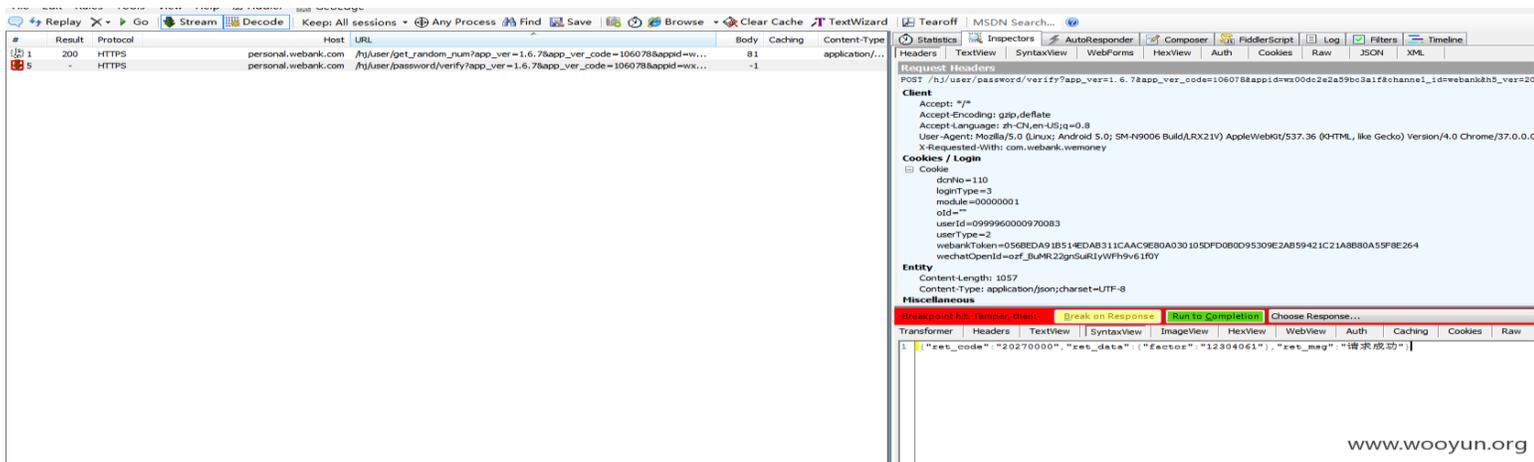
LV2 绸袍神族 发表于 2015-8-20 17:10 | 只看该作者

3947

1.MonkeyTest此木马是8.19升级后，用系统查杀出，但无法删除。后用安装360查杀，查出无法删除。2.机型及版本 [Redacted] 将系统root但此机型目前可root的软件。4自带杀毒软件杀不掉，接入计算机安装360报警仍然杀不掉。平时安装APP均是 [Redacted] 更新系统提示更新。6.均是以前安装的系统，前几次升级系统未检测出病毒，出现这种情况应该是最近的版本。7手机上软件商店目前只有 [Redacted]。



不对称——企业的业务发展与企业的安全意识的平衡





不对称——安全诉求和威胁与实际的安全能力的不平衡

移动应用被攻击方式

伪装/钓鱼

界面劫持

钓鱼应用

隐藏图标

重打包

信息窃取

短信监听/拦截

截屏

ID窃取

环境录音

其他攻击

进程注入

条款欺诈

输入法劫持

逻辑漏洞



不对称——安全诉求和威胁与实际的安全能力的不平衡

信息不对称

安全技术

应用安全

安全认知

环境安全

安全能力

用户需求

安全意识

业务发展

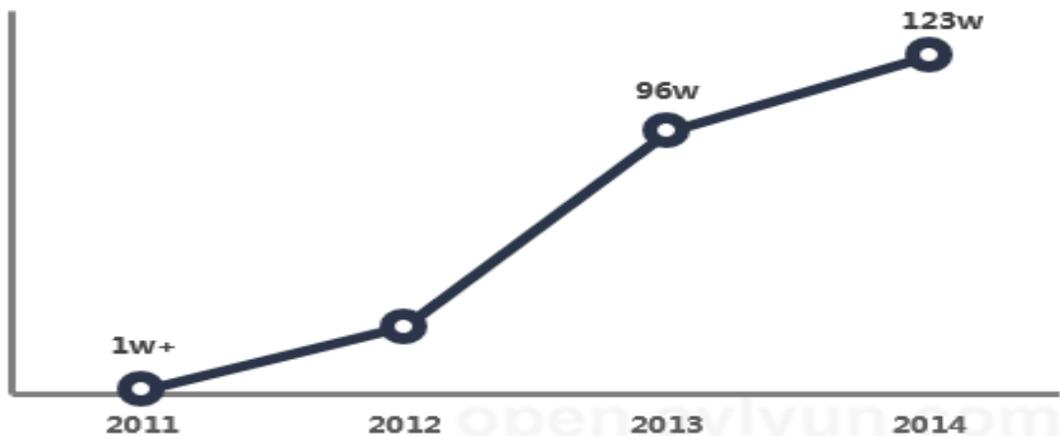
感知能力

业务能力

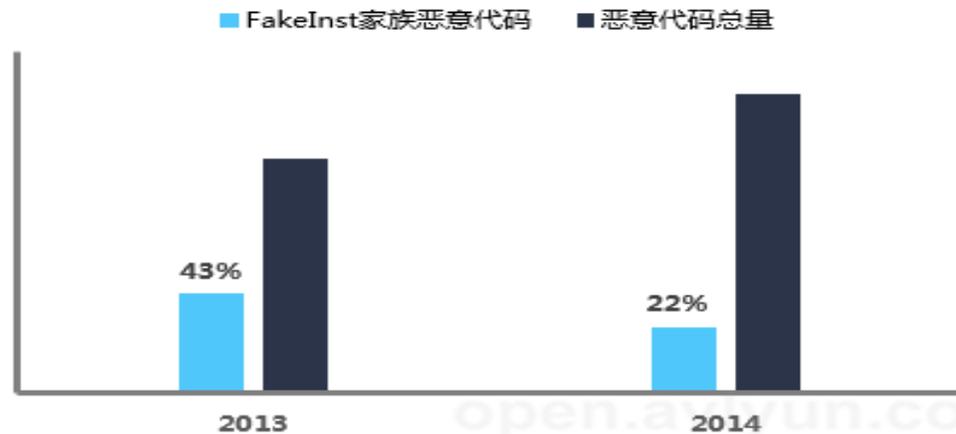


数据不等于情报，有价值的信息也不等于情报

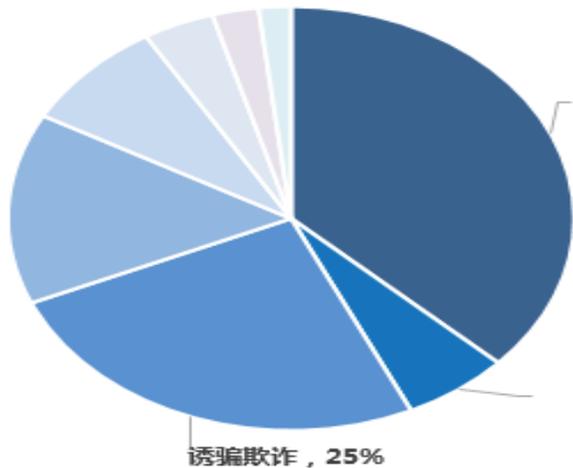
Android恶意代码数量变化情况



FakeInst家族恶意代码占总量比例情况



2013年恶意代码类型分布

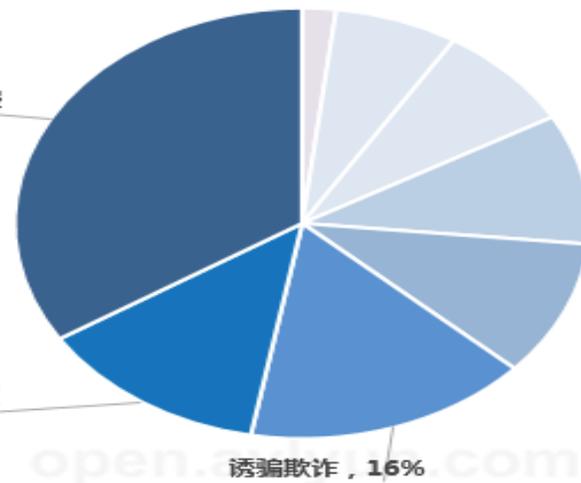


2014年恶意代码类型分布

34%，恶意扣费

13%，隐私窃取

隐私窃取行为大幅增加。



CONTENT

1 · 2014 年网络安全	3.2 “飞客” 蠕虫监测情况 84
1.1 我国互联网网络安全	3.3 恶意程序传播活动监测 86
1.2 数据导读	3.4 通报成员单位报送情况 88
2 · 网络安全专题	4 · 移动互联网恶意程序传播和活动情况 96
2.1 移动互联网恶意程序	4.1 移动互联网恶意程序监测情况 96
2.2 分布式反射型拒绝服务	4.2 移动互联网恶意程序传播活动监测 98
2.3 智能硬件蠕虫威胁互连	4.3 通报成员单位报送情况 100
2.4 短信拦截黑客地下产	5 · 网站安全监测情况 112
2.5 12306 泄密事件剖析	5.1 网页篡改情况 112
2.6 工业控制网络安全分	5.2 网页挂马情况 121
3 · 计算机恶意程序	5.3 网页仿冒情况 124
3.1 木马和僵尸网络监测	5.4 网站后门情况 130
	6 · 安全漏洞预警与处置 136
	6.1 CNVD 漏洞收录情况 136
	6.2 高危漏洞典型案例 139
	6.3 CNVD 行业漏洞库 146
	6.4 CNVD 漏洞处置情况 150

数量

- 恶意代码，家族，变种，TOP
- 平台类型，Hash规模

行为

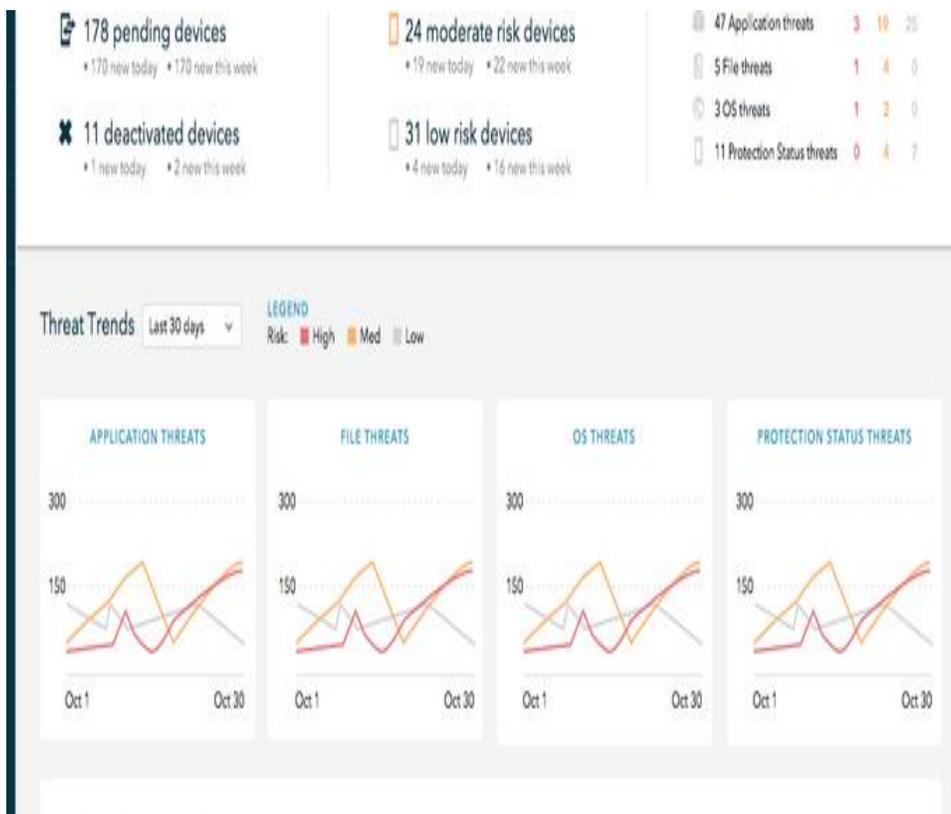
- 类型
- 攻击行为
- 行为模式和特征

渠道

- 应用
- 传播方式



数据组织的方式——“设备&资产视角”



设备

- 激活，越狱
- 设备管理，访问控制

威胁

- 威胁类型
- 威胁程度
- 响应和解决

策略

- 分组&控制
- 管理&策略下发



漏洞

- 业务接口暴露
- 关键数据泄露

风险/脆弱点

- 自身编码
- 第三方SDK引入
- 权限过多开放

仿冒&分发安全

- 仿冒/山寨应用
- 分发渠道



数据组织的方式——尝试用情报的描述结构的拆解





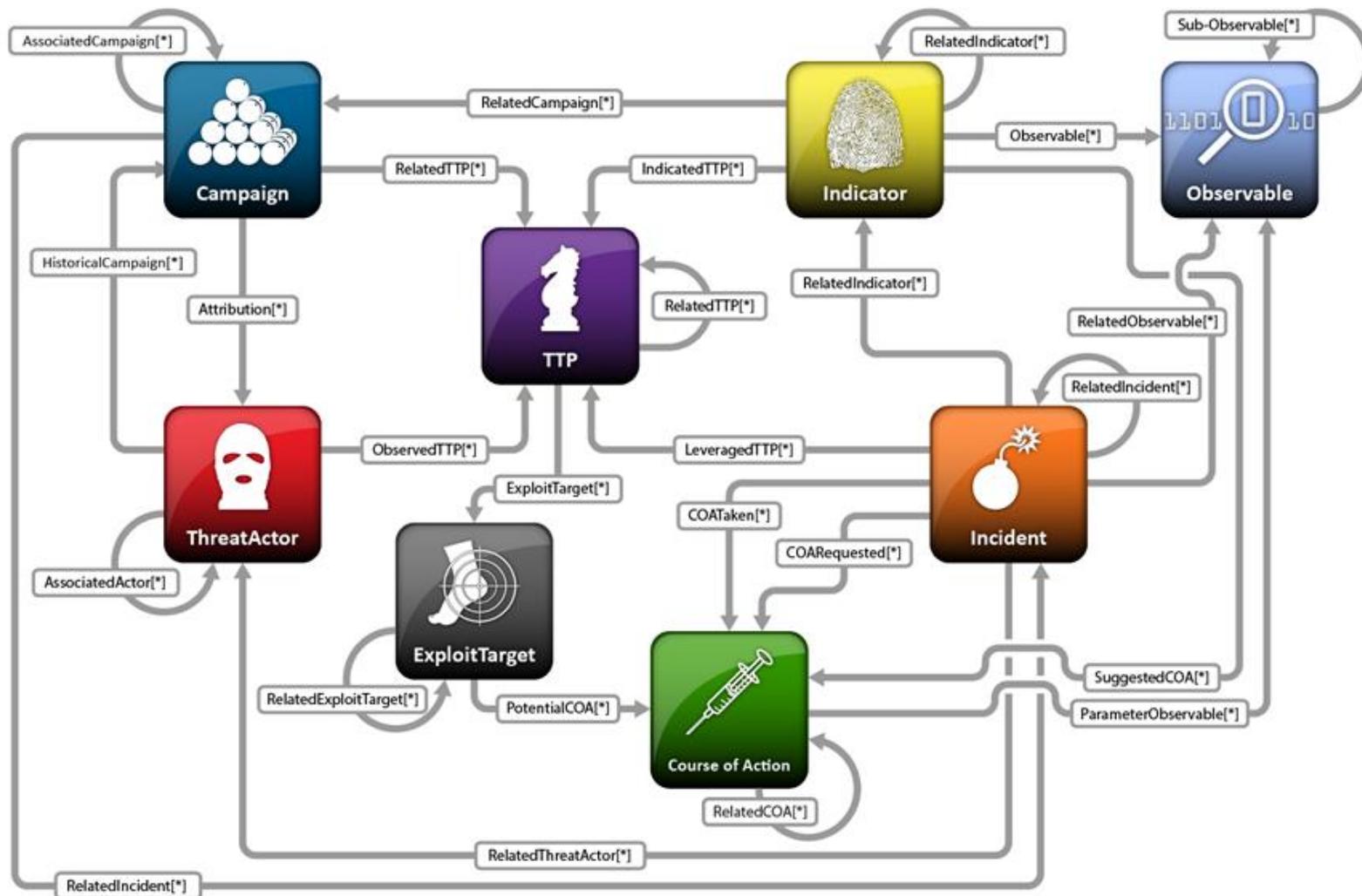
我们认为的威胁情报的价值观——情报不是从石头里面蹦出来的

相关的概念体系	出现的背景
Threat/Risk/Exposure/Asset.....	西方的IT管理和标准化的背景
DREAD,STRIDE,PASTA, Attack Tree.....	微软和相关安全厂商所推出的风险管理模型
CAPEC,CWE,CVE,CVRF , MAEC , NVD.....	对攻击模式, 脆弱点, 漏洞等各种基础的安全元素的标定和描述结构
Threat Modeling	各种威胁建模的方法论, 工具, risk-centric, data-driven等等
Kill Chain,钻石分析,TTP.....	面向Cyber和更高强度的攻击和对抗的场景的分析工具和分析方法
CybOX,TAXII , OpenIOC.....	面向Cyber和信息交换的描述和标准体系
STIX	面向更完整的综合性的情报分析/作业/交换的体系

强烈的外在和内在的面向威胁的知识管理体系/方法



我们认为的威胁情报的价值观——情报是高度具备驱动力的数据流转和响应驱动体系



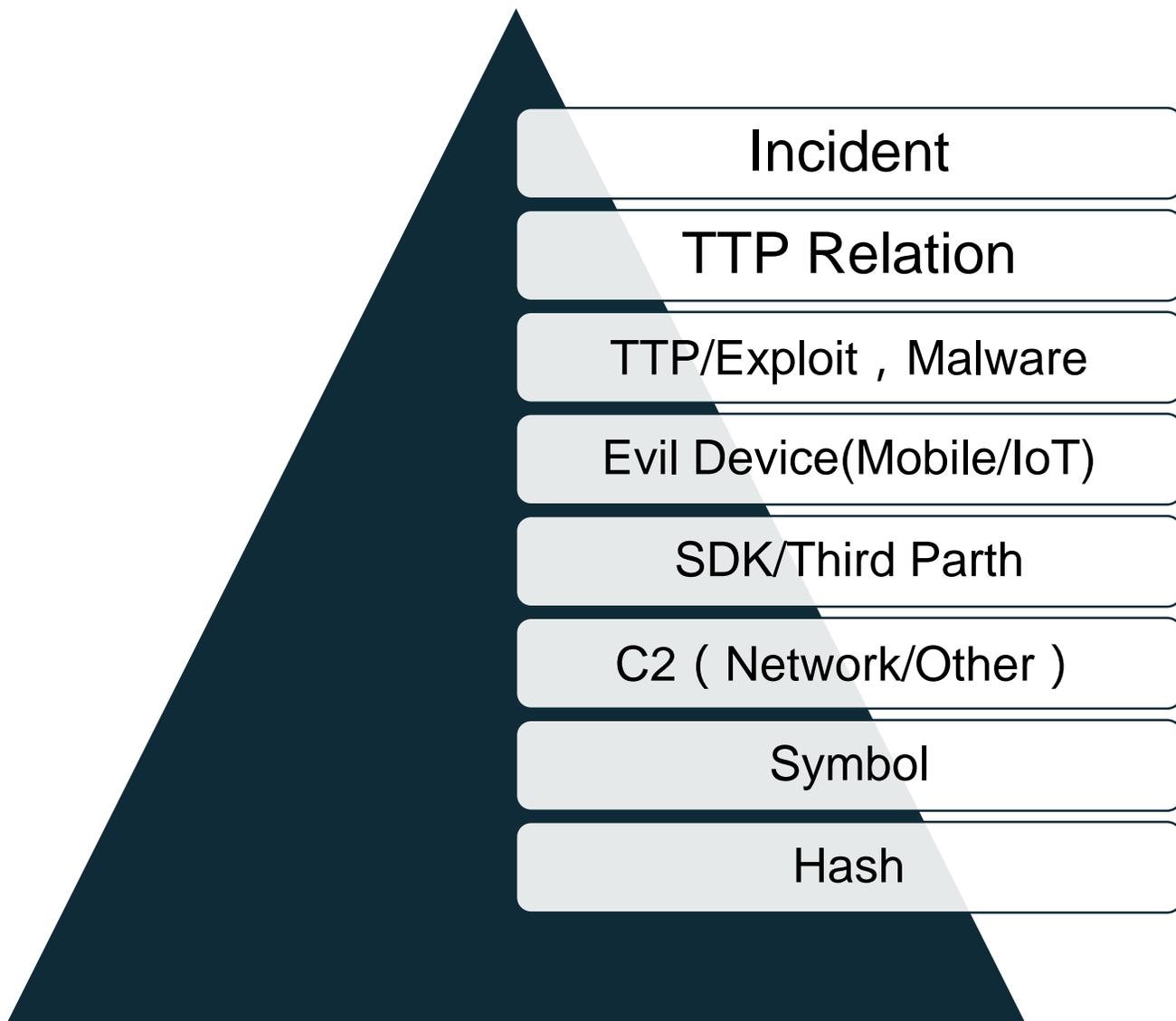


情报的认识和移动威胁情报的差异性

- 情报的认识
 - 数据（线索），有价值数据不等于情报
 - 情报是有驱动力的有价值数据
- 移动威胁情报和Cyber威胁情报的差异性
 - 具备更强的实效性
 - 关联的关系复杂度在规模上更大
 - 情报的数据和信息的构成多样化



移动威胁情报的困难度金字塔



隐晦

复杂

高对抗

穿透

不可控

方式多样性

符号多样性

繁琐，低效



面向移动威胁的情报作业实践

感知&发现

- Incident
- Asset , Impact , Victim

分析&呈现

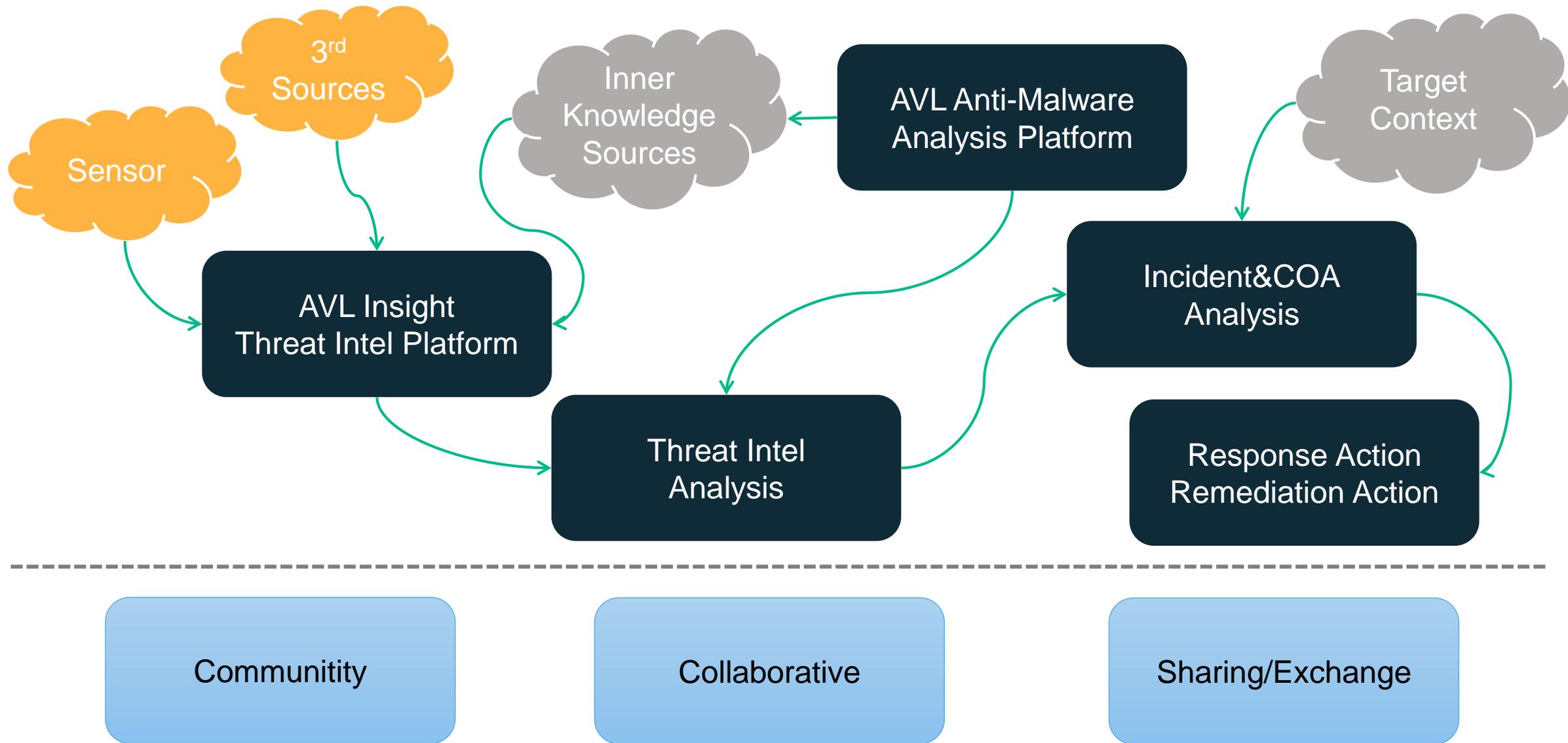
- TTP+
- Malware/Exploit/AttackPatterns
- Technique Details
- ThreatActor/Targets

决策&响应

- COA



面向移动威胁的情报作业实践





面向移动威胁的情报作业实践——数据源体系

面向威胁作业



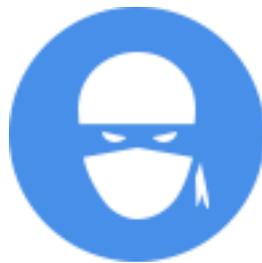
TTP+情报



威胁关联关系

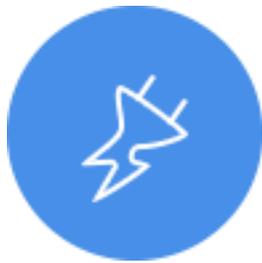


受害源/Victim



攻击源*/ThreatActor

面向元数据



引擎探头



样本库



网络探头



风险库*/Exploit+Vuln

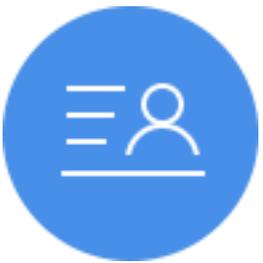
面向基础数据



应用商店监控



技术新闻情报

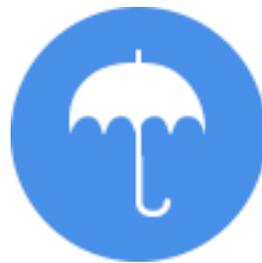


Whois

面向威胁量化和响应



威胁事件*/Incident



响应形成*/COA

基于情报和威胁分析的去不平衡



引擎终端探头

样本库

感知



TTP+情报

样本库

分析



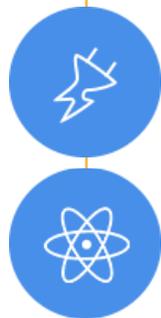
威胁事件*/Incident

响应形成*/COA

决策

• 某银行APP一个月监控数据

- 非正版下载量：2499
- 非正版下载源：223



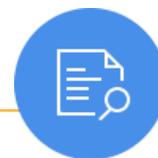
- 恶意代码变种：3
- 恶意代码总量：6
- 广告件总类：4
- 广告件数量：24
- 支付件：0
- 用户环境中存在恶意代码变种：405
- 用户环境存在恶意代码数量：5014
- 用户环境中存在风险应用：253264



- 应用商店：25
- 网盘：4
- 未知：5



- 用户环境存在大量安全问题
- 安全问题与业务关联
- 少量应用被篡改



- 开发者场景
 - 威胁
 - 风险
- 企业场景
 - 办公场景
 - IT场景

感知

- 威胁
- 风险

最好有个企业内的实例

分析

- 度量
- 趋势

响应

- 策略
- 监控



下面进入演示环节

- 下面进入演（ zhuang ）示（ bi ）环节

THANKS!

AV 移动安全·安天

YOU CAN TRY IT

微信扫一扫

下载手机安全防护软件

AVL Pro



微信扫一扫

体验安天企业级安全防护

