网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

内部资料

安天2018网络威胁年报发布

安天副总工程师　李柏松

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

报告主要内容


安天
2018 网络安全威胁的回顾与展望
Antiy Annual Security Report
初稿完成时间：2018年12月20日 17时20分
首次发布时间：2019年01月08日 10 时00分
本版更新时间：2019年01月08日 10 时00分
安天安全研究与应急处理中心

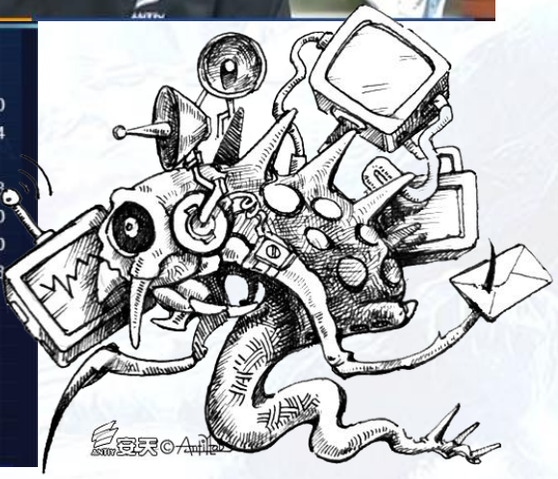

APT
威胁泛化
漏洞响应
供应链安全
勒索挖矿
数据泄露

01 APT

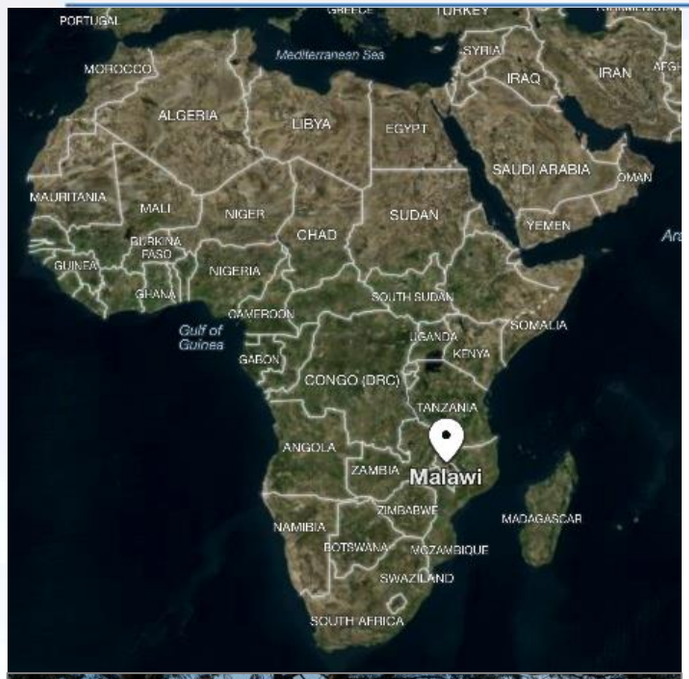
地缘政治和国家利益竞合是APT攻击的主要源动力

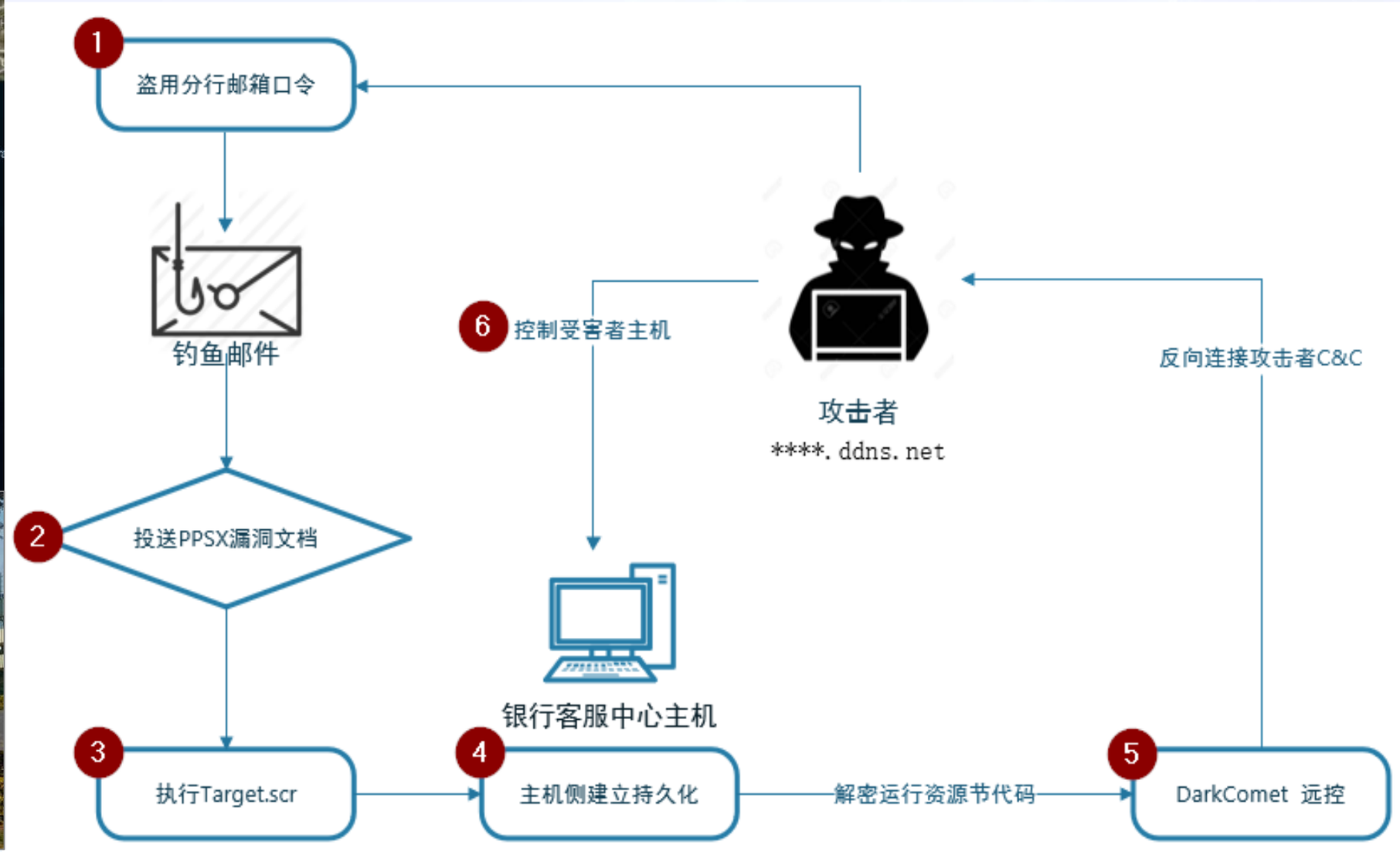
曝光APT事件的威慑作用正在下降

网空威胁行为体地缘政治背景明显



第三世界国家信息基础设施更易受到网络攻击挑战



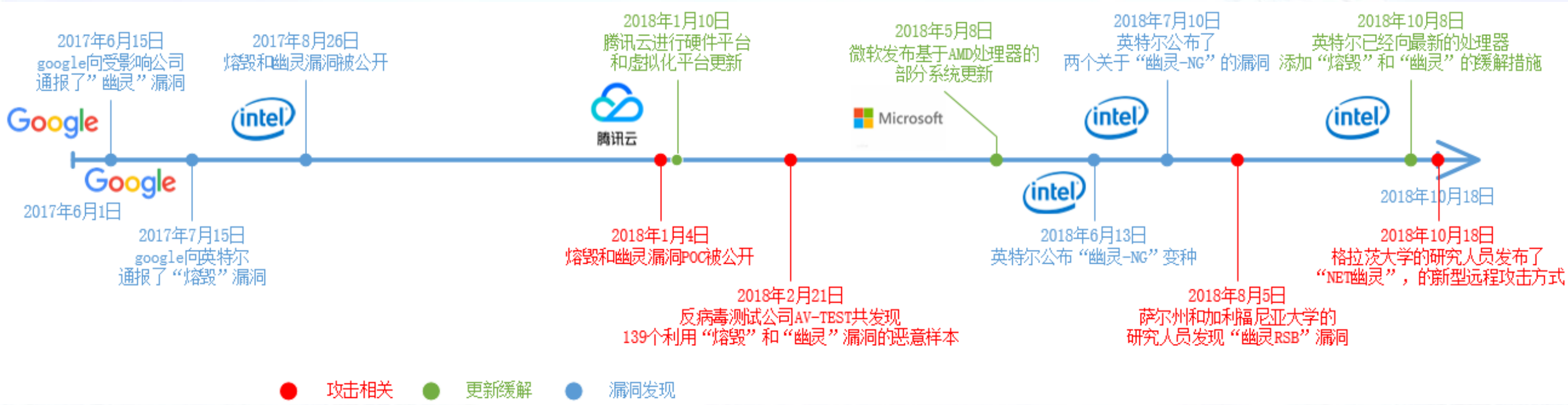


02 漏洞响应

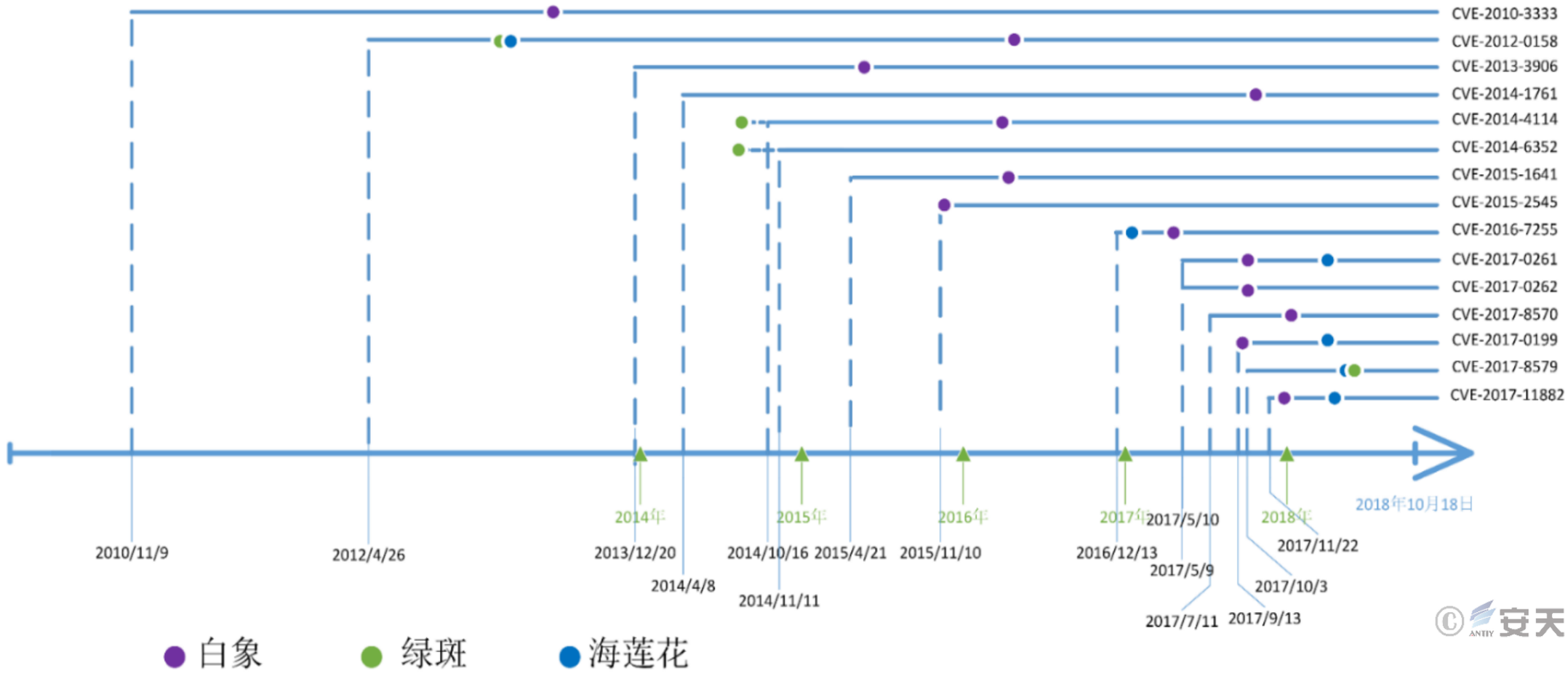
以敌情想定为前提更好地支撑漏洞响应与处置

漏洞处置需深入分析脆弱性敞口与攻击窗口之间关系

长达6个月的攻击窗口期



已知漏洞在APT攻击中依然大量存在



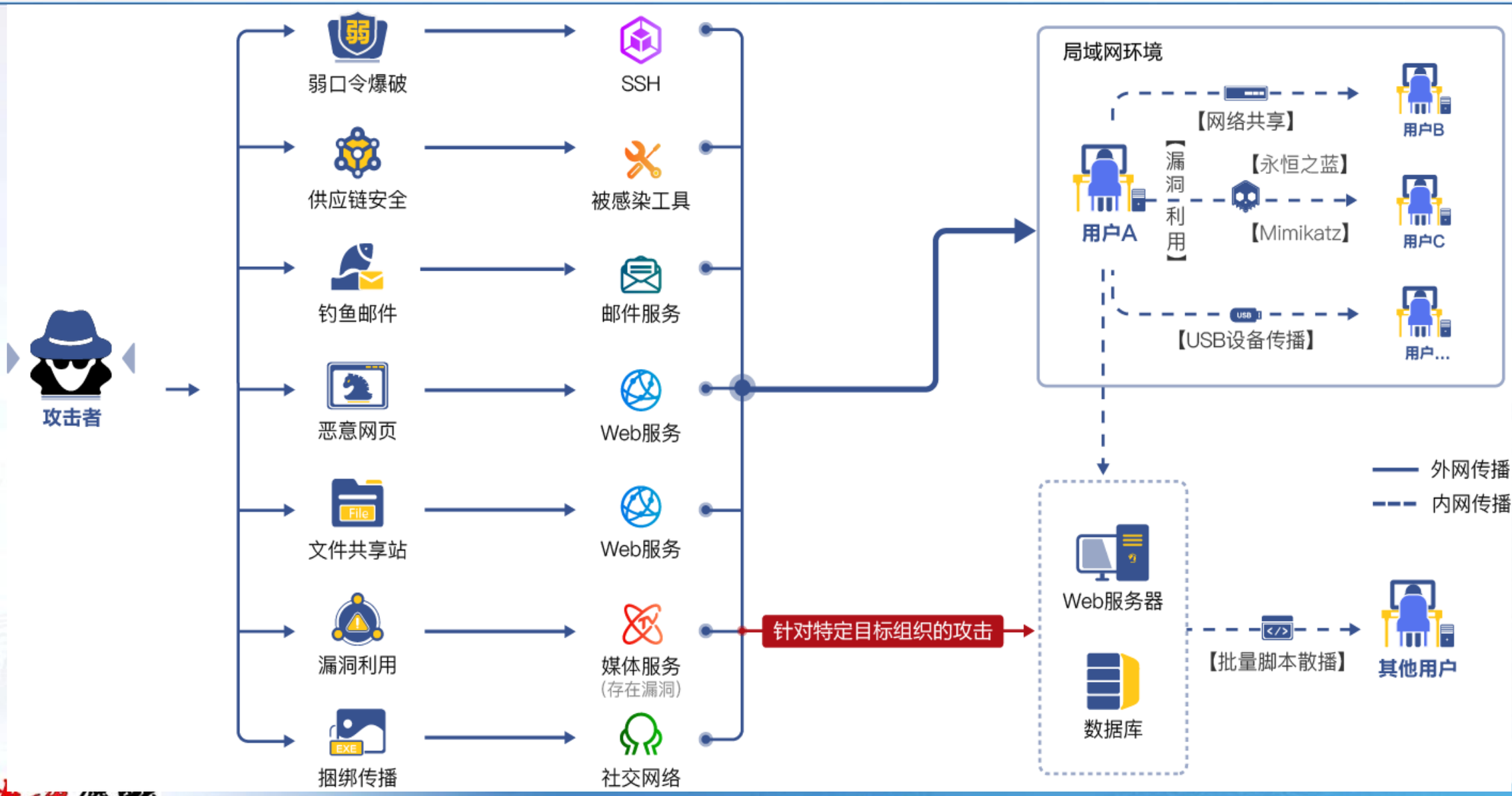
注：图中三个圆点是白象、绿斑和海莲花对漏洞的首次使用时点；

03 勒索、挖矿

缺乏有效安全防御已成为终端安全最大隐患

挖矿木马成为2018年感染量最多的恶意代码

缺乏有效安全防御已成为终端安全最大隐患



04 其他.....

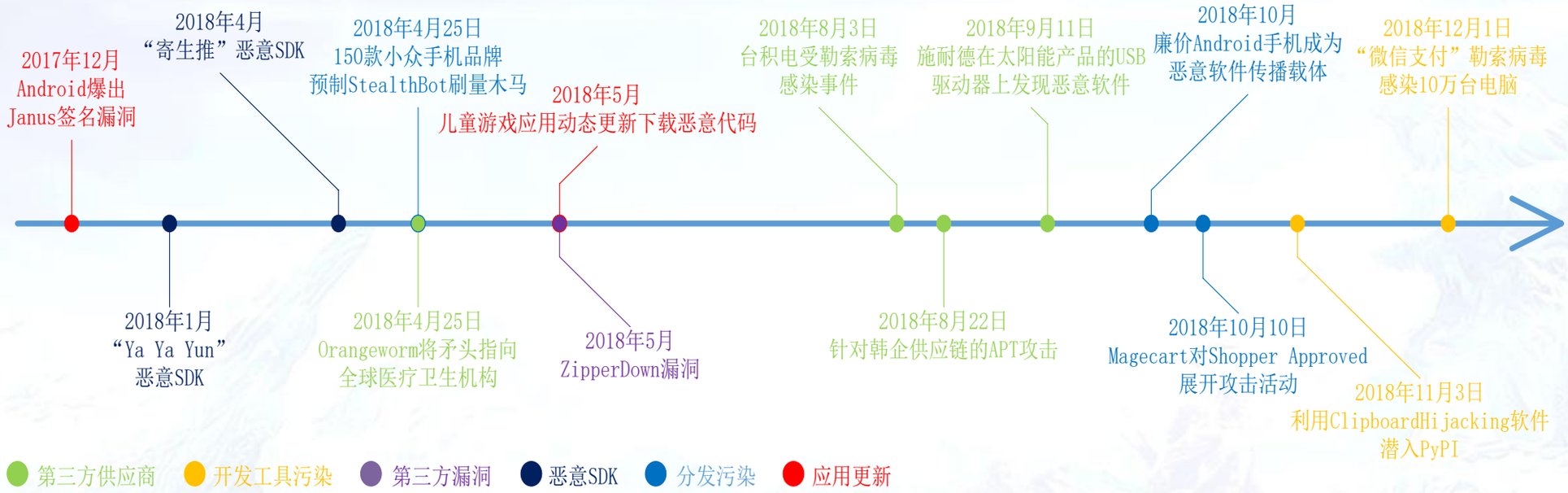
数据泄露、供应链安全、威胁泛化

数据泄露使用户画像更加精准，隐私保护面临多方面难题

印度公民信息数据库Aadhaar	1月	11亿
英国顶级律师事务所		120万
珠宝电商公司MBM Company	2月	130万
美国LocalBlox数据公司		4800万
社交网站Facebook	3月	1.2亿
在线旅行网站Orbitz		88万
美国体育运动装备品牌UnderArmour		1.5亿
约会应用程序Grindr		300万
老牌百货公司Hudson's Bay	4月	500万
美国连锁面包店Panera		3700万
俄罗斯视频监控公司Did iVideon	5月	82万
在线票务网站Ticketfly	6月	2700万
DNA检测公司MyHeritage		9200万
Sacramento Bee日报		1950万
英国电商Dixons Carphone		590万
弹幕视频网AcFun		800万
圆通快递		10亿
营销公司EXACTIS		3.4亿
第三方应用程序Nametests.com		1.2亿
应用程序Timehop	7月	2100万
SpyHuman间谍软件公司		4.4亿
顺丰快递		3亿
新加坡卫生部		150万
墨西哥	8月	200万
华住旗下连锁酒店		5亿
Apollo公司	9月	2亿
数据管理公司Veeam		4.45亿
技术公司AccuDoc	10月	265万
Google+		50万
国泰航空		940万
美通信公司Voxox	11月	2600万
美证券交易所American Express		70万
美国邮政		6000万
万豪酒店		5亿
国外知名问答社区Quora	12月	1亿
搜索服务器Elasticsearch		5700万
问答网站Quora		1亿
FBI等多国情报机构		2万

公共医疗机构 企业 生活服务类 互联网 政府

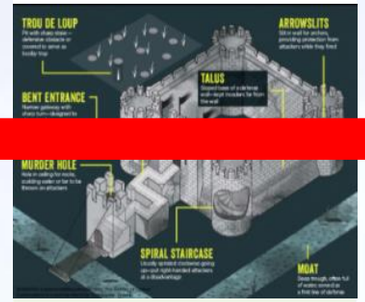
供应链环节成网络攻击中关键载体



- 软件供应链各个环节都可能成为攻击者突破口
- Android 软件供应链环节安全威胁呈上升趋势
- 第三方供应商成为软件供应链攻击中的焦点

2018网络安全威胁泛化与分布

以全面能力导向推动动态综合网络安全防御体系建设



基础结构安全
Architecture

纵深防御
Defense in Depth

态势感知与积极防御
SA & Active Defense

威胁情报
Intelligence

攻击与反制
Counter

叠加演进是安天从能力型安全厂商的公共安全模型滑动标尺演绎发展的一套模型，滑动标尺模型由SANS提出，由安天翻译引入国内，并与国内能力型厂商约定为公共安全模型，参见：《网络安全滑动标尺模型—从架构安全到超越威胁情报的叠加演进》中文译本，安天公益翻译组翻译。

在信息系统建成后，进行的外挂式防御已经不能满足需求，而是必须将网络规划为一个可防御网络，而可防御网络的前提是可管理网络。

要实现一个可管理网网络，就必须在系统全生命周期遵从“三同步”原则，即在

- 网络的规划设计阶段
- 建设实施阶段
- 运行维护阶段

都要考虑安全问题。

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰