安全的供应链和信息流视角的若干案例解读

安天 肖新光

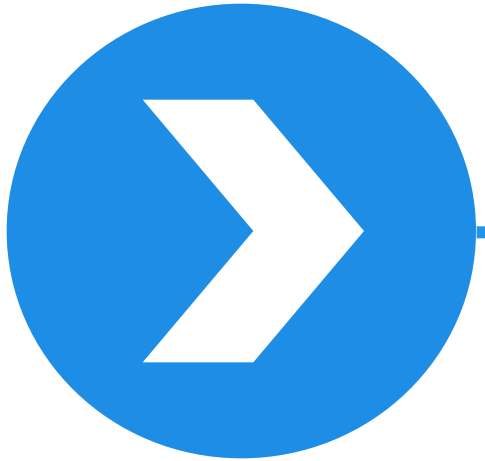
提纲

01 引子—IoT僵尸网络与威胁的泛化

02 供应链案例—环境、物流、工具

03 信息流案例——模式变化、运营商、第二信道

04 总结—防御的全域融合



引子

- IoT僵尸网络
- 威胁的泛化

为什么要在物联网安全会议上谈这个问题

A 物联网带来的安全威胁

- 提升网络攻击对实体空间数据的获取能力
- 增大网络攻击转化为实体空间后果的风险
- 为网络攻击提供更多可利用的节点和能力

B 当前国内网络的认知

- 以基础核心技术的短板为核心焦虑
- 以合规检查和单点环节对抗为主要手段
- 对系统的整体性、威胁的流动性和连接部的脆弱性考虑不足

引子：从IoT设备攻击北美DNS服务谈起

家族名称	变种数量	样本HASH数量
Trojan[DDoS]/Linux.Mirai	2	大于100
Trojan[DDoS]/Linux.Xarcen	5	大于1000
Trojan[DDoS]/Linux.Znaich	3	大于500
Trojan/Linux.PNScan	2	大于50
Trojan[Backdoor]/Linux.Mayday	11	大于1000
Trojan[DDoS]/Linux.DnsAmp	5	大于500
Trojan[Backdoor]/Linux.Ganiw	5	大于3000
Trojan[Backdoor]/Linux.Dofloo	5	大于2000
Trojan[Backdoor]/Linux.Gafgyt	28	大于8000
Trojan[Backdoor]/Linux.Tsunami	71	大于1000
Worm/Linux.Moose	1	大于10
Worm[Net]/Linux.Darlloz	3	大于10

安天所监控的当前国内主要IoT僵尸网络情况

作为一场DDoS事件，Dyn遭遇攻击停摆事件被严重夸大了，而大量IoT设备早已被木马感染这个事实反而被忽视了，这些设备并不只是攻击的工具和跳板，其就是社会的基础传感器和感知单元，最坏的事情，并不是其入侵后被用于DDoS其他节点，而是其被入侵这个事实本身。

图 4-1 物联网组成示意图

图及表格引自安天《**IOT僵尸网络严重威胁网络基础设施安全**》（2016.10.24）

安全威胁的两大走向

纵深

随**互联网+（信息化加速）**向**传统领域**延展

随**智能化**向**新型领域**延展

泛化

威胁泛化—2014

本图引自《安天实验室2014网络安全年报》© 安天

威胁泛化的加剧-2015

2015网络安全威胁泛化与分布

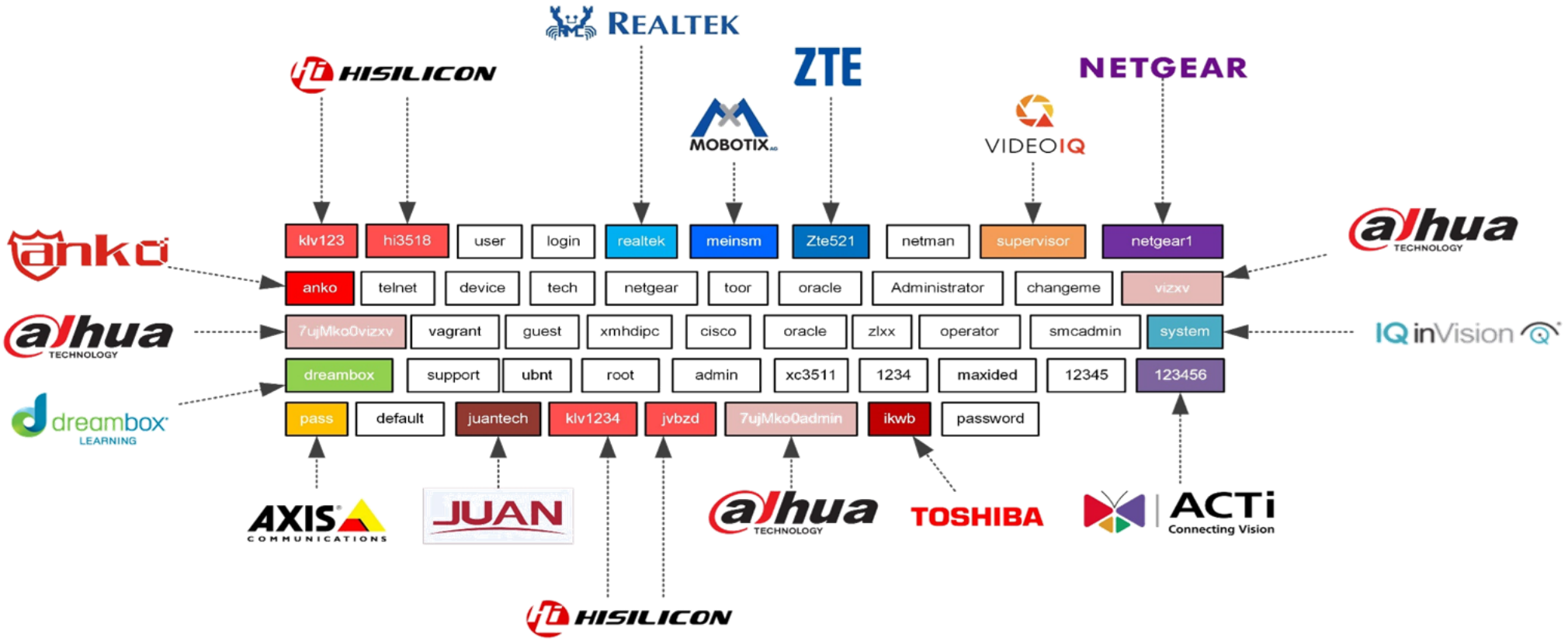
供应链视角的若干案例

- 从Mirai的密码破解档说起
- 地下供应链、工具链
- 战场预制

供应链带来弱点引入-方便性和安全性的矛盾

Mirai的破解密码档针对品牌的映射

2016年10月 安天实验室制图



而根据我们对国内摄像头行业的调研，其客服问题比例最高的为遗忘管理口令。彰显了安全和便利的矛盾。

“地下”供应链：仿冒、盗版、“第三方”汉化

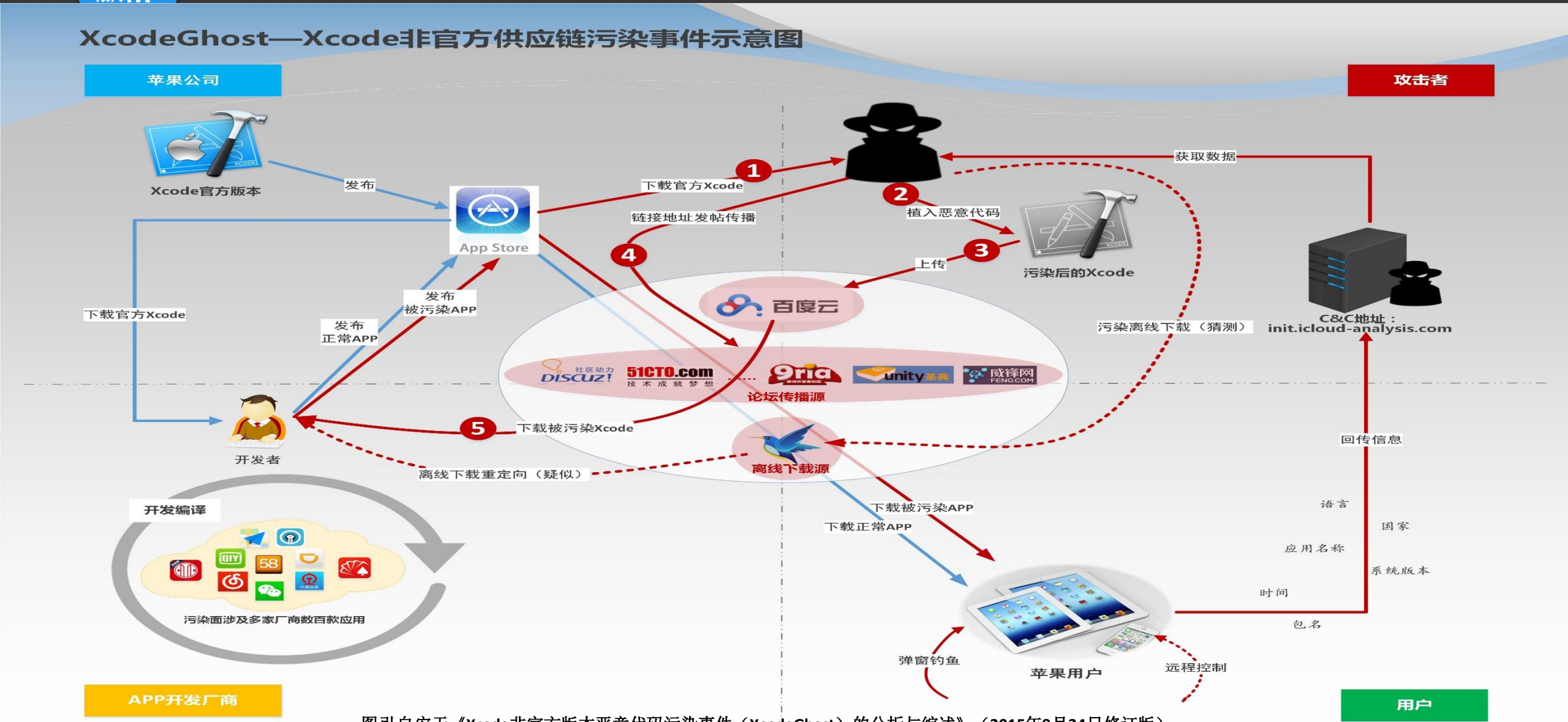
盗版操作系统 弱化安全能力与策略

装机与刷机 预制木马与广告件

注册机、破解器、第三方汉化的盈利模式

FakeAV

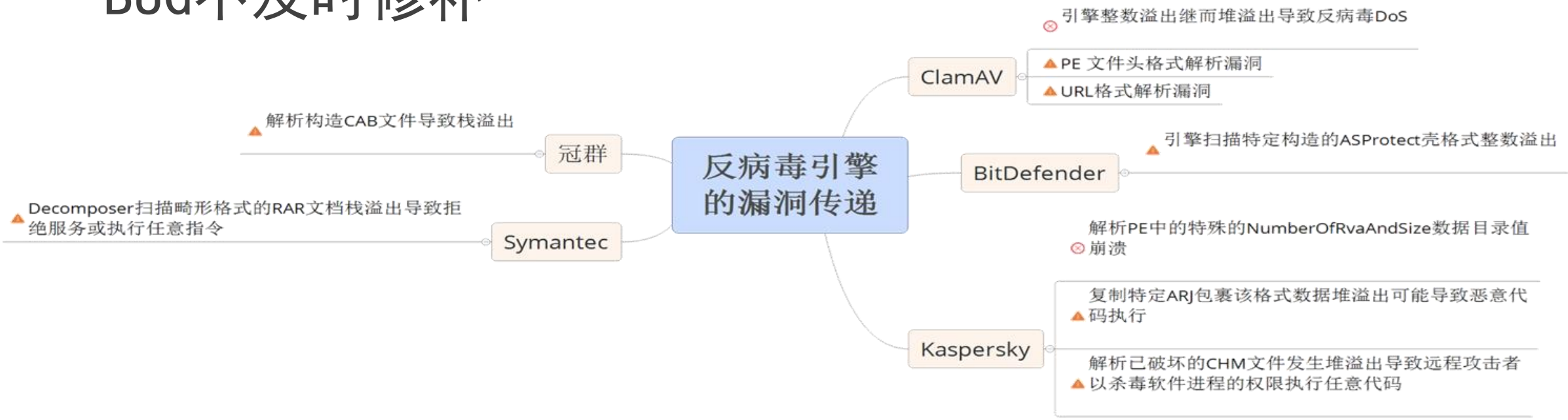
封闭体系更隐蔽的入口：工具链



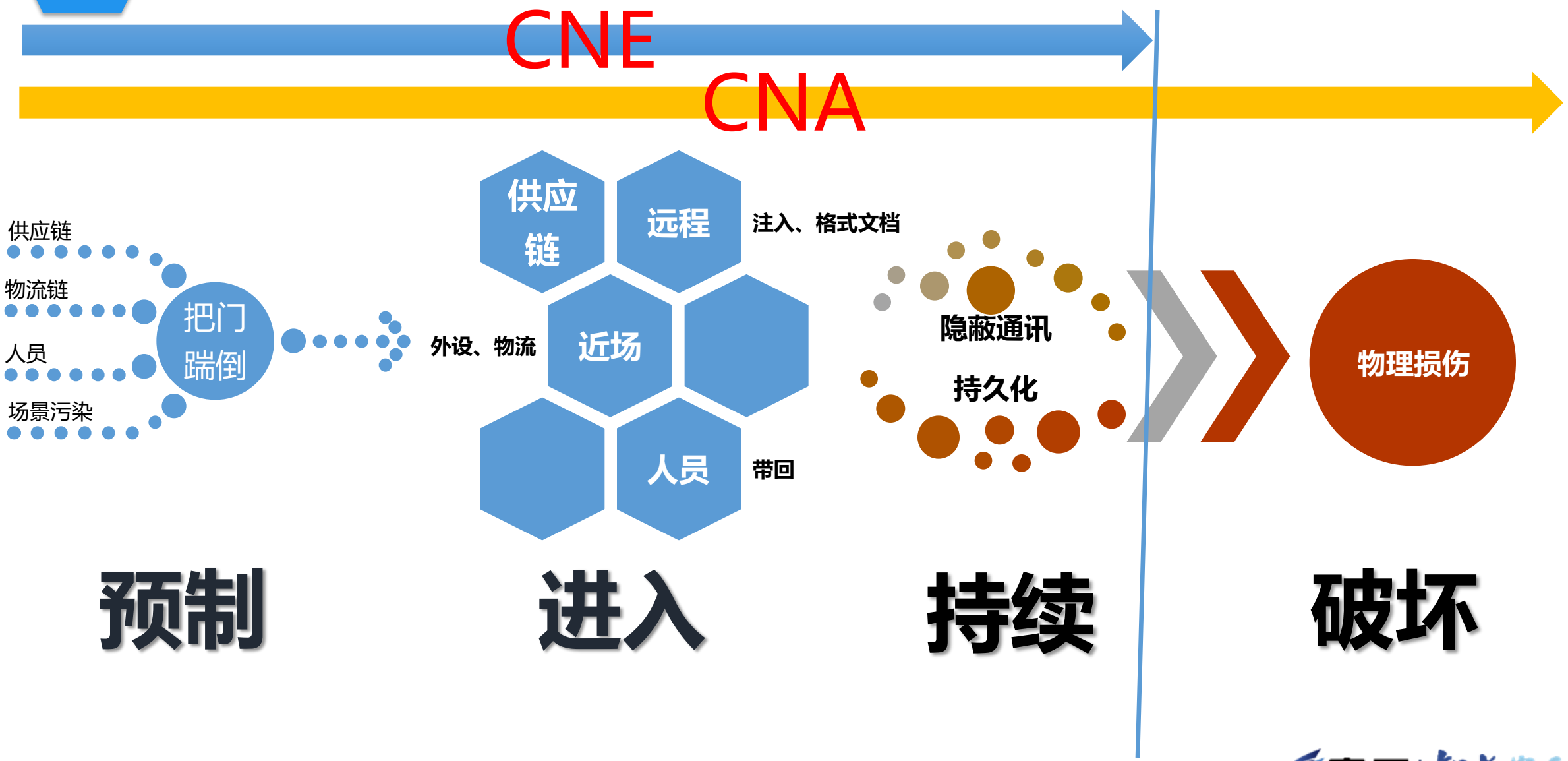
图引自安天《Xcode非官方版本恶意代码污染事件（XcodeGhost）的分析与综述》（2015年9月24日修订版）

供应链的非透明化在漏洞的传递后不能及时修补

- 基于开源的研发，自称“重头编写”，遇到漏洞时掩耳盗铃
- 使用第三方杀毒引擎，但因自称“自主研发”，导致BUG不及时修补



从信息战的角度来看



塑造战场：基础供应链的穿透

固件——攻击点、持久化与隐蔽入口

恶意代码事件	时间	目标设备	攻击原理
CIH病毒	1998	各种计算机主板	擦除主板板载存储器器中的BIOS，导致主板无法工作
震网蠕虫	2010	西门子 S7-300/ S7-400 PLC	PLC被下载恶意篡改的组态逻辑，引起被控设备工作异常，导致被控设备损毁
方程式	2015	10余种不同品牌、型号的硬盘：包括三星、西数、希捷、迈拓、东芝以及日立等	硬盘固件被篡改，恶意逻辑代码储存在硬盘的保留区。实现恶意程序的隐蔽驻留，实现对抗常规擦除和格式化的持久化能力
乌克兰电网事件	2015	串口-以太网转换网关	攻击者覆写了变电站的关键性设备（串口-以太网转换网关）固件。运维人员无法远程操作设备，需要以手动方式控制断路器，制造障碍延缓操作人员恢复电网工作
Mirai	2016	网络摄像机等IoT设备	利用设备固件出厂默认账号口令，登录并感染设备固件，发起DDoS攻击

物流与仓储：供应链安全上的 “脆弱连接部”

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

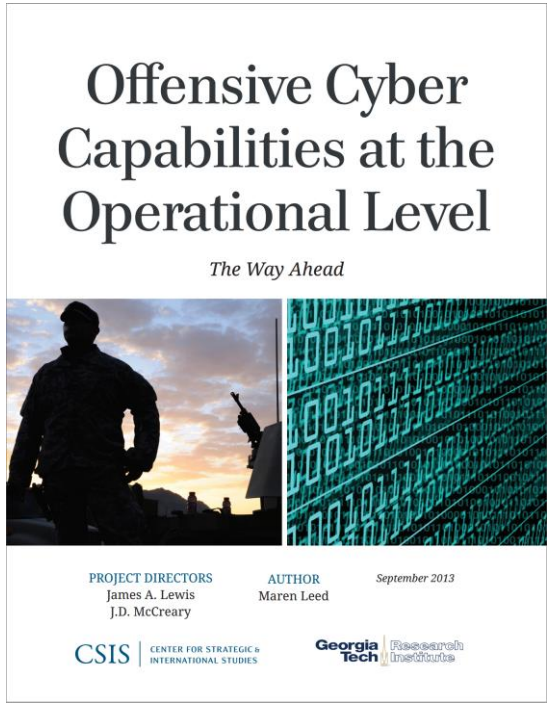
在物流链劫持，人员带入等方式实现把门踹倒的背景下，基于持久化节点的“横向移动”和，在这个场景下，隔离的内网因为没有成为最不安全的环节，对手一经植入则横扫全网。单点孤岛节点更有可能成为“最最”不安全的节点，因为其根本不受到有效的安全感知和持续性的安全保障。

深度污染：更深层次的供应链预制

供应链攻击的方法准备

网络武器具有无与伦比的多功能性，它们可用于从参与到高端作战的所有军事行动。因为它们的影响是可逆的，所以非常适合于作战的所有阶段，包括环境塑造、高烈度对抗以及目标重建。它们**可以在多个时间点发起攻击，包括针对早期开发过程。**

——《Offensive Cyber Capabilities at the Operational Level》



Maren Leed：美国国际战略研究中心（CSIS）国防政策研究的高级顾问

另一种供应链：商业军火引发的军备扩散

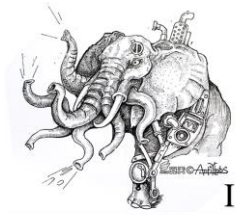
图引自安天报告《一例针对中国官方机构准APT攻击中的样本解析》2015.05.27

武器输送带来的格局影响

行动能力

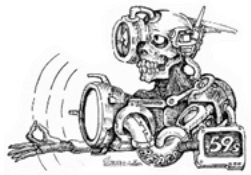
成本投入

初级的APT



2013.5
白象I代

商业军火支持的APT

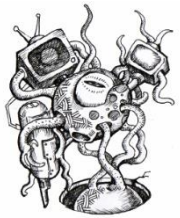


2015.5
APT-TOCS

常规的APT

2015.12
白象II代

A2PT



2007或2008
Duqu
毒曲

2009.6
Stuxnet
震网

2015.2
Equation
方程式

2010.3
Flame
火焰

信息流视角的若干案例

- 普通恶意代码的劫持、应用升级通道
- Camberdada计划，基于运营商持久化的收割
- 边信道与主动构筑第二信道

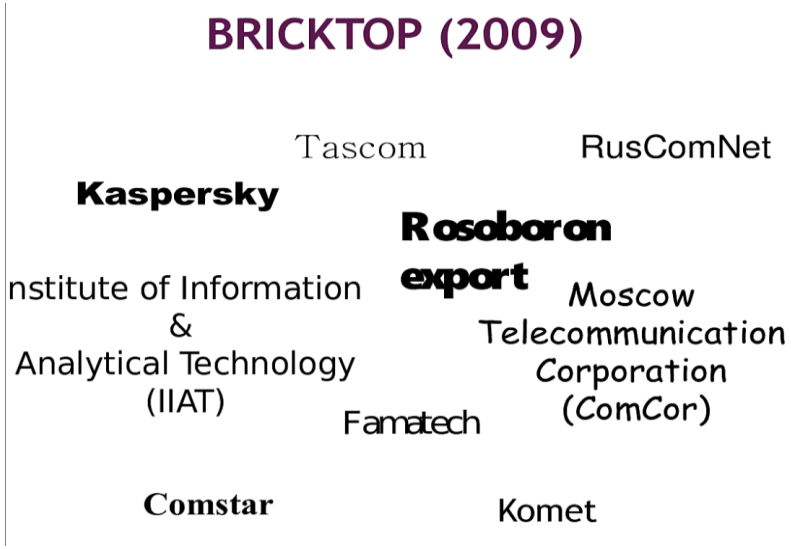
信息流带来新的攻击入口

美国安全厂商PaloAlto Networks 在对Infy的分析中，劫持相关伊朗攻击组织的C2C服务器，达成反控。

不验证的远程升级
有漏洞的签名验证机制

普通的恶意代码感染，同样可以被情报组织利用。软件、固件升级通道也是如此。

信息流-CamberDADA计划的的运营商视角



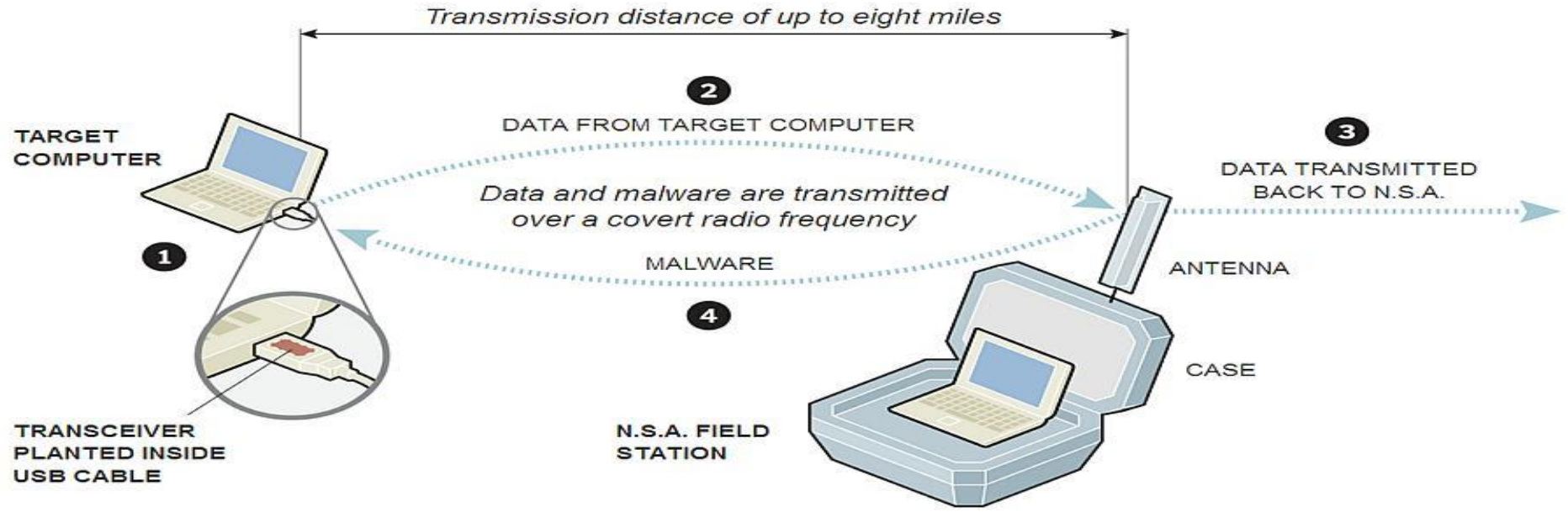
英文名称	说明
Rosoboron export	俄罗斯国防产品出口公司
Institute of Information & Analytical Technology	信息与分析技术研究所
Tascom	莫斯科城市电话公司
MOSCOW Telecommunication Corporation	莫斯科电信公司
Komet	俄罗斯电信公司
Comstar	俄罗斯电信运营商
RusComNet	俄罗斯电信运营商
Famatech	软件公司，其软件产品 Radmin 为远程控制软件

左图引自：《An Easy Win：Using SIGHT to Learn about New Viruses》,斯诺登泄露文档

边信道与主动构筑第二信道

How the N.S.A. Uses Radio Frequencies to Penetrate Computers

The N.S.A. and the Pentagon's Cyber Command have implanted nearly 100,000 "computer network exploits" around the world, but the hardest problem is getting inside machines isolated from outside communications.



1. Tiny transceivers are built into USB plugs and inserted into target computers. Small circuit boards may be placed in the computers themselves.

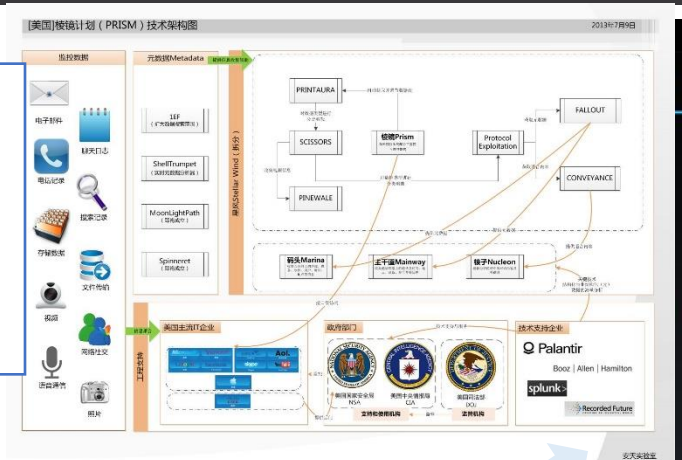
2. The transceivers communicate with a briefcase- size N.S.A. field station, or hidden relay station, up to eight miles away.

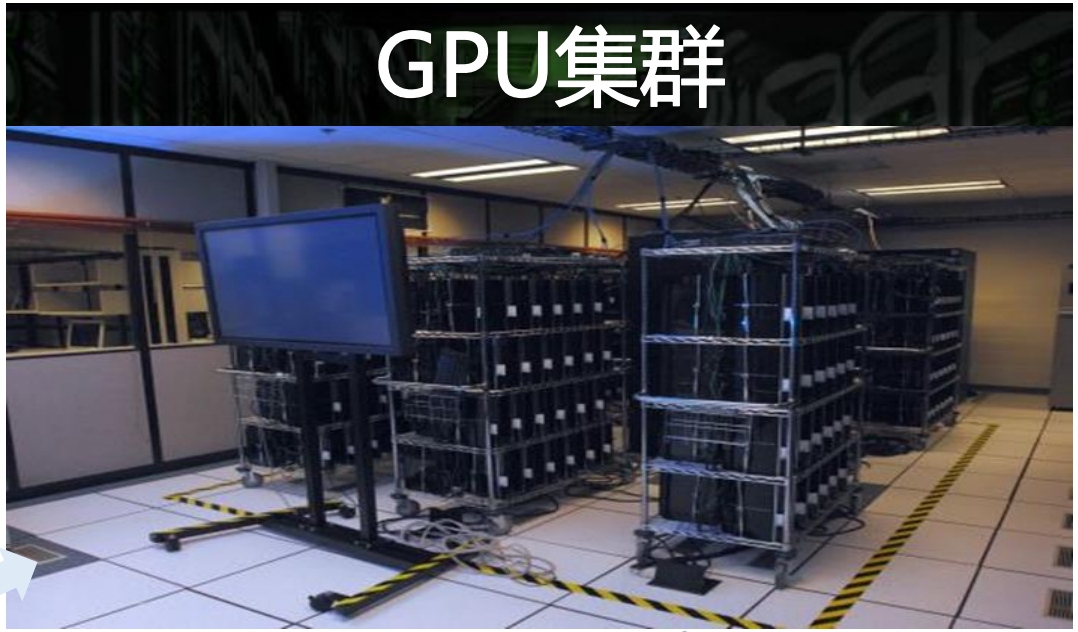
3. The field station communicates back to the N.S.A.'s Remote Operations Center.

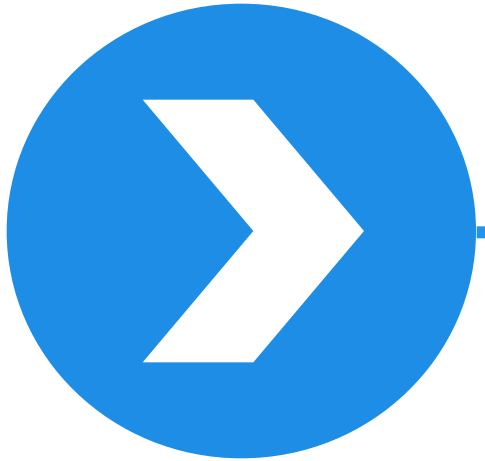
4. It can also transmit malware, including the kind used in attacks against Iran's nuclear facilities.

信息聚合改变游戏规则和大国平衡

从传统基于大量计算、存储、带宽资源的网络节点信息获取和破解，到互联网+棱镜模式，安全的大国博弈手段发生了重大变化。







总结

总结

安全开发过程	工具链与环境	物流配送
SDL和机制的引入 开发场景的安全	官方供应链 审核与检查 收敛IT环境	高安全环境需要增加物流与仓储的审查

运营商与信道	供应商	还有很多
VPN的使用 PKI的普及	供应商审查&稳定供应商名单 互联网厂商的去互联网化	

安天全域融合防御

能力体系

安全大数据 | 规则与信誉 | 知 识 | 威胁情报

感知：蜜罐捕获、引擎生态、终端捕获、流量感知、主动爬取、资源交换

分析：大数据分析、机器学习、自动分析、全向量提取、人工分析

部署：态势分析、引擎检测、边界阻断、补丁分发、异步分析、系统加固、流量还原、主动防御

响应：离线检查、综合通报、取证恢复、定点专杀、联动止损

服务：云端支持、产品升级、人工服务

厂商视角

解决方案

BYOD
智甲 智能设备版

个人用户
AVL SDK 反病毒引擎

能力生态
AVL SDK 反病毒引擎

追影威胁分析系统
探海威胁检测系统
镇关威胁阻断系统
捕风蜜罐系统
办公区
智甲终端防御系统
传统IT网络
智甲 服务器版
捕风蜜罐系统
服务器区

态势感知 通报预警
态势感知与通报预警平台
觅踪主机检查系统
用户响应团队

工控领域
智甲 专用节点防御版
捕风 工控版

公/私有云
智甲 虚拟化版
私有云
公有云
捕风 云端版

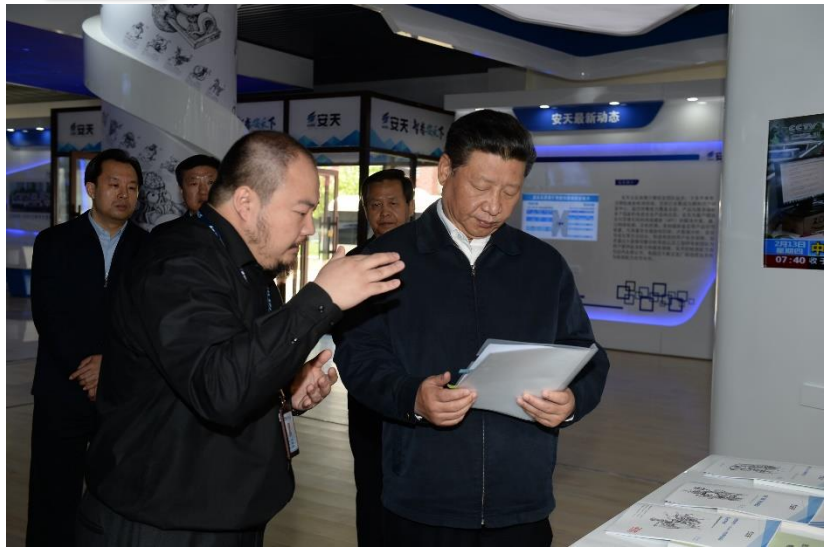
用户视角

威胁对抗

检测阻断 踩点接触
检测阻断 建立连接
主动防御 提升权限
分析发现 内部侦查
拦截呈现 横向移动
勘察处置 保持存在
拦截止损 秘密回传

对抗视角

不负重托 携手前行



5月25日，习近平总书记在黑龙江考察期间视察了安天哈尔滨总部，在听取汇报后对安天人说：“**你们也是国家队，虽然你们是民营企业。**”这是总书记视察的第一家网络安全企业。