多种网络环境下应急响应的探索

龚玉山　360企业安全集团观星实验室负责人

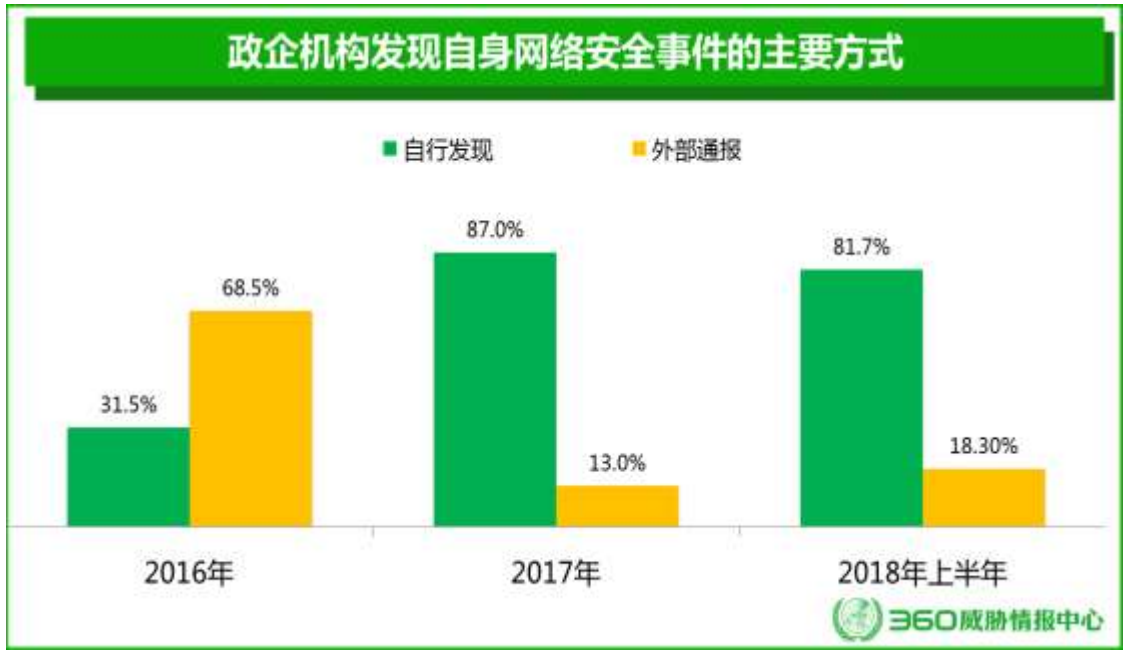
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018　Beijing · China
（原“中国互联网安全大会”）

目录 concents

01 2018年应急响应事件盘点

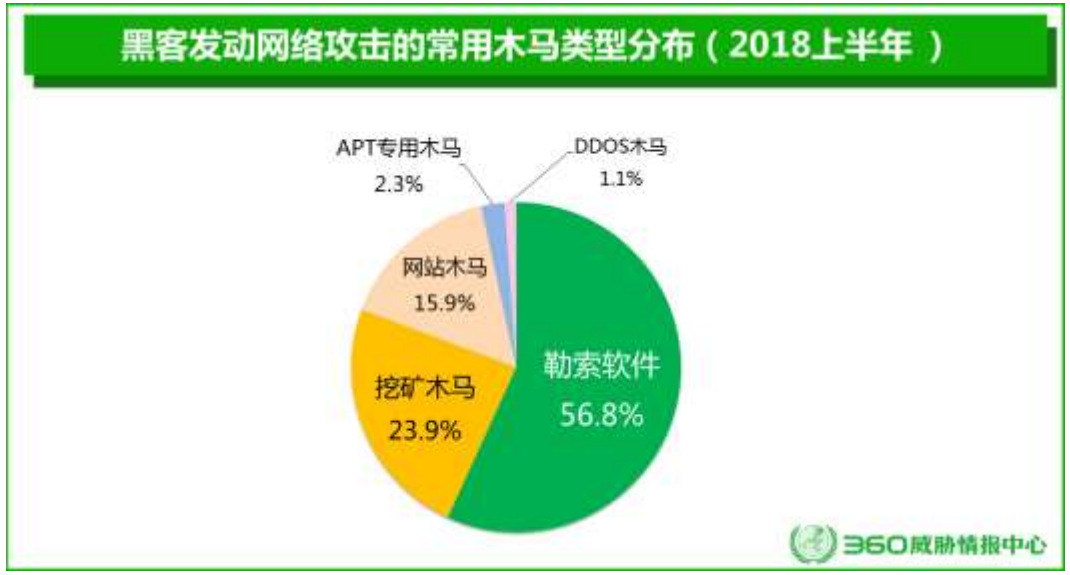
2018年应急响应事件盘点

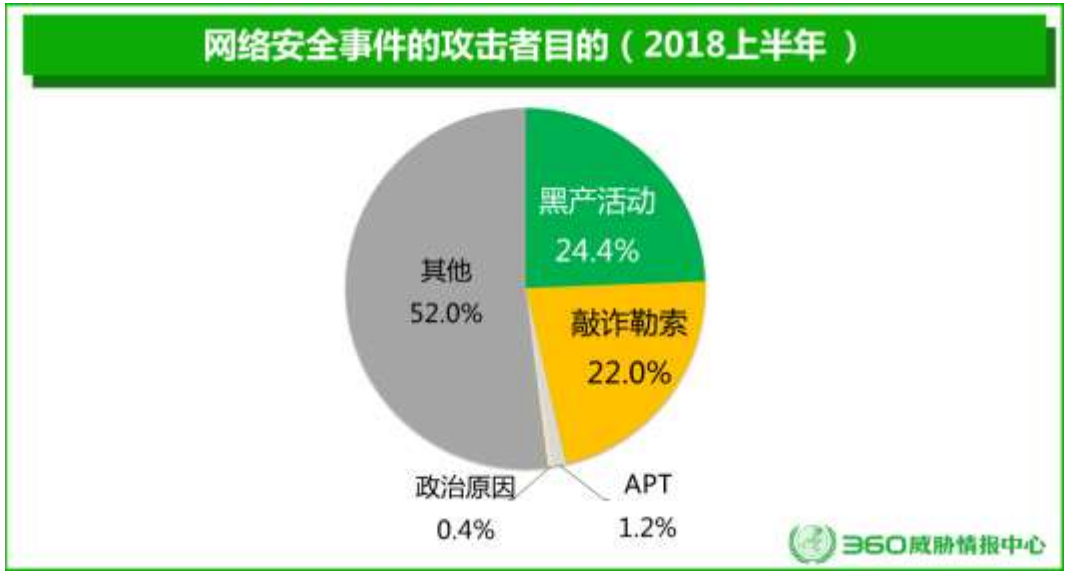
2018年上半年，360安服团队共为全国各地政企机构提供250次应急响应服务，保障其网络安全。360安服团队共为政府部门提供41次应急响应，累计704小时，平均每次应急响应时间为15小时。



2018年应急响应事件盘点

在2018年上半年，360安服团队现场处置的250次网络安全事件中，共有88次安全事件属于比较单纯的木马攻击事件。其中，勒索软件占比最高，为56.8%；其次是挖矿木马，占比为23.9%；网站木马占比为15.9%

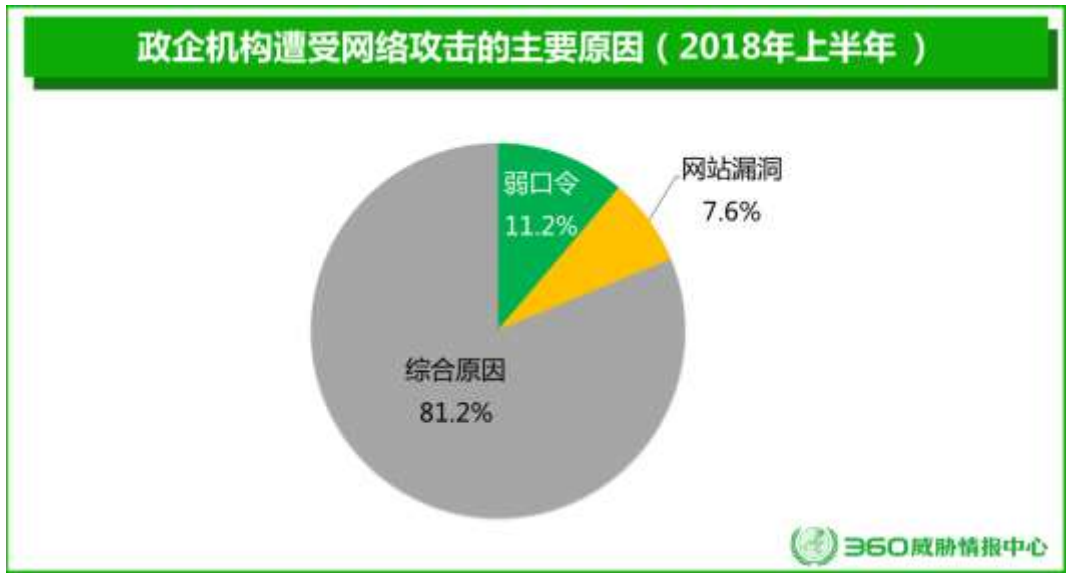


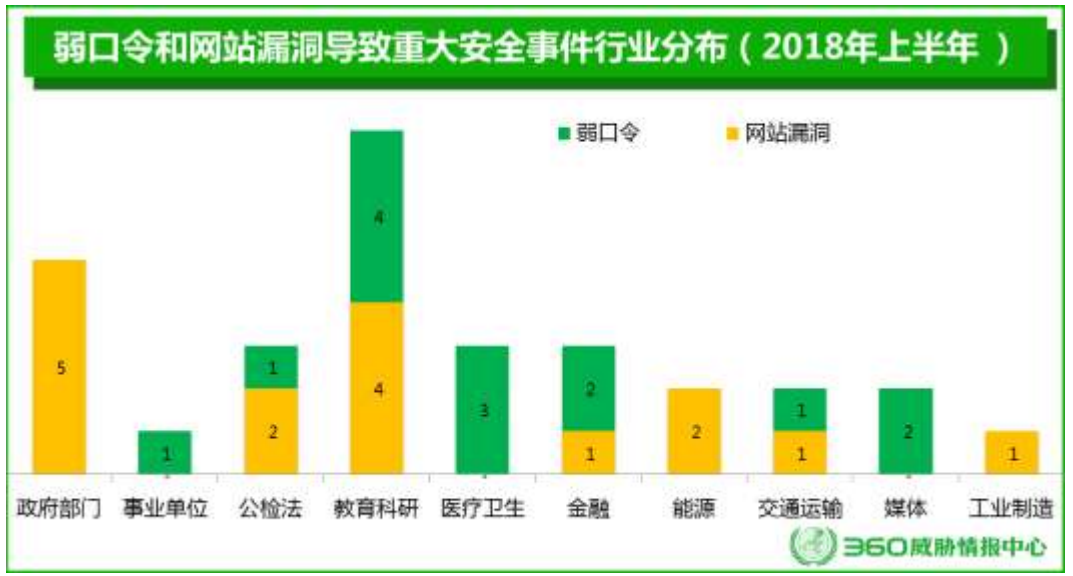


24.4%的网络安全事件背后有明显的黑产活动的影子；其次，22.0%的安全事件属于敲诈勒索事件，包括勒索软件、DDoS勒索，以及其他各种形式的勒索。特别的，还有3起事件（占比1.2%）属于APT事件，1起事件（占比0.4%）带有明显的政治目的。

2018年应急响应事件盘点

2018年上半年参与处置的250起网络安全事件中，11.2%的事件与相关设备或系统使用弱口令有关，7.6%的事件与网站存在已知（业界已知，但相关机构可能不知道）但未及时修复的安全漏洞有关。





弱口令和网站漏洞导致的部分关键行业网路安全事件的分布情况。

02 应急响应中典型场景以及案例

典型客户

典型场景-政府行业

网络特点

网络结构复杂，如分为**政务外网**、**政务内网**、**互联网**及**办公网**等，部分行业还自建了覆盖全国的**专网**，各个网络之间既有**相互隔离**的环境也有**相互连接**的地方。

ACL复杂，往往连管理员都很难分清楚不同区域之间的访问策略，一旦有安全事件的发生，很难进行事态控制以及溯源。

高频安全事件

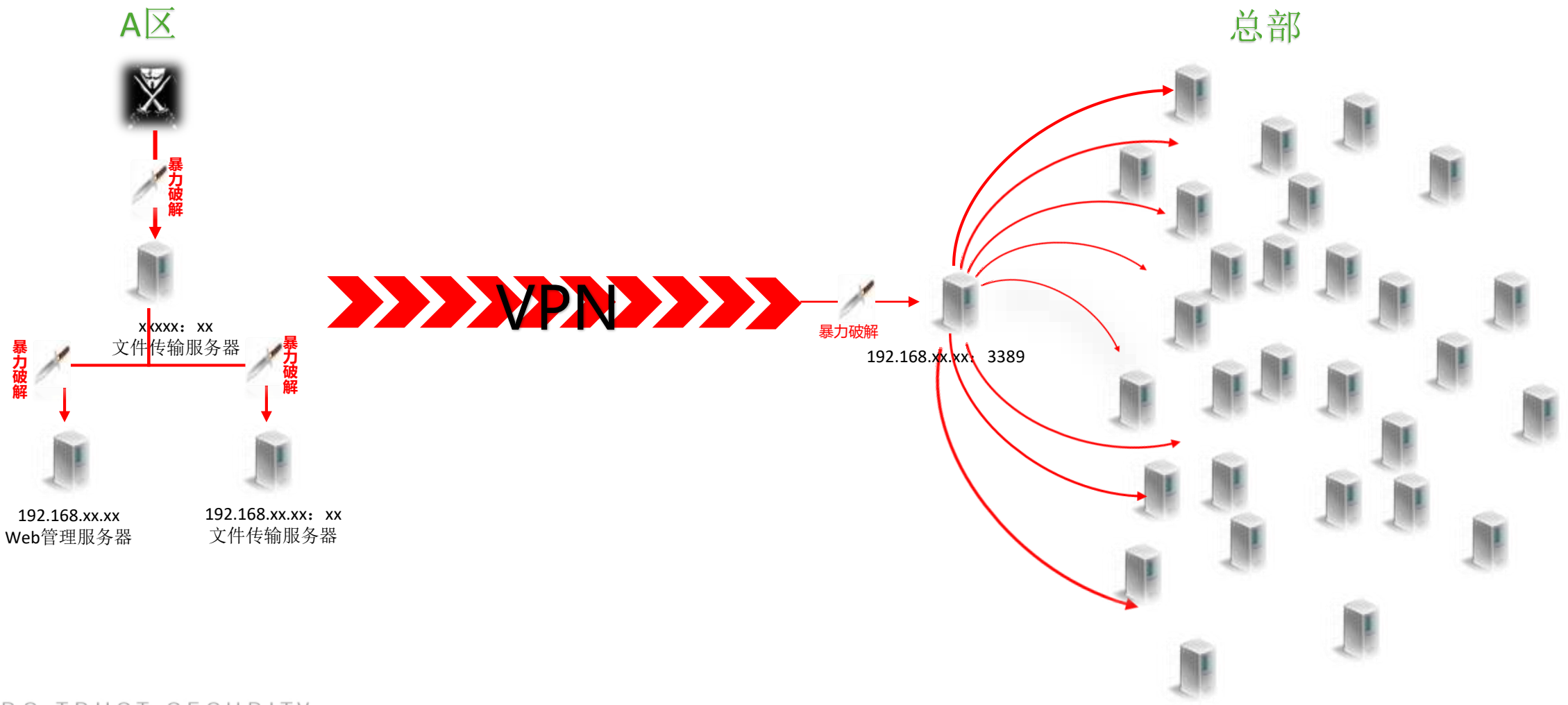
网站被入侵传后门、勒索软件、APT攻击

应急响应难点

大部分没有审计设备、内部资产混乱、溯源难度大。

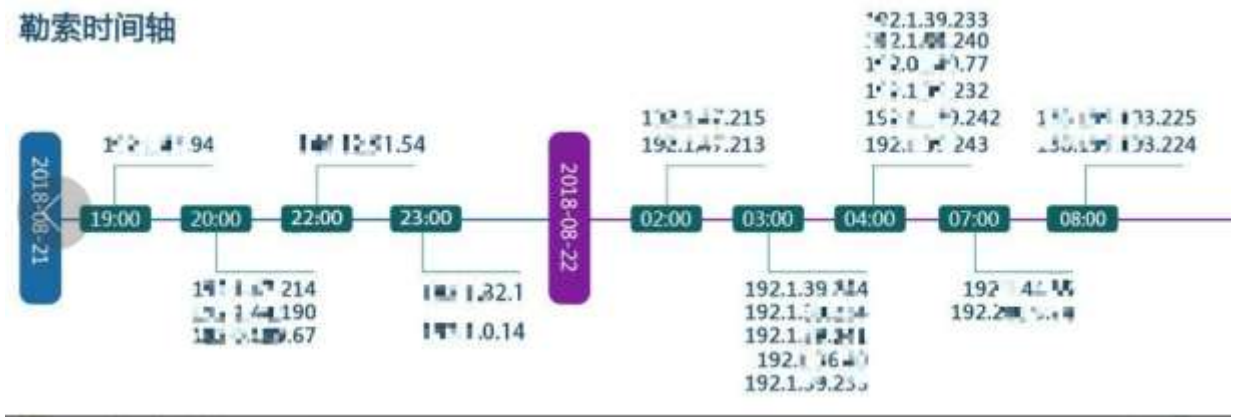
典型案例-政府行业

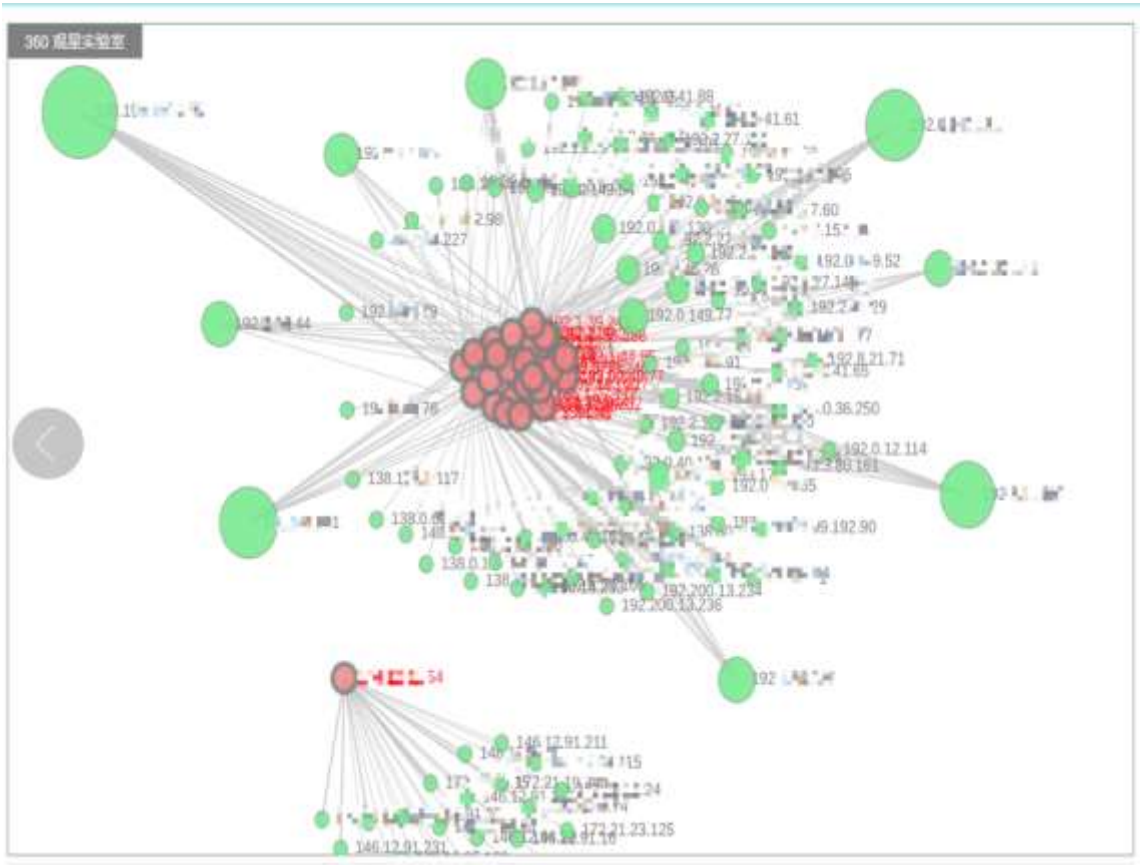
某政府客户大范围被植入勒索软件



典型案例-政府行业

某政府客户大范围被植入勒索软件，只依赖WINDOWS 系统日志进行了攻击溯源。





典型场景-运营商行业

网络特点

网络结构复杂，分为**IP承载网**、**传送网**、**固定通信网**、**接入网**、**同步网**、**信令网**、**支撑网**等，从用途上又分**生产网**、**网管网**、**办公网**等，部分安全域划分不明确，各个网络之间既有相互隔离的环境，也有相互连接的地方。总体网络结构复杂，有的系统平台部署在简单的网络结构上，有的系统部署在私有云上平台上。

高频安全事件

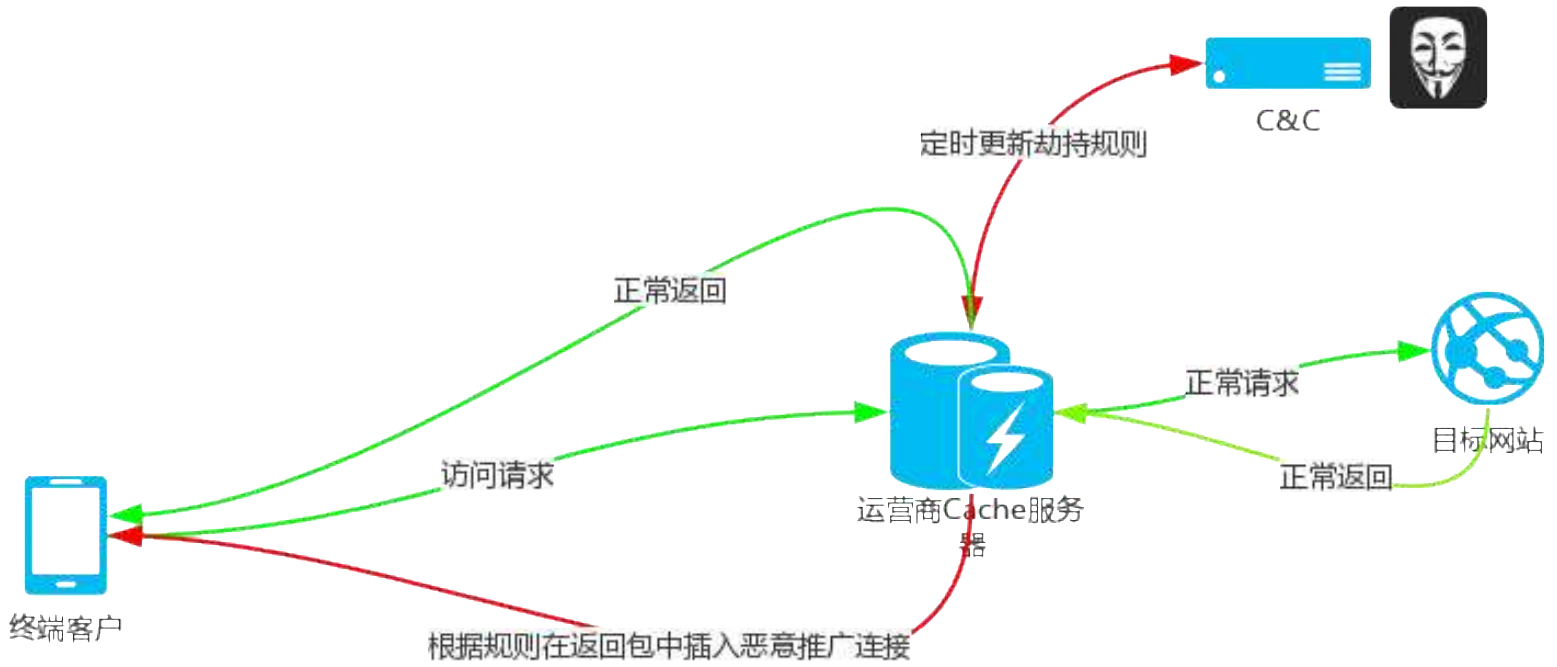
链路劫持、中间件漏洞、
敏感数据泄露、DDOS攻击

应急响应难点

网络结构大、资产数量多，系统多，开发厂家多，部分资产归属不清，有的平台没有审计设备，没有安全设备，溯源困难。

典型案例-运营商行业

某省运营商链路劫持事件

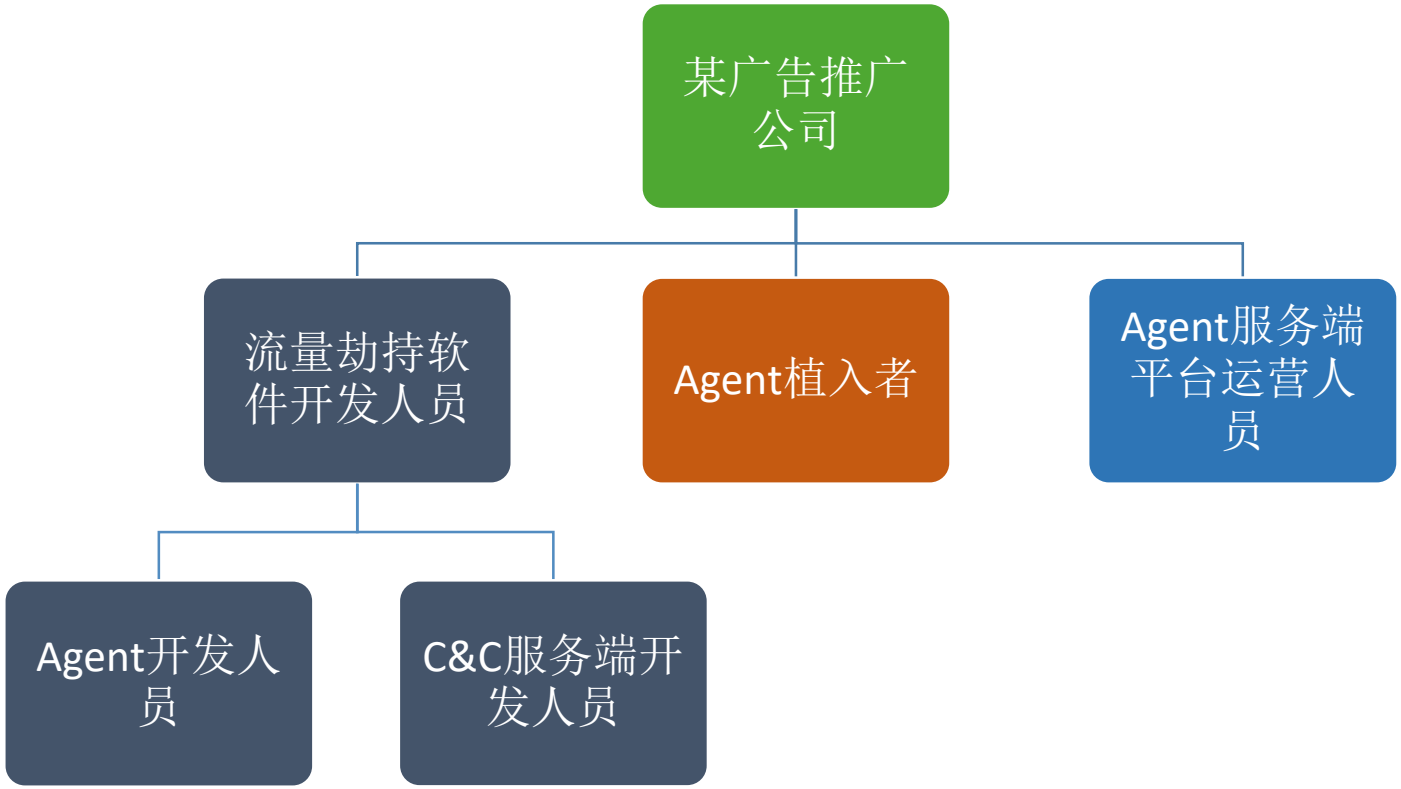


2018年3月份某省手机4G用户投诉在使用“某APP”过程中，会出现广告及跳转游戏下载界面的现象，使用联通和电信网络都不会出现此问题。

IOS系统打开页面除出现广告外，还会自动跳转到APPSTORE某游戏下载界面。

典型案例-运营商行业

某省运营商链路劫持事件



1.将Agent植入到运营商Cache服务器

2.紧急情况下下线删除Agent（最新版本支持远程卸载）并且抹掉系统相关日志

1. APP安装量推广
2. 精准广告推广

1.Agent版本多达18个，版本越来越趋于自动化，支持直接远程控制Cache服务器进行规则修改，程序更新等功能

2.支持劫持exe、apk、js等后缀的URL

1.维护劫持规则以及策略

典型场景-医疗行业

网络特点

网络结构相对简单，分为**医疗办公网**、**医疗业务网**两个大网，医疗办公网络内分**WEB综合平台**、**OA**、**办公终端**，办公网络互通，很多WEB服务器使用外联网络，医疗业务网络业务复杂，**内部连接和外联网络共存**。ACL策略相对简单，**办公网和业务网可以直连，并都有外联网络。**

高频安全事件

勒索软件、

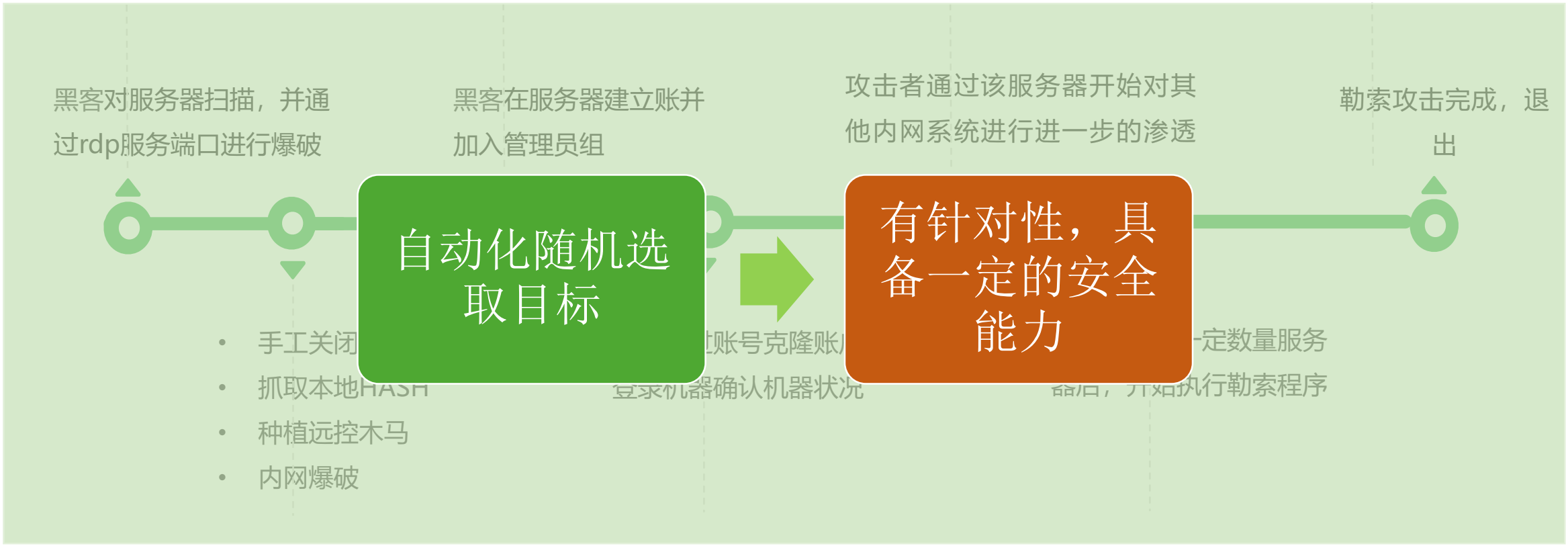
蠕虫终端大面积蓝屏（MS17010）

应急响应难点

大部分没有审计设备、基础安全水平薄弱，内部资产混乱、溯源难度大。

典型案例-医疗行业

某医院GLOBEIMPOSTER勒索事件



特殊点： 抓明文密码、使用远程控制软件、使用专门结束杀软的工具

典型场景-金融行业

网络特点

银行的网络分成办公网、生产网和互联网，一般来说，办公网和生产网之间是逻辑隔离，但是互联网与其他两个网络可能物理隔离，也可能是逻辑隔离。

银行的办公网和生产网之间ACL访问控制严格，并且有严格的配置变更管理（CMDB）。

安全数据采集比较全面，并且建设有完善的SIEM平台。

高频安全事件

勒索软件、挖矿、
SQL注入、APT攻击

应急响应难点

内部资产相对清晰、但是因为内部做了大量的NAT策略和服务器的负载均衡，导致溯源也存在一定的难度。

典型场景-航空行业

网络特点

历史包袱重，网络结构复杂，**重建轻管，边界不清晰。**

网络区域大致分为DMZ区，内部服务器区，INSIDE（OA、运维等）**访问控制不够严格，内部互通。**

缺乏总体拓扑图，**资产管理混乱**，出现问题难以定位到设备和责任人。

高频安全事件

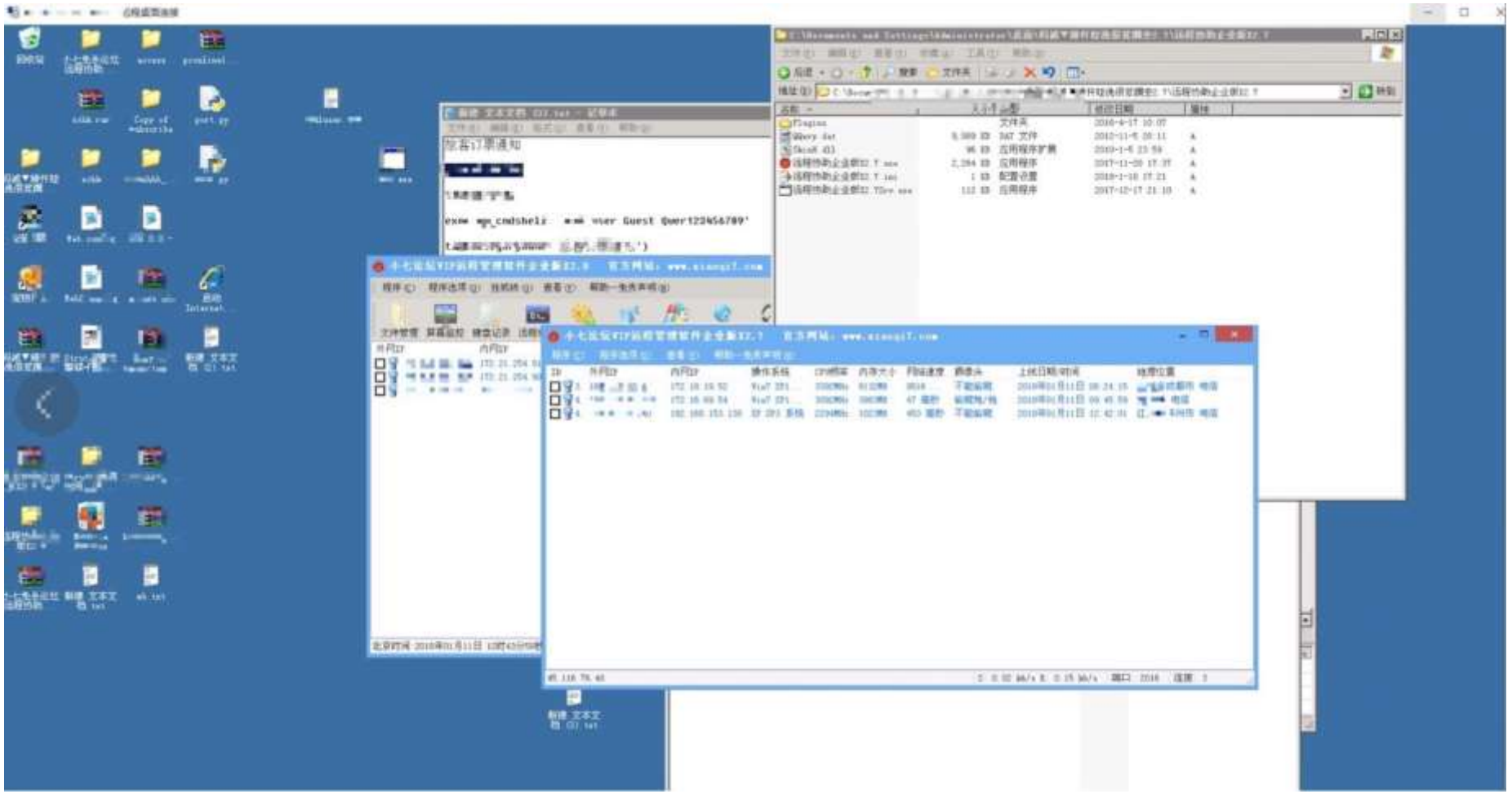
网站入侵、数据泄露、服务器挖矿、退票诈骗

应急响应难点

缺乏审计类系统、资产不清、通用密码排查范围大。

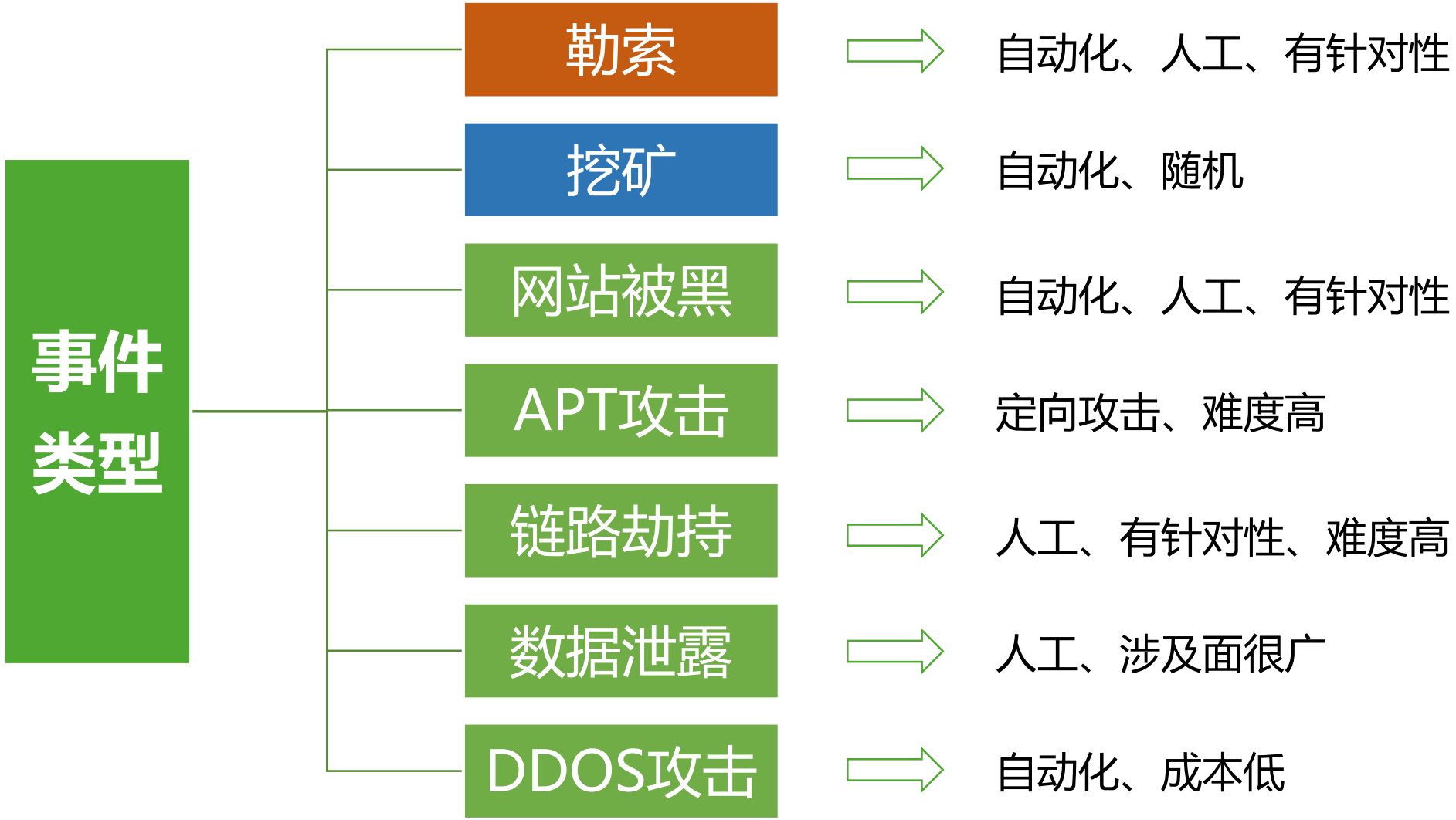
典型案例-航空行业

某航空公司被黑客入侵（长期控制）内网机器被映射到黑客公网VPS，导致客户信息泄露



03 不同场景下应急响应的探索

应急响应典型行业应急事件总结



应急响应中典型行业存在的问题

	政府行业	运营商行业	医疗行业	金融行业	航空行业
资产混乱	√	√	√		√
通用密码（弱）	√		√		√
网络架构混乱	√				
无安全审计设备	√	√	√		√
无日志集中收集	√				
安全能力缺失	√	√	√		√
供应链问题	√	√		√	

应急响应中具备的能力


事件分析能力
能进行多维度关联分析
能还原完整杀伤链
能结合具体业务进行深度分析
事件研判能力
能确定对攻击者的动机以及目的
能确定事件的影响面以及影响范围
能确定攻击者的手法
等等
事件发现能力
能发现 APT 攻击
能发现 WEB 攻击
能发现数据泄露
能发现失陷主机
能发现弱口令以及企业通用口令
能发现主机异常行为
等等
事件处置能力
能第一时间恢复业务正常运行
能对发现的病毒、木马进行处置
能对攻击者所利用的漏洞进行修复
能对问题机器进行安全加固
企业应急响应
具备的 6 大能力
数据采集、 存储和检索能力
能对全流量数据协议还原
能对还原的数据进行存储
能对存储的数据快速检索
攻击溯源能力
具备安全大数据能力
能根据已有线索（IP、样本等）对攻击者的攻击路径、攻击手法以及背后组织进行还原

应急响应典型行业能力评估

注：整体能力5颗星

	政府行业	运营商行业	医疗行业	金融行业	航空行业
数据采集、存储、检索能力	***	***	**	****	**
事件发现能力	**	***	**	****	**
事件分析能力	**	***	*	****	**
事件研判能力	**	***	*	****	**
事件处置能力	*	***	*	****	**
攻击溯源能力	**	***	*	***	**

应急响应中的基础能力

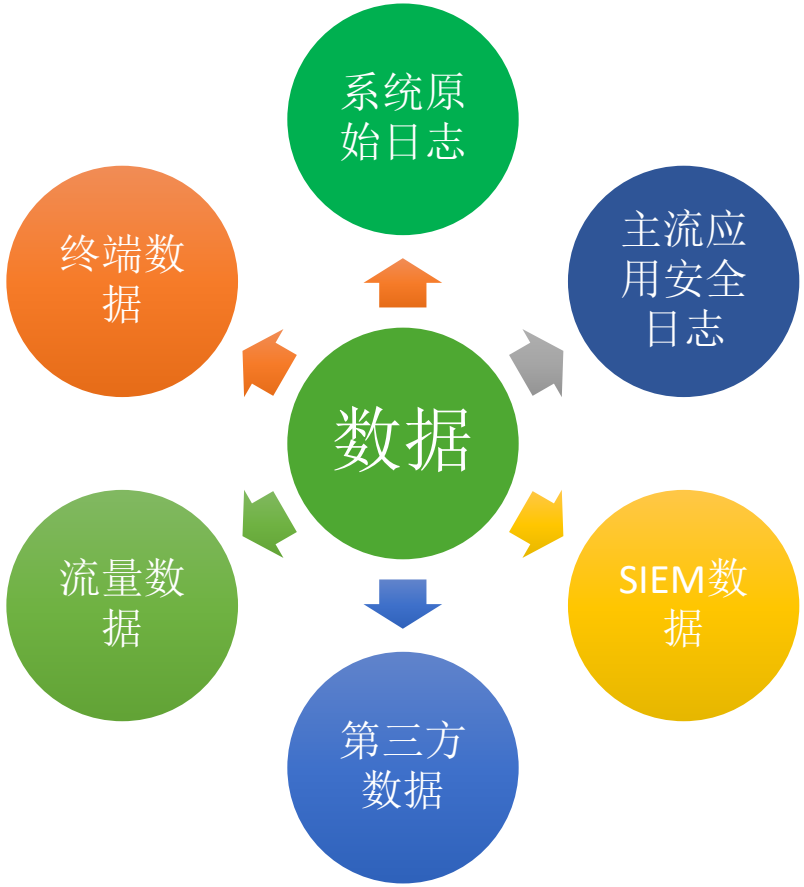
甲方自己的安全团队

外界的专业安全团队

基础安全数据是指在应急响应过程中对事件进行分析溯源的不可或缺的数据

应急响应中的基础安全数据

Windows/Linux主机日志等



系统安装主流软件的日志、例如中间件

默 认 、 Linux(/var/log 下面)audit日志

网络设备日志、主机日志、WEB应用日志

威胁情报数据

DNS、HTTP/WEBMAIL、FTP SMTP/POP3/IMAP、SMB、LDAP/SSL ORACLE/MYSQL/SQLSERVER

进程日志、杀毒日志等

04 企业如何提升应急响应的能力

从安全体系的改进建议

1、需做好网间安全隔离建设；
2、需加强安全设备安全策略统一监管；
3、需加强人员驻场运维；
4、需加强人员基础安全意识培训。
5、需提升互联网资产发现能力。

1、需对服务器、终端进行有效的安全加固；
2、需加强全局监测预警能力；
3、需加强应急处理能力。
4、需增加全网动态监控能力；

1、需增加全流量采集能力。
2、需增加全流量风险分析能力。
3、需加强人员安全技能培训。
4、需加强实战型攻防演习。

1、需增加威胁情报协同联动能力；
2、需建立安全事件的协同通报机制。

通过前面4个阶段，对攻击者进行预判，提前采取有效安全防卫行为。


ISC
2018
ISC互联网安全大会
360互联网安全中心
谢 谢!
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）