第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

披坚执锐 决战终端

安天 端点安全产品中心

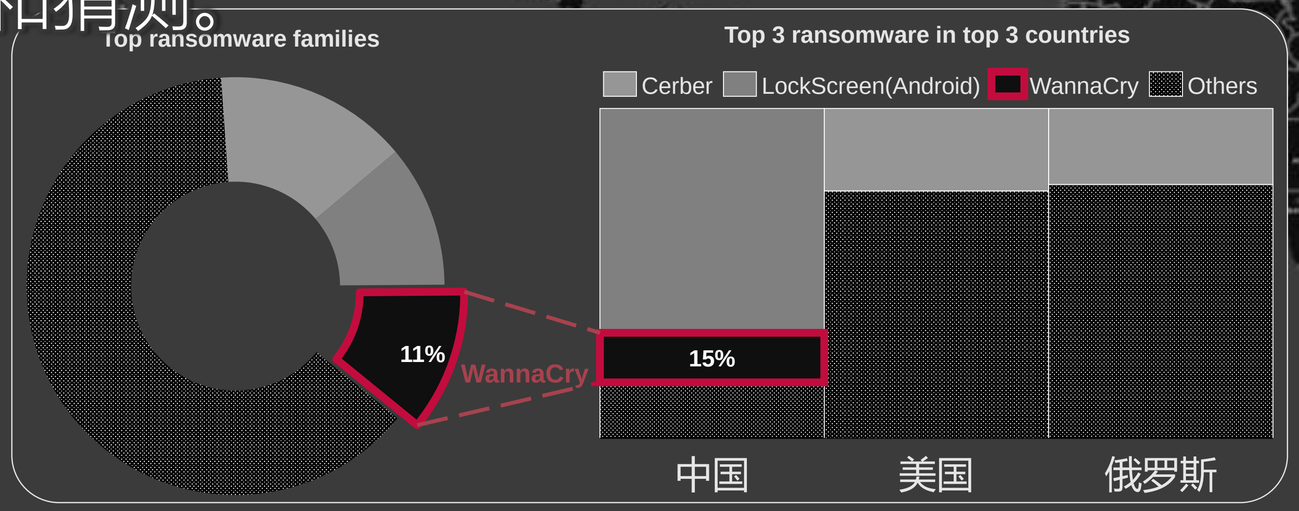
红旗漫卷

敌情想定是前提，网络安全实战化

勒索软件席卷全球终端

The global impact of ransomware

- 2015-2017年全球勒索软件造成的损失已增长到**50亿**美元；
- 勒索软件威胁全球，中国、美国、俄罗斯遭受了最多攻击；
- 以Wannacry为代表的勒索软件感染事件，表明很多终端安全软件没有为用户提供“有效防御”；
- **Wannacry**具备勒索软件的全部要素，尽管出现了很多新的关于它的起源的分析和猜测。



数据引自：

https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

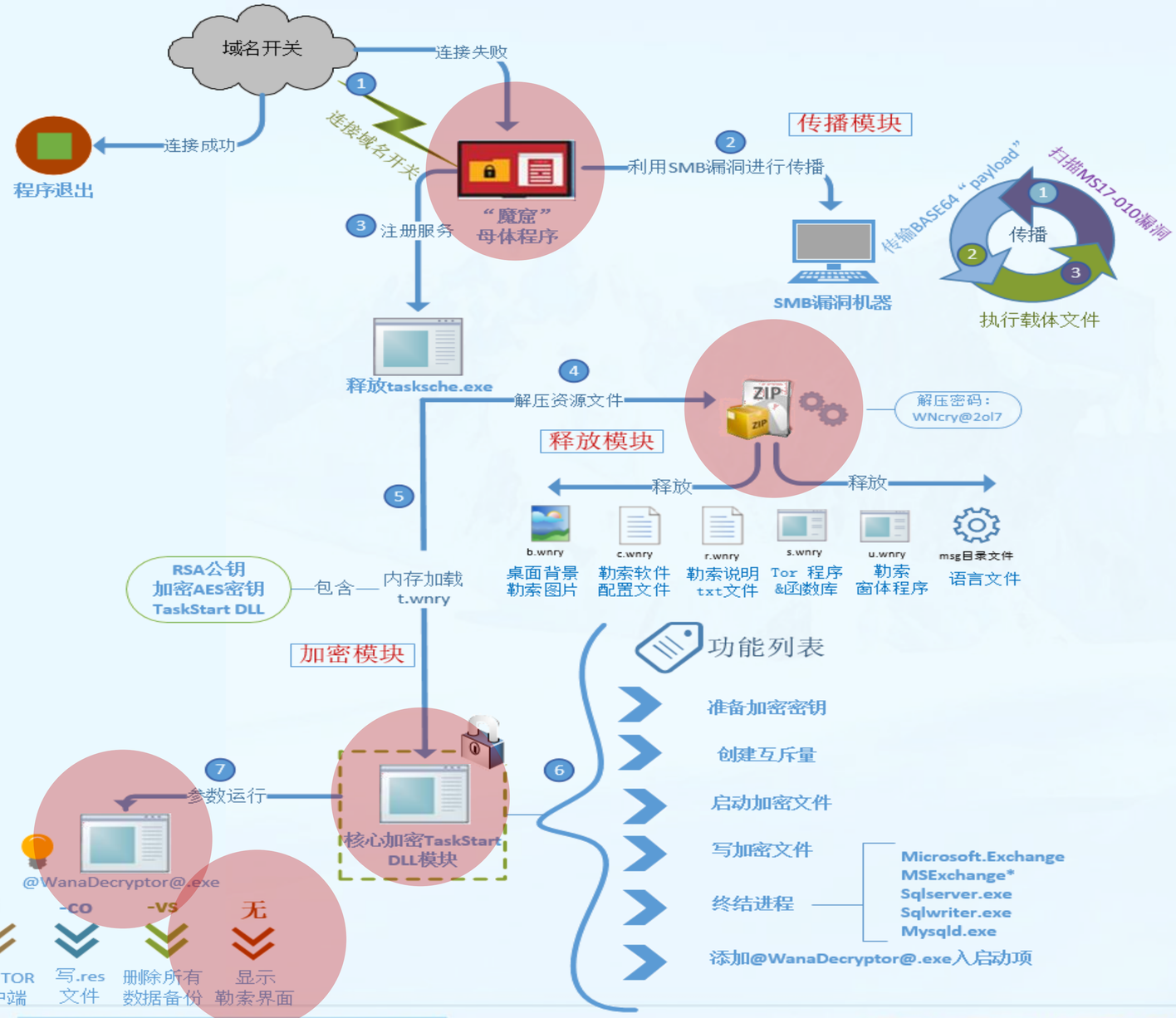
https://blogs.technet.microsoft.com/mmpc/2ransomware-1h-2017-review-global-outbreaks-reinforce-the-value-of-security-hygiene017/09/06//

https://www.microsoft.com/en-us/wdsi/threats/ransomware

勒索软件对终端造成的威胁

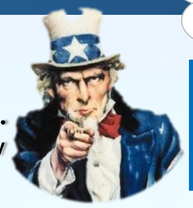
以安天对魔窟(Wannacry)的分析为例。

1. 进入主机获得执行机会
2. 释放资源
3. 加密文件
4. 启动暗网
5. 显示勒索



针对终端的高级持续性攻击频发

- 在多数高级威胁攻击场景中，端点是攻击落地首要目标；
- 商业军火进一步增强了高级威胁的攻击能力，其中，针对端点的商业军火占很大比例，包括：漏洞利用工具、攻击载荷投放工具和端点侧的恶意代码。

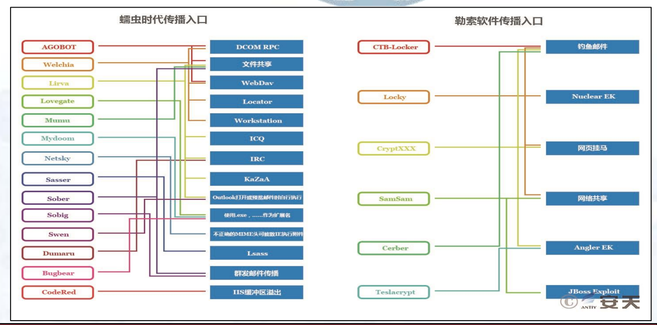


国家和政治经济集团为背景发动

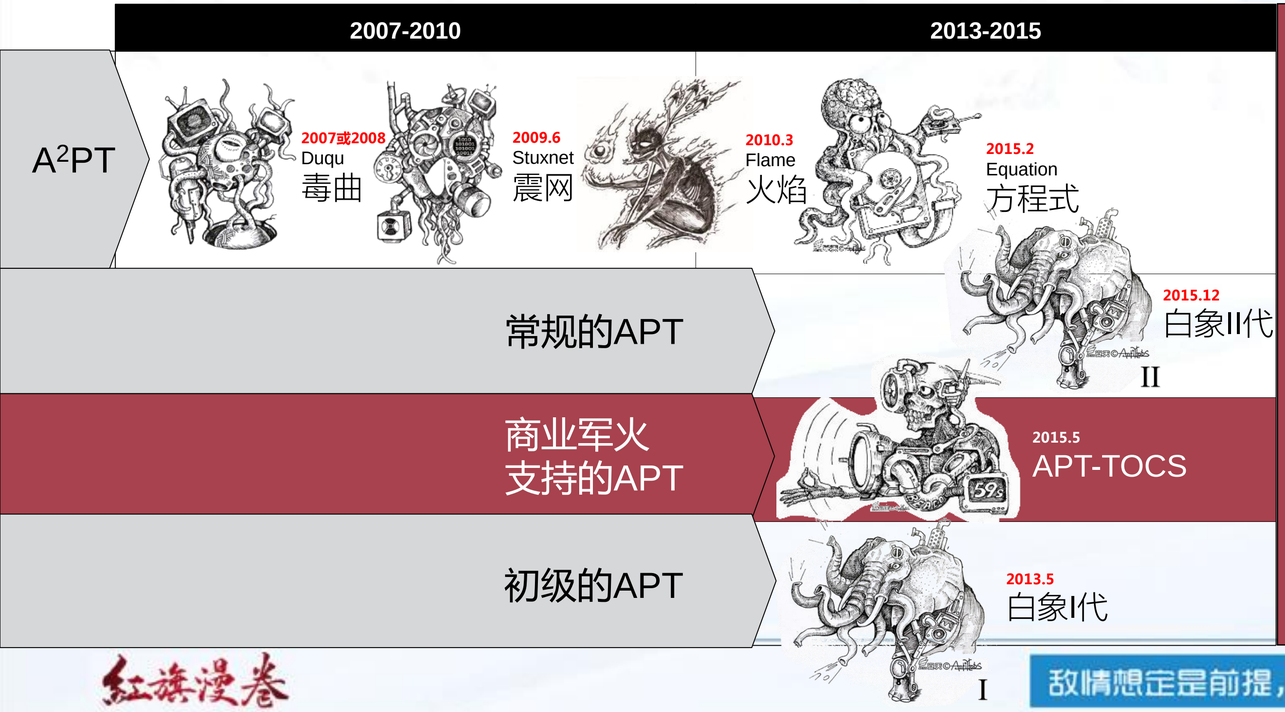
横向移动 水坑攻击
SNS夹带 0Day漏洞 数字伪装
格式文档攻击 本地化反弹

反复进入
坚定动机 隐蔽通讯 人员带入
作业意志 持久化

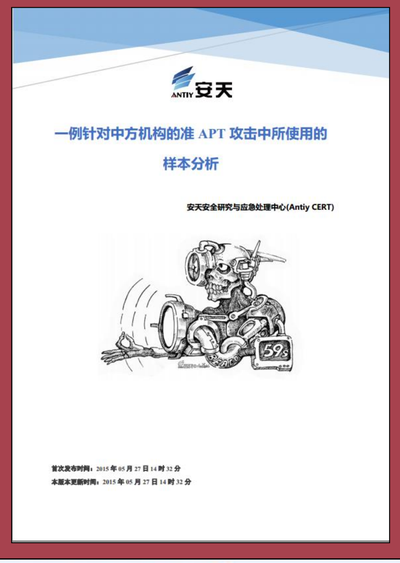
Advanced × Persistent = Threat
高级（能力） 威胁 持续性（意图）



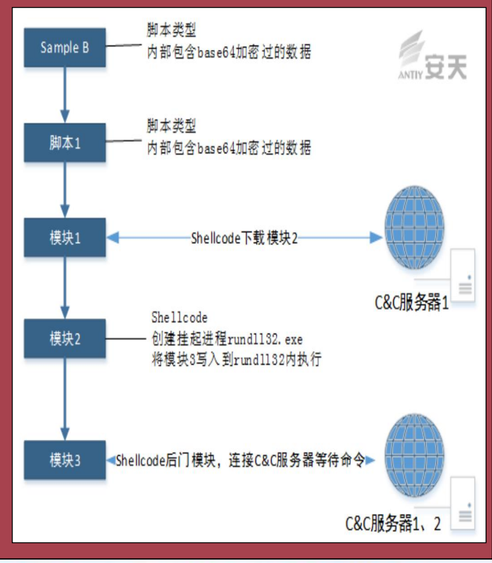
安天对高级持续性威胁的分类和时间线



安天对APT-TOCS事件的分析报告



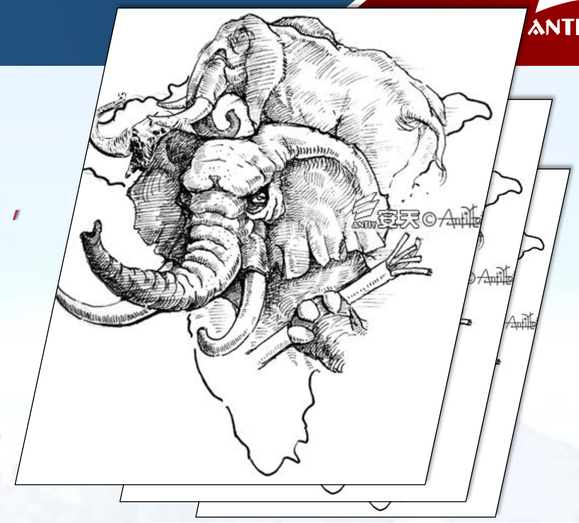
APT-TOCS攻击中各模块之间的衍生关系和模块主要功能



地缘政治引发的网络纷争从未停歇

从“白象”到“象群”——以南亚某国的多个组织的攻击为例，窃取终端的机要信息。

- 虽然目前尚未找到相关组织、行动之间的内在关联，但可以确定，**他们都具有相似的目的和相同的国家背景，并且其中大部分攻击目标包括中国。**我们将这一系列网络攻击组织和行动称之为——“潜伏的象群”；
- 来自南亚某国的系列网络攻击**自2012年至今**从未间断活动。攻击组织为达成战略目的会不断更新、修改战术，**但都试图在网络空间窃取机要信息，威胁其攻击目标的整个信息化体系**；
- 随着具有国家背景的攻击组织不断被曝光，我们需警惕各类对手在网络军备方向的发展；同时**有效防御是战略能力的基本盘**，只有建立起综合体系防御能力，才能成为网络空间强国的基石。



“白象”(WhiteElephant)组织	“阿克斯”(Arx)组织	“女神”(Shakti)行动	“苦酒”(BITTER)行动
白象一代：2012.07-2013.10 白象二代：2012.05-2016.07 **最新活动：2016.11-2017.12**	活动时间：2013.09-2013.11	活动时间：2012.04-2015.01	活动时间：2013.11-2016.10
1. 组织介绍： “白象”组织来自南亚某国，自2012年以来持续针对中国、巴基斯坦等国进行网络攻击，长期窃取目标国家的科研、军事资料。 **2. 攻击手法：** 过去“白象”组织通常采用鱼叉式钓鱼邮件进行攻击，大部分邮件被插入恶意链接，之后攻击者通过精心构造的诱饵内容诱导受害者打开链接，而一旦打开就会**下载带有漏洞的恶意文档**。2017年最新的“白象”组织活动则通过仿冒诱饵网站进行攻击，通过伪造一些官方网站如邮箱网站，诱导用户输入账户及密码。除此之外，还有通过向热点事件网站挂载恶意代码的方式，以更新的名义诱导用户**下载执行恶意载荷。** **3. 攻击特点：** 鱼叉式钓鱼攻击、网站钓鱼攻击、入侵网站作为C&C、模块化与组合作业	**1. 组织介绍：** “阿克斯”组织大约攻陷了600多个目标，大部分位于南亚某国和巴基斯坦。 • 从该漏洞利用的时间点上来分析：“阿克斯”组织对该漏洞的掌握可能早于“白象”组织； • 从传播细节和最终执行的恶意代码来看，“阿克斯”组织似乎与“白象”组织并不存在明显联系； • 从其攻击目标和相关C&C基础设施的注册信息来看，“阿克斯”组织可能也来自南亚某国； • 对0day漏洞的利用上来看，其可能是“象群”中第一个使用**0day漏洞**且具有较高技术水平的组织。 **2. 攻击手法：**钓鱼邮件 与常规传播银行木马的手法非常相似，其通常以标题为“SWIFT支付”的电子邮件形式发送恶意软件至目标机器，很容易将自身隐藏在常规钓鱼邮件之中，而不被引起重视。	**1. 组织介绍：** “女神”（Shakti）行动是安天在追踪“白象”组织的过程中发现的一起长期窃取用户文档、文件等重要信息的攻击事件。 • 其幕后攻击者利用木马程序进行窃密行为已持续四年之久，其攻击目标主要是波兰、以色列、巴勒斯坦和中国等。 • 目前尚未发现其与“白象”组织存在明确联系。该样本内部PDB字符信息“Shakti”是隶属于印度教女神的象征，因此安天将此次攻击事件命名为“女神”行动。 **2. 攻击手法：**无文件实体 • 包含两个加密的dll模块，第一个dll模块的主要功能是反沙箱、反调试和完成启动项服务；第二个dll模块为核心**窃密模块**，主要功能是窃取用户系统信息和文档文件。 • 样本运行时会在内存中解密第一个dll模块，同时将第二个dll模块解密后**注入到浏览器**进程中，两个dll模块都被直接注入到内存中运行。	**1. 组织介绍：** 主要通过鱼叉式邮件以及系列攻击组件的应用，对巴基斯坦进行针对性攻击，同时此次行动的攻击者可能参与了多起网络攻击事件。安天认为该行动的相关证据线索表明该行动与南亚某国有密切联系，是“象群”中一起易被忽视的针对性攻击。 **2. 攻击手法：**鱼叉式攻击；RAT窃密组件、远控组件、Android组件 • 使用鱼叉式邮件来投递攻击载荷，通过邮件中附带经典**漏洞“CVE-2012-0158”**的格式溢出文档或**伪装成图片的EXE可执行文件**诱骗用户下载查看。 • 部分RAT组件能够记录受害主机上的文件和时间戳，其2014年的样本还具有收集指定类型文件的功能，在样本中即有相关的文件类型硬编码。

重压之下的终端安全

终端面临勒索软件肆虐，高级持续性攻击，地缘政治背景的网络纷争等多重威胁。

“物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。

——引自习近平总书记《在网络安全和信息化工作座谈会上的讲话》

以真实的敌情想定为前提，以实战化作为网络空间安全防御的第一要求。

- ✗ 物理隔离+好人假定+规定推演，构成了当前最大的自我安全麻痹。
- ✗ “隔离就是安全，连接就是风险”带来巨大的安全负资产。
- ✗ 隔离场景面临重重困难，包括运维、成本、漏洞修复、安全能力等致命问题。

路径清楚

- 内网：已经被渗透
- 供应链：被上游控制
- 运营商网络：关键路由节点被控制
- 物流仓储：被渗透劫持
- 关键人员和周边人员：被从互联网进行定位摸底
- 内部人员：有敌特的人员派驻或被发展

敌人为达成战略目的选择战术，终端安全存在无效防御。

- ✗ 以Wannacry/NoPetya为代表的准APT级的勒索软件事件，攻击了大量终端。
- ✗ 以Cobalt Strike为代表的商业军火平台，降低了发动针对终端的APT成本。
- ✗ 以“象群”为代表的国家级攻击组织，为达成战略意图不断突破终端安全的防御防线。

战术选择

- （战时）高强度对抗
- （平时）持续性对抗
- （平战）无底线对抗
- （平战）高成本对抗

勒索软件

商业军火

国家级组织

……

实战化处置威胁，实现用户价值，终端有效防御是构成战略威慑力的重要环节。

- ✓ 终端需要具有合理的架构安全体系，增强安全运维能力，减少攻击面。
- ✓ 防御体系具有纵深防御能力，多维度发现威胁，抵御威胁
- ✓ 具有与威胁对抗的实战能力，可以根据现有防御资源，快速生成并实施有效的防护策略

网络安全滑动标尺模型介绍

架构安全（Architecture）

侧重于“强身健体”专注于“尽责应该做的”假设攻击者存在，但主要不关注对抗

自身加强

在系统规划、建立和维护的过程中充分考虑安全

三同步

被动防御（Passive Defense）

不足以应对具有充足资源和“鉴定意志”的高级威胁对手。

消耗攻击者资源

在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统

强调了安全防护在基础设施上的附加特点

闭环中未考虑人员静态防御

积极防御（Active Defense）

以分析人员为中心，以相应流程驱动，通过行动对抗威胁，并动态适用调整安全策略（反过来影响被动防御和架构）

监控威胁、响应对抗了解威胁，持续提升

分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程

从监控到响应，加上经验积累，有人员在闭环内的积极动态防御

消费情报

情报（Intelligence）

收集数据，处理利用分析评估，生产情报
—聚焦有机会、有能力和意愿造成伤害的威胁
—关注情报所能驱动的决策与行动

填补对攻击者情况了解的差距，提供积极防御所需要消费的情报

收集数据、将数据利用转换为信息，并将信息生产加工

反馈到积极防御体系才能发挥作用

从数据加工到情报

情报的引入减少了不确定性

威胁情报要发挥做做，需要先打好基础，否则无异于打嘴炮

有效使用威胁情报的先决条件：
—知己
—知彼
—敢动：支持防御人员采取行动

进攻（Offensive）

对于民间机构来说只有法律反制措施和自卫反击具有可能性，但是民间机构很难达到效果

在我方网络之外对攻击者采取直接行动

对抗攻击者的法律反制措施、自卫反击行动

合理自卫和防卫过当之间度，是一个问题

Architecture：考虑系统自身的正常运行

Passive Defense：考虑攻击者存在的防御

Active Defense：主动监控攻击者并采取措施干预的积极防御

Intelligence：采取情报分析手段获得攻击情报改变信息不对称情况，降低防御的不确定性和覆盖面

Offensive：在自身网络之外采取行动攻击攻击者

*来源安天公益翻译组翻译《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》

基于滑动标尺模型的终端防御体系

架构安全（Architecture）

在系统规划，建立和维护的过程中充分考虑安全

被动防御（Passive Defense）

在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统

积极防御（Active Defense）

分析人员对处于所防御网络内的威胁进行监控，响应，学习（经验）和应用知识（理解）的过程

情报（Intelligence）

收集数据，将数据利用转换为信息，并将信息生产加工

进攻（Offensive）

情报

外部

-观察

进程行为

终端信息

-调整

APT事件

漏洞利用

封堵漏洞

病毒追溯与清除

执行被动防御策略

威胁取证

威胁处置
-行动

防御策略智能决策
-策略

终端加固

威胁查杀

被动防御

架构安全

配置加固：弱口令检测；软件管理；主机加固（STIG）

资产管理：资产信息采集；资产监控；资产展示；软件资产信息

网络控制：网络准入；非法外联监测与控制；无线网络控制

漏洞修复：漏洞检测；补丁更新

外设管控：USB外设管控；其他外设控制；光驱审计；蓝牙红外wifi管控

被动防御

文件防御：文件监控；文件信息提取；重要文件保护；防勒索；宏病毒检测；MBR保护；数字签名验证

进程防御：进程运行监控；启动链审计；敏感指令调用；注册表防御；虚拟补丁加固；脚本程序检测与防御；注入检测与防御；浏览器漏洞利用检测

边界防御：移动介质管控；文件落地检测；浏览器下载防护；邮件下载附件保护

主机防火墙：IP与端口控制；入侵监测；恶意域名拦截；网络行为记录；C&C检测；ARP检测

基于滑动标尺模型的终端防御体系

情报

外部

情报利用

文件属性转换

APT追溯信息

YARA规则

情报基础数据

文件静态分析

文件历史建档

文件向量提取

终端资产信息

情报数据同步

积极防御

生成情报

数据采集

文件信息

网络行为

进程行为

终端信息

威胁数据采集
-观察

Observe

Orient

威胁模式匹配
-调整

勒索行为

恶意行为

APT事件

漏洞利用

模糊指令

Act

Decide

封堵漏洞

病毒追溯与清除

执行被动防御策略

威胁取证

威胁处置
-行动

防御策略智能决策
-策略

终端加固

威胁查杀

被动防御

决策结果

态势感知系统

设置防御策略

架构安全

配置加固

弱口令检测

软件管理

主机加固（STIG）

资产管理

资产信息采集

资产监控

资产展示

软件资产信息

网络控制

网络准入

非法外联监测与控制

无线网络控制

漏洞修复

漏洞检测

补丁更新

外设管控

USB外设管控

其他外设控制

光驱审计

蓝牙红外wifi管控

被动防御

文件防御

文件监控

文件信息提取

重要文件保护

防勒索

宏病毒检测

MBR保护

数字签名验证

进程防御

进程运行监控

启动链审计

敏感指令调用

注册表防御

虚拟补丁加固

脚本程序检测与防御

注入检测与防御

浏览器漏洞利用检测

威胁检测引擎

边界防御

移动介质管控

文件落地检测

浏览器下载防护

邮件下载附件保护

主机防火墙

IP与端口控制

入侵监测

恶意域名拦截

网络行为记录

C&C检测

ARP检测

*来源安天公益翻译组翻译《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》

终端威胁防御体系——架构安全

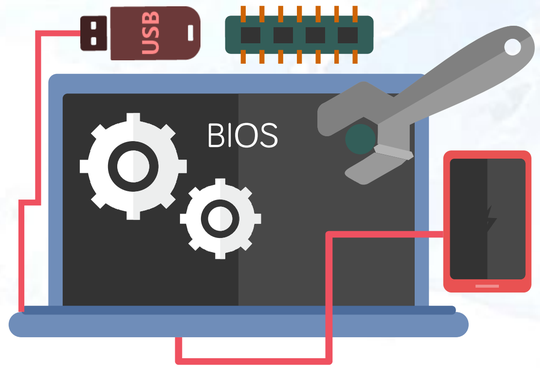
基础架构安全 | 被动防御 | 积极防御 | 情报

定义：终端系统规划、建立和维护的过程中充分考虑安全防护。

规划合理的健全的架构安全体系，可以有效降低终端遭受攻击风险，提升攻击难度。

网络控制

资产管理



外设管控

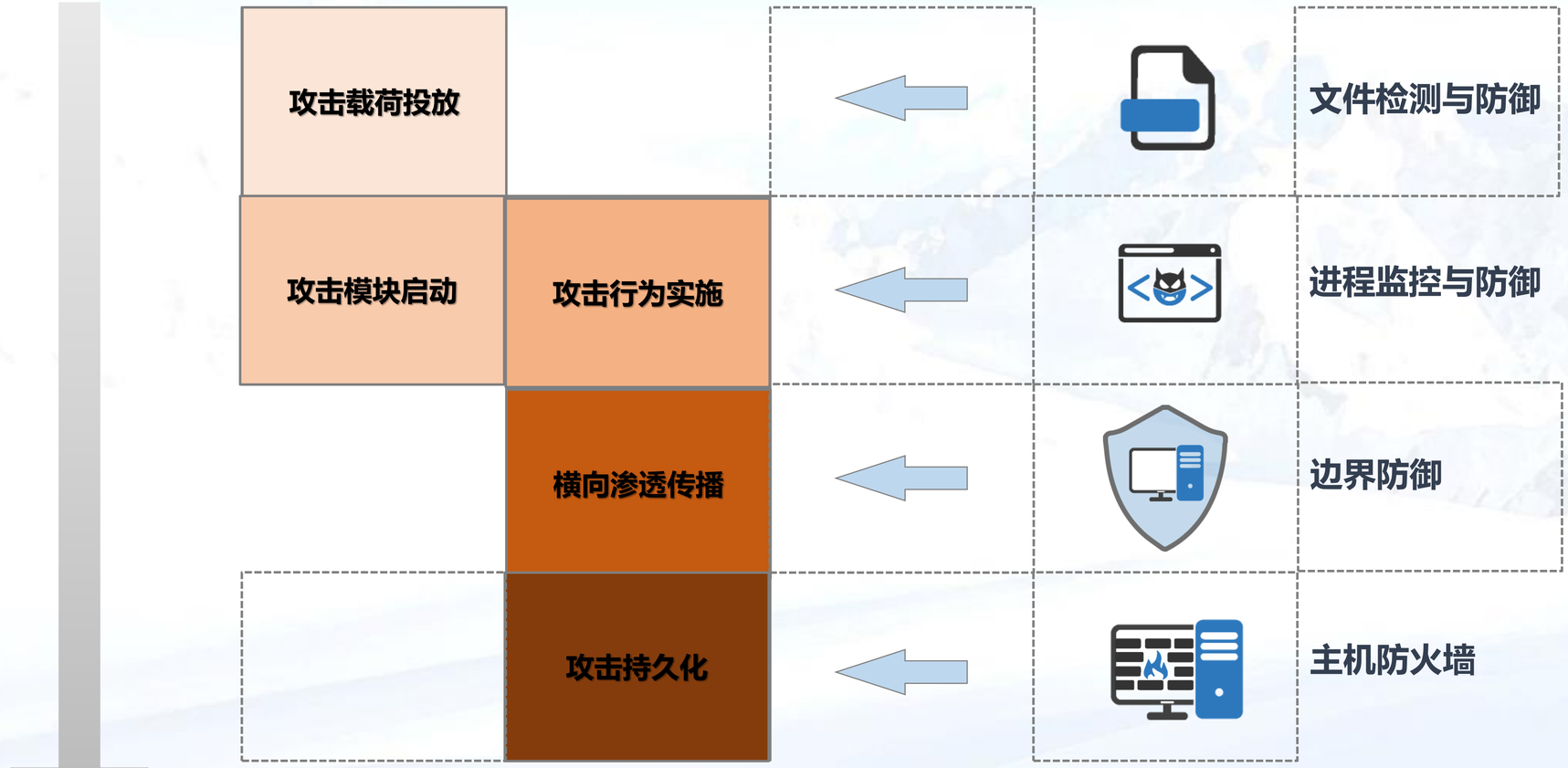
漏洞修复

配置加固

终端威胁防御体系——被动防御

基础架构安全 | 被动防御 | 积极防御 | 情报

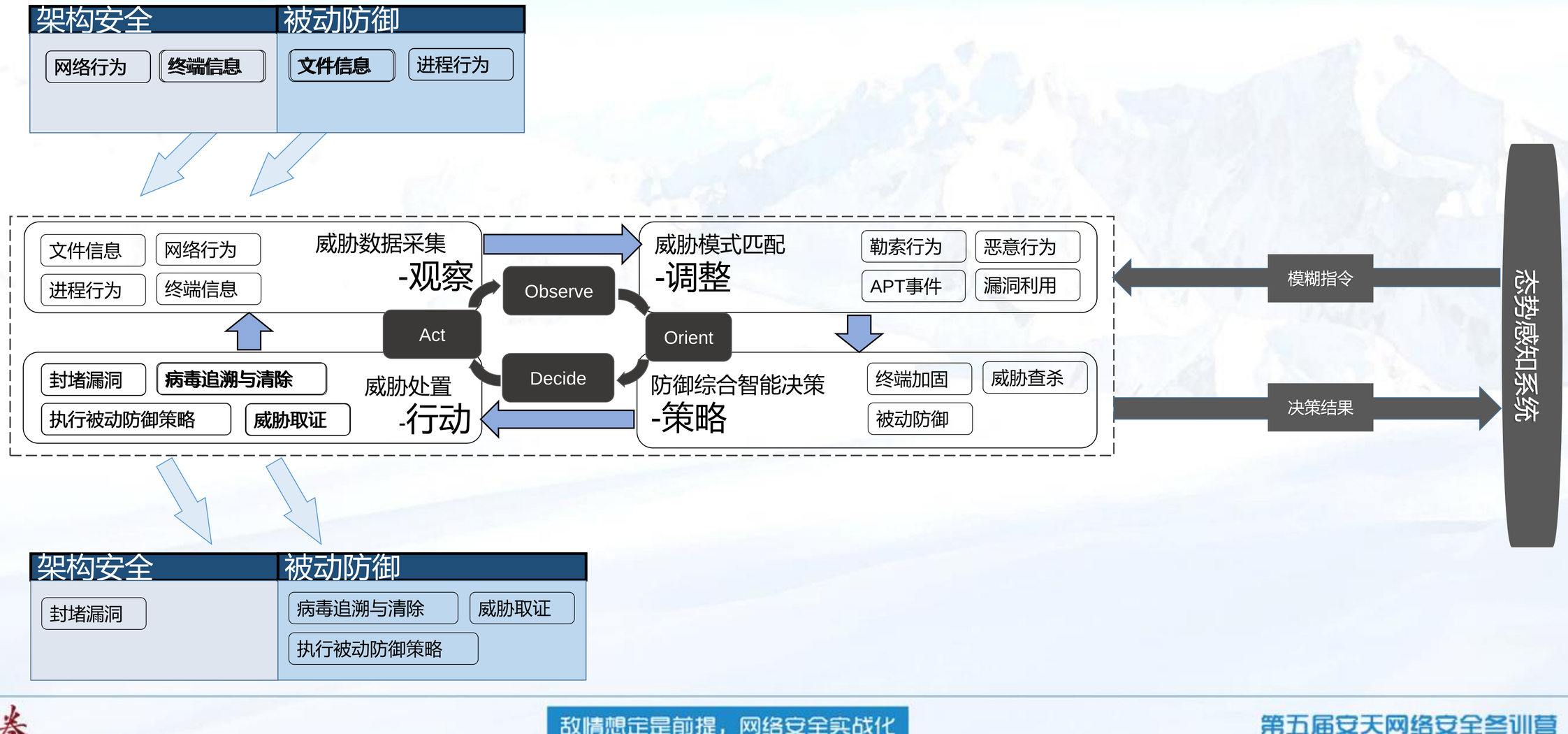
定义：在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统。



终端威胁防御体系——应用OODA的积极防御

基础架构安全 | 被动防御 | 积极防御 | 情报

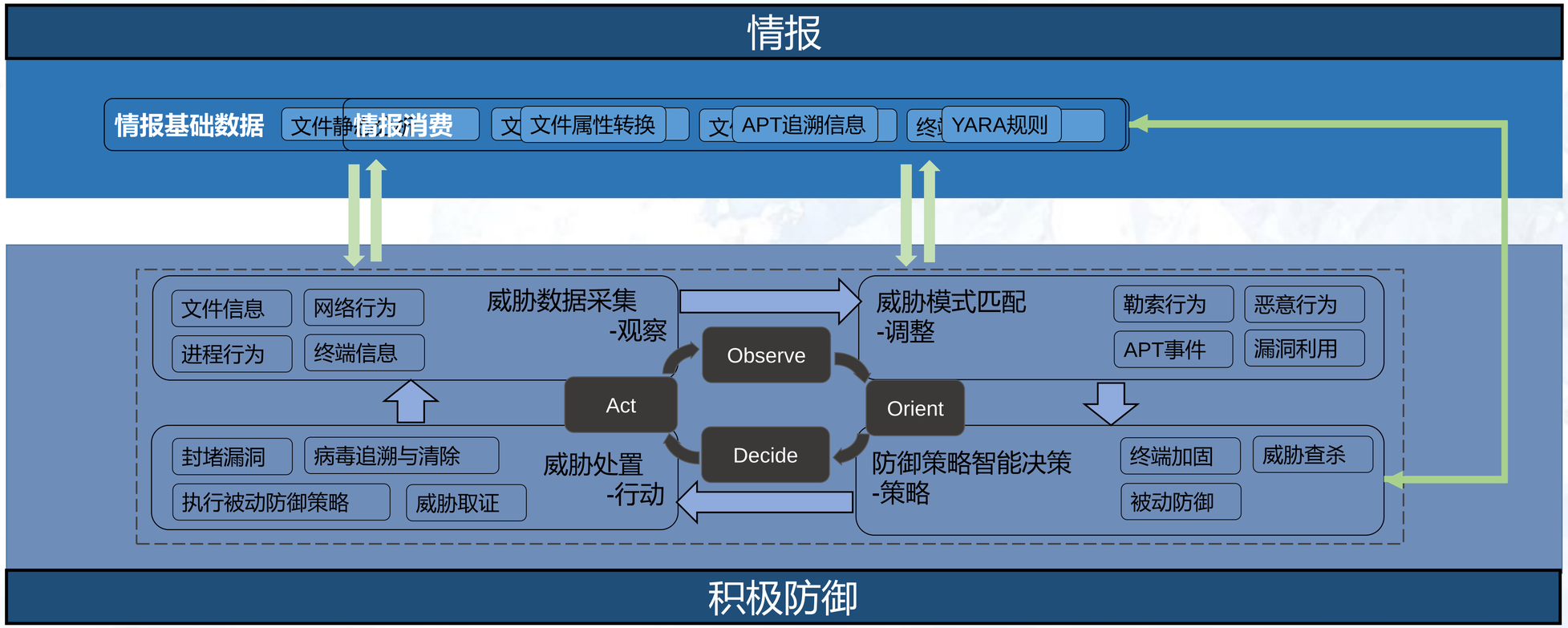
定义：分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程。



终端威胁防御体系——情报

基础架构安全 | 被动防御 | 积极防御 | 情报

定义：情报消费措施属于积极防御类别，但情报生产措施却属于情报类别。

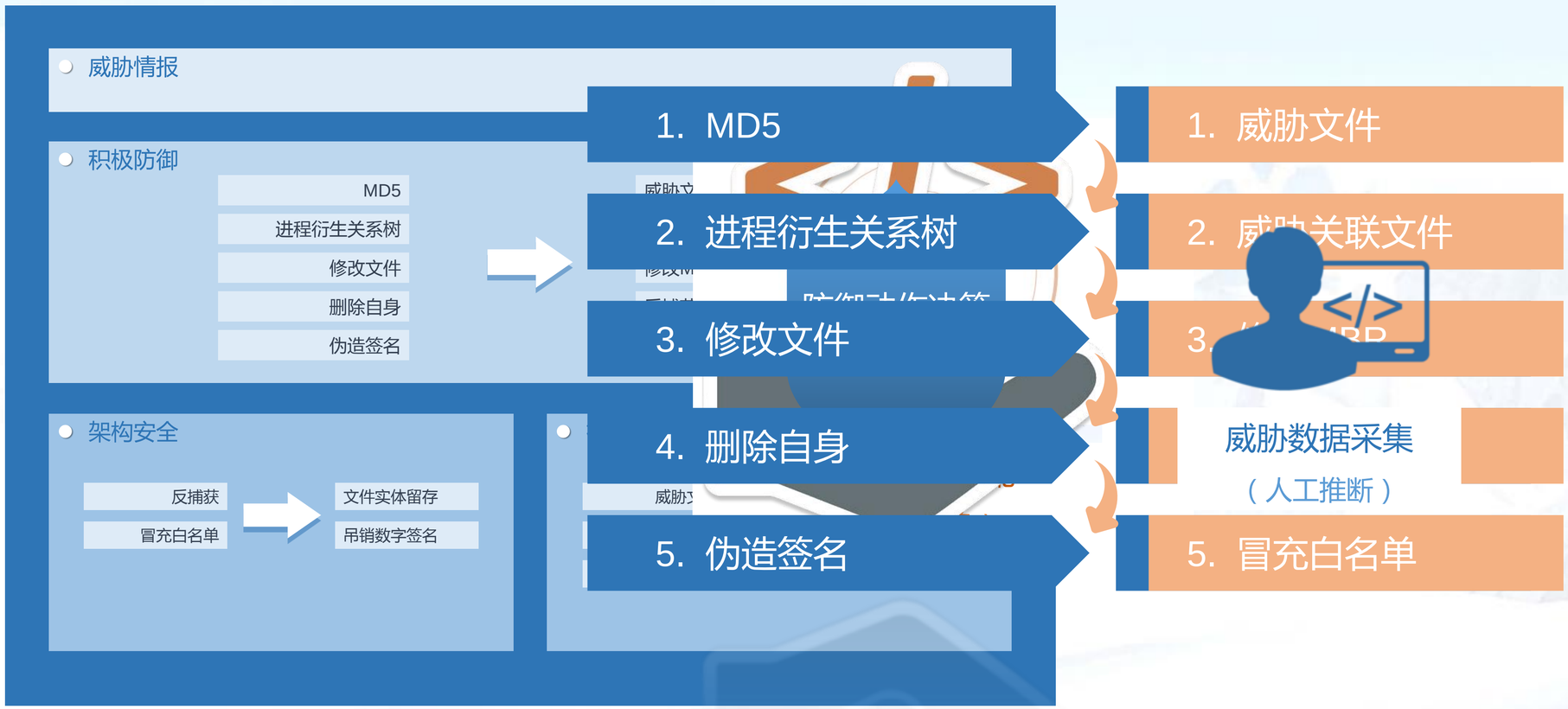


终端安全实战场景(1)--威胁情报驱动终端防御

- 应用威胁情报
- 威胁数据采集
- 威胁模式匹配
- 防御动作决策
- 执行防御策略

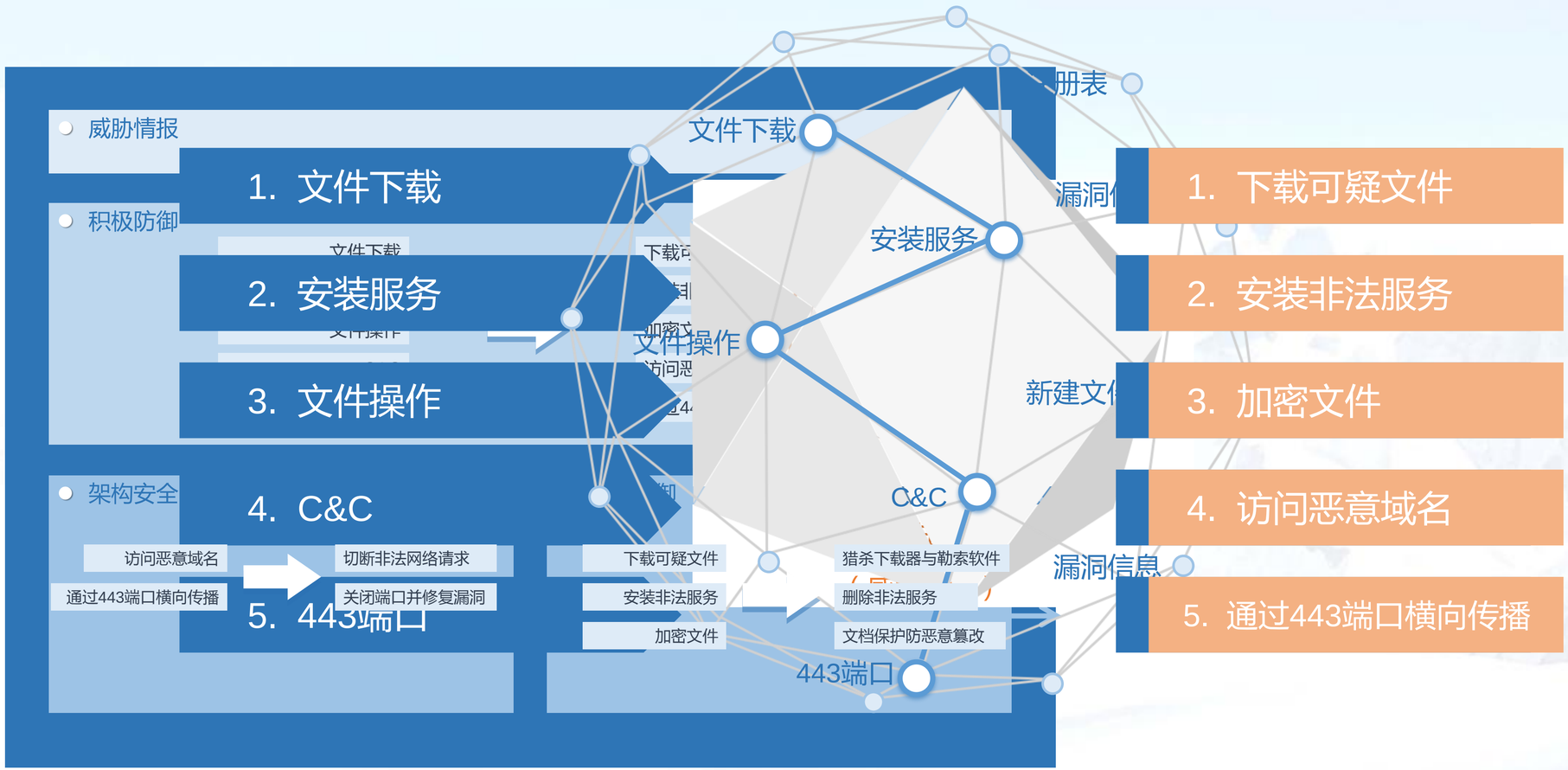
常规威胁处置模型

终端安全实战场景(2)--安全专职人员应对突发威胁



常规威胁处置模型

终端安全实战场景(3)--威胁大数据与AI驱动下的终端防御



- 海量数据采集
- 智能数据分析
- 威胁模式匹配
- 防御动作决策
- 执行防御策略

未知威胁识别模型

在实战场景，提供终端的有效防御

为何许多终端安全产品防御无效？

①多数防护软件还停留在黑白名单为基础的威胁检测方式，这种方式无法有效检测新型变种威胁。

②多数防护软件的行为检测局限于可执行文件，对文档文件默认放过监控。

③缺少针对勒索软件行为的持续深入的分析，无法准确区分勒索行为与正常文档操作行为。

智甲在不依赖病毒检测，不升级软件的情况下，可有效防御多数勒索软件。

*数据源自经测试85个家族的322个有效的勒索软件样本。

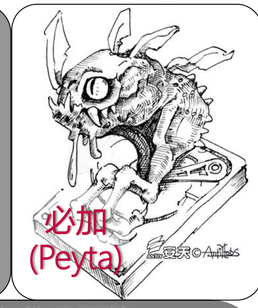
智甲的2016年10月版本可有效防御魔窟(Wannacry)。

安天在国内较早专门针对"勒索软件"发布分析报告并持续跟进。

2012年起

魔窟
(Wannacry)

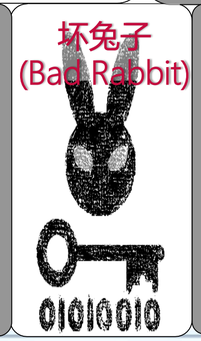
蠕虫
漏洞利用
开关域名
比特币
RSA+AES加解密
横向传播



必加
(Peyta)

蠕虫+邮件+下载器
权限提升
修改MBR
创建计划任务
RSA+AES加解密
横向传播

加密文件
修改MBR
添加任务计划
横向传播



坏兔子
(Bad Rabbit)

恶意软件
横向传播
漏洞利用
变种

伪必加(NotPeyta)

暗云III
(RainbowDay)

僵尸网络
DDoS
下载DLL文件
修改MBR

有效防护截图

智甲客户端界面

智甲可跨平台集中管理，覆盖全面的终端类型并与国产化适配

防护覆盖所有端点，端点防护产品不仅仅是反病毒产品。

智甲可跨终端、跨平台、跨系统进行统一管理。

智甲

通用操作系统

Windows 7 redhat

Windows 8 ubuntu

Windows 10 CentOS

Windows Server 2003 debian

国产化软硬件

中标麒麟 NeoKylin　银河麒麟 KYLIN　德 NFS-China

LOONGSON 龙芯

兆芯

专用终端

操作员站　工程师站

ATM终端

虚拟化平台

阿里云 aliyun.com

KVM

Xen Server™

vmware

移动终端

YUNOS

智甲终端防御系统的典型用户

监管部门	其他部委	能源	高校与科研	运营商	金融	其他
国家互联网应急中心	国税系统	国家电网某省公司	清华大学	中国移动	中国银联	CETC某研究所
国家计算机病毒应急处理中心	中国海关	中国石化	北京大学	中国联通	黄河银行	数据所
工信部通信管局	中华人民共和国水利部	中国石油	国防科技大学	中国电信	石嘴山银行	阿里云
国家信息安全漏洞共享平台	中国电子口岸	南方电网广西公司	哈尔滨工业大学		哈尔滨银行	上海商飞
北京公安、天津公安	昆明市财政局	华北电网	北京理工大学			铁路总公司

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

端点在，智甲的有效防护就在

关注安天冬训营官网

关注安天微信公众号

红旗漫卷

敌情想定是前提，网络安全实战化