SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

勒索病毒防御解决方案

深信服 安全BU

勒索病毒的发展和进化

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

AIDS木马
世界首例勒索病毒

1989

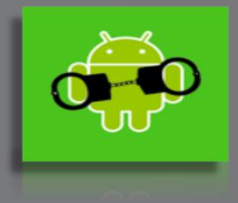
无特定目标
勒索手段粗糙

Archievus木马
首次采用非对称加密

2006

针对特定目标
难以解密、追踪
15年损失约3.15亿美元

LockerPin
首例安卓勒索软件



2015

WannaCry
军用级漏洞利用

2017

大规模破坏
损失2年增长15倍
勒索即服务（RaaS）
市场规模年增长 25 倍

利用机器学习
物联网设备
.....

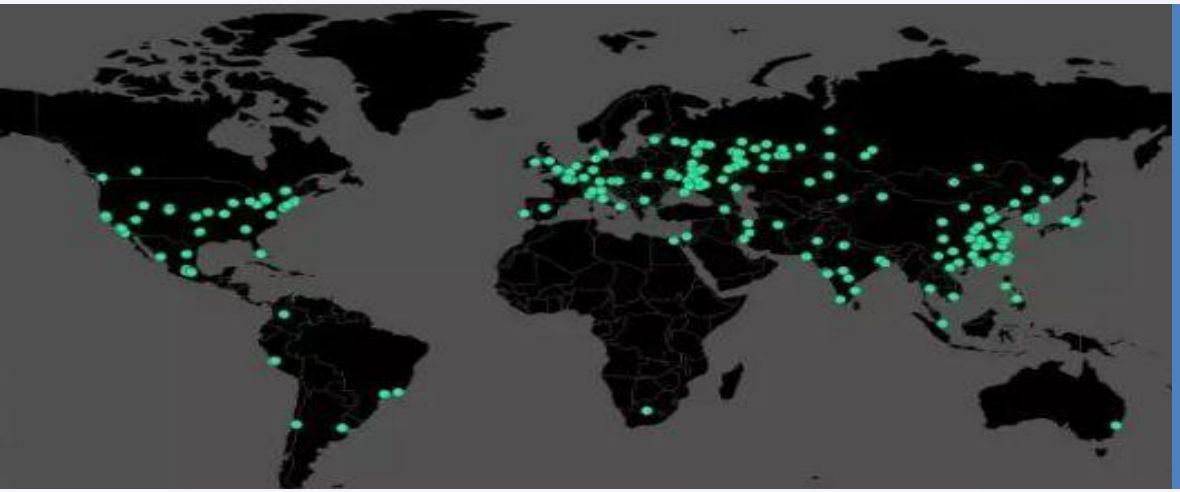
2019

每14秒一次勒索攻击
病毒数量指数级增加
损失将达到115亿美元

近期爆发的勒索病毒

序号	勒索病毒名称	发现时间	感染与传播方式
1	Cerber	2016年3月	Web漏洞+脚本注入
2	SamSam	2016年4月	网站漏洞、垃圾邮件，RDP爆破等
3	Crysis	2016年6月	钓鱼邮件+RDP爆破
4	Erebus	2016年9月	恶意广告
5	Wannacry	2017年5月	永恒之蓝漏洞、自我复制
6	BadRabbit	2017年5月	水坑站点+EternalRomance永恒浪漫
7	Satan	2017年1月	Web 漏洞+永恒之蓝
8	LockCrypt	2017年6月	RDP爆破，没有用到漏洞攻击和电子邮件等方式
9	Scarab	2017年6月	前期通过僵尸网络；后期：RDP爆破+人工、捆绑软件
10	Petya	2017年6月	钓鱼邮件+永恒之蓝
11	GandCrab	2018年1月	网站挂马、伪装字体更新程序、邮件、漏洞、木马程序等
12	GlobeImposter	2018年8月	社会工程、RDP暴力破解、恶意程序捆绑等
13	Planetary	2018年12月	垃圾邮件、RDP爆破
14	Attention	2019年5月	社会工程、RDP远程爆破等方式手动投放

感染与传播方式总结



勒索病毒需要传播植入到受害者主机的常见方式

钓鱼邮件

恶意代码伪装在邮件附件中，诱使打开附件
典型案例：Hermes、Petya
主要对象：个人PC

外到内

蠕虫式传播

通过漏洞进行网络空间中的蠕虫式传播
典型案例：WannaCry、Petya变种
主要对象：无定向，自动传播都有可能

横向

恶意软件捆绑

通过捆绑正常软件或恶意软件来分发勒索软件
典型案例：GlobeImposter
主要对象：个人PC

外到内

暴力破解

通过暴力破解RDP端口、SSH端口，数据库端口
典型案例： Matrix、Planetary、Crysis
主要对象：开放远程管理的Server

横向、外到内

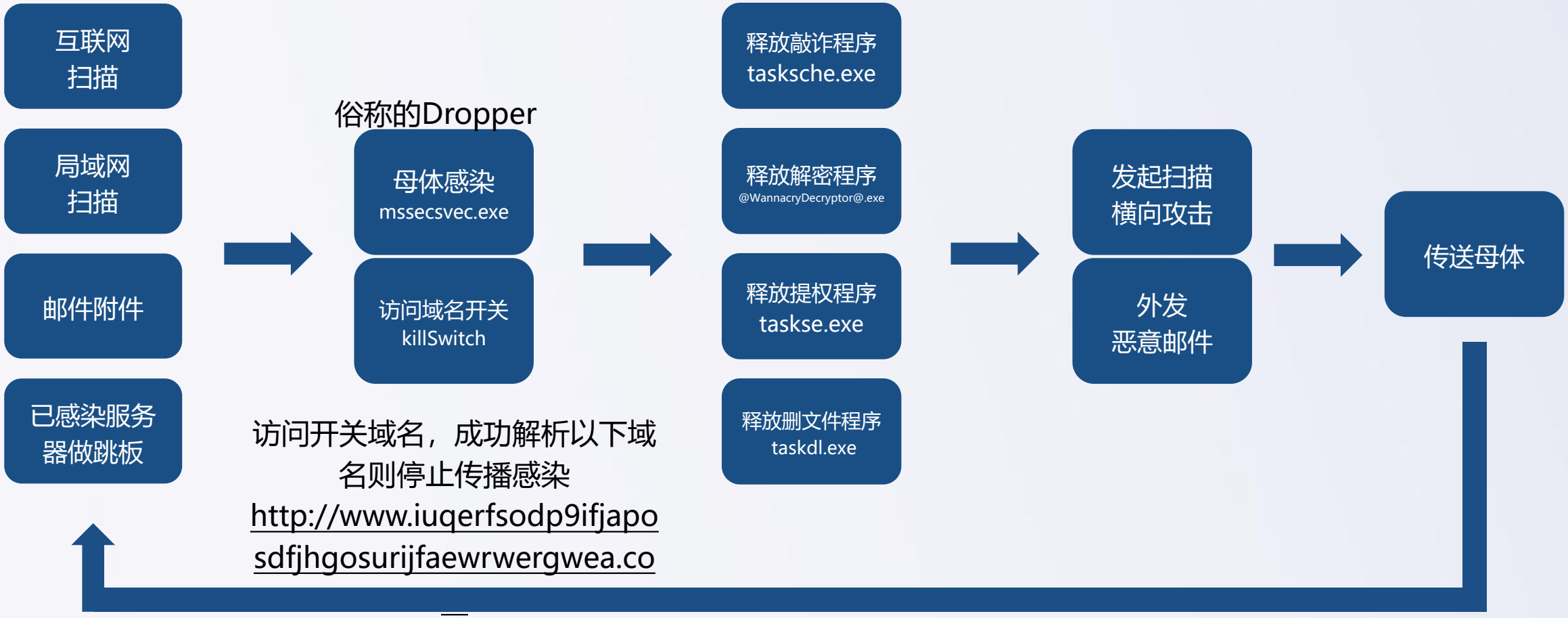
Exploit Kit分发

通过黑色产业链中的Exploit Kit来分发勒索软件
典型案例：Cerber
主要对象：有漏洞的业务Server

外到内

感染到传播的过程 组合方式一：泛感染+泛传播

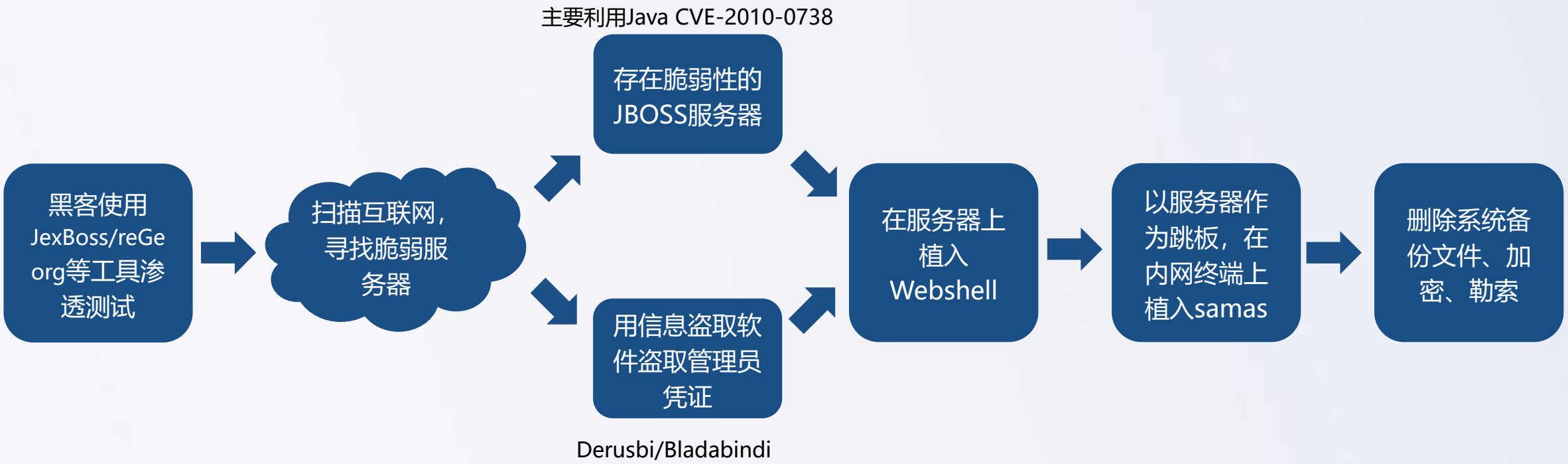
通过钓鱼邮件、恶意程序捆版、水坑站点等多种方式传播；内网感染后通过多种方式继续传播
典型代表：WannaCry、 GlobeImposter、 GandCrab | 影响力排前三的均属于这一类



案例一：WannaCry工作机制

感染到传播的过程 组合方式二： Web漏洞攻击+持续渗透

以服务器作为跳板，利用web应用系统漏洞植入Webshell，再进而定向持续渗透或广播式的感染内部主机
典型代表：Cerber、Satan、Samas、SamSam、Jcry、Lucky等



案例二：samas/SamSam工作机制

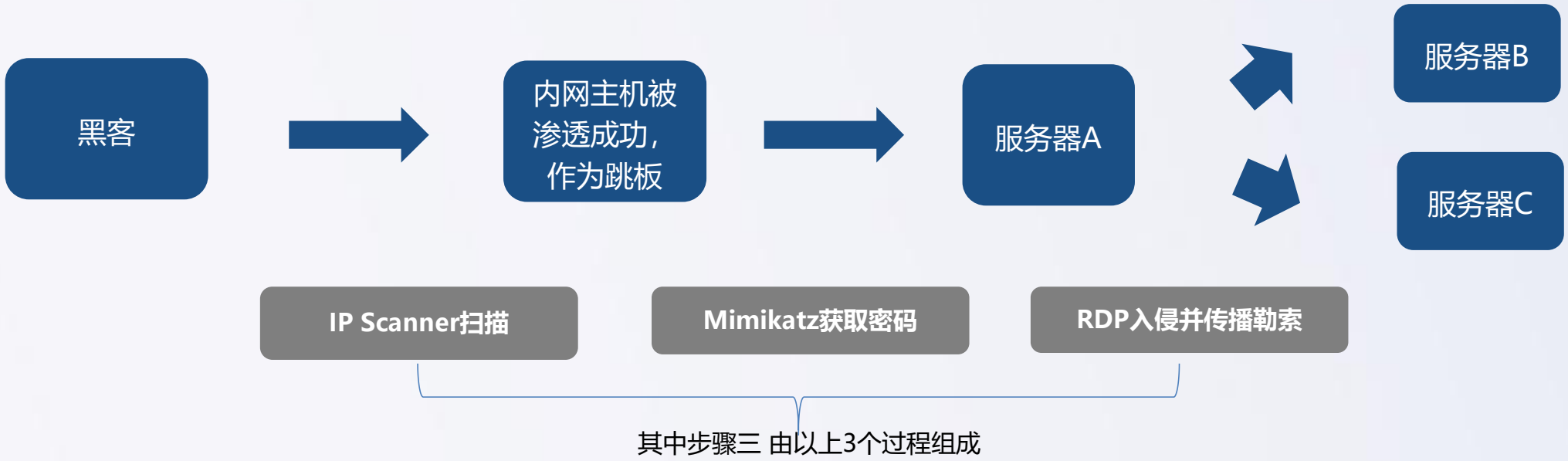
感染到传播的过程 组合方式三：RDP爆破为主的感染控制

先通过钓鱼邮件/钓鱼网站再RDP爆破，或者直接RDP爆破
典型代表：LockCrypt、 Crysis 、Planetary、GlobeImposter等

步骤一：
黑客通过钓鱼等方式控制主机

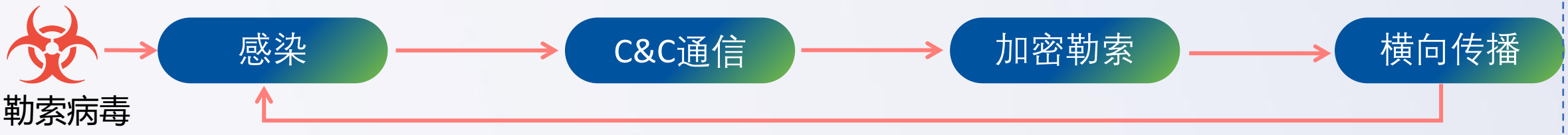
步骤二：
RDP爆破

步骤三：
使用服务器A的密码，
通过RDP入侵其他服务器



案例三：LockCrypt勒索病毒工作机制

传统勒索病毒防护方案失效的根因分析



第一步

外网到内网的传播

- 钓鱼邮件/水坑站点/捆绑下载
- Web漏洞利用
- RDP爆破
- U盘传播

第二步

安装与C&C通信

- 下发提权程序
- 下发勒索加密密钥
- 下发操作指令
- 宿主信息提交上传

第三步

漏洞利用提权/加密勒索

- 执行提权程序
- 执行加密程序
- 勒索弹窗或直接破坏

第四步

横向持续扩散

- RDP爆破
- 蠕虫式传播
- 系统漏洞利用传播

技术难点

钓鱼邮件难检测

C&C通信加密难检测

代码高度混淆难检测

慢速扫描难检测

单点防御型：仅作用以上过程的某种方式，若突破或绕过防御则满盘全输，病毒一旦进入内网可通过多种方式快速横向扩散

产品驱动型：未从勒索软件生命周期的原理，分析作用于哪个传播环节，说不清产品的实际价值

事后恢复型：作用于加密勒索破坏后，已经影响业务，仍需解决已进入内网中的病毒，依然需要建立有效的防护手段防止再次感染

深信服解决思路：风险驱动、立体保护、主动防御

产品驱动 ✗

风险驱动： 围绕勒索软件生命周期形成防护方案

- 围绕“感染、C&C通信、加密勒索、横向传播“威胁全过程分析
- 有效解决技术难点，如隐蔽通信、混淆代码难检测、慢速扫描等

单点保护 ✗

立体保护： 云、网、端、管理各个层面进行防护

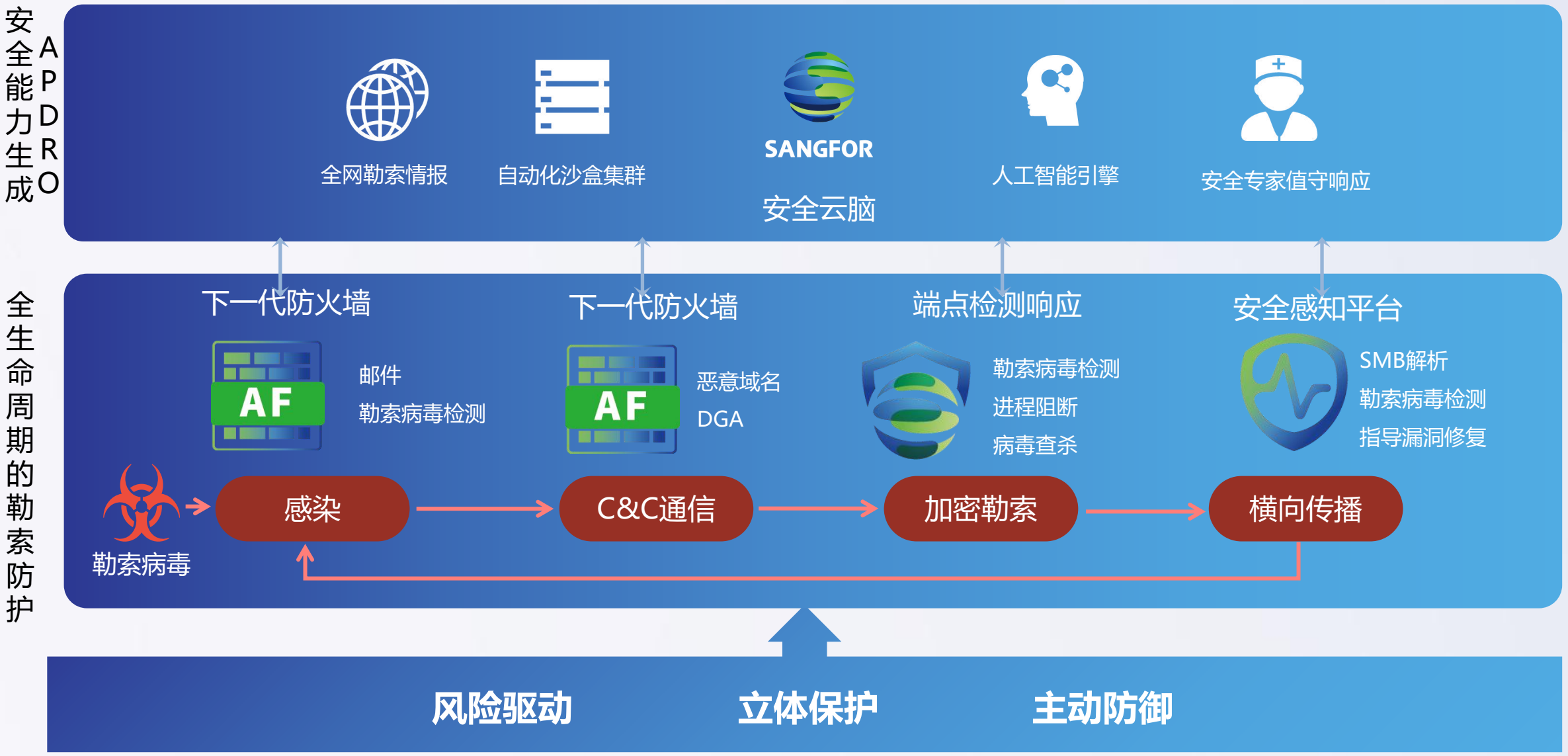
- 实现对内连威胁、外连威胁、内部横向传播的立体检测和响应
- 实现“网络流量行为异常+终端文件行为异常”组合关联分析
- 技术和管理结合，提前安全加固，提高安全意识

事后恢复 ✗

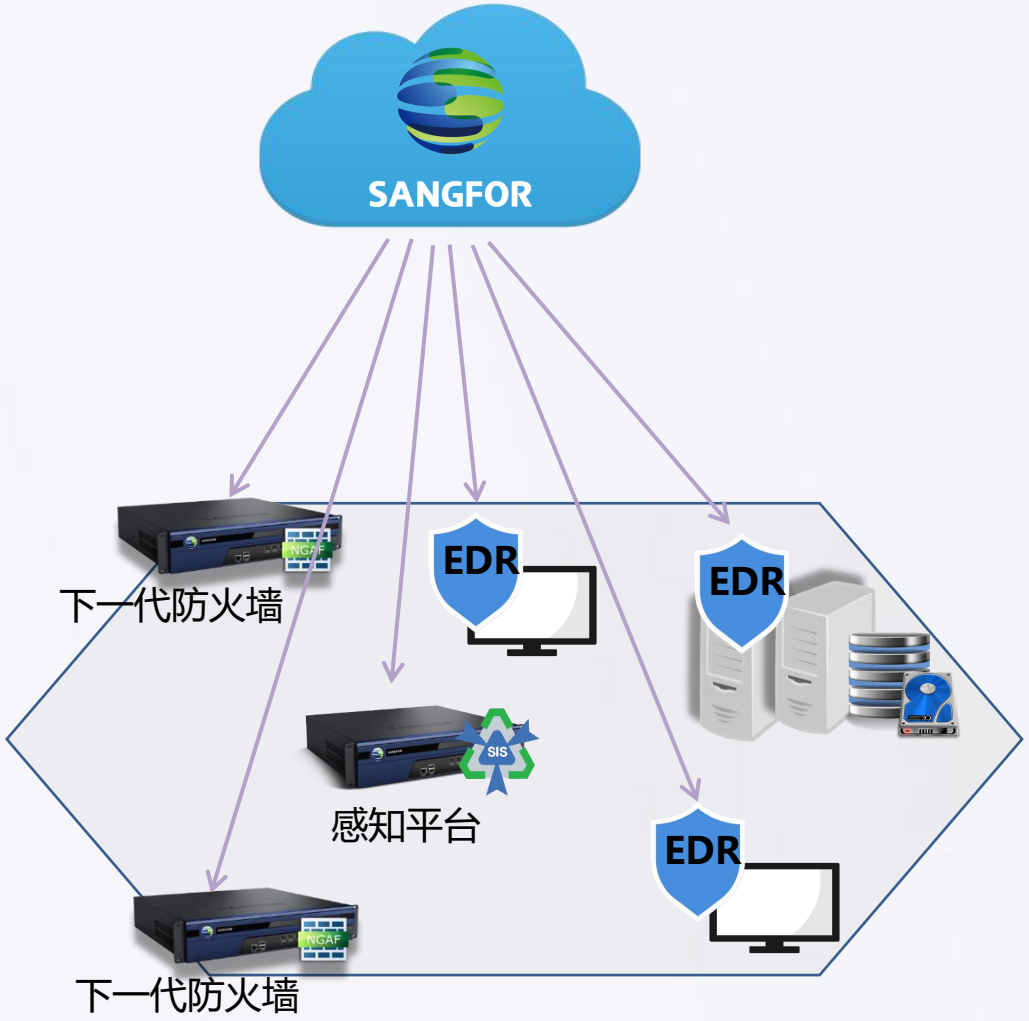
主动防御： 持续威胁监测、预警和响应

- 在威胁进入前 提前安全预警，在隐患利用前 提前修复漏洞
- 在横向扩散前 提前隔离控制，持续可视化监控快速锁定感染源

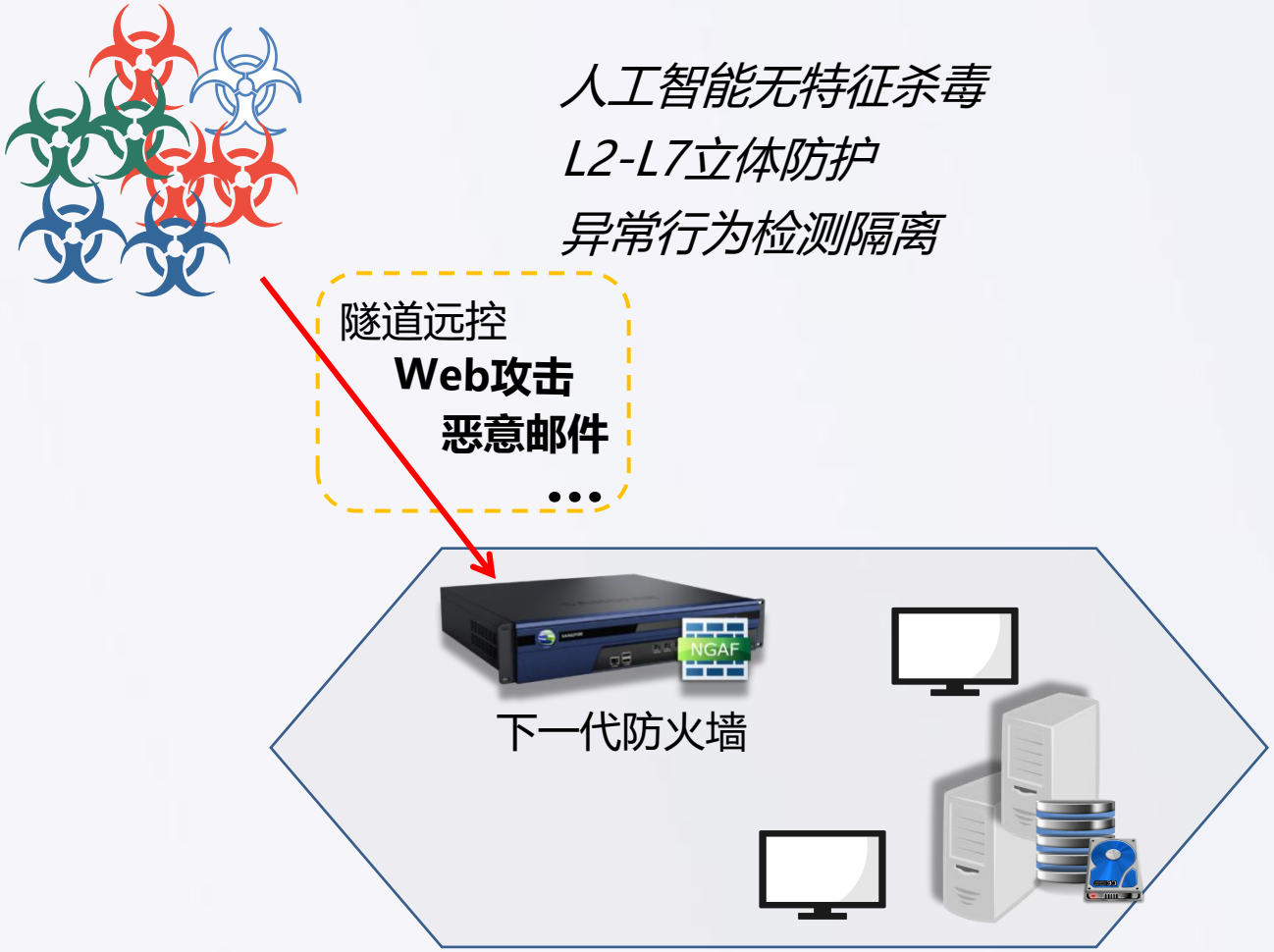
深信服勒索病毒风险防护方案



勒索情报、检测算法、防护策略下发

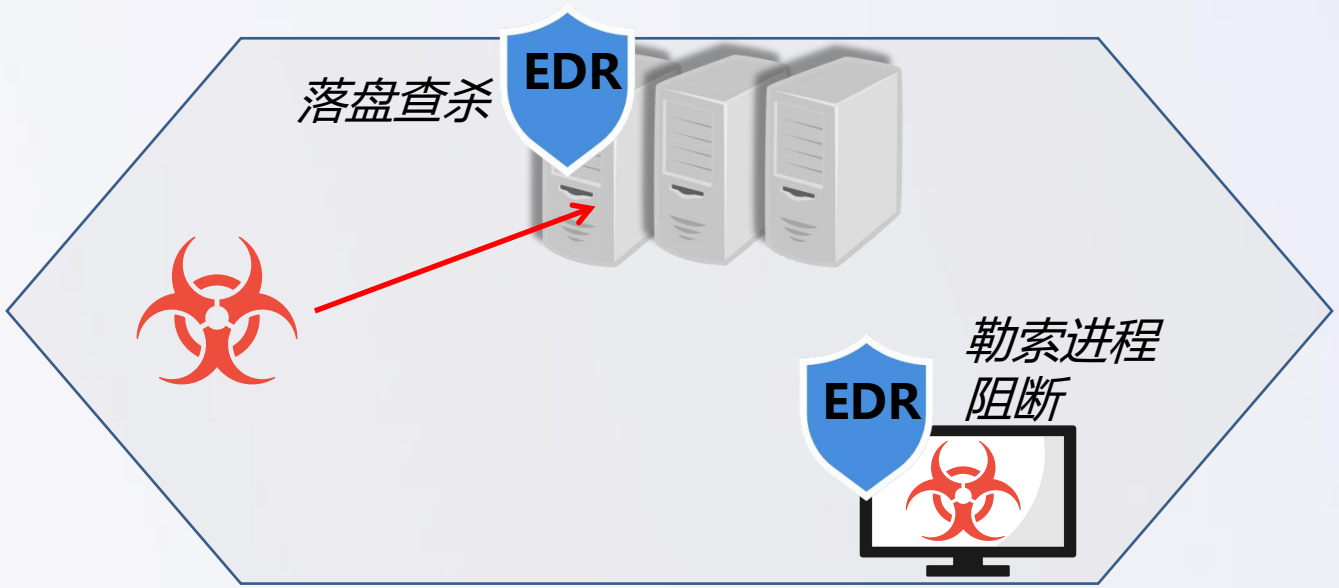


基于下一代防火墙的智能立体防护



- L3 拦截c&c远控恶意IP
- L4 阻断高危端口通信
- L7 拦截恶意邮件、web入侵、高危程序等
- 未知威胁云端实时分析

基于EDR的终端防护



- 端点检测响应，落盘即查杀
- 集成SAVE引擎、多维行为分析、及时判别勒索程序
- 未知威胁云端协同实时分析，实时获取云端最新检测能力

基于感知平台&防火墙持续检测能力的主动防御

- 感知平台实时关联分析网端数据，通过攻击链锁定威胁范围
- 基于分析结果及时下发策略到AF阻断外联通信,下发到EDR阻断横向传播
- 感知平台全网流量行为学习，通过大数据关联分析定位隐藏威胁

构建高效的勒索病毒防护体系

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

全球威胁情报共享中心 | 云端大数据智能分析中心 | APT检测云服务

网页恶意代码（http） 黑客 邮件病毒

Internet

①云端威胁情报实时同步，快速应对新型威胁

②下一代防火墙，融合的边界防护，一键阻断，智能封锁外部IP

④依据"安全云脑和感知平台分析的结果"阻断C&C外联

安全感知平台（SIP）

安全管理区

STA 潜伏威胁探针

⑤安全大数据平台持续监测全网异常， DGA隐蔽信道分析&攻击链分析&行为异常分析等，快速定位和响应处置

③端点安全EDR，落盘查杀、终端行为异常检测、微隔离

AF

APP VM aSAN EDR

数据中心区

办公区

分支区

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

核心技术优势

强大的企业级威胁情报库，提前预警

攻关技术难点：勒索程序制作成本低、变种多、传播范围广、破坏程度大；企业需要具备足够的企业级威胁情报数据和基于大数据的AI训练算法，来快速检测新型未知勒索程序。

威胁情报	检测效果（持续增强）
• 1亿+文件样本 • 2亿+文件HASH • 2000w+域名/URL/IP信息	• 每月1亿次+的僵尸网络查杀 • 每月1000w+的恶意链接查杀 • 每月1亿次+的文件云查

案例解析：

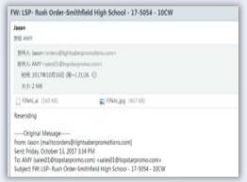
- 2019 年 3月，大连市某局内网服务器及多台终端遭到挖矿病毒攻击，将病毒样本送入云端鉴定引擎，分钟级判黑；经分析，**该病毒是国内外首例集成了众多免杀技术的WannaMine病毒**
- 提取的病毒相关特征录入安全云脑中形成威胁情报后，**发现深圳市xx人民医院、 xx酒店集团股份有限公司和xx汽车有限公司等1000多个客户也受到影响**，有效阻止病毒利用服务器主机挖矿和病毒的进一步扩散

利用人工智能实现“未知”到“已知”；利用“威胁情报”快速扩大“已知”范围

基于AI的融合邮件检测与拦截

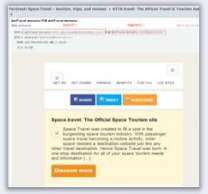
攻关技术难点：传统沙箱或者防病毒网关以对“附件内容”检测为主，由于勒索感染过程所使用的恶意链接、伪装发件人邮箱、邮件传输行为等难以和正常情况进行分区，往往被忽略不作检测。深信服采用AI技术，通过机器学习广泛训练检测算法来识别勒索行为。

钓鱼邮件



病毒邮件

垃圾邮件

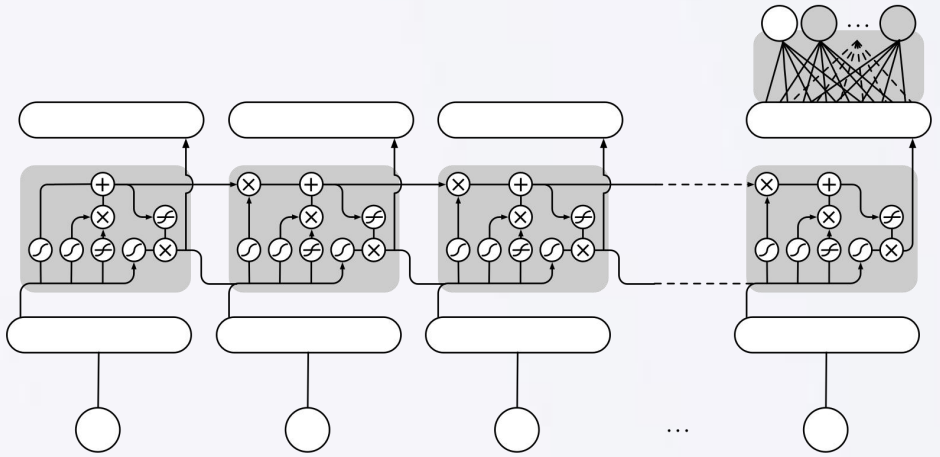


鱼叉式钓鱼

有效应对勒索感染过程

基于AI的C&C通信检测与阻断

攻关技术难点： DGA(域名生成算法)是一种利用随机字符来生成C&C域名，从而逃避域名黑名单检测的技术手段。**深信服感知平台采用LSTM循环神经网络（RNN）算法，学习人类记忆的过程，通过来记忆的上下文语意的合理程度判断是否为异常行为。**DGA检测就是供给大量的训练数据给LSTM算法，算法会通过自己记忆过的上下文信息判断一个域名是否正常，类似人类记忆事情的原理。



长短期记忆神经网络

Long Short Term Memory Network（LSTM）

4.18 、10.0.202.3（未处理）

该用户失陷确定性为高可疑，威胁等级为中威胁

所处威胁活动阶段为 C&C 通信

该用户共检测到 1 个高可疑事件，以下是按失陷确定性排序 TOP10 的事件举证：

事件 1	主机多次访问疑似恶意软件特定家族的 DGA 域名		
失陷确定性	高可疑	威胁等级	中威胁
举证	其中 100.0%（13 个）属于 other_dga 家族恶意软件，访问的域名（TOP10）：ihq8jj1vcytnk7f9eay4.com，eoeqwi8r8vscqnobo.com，0salgryv9egrxcqiajd.com，pylzmo6xwebp0my5t9wqoad096.com，c8pkfl7q2pmb0skecb5pd2080.com，xm9x77bzz8wtfb57zivcgmw.com，ry0wpefd1uocjh3oazv1z46rhs.com，woarvmgwodq5qypwigqp4x.com，p3wn2cjc4xdk98t3zb13ke.com，nkn5gn9ba6obo4tkdwgdc9.com；		

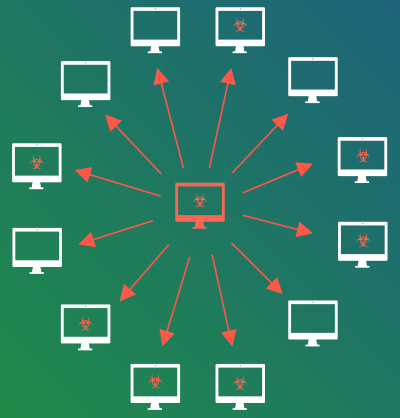
通过LSTM技术在“能否检测出C&C通信”问题上达到99.7%的精确度

在“检测出具体是哪一个家族”的问题上达到了平均90.3%的精确度

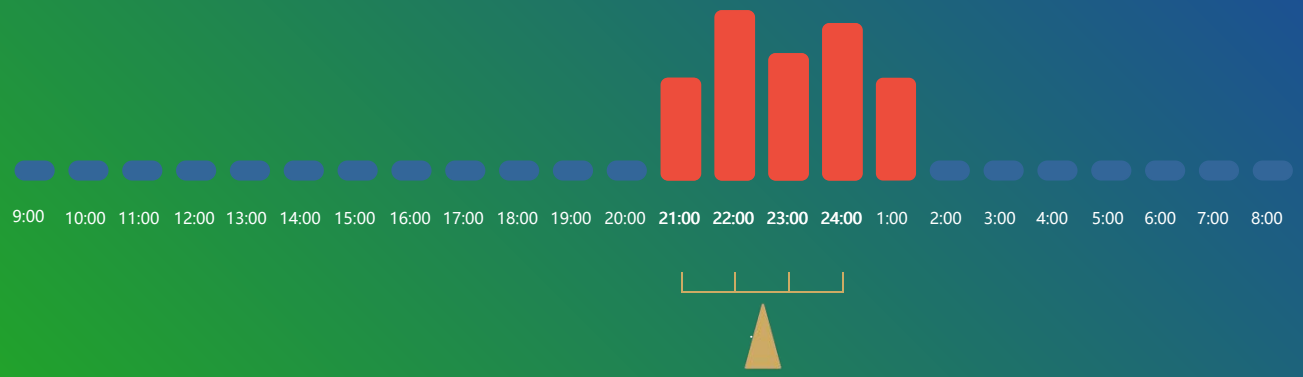
在某省建筑设计院发现的新型的DGA病毒家族

确认为新型勒索软件“狮鹫”

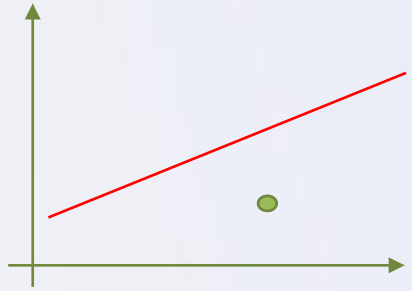
基于机器学习的慢速扫描检测



攻坚技术难点：横向传播过程中勒索软件会主动发起扫描攻击，寻找感染目标。扫描时在流量上会呈现出波动。传统的基于阈值的检测方法可以一定程度上检测出扫描流量。但，新型的扫描攻击更聪明，把扫描行为分散在各个时间段里，即慢速扫描，这种方式能成功避开阈值方法的检测。



使用增量式机器学习技术，将主机行为转化成空间中的特征向量（点）。点在模型（红线）下方时，表示判定主机无扫描行为；在模型（红线）上方式，表示判定主机存在扫描行为。



技术优势

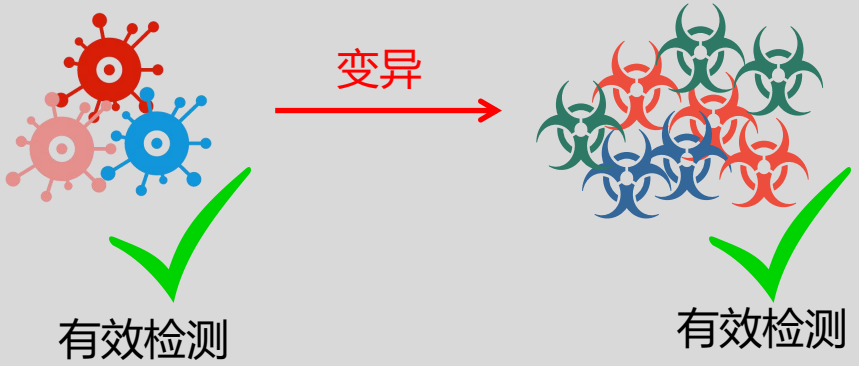
- **能检测出慢速扫描（传统方法无法检测）**
- **极小的性能开销，新的数据来了，只需更新点的位置**
- **数据红利，参与的数据越多、时间越长，检测结果越准**

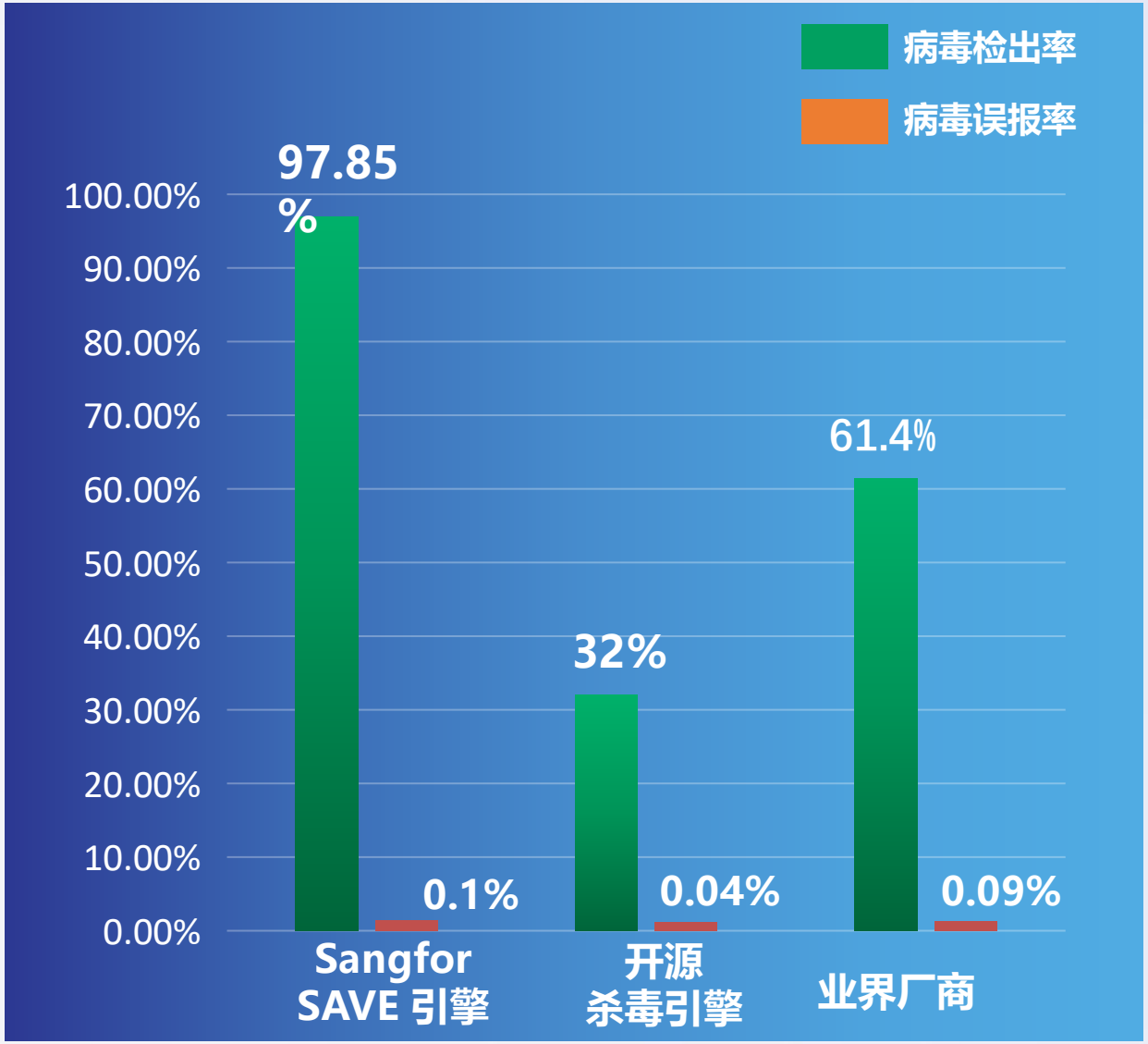
基于AI的恶意（勒索）软件检测与隔离

攻关技术难点：基于”特征或字节”的检测技术难以识别勒索新型变种，尤其是被特殊改造高度混淆后的勒索程序。

深信服人工智能杀毒引擎SAVE
Sangfor Anti-Virus Engine

人工智能无特征技术
准确检测未知病毒

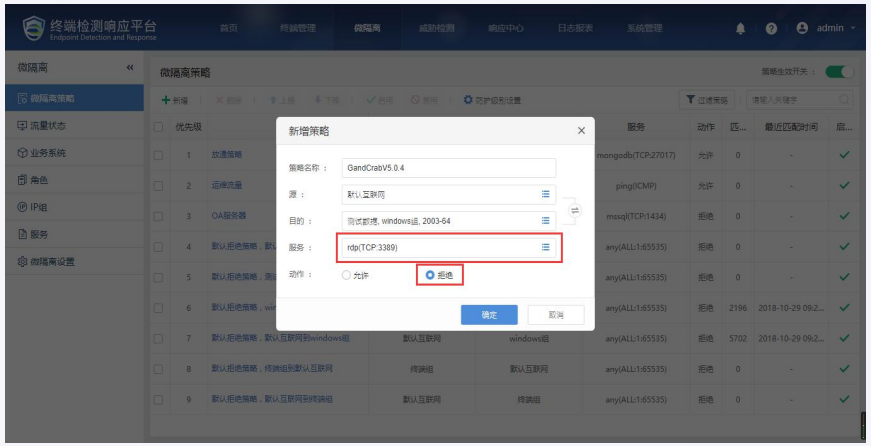




东西向微隔离与风险控制

攻关技术难点：a、虚拟化场景下，勒索病毒传播不可视、东西向传播快；b、EDR分为云主机版和物理主机版，两套管理平台难以统一管理。

深信服采用EDR云主机版不仅可以实现虚拟场景安全可视和东西向微隔离，还支持一套管理平台兼管所有部署场景。



横向传播路径可视

自动编绘完整的业务流量拓扑图，并通过交互式设计，提供针对流量和策略更加方便的钻取和控制能力

灵活的东西向控制

必要时可通过策略控制高危端口的使用，如3389、445、139等，支持按租户和业务域进行安全隔离

感染主机快速控制

通过安全自查快速定位感染主机；支持管理平台统一处置，支持AF/SIP联动隔离处置

底层虚拟化解耦合

支持公有云、私有云、混合云，适配包括Vmware、OpenStack、Hyper-v、超融合等所有云平台

国内领先的恶意软件研究与响应支撑团队

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

KrakenCryptor2.0.7勒索变种来袭!

警惕GandCrabV5.0.4勒索病毒，医疗行业已有中招案例

预警：SamSam勒索病毒最新变种来袭

Blackout勒索病毒再度来袭

揭秘勒索界海王如何横扫中国

预警：新型Sigrun勒索病毒来袭

预警：通过知名远程桌面工具传播的BlackRouter勒索病毒

BlackHeart勒索病毒再度来袭

FilesLocker2.1圣诞特别版勒索病毒与早期版本解密工具

Petya勒索病毒详细分析

GhostPetya骷髅头勒索病毒袭卷半导体行业，深信服率先推出解决方案!

Satan勒索病毒最新变种预警

紧急预警：GlobeImposter勒索最新变种爆发，用户怒怼黑客!

冒用有效签名：Clop勒索病毒这股”韩流“已入侵国内企业

Matrix勒索病毒PRCP变种侵入政企单位，警惕中招

预警：CrySiS勒索病毒变种再度来袭

勒索软件变种来袭，你的数据安全防护该升级了

还原最新勒索病毒GandCrabV5.0.3的完整攻击场景

注入型勒索病毒Ryuk，伸向x64系统的魔爪

警惕！一款注入型勒索病毒Ryuk，拉开2019年勒索病毒攻击的序幕

PowerWare：勒索软件如何温柔地借刀杀人

【附专杀工具】WannaCry变种来袭，勒索变蓝屏

”天堂“竟然伸出恶魔之手？Paradise勒索病毒再度席卷

CrySiS勒索病毒变种来袭，你中招了吗?

千里传音--勒索软件 | 第1期

SamSam勒索病毒变种预警

利用Telegram通信的勒索病毒Vendetta，你有见过吗?

勒索病毒攻防演练

当心穿VB马甲的新型勒索病毒Tater!

GlobeImposter勒索样本分析报告

变种入侵？keqiCryptomix勒索病毒最新变种预警

警惕！你下载的软件可能携带STOP勒索病毒变种!

预警：GandCrabV4.0勒索病毒来袭

预警：Scarab勒索病毒变种来袭

追踪Satan勒索病毒家族

Scarab勒索病毒最新变种，希特勒“冠名”

统一的RDP弱密码有多危险？CrySiS勒索分分钟搞瘫大片业务

预警：GlobeImposter勒索在国内爆发

Xbash勒索挖矿样本分析

勒索病毒GandCrabV5.0最新变种来袭

！有效！深信服率先发布Oracle数据库勒索病毒自检工具

CTB-Locker for Websites：首款专门针对 Web 网站的新型勒索软件

警惕Rapid勒索病毒新变种

一款伪装成docx文档的新型勒索病毒PyLocky，谨防误点!

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

THANK YOU