C3安全峰会
CYBER | CLOUD | COMMUNICATION

New generation terminal security driven by AI engine

AI引擎驱动的新一代终端安全

汪晨
终端安全产品总监

C3安全峰会
CYBER | CLOUD | COMMUNICATION

亚信安全成功抵御全球第一只勒索蠕虫WannaCry

5月12日 15:00
亚信安全接到第一起某省级运营商的报案

5月12日 15:10
亚信安全即时向全国用户发布预警&措施

5月12日
确保所有用户产品配置到位免受威胁

5月13日
亚信安全与四川公安共同发布勒索病毒预警

5月13日
亚信安全与国家计算机病毒应急处理中心推荐用户下载专杀工具

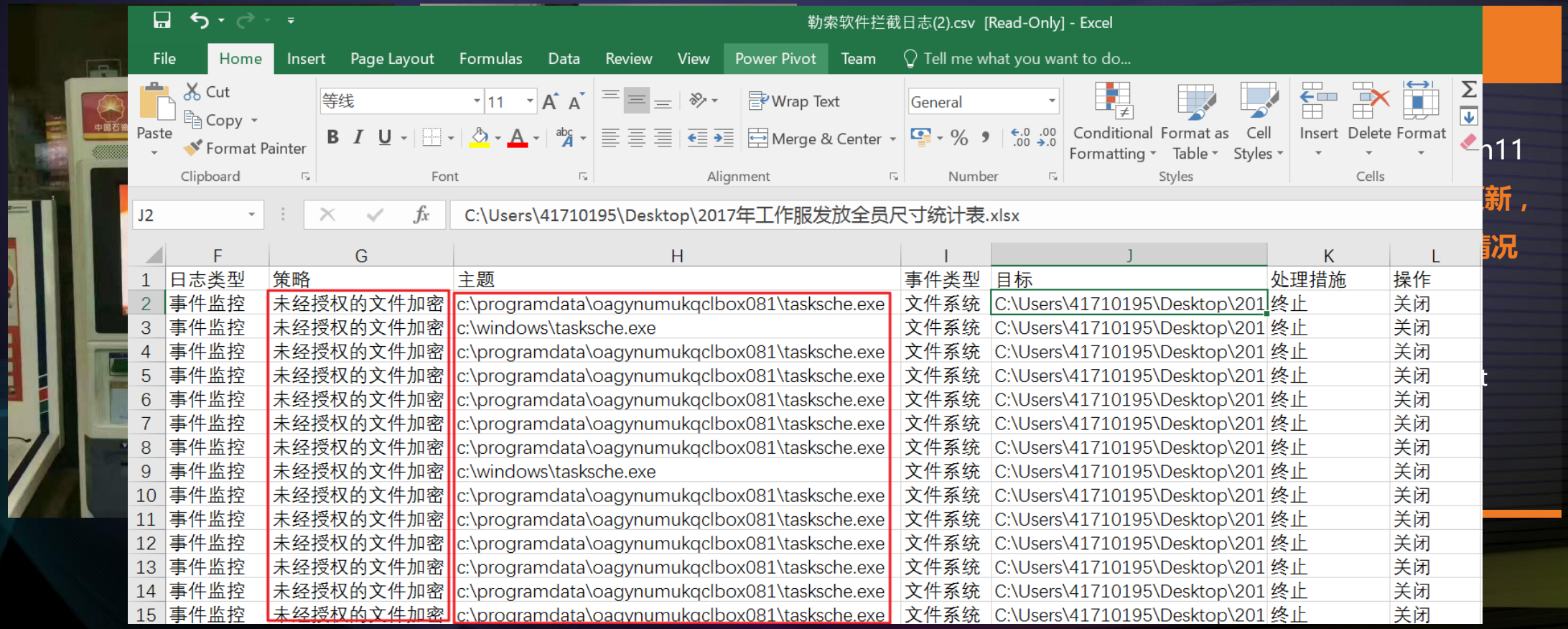
5月13日
为运营商/公安/学校/医院/银行等>100家客户提供现场PSP服务，确保所有客户免遭勒索

5月14日 24:00
再次确认所有部署亚信安全officeScan 11 SP1的用户全部幸免WannaCry的勒索

C3安全峰会
CYBER | CLOUD | COMMUNICATION

亚信安全成功抵御全球第一只勒索蠕虫WannaCry

上海某电站启用OfficeScan 11行为监控功能后，成功防御了WannaCry勒索加密行为



	F	G	H	I	J	K	L
1	日志类型	策略	主题	事件类型	目标	处理措施	操作
2	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
3	事件监控	未经授权的文件加密	c:\windows\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
4	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
5	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
6	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
7	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
8	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
9	事件监控	未经授权的文件加密	c:\windows\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
10	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
11	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
12	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
13	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
14	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
15	事件监控	未经授权的文件加密	c:\programdata\oagynumukqclbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭

基于特征码比对的一代技术

根据已知样本生成特征码

技术

病毒引擎+病毒库

手段

效率高，毫秒级别的发现能力

优势

滞后

局限性

全，快，准

竞争优势

早期恶意程序
T700

亚信安全共享全球数据，已知恶意软件的数量和种类更全，获取样本速度更快。25年的病毒处理技术，流程和经验，能够快速制作出极低误报率的特征码，并快速部署，从而领先绝大多数厂商提前更新。

基于行为分析的二代技术

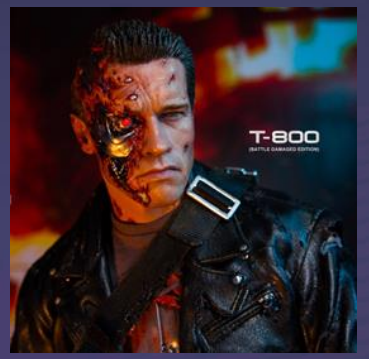
技术：根据已知行为规则拦截恶意软件

手段：沙盒，行为分析

优势：在无特征码情况下拦截未知的恶意软件

局限性：利用预设的行为规则聚焦于某些恶意攻击，如勒索和APT

竞争优势：技术实力，联动，恶意行为规则库，误报率



加了伪装的恶意程序
T800

亚信安全OSCE 使用 AEGIS 内核级别的行为分析引擎，从最底层Hook来监控软件的行为，使用多年累积的规则库来匹配，并通过全球海量的云数据来消除误判。OSCE和TDA等其它亚信沙箱产品实现联动，可自动获取沙箱恶意软件情报，也可主动提交可疑样本，利用联动实现终端及时防护。

基于机器学习的三代技术

技术：通过大数据训练，使用机器学习算法， 通过文件DNA和执行行为的意图进行判断

手段：AI-机器学习引擎

优势：快速发现未知的恶意软件

局限性：无法识别缺乏训练样本的恶意软件，误报率

竞争优势：数据量，恶意软件特征处理经验，技术能力，误报率

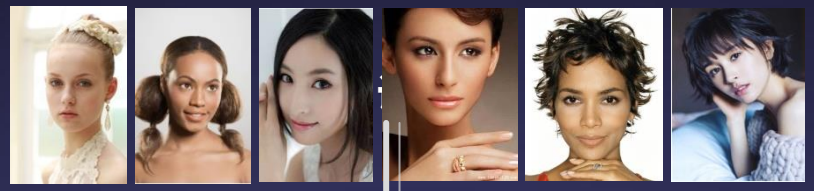
能变形的恶意程序
T1000

亚信安全OSCE 使用全球不断累积的海量样本训练数据，10年磨砺的机器学习算法，25年恶意软件处理经验，提供识别率最高的静态和动态双重机器学习引擎。同时，海量的好文件样本学习与云数据的统计算法保障极低误报率。

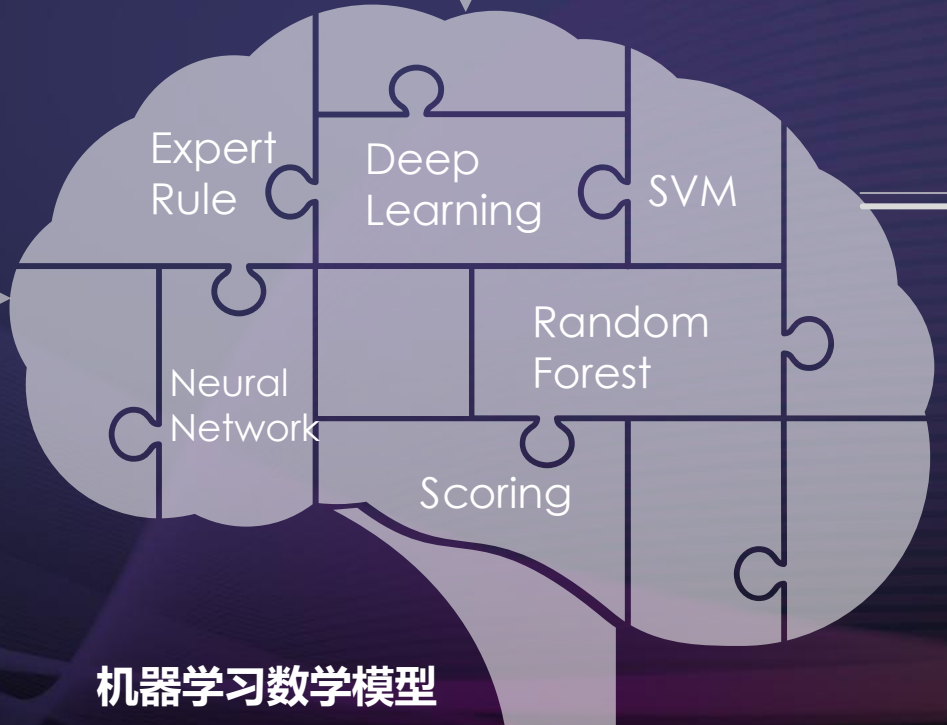
亚信终端安全解决方案

「持续战斗25年」

AI引擎使用的机器学习技术介绍



未知人种DNA



机器学习数学模型

预测

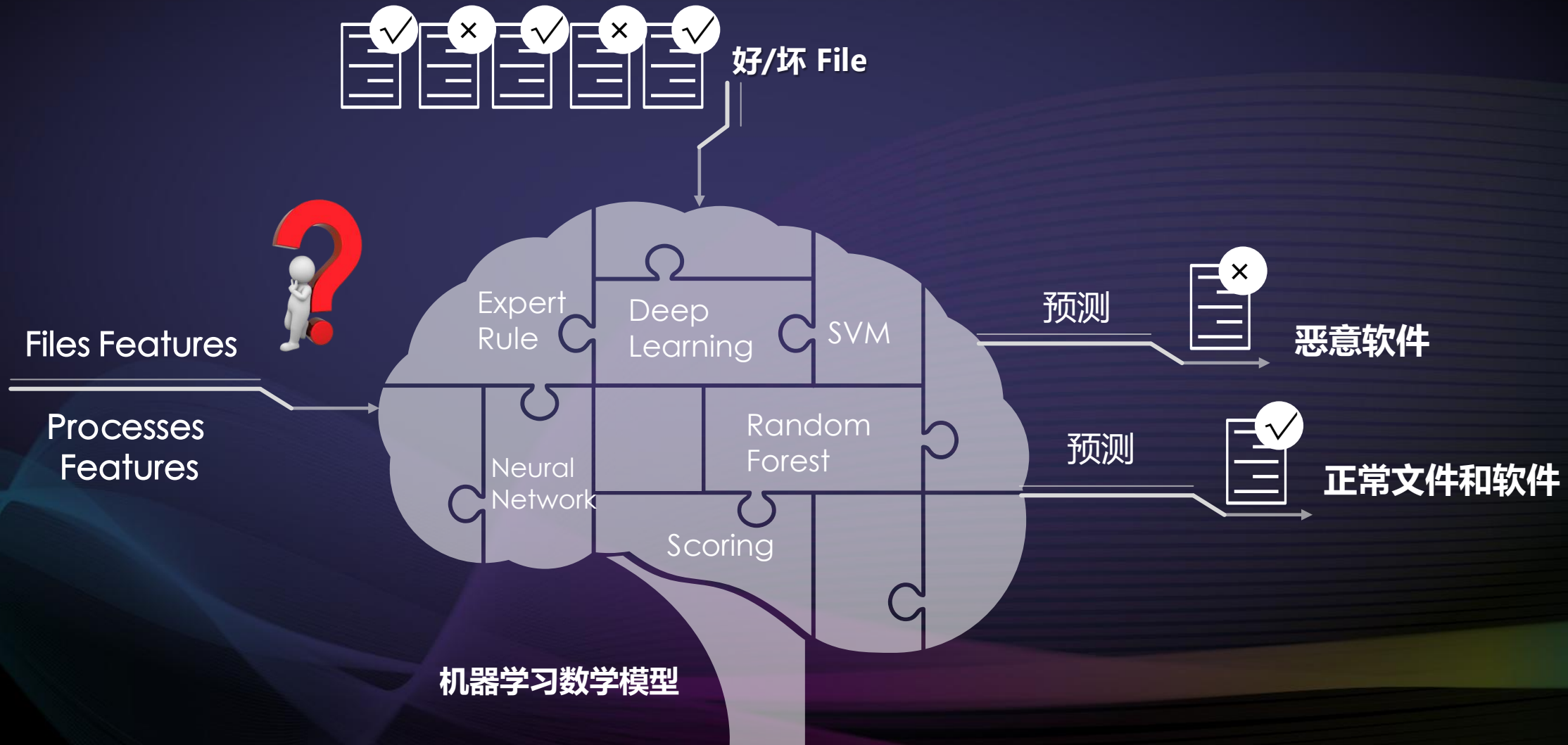
白种人

黑种人

黄种人

AI引擎使用的机器学习技术介绍

「亚信安全使用被训练过的机器学习模型可以预测未知的文件是否是恶意软件还是正常文件」



机器学习过程

训练机器学习的数据量和文件特征处理的能力最重要

100TB/天
50万新恶意软件/天
10亿白名单

海量

数据

全球数据，交给机器学习的恶意软件和正常文件的样本数量最多，种类最全

精准

特征

25年以上恶意软件鉴别知识和技术的积累，更精准的定义和优化恶意软件的特征

算法

算法

10年以上机器学习算法技术积累

轻简

模型

高精准,低功耗双重机器学习威胁检测模型

机器学习文件特征示列-特征可视化处理

C3安全峰会
CYBER | CLOUD | COMMUNICATION

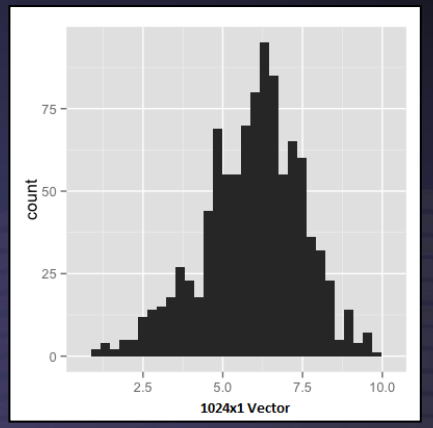
特征集1 Opcode（CPU操作码）

```
00453820  $  60          PUSHAD
00453821  .  BE 00604400  MOV ESI,35fb2dae.00446000
00453826  .  8DBE 00B0FBFF  LEA EDI,DWORD PTR DS:[ESI+FFFBB000]
0045382C  .  57          PUSH EDI
0045382D  .  83CD FF     OR EBP,FFFFFFFF
00453830  .v EB 10       JMP SHORT 35fb2dae.00453842
```

PUSHAD MOV LEA PUSH OR JMP

归一化处理

可视化特征

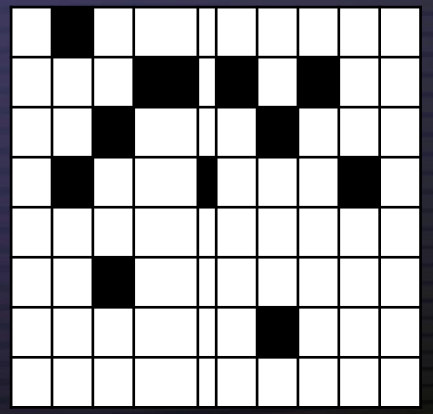


特征集2 Import table（导入表）

FindFirstFile	1
FindNextFile	2
……	……
WriteFileEx	443
……	……

归一化处理

可视化特征



机器学习文件特征示列-选取2个同类训练样本

- 测试样本A Ransomware.Tescrypt.H
- Size: 326380 bytes

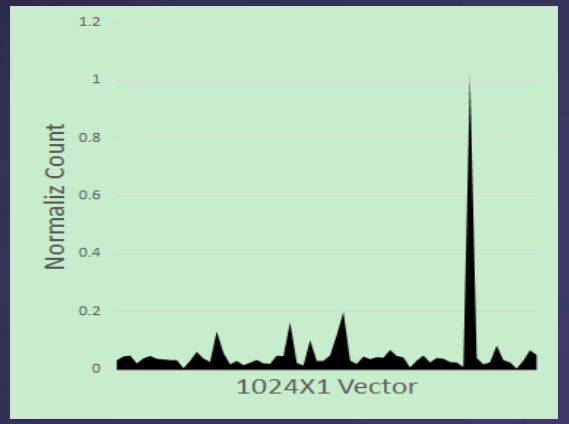
机器学习文件特征示列训练样本特征可视化后对比

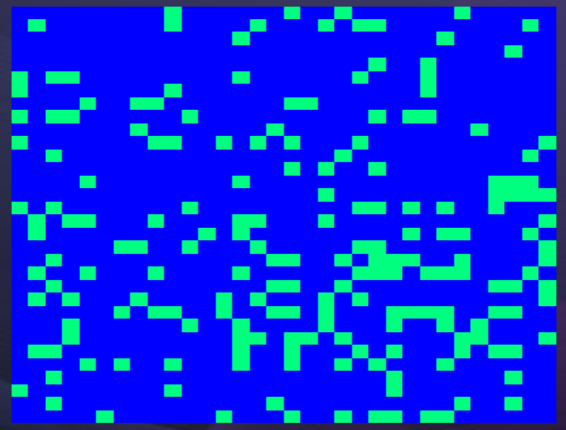
Opcode

Import Table

Ransom-Tescrypt

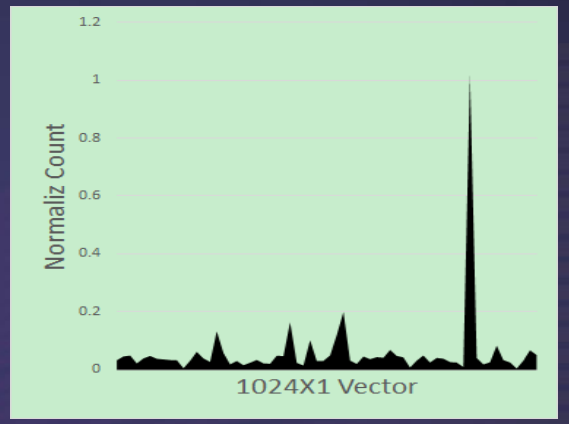
Size: 326144 bytes

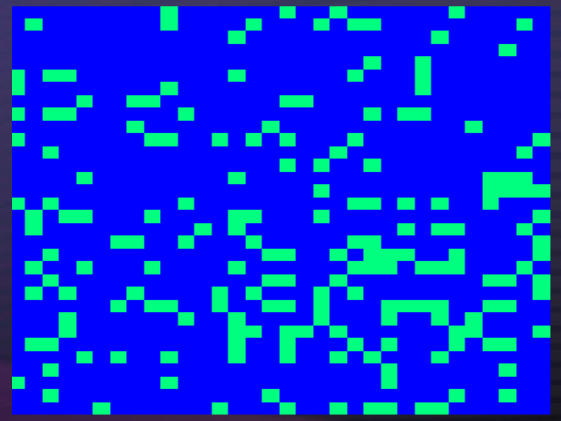




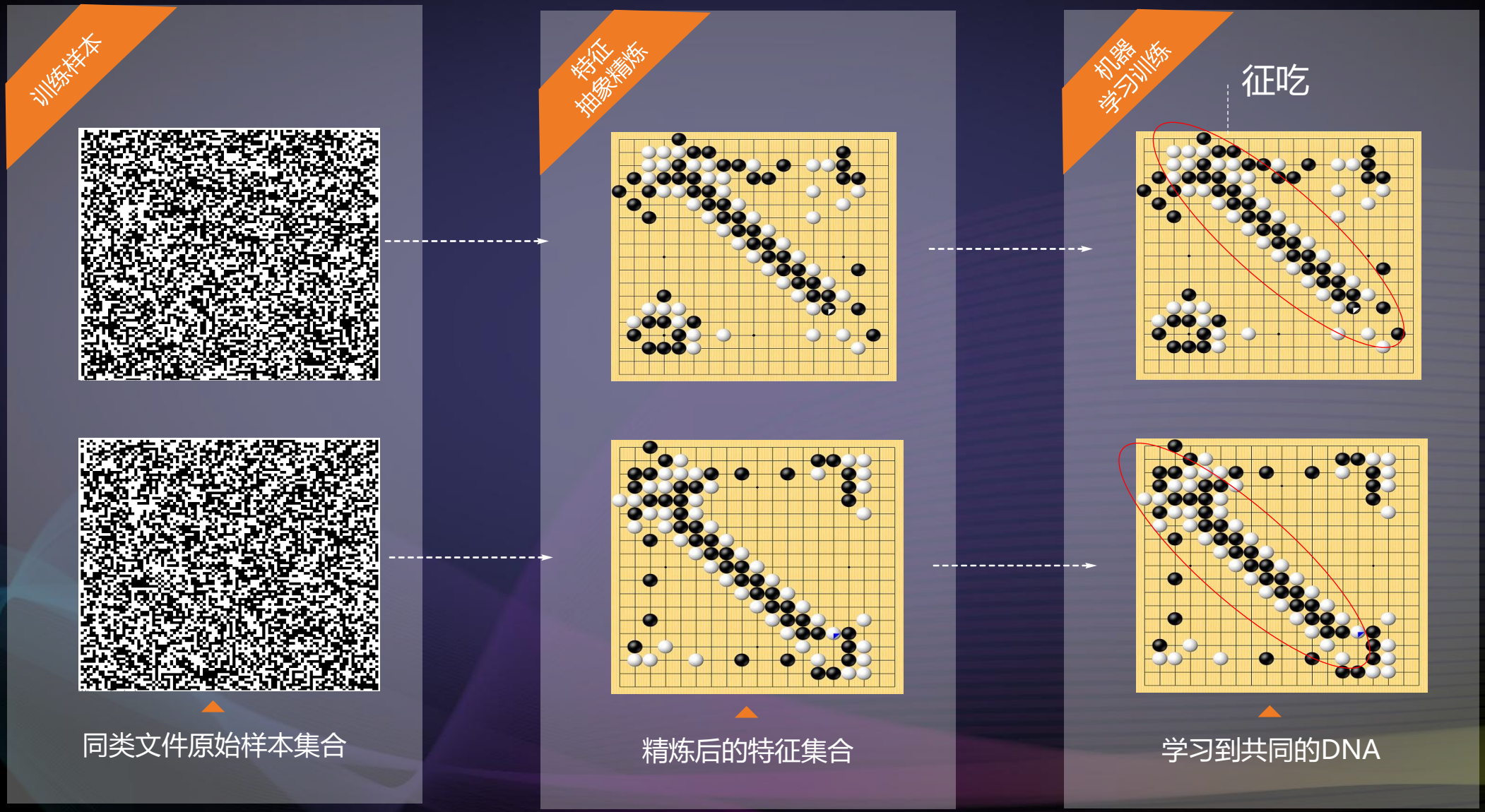
Ransom-Tescrypt.H

Size: 196380 bytes





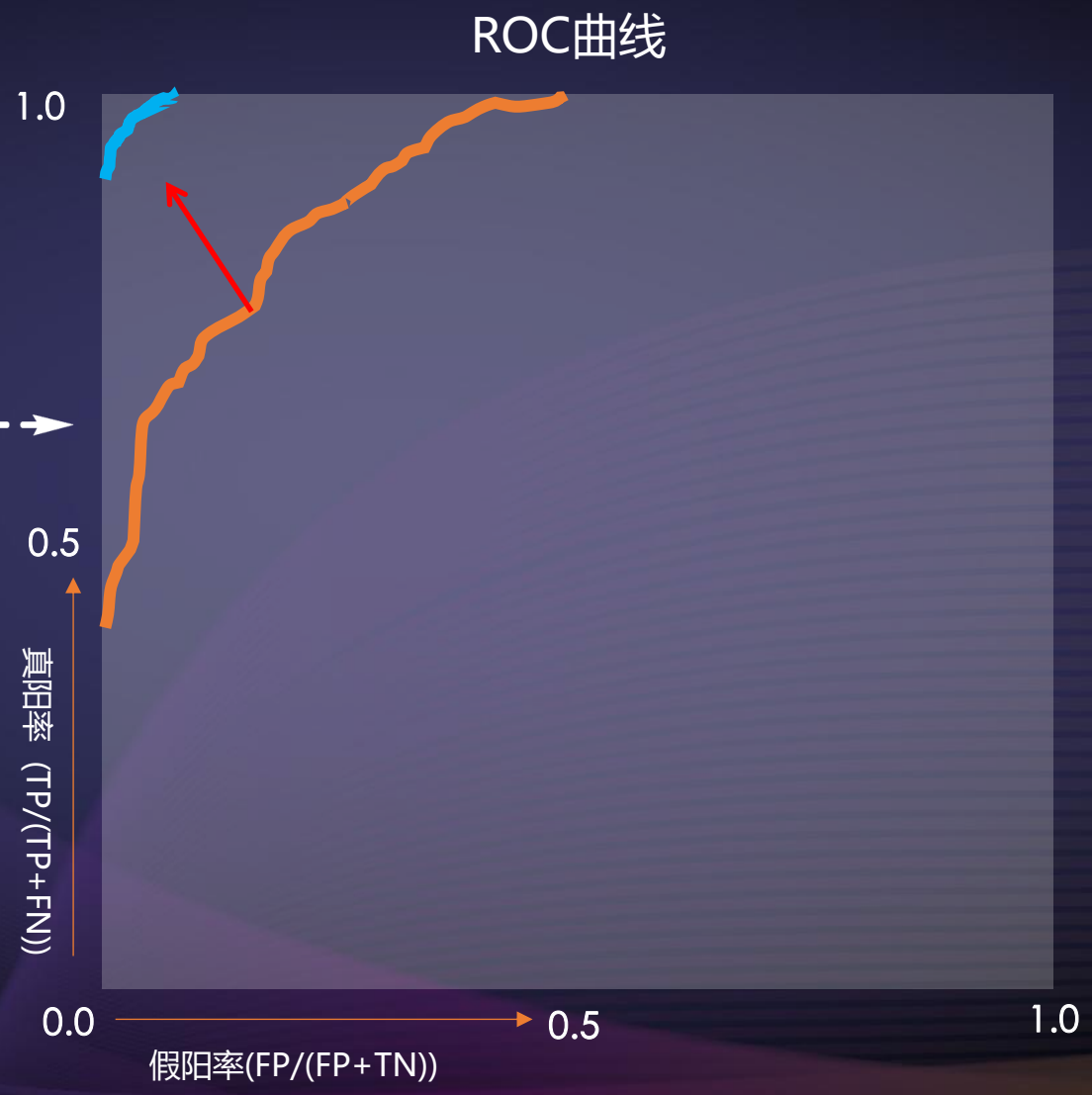
机器学习训练过程介绍



机器学习模型调试过程示例

测试样本集合

测试



TP	正样本检测为正
FP	负样本检测为正
FN	正样本检测为负
TN	负样本检测为负

测试结果的目标：

高真阳率

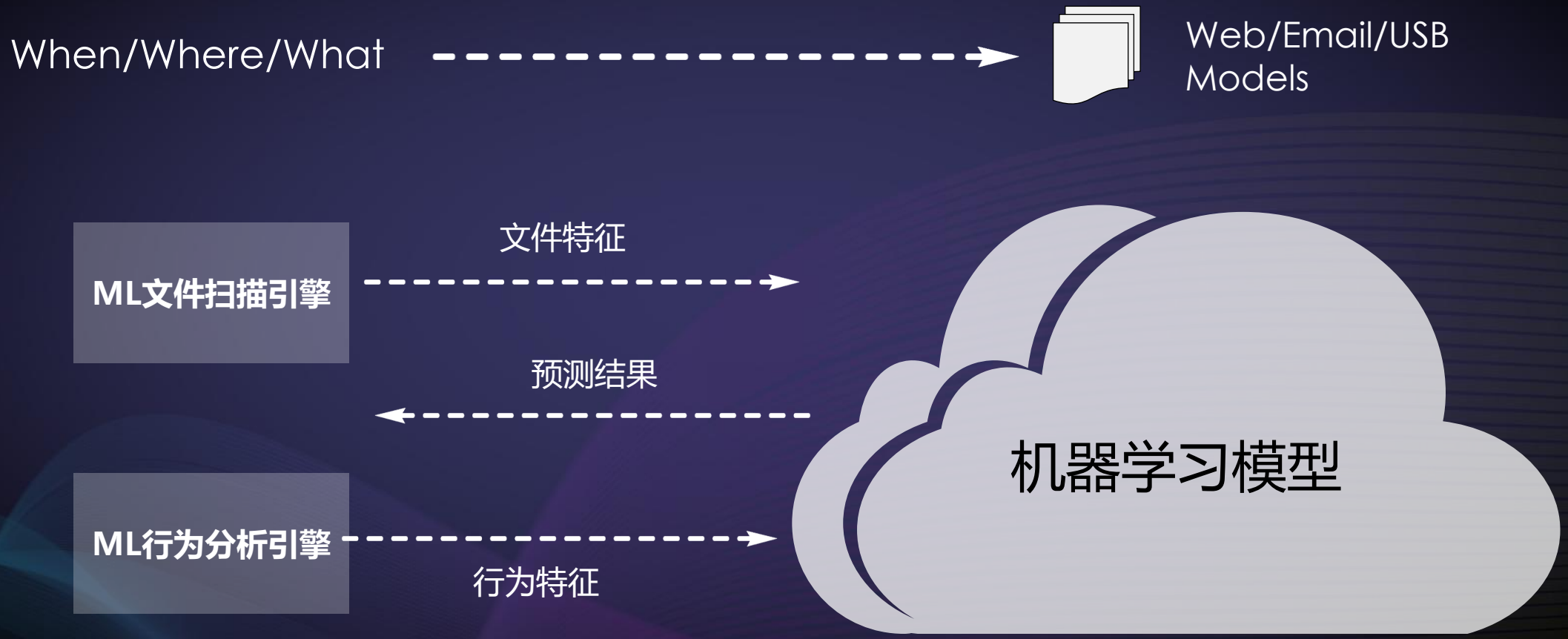
低假阳率

测试结果ROC曲线越趋向左上角越好，意味高检测率，低误报率

就是说样本集合中恶意软件能被检测出，正常文件没有误判。

机器学习调试过程是训练,测试，调参，再训练，再测试，再调参，不断迭代，直到ROC曲线达到目标。

机器学习引擎的工作过程



机器学习引擎截获未知恶意程序日志-WannaCry

预测机器学习日志详细信息

Ransom.W

2017/5

已隔离

什么时

Web

C:\Users\aaa\Downloads\

什么位置 Where

威胁指示器

威胁概率

100%

亚信安全预测

文件功能检测新兴未知安全风险。

RANSOM_HPCRYPTESLA.SM2

September 05, 2016

Analysis by: Michael Jay

相似的恶意软件在2016年9月就已经出现，使用学习过这些样本的机器学习引擎可以有效拦截

ALIASES: Win32/Filecoder.TeslaCrypt.K (ESET), Trojan.Cryptolocker.N (Symantec), Trojan.Win32.Filecoder (Ikarus)

PLATFORM: Windows

OVERALL RISK RATING:

DAMAGE POTENTIAL:

DISTRIBUTION POTENTIAL:

REPORTED INFECTION:

INFORMATION EXPOSURE:

- CreateProcessA
- CreateServiceA
- DeleteCriticalSection

WannaCry存在可疑行为的系统接口调用列表

文件DNA

类似已知威胁

Ransom_HPCRYPTESLA.SM2

相似已知恶意程序列表

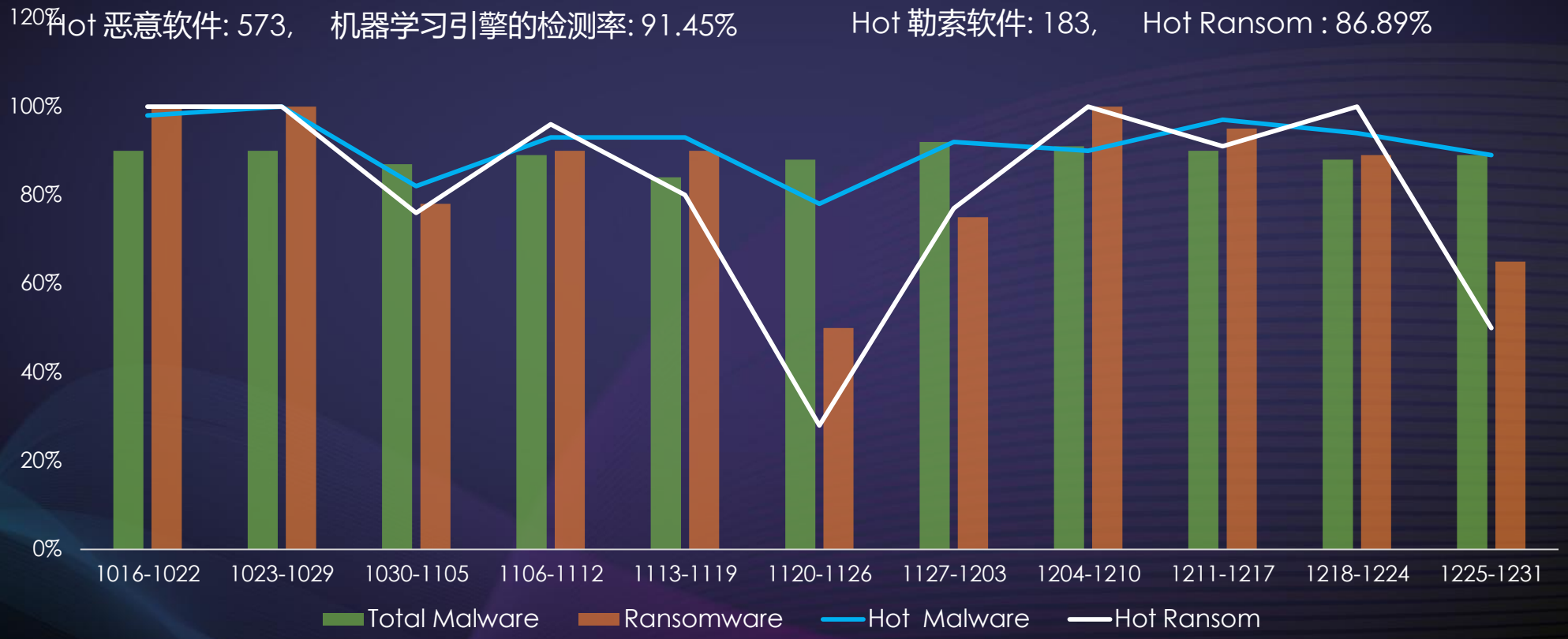
测试传统引擎无法检测的新的恶意软件样本

总数: 2565， 机器学习引擎的检测率: 88.73%

Hot 恶意软件: 573， 机器学习引擎的检测率: 91.45%

Hot 恶意软件: 573， 机器学习引擎的检测率: 91.45%

Hot 勒索软件: 183， Hot Ransom : 86.89%



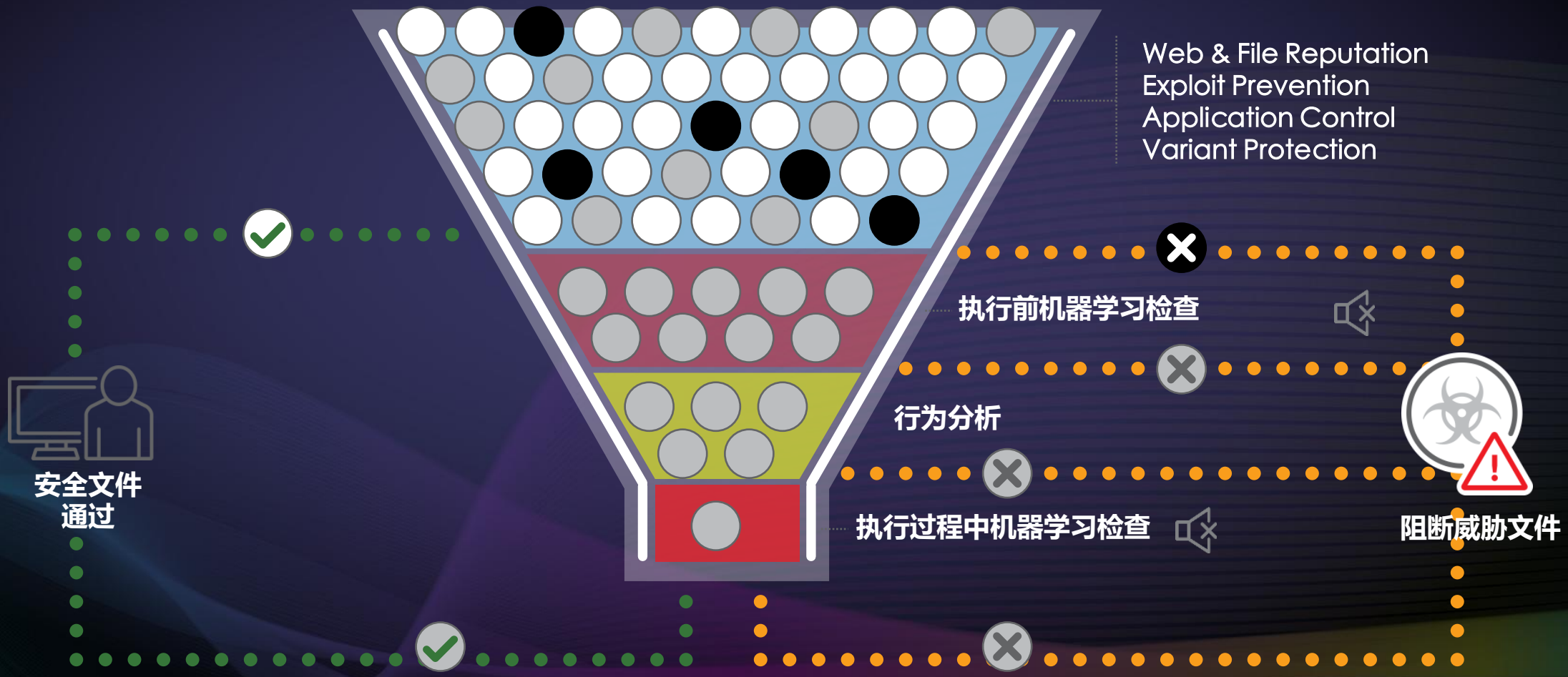
数据源：2016.10.16 – 2016.12.31所有客户提交给病毒中心供人工分析的PE文件

跨代融合的终端安全防护

C3安全峰会
CYBER | CLOUD | COMMUNICATION

AI-机器学习技术和其它防护技术结合，
提供更高效的全面防护

图例：已知的好文件　已知的坏文件　未知文件　消除噪声



最新评测，依然领先

2017最新报告被推荐，
获得误报率为0的好成绩

2016 获得所有的Award，
误报率评测获Gold Award

持续3年累积评测得分最高

2017 Gartner **终端安全魔力象限**

C3安全峰会
CYBER | CLOUD | COMMUNICATION

THANKS

AsiaInfo | 亚信安全