

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



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

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

勒索软件拦截日志(2).csv [Read-Only] - Excel

	F	G	H	I	J	K	L
	日志类型	策略	主题	事件类型	目标	处理措施	操作
1	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\2017年工作服发放全员尺寸统计表.xlsx	终止	关闭
2	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\2017年工作服发放全员尺寸统计表.xlsx	终止	关闭
3	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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\2017年工作服发放全员尺寸统计表.xlsx	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

根据已知行为规则拦截恶意软件

技术

沙盒，行为分析

手段

在无特征码情况下拦截未知的恶意软件

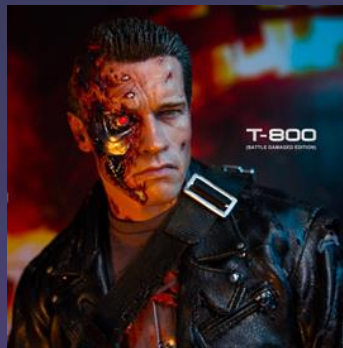
优势

利用预设的行为规则聚焦于某些
恶意攻击，如勒索和APT

局限性

技术实力，联动，恶意行为规则库，误报率

竞争优势



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

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

技术

AI-机器学习引擎

手段

快速发现未知的恶意软件

优势

无法识别缺乏训练样本的恶意软件，误报率

局限性

数据量，恶意软件特征处理经验，技术能力，误报率

竞争优势



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。



「持续战斗25年」

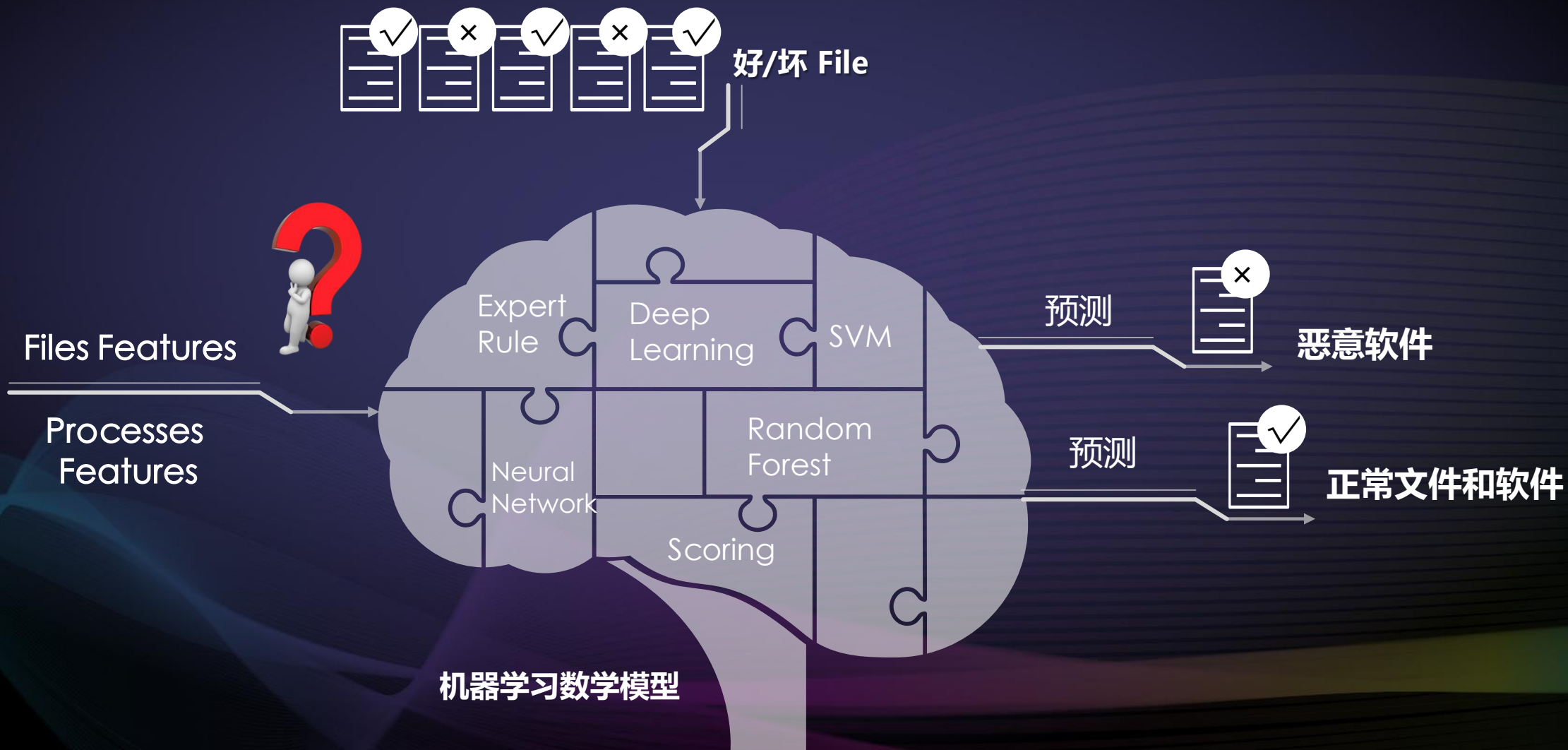


AI引擎使用的机器学习技术介绍



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



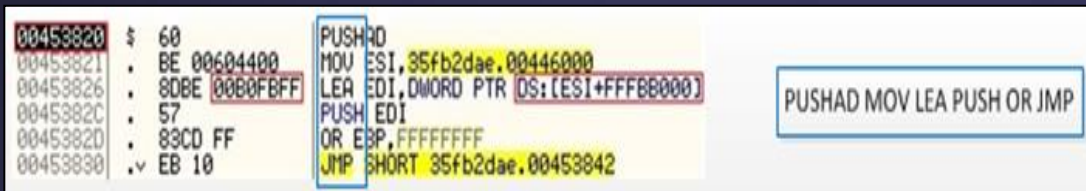
训练机器学习的数据量和文件特征处理的能力最重要





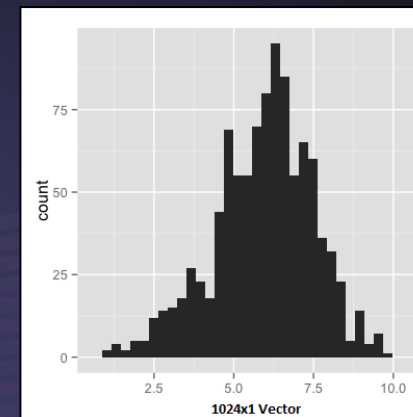
机器学习文件特征示例-特征可视化处理

特征集1 Opcode (CPU操作码)



归一化处理

可视化特征

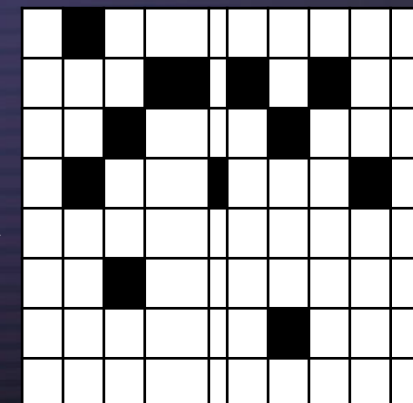


特征集2 Import table (导入表)

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例-选取2个同类训练样本

```
0004ba0 158b d230 0041 5589 a1b0 d234 0041 4589 | 0004ba0 0d8b e1c4 0041 8d89 ff4c ffff 158b e1c8
0004bb0 8bb4 380d 41d2 8900 b84d 158b d23c 0041 | 0004bb0 0041 9589 ff50 ffff cca1 41e1 8900 5485
0004bc0 5589 a1bc d240 0041 4589 8bc0 440d 41d2 | 0004bc0 ffff 8bff d00d 41e1 8900 588d ffff 8bff
0004bd0 8900 c44d 158b d248 0041 5589 a1c8 d24c | 0004bd0 d415 41e1 8900 5c95 ffff a1ff e1d8 0041
0004be0 0041 4589 8bcc 500d 41d2 8900 d04d 158b | 0004be0 8589 ff60 ffff 0d8b e1dc 0041 8d89 ff64
0004bf0 d254 0041 5589 a1d4 d258 0041 4589 8bd8 | 0004bf0 ffff 158b e1e0 0041 9589 ff68 ffff e4a1
0004c00 5c0d 41d2 8900 dc4d 158b d260 0041 5589 | 0004c00 41e1 8900 6c85 ffff 8bff e80d 41e1 8900
0004c10 a1e0 d264 0041 4589 8be4 680d 41d2 8900 | 0004c10 708d ffff 8bff ec15 41e1 8900 7495 ffff
0004c20 e84d 158b d26c 0041 5589 a1ec d270 0041 | 0004c20 a1ff e1f8 0041 8589 ff78 ffff 0d8b e1fc
0004c30 4589 8bf0 740d 41d2 8900 f44d 158b d198 | 0004c30 0041 8d89 ff7c ffff 158b e200 0041 5589
0004c40 0041 5589 a1f8 d04c 0041 8589 fed4 ffff | 0004c40 a180 e204 0041 4589 8b84 080d 41e2 8900
0004c50 0d8b d048 0041 8d89 fed8 ffff 158b d044 | 0004c50 884d 158b e20c 0041 5589 a18c e210 0041
0004c60 0041 9589 fedc ffff 40a1 41d0 8900 e085 | 0004c60 4589 8b90 140d 41e2 8900 944d 158b e218
0004c70 fffe 8bff 3c0d 41d0 8900 e48d fffe 8bff | 0004c70 0041 5589 a198 e21c 0041 4589 8b9c 200d
0004c80 3815 41d0 8900 e895 fffe a1ff d034 0041 | 0004c80 41e2 8900 a04d 158b e224 0041 5589 a1a4
0004c90 8589 feec ffff 0d8b d030 0041 8d89 fef0 | 0004c90 e228 0041 4589 8ba8 2c0d 41e2 8900 ac4d
0004ca0 ffff 158b d050 0041 9589 fef4 ffff 00a1 | 0004ca0 158b e230 0041 5589 a1b0 e234 0041 4589
0004cb0 41d0 8900 a885 fffe 8bff 040d 41d0 8900 | 0004cb0 8bb4 380d 41e2 8900 b84d 158b e23c 0041
0004cc0 ac8d fffe 8bff 0815 41d0 8900 b095 fffe | 0004cc0 5589 a1bc e240 0041 4589 8bc0 440d 41e2
0004cd0 a1ff d00c 0041 8589 feb4 ffff 0d8b d010 | 0004cd0 8900 c44d 158b e248 0041 5589 a1c8 e24c
0004ce0 0041 8d89 feb8 ffff 158b d014 0041 9589 | 0004ce0 0041 4589 8bcc 500d 41e2 8900 d04d 158b
0004cf0 febc ffff 18a1 41d0 8900 c085 fffe 8bff | 0004cf0 e254 0041 5589 a1d4 e258 0041 4589 8bd8
0004d00 1c0d 41d0 8900 c48d fffe 8bff 2015 41d0 | 0004d00 5c0d 41e2 8900 dc4d 158b e260 0041 5589
0004d10 8900 c895 fffe a1ff d024 0041 8589 fecc | 0004d10 a1e0 e264 0041 4589 8be4 680d 41e2 8900
0004d20 ffff 0d8b d028 0041 8d89 fed0 ffff 158b | 0004d20 e84d 158b e26c 0041 5589 a1ec e270 0041
0004d30 d284 0041 9589 fdd8 ffff 88a1 41d2 8900 | 0004d30 4589 8bf0 740d 41e2 8900 f44d 158b e198
0004d40 dc85 fffd 8bff 8c0d 41d2 8900 e08d fffd | 0004d40 0041 5589 a1f8 e04c 0041 8589 fed4 ffff
0004d50 8bff 9015 41d2 8900 e495 fffd a1ff d294 | 0004d50 0d8b e048 0041 8d89 fed8 ffff 158b e044
```

- 训练样本A Romsoom-Tescrypt.H
- Size: 326380 bytes



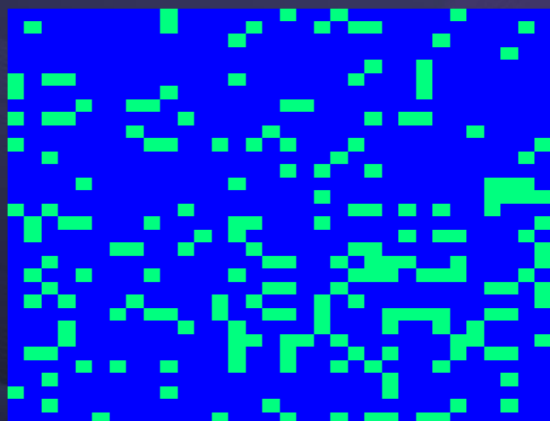
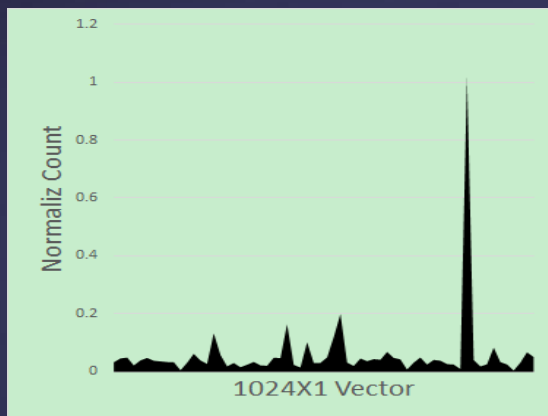
机器学习文件特征示例训练样本特征可视化后对比

Opcode

Import
Table

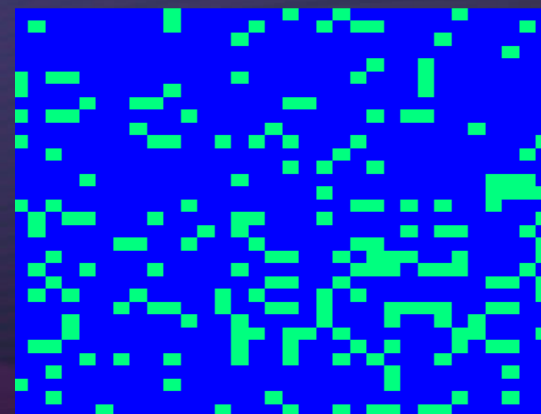
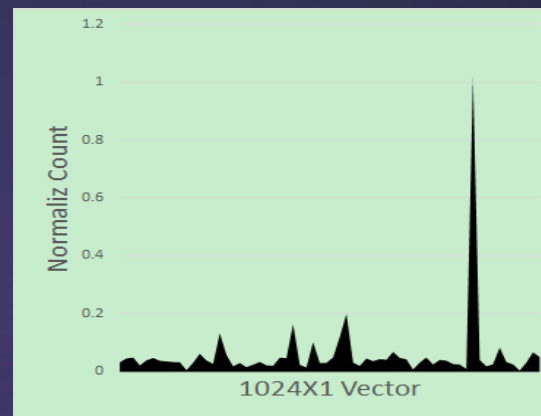
Ransom-Tescrypt

Size: 326144 bytes



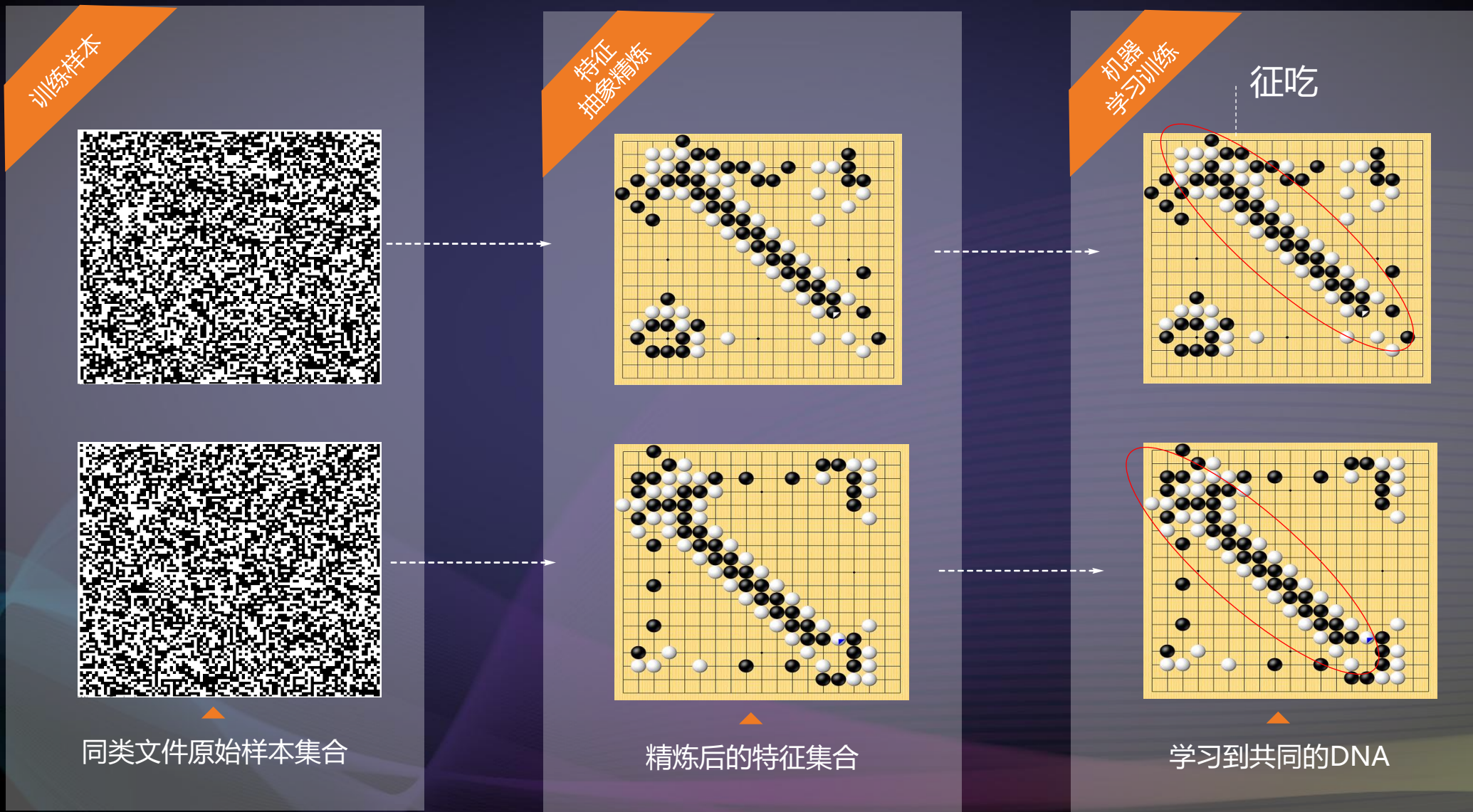
Ransom-Tescrypt.H

Size: 196380 bytes

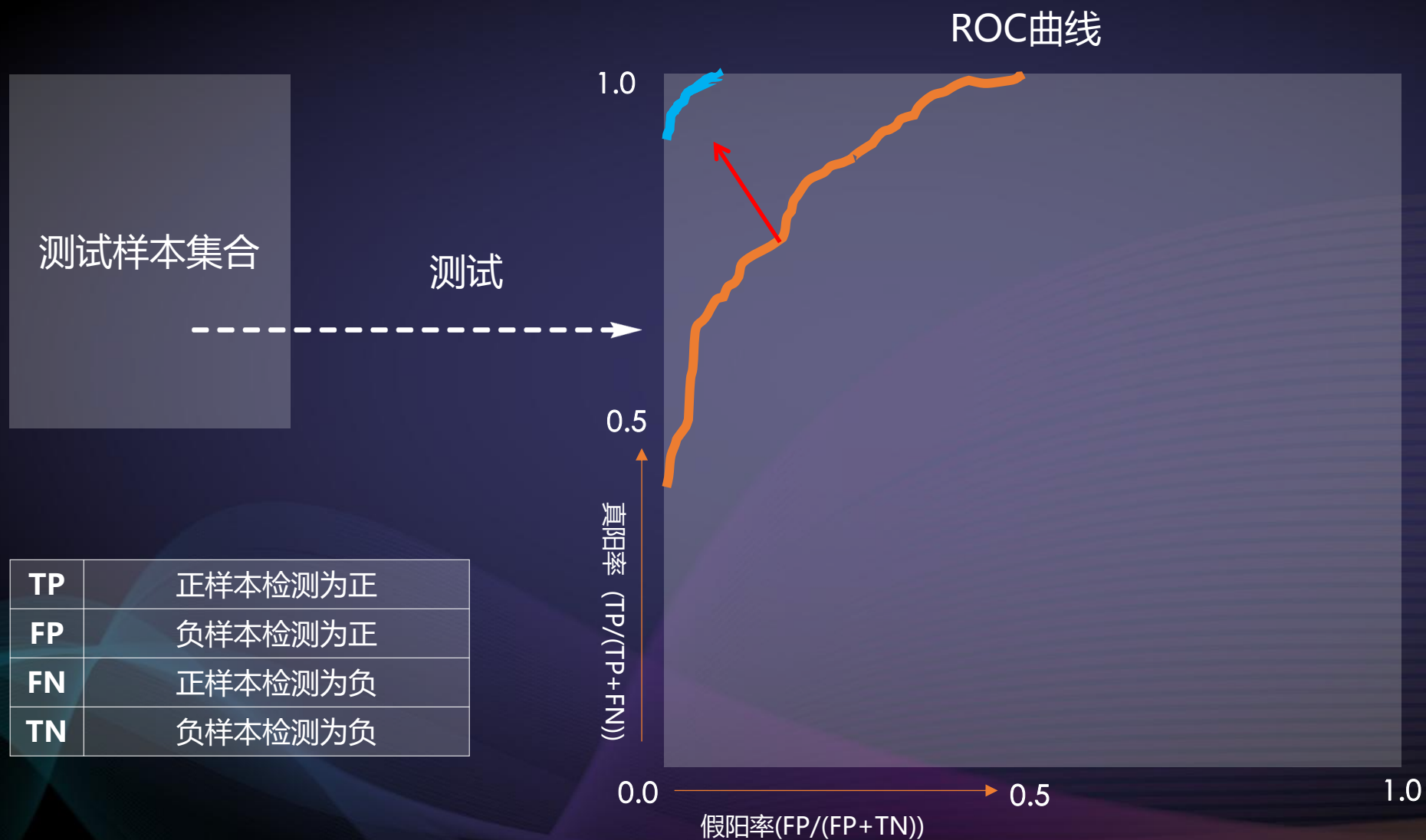




机器学习训练过程介绍



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

When/Where/What



Web/Email/USB
Models

ML文件扫描引擎

文件特征



预测结果



ML行为分析引擎

行为特征



机器学习模型





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

什么时候

威胁指示器

威胁概率
100%

亚信安全预测

文件DNA

RANSOM_HPCRYPTESLA.SM2

September 05, 2016

Analysis by: Michael Jay

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:

Web
C:\Users\aaa\Downloads\

什么位置 Where

文件功能检测新兴未知安全风险。

类似已知威胁
Ransom_HPCRYPTESLA.SM2

相似已知恶意程序列表

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

WannaCry存在可疑行为的系统接口调用列表

- CreateProcessA
- CreateServiceA
- DeleteCriticalSection



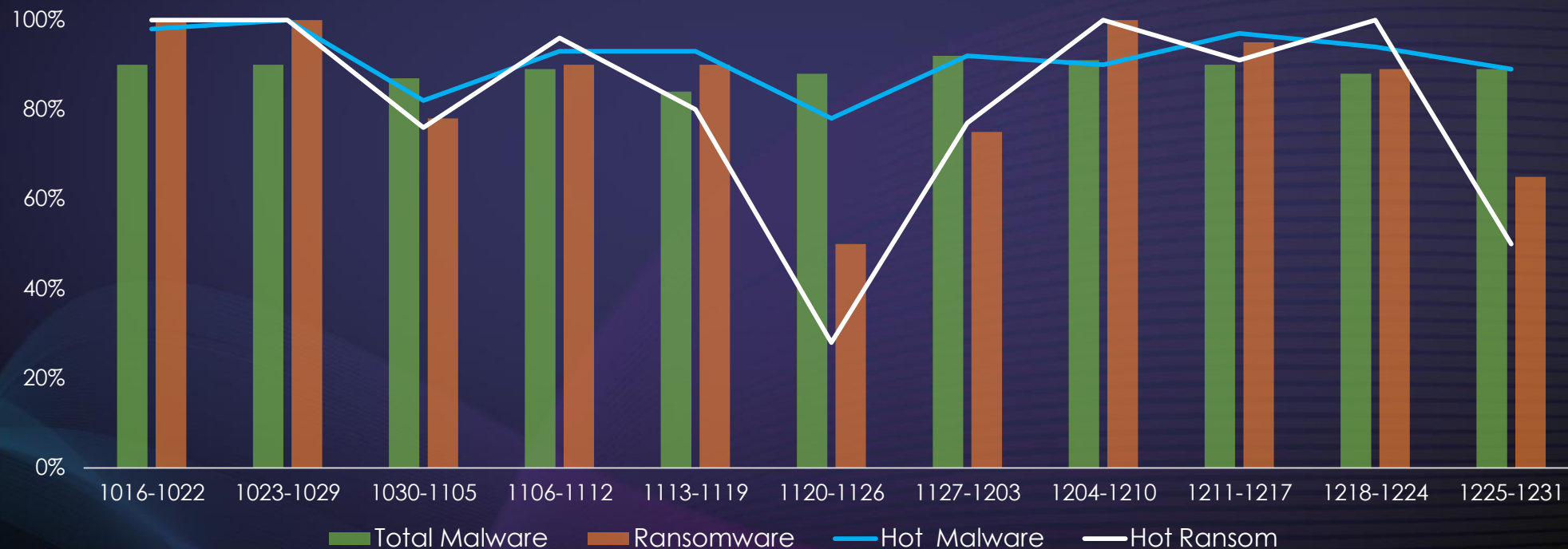
测试传统引擎无法检测的新的恶意软件样本

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

AI-机器学习技术和其它防护技术结合,
提供更高效率的全面防护

图例

- 已知的好文件
- 已知坏文件
- 未知文件
- 消除噪声





最新评测，依然领先

2017 Gartner 终端安全魔力象限



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

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (January 2017)

THANKS

 | 亚信安全
AsialInfo

C3