AI人工智能技术的“一念魔与一念佛”

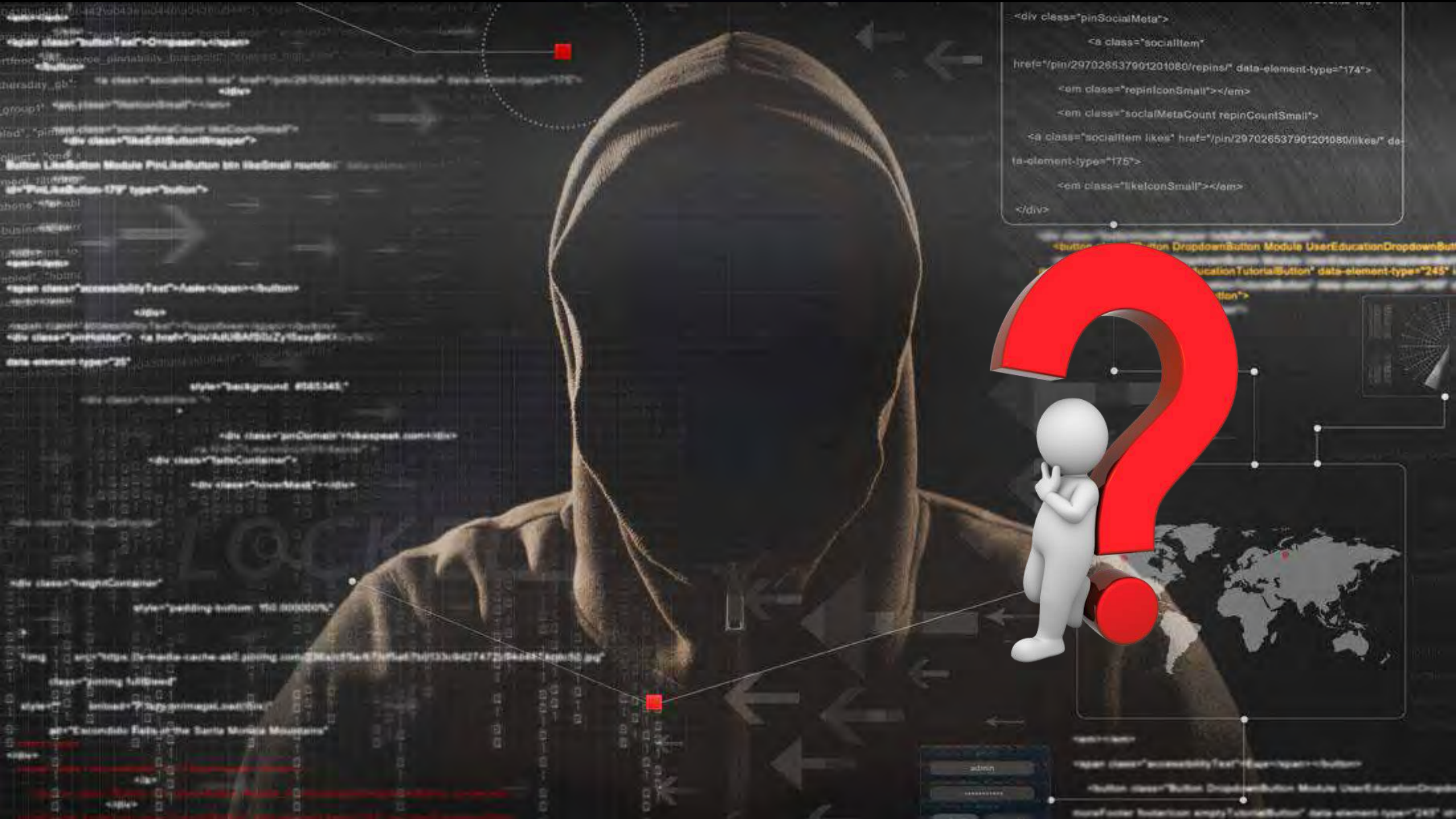
亚信网络安全产业技术研究院
产品总监 汪晨

2017年5月12日

WannaCry病毒爆发

192个国家

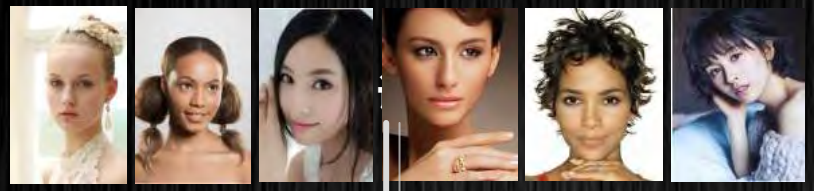
30万台 Windows机器



<a class="socialItem"
href="/pin/297026537901201080/repins/" data-element-type="174">

<a class="socialItem likes" href="/pin/297026537901201080/likes/" da-
ta-element-type="175">

AI引擎使用的机器学习技术介绍



未知人种DNA

Expert Rule

Deep Learning

SVM

Neural Network

Random Forest

Scoring

机器学习数学模型

预测

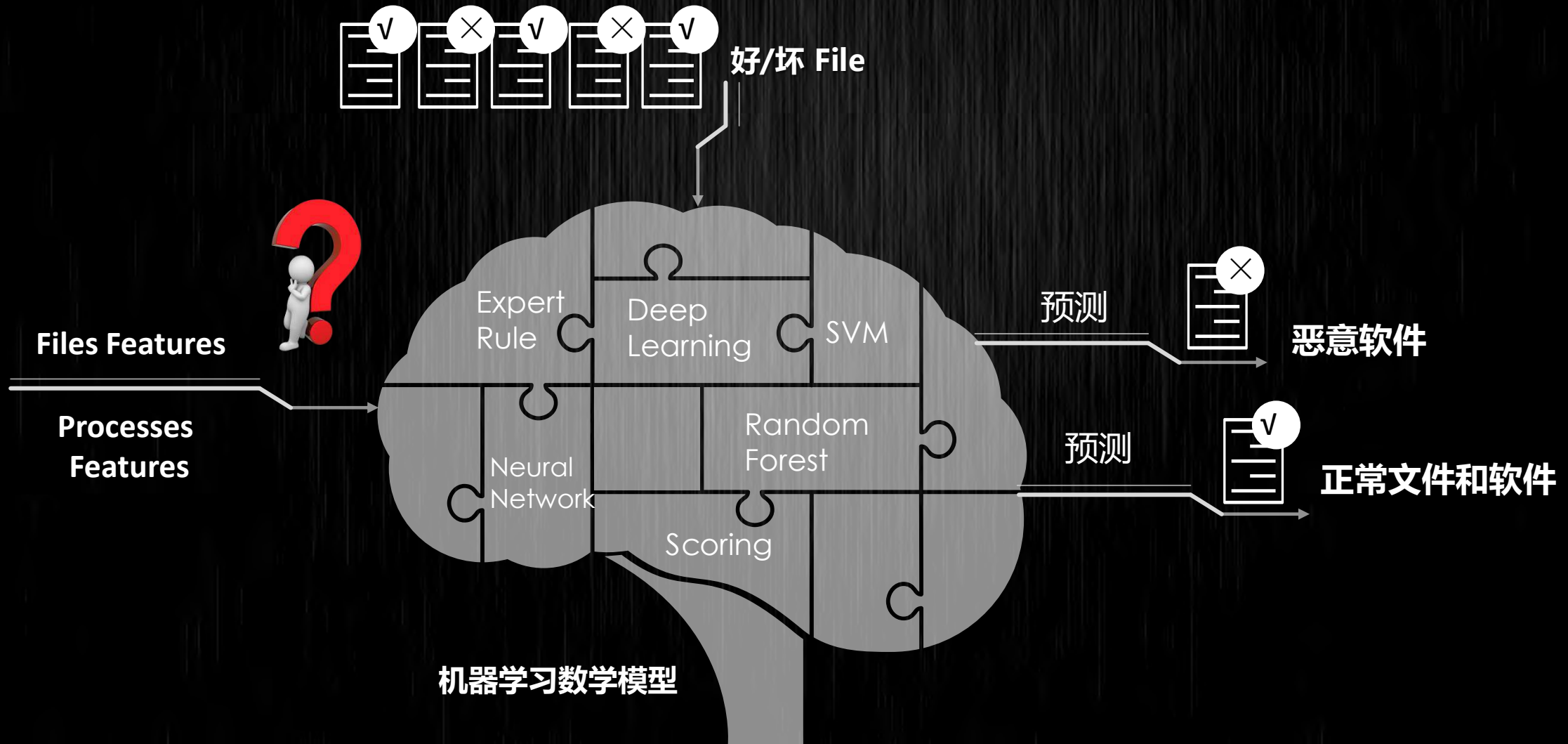
白种人

黑种人

黄种人

AI引擎使用的机器学习技术介绍

「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

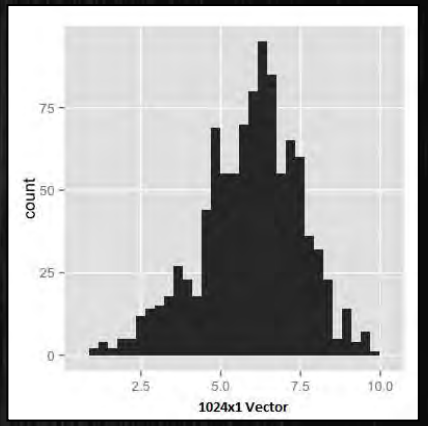
特征集1 Opcode （CPU操作码 ）

```
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

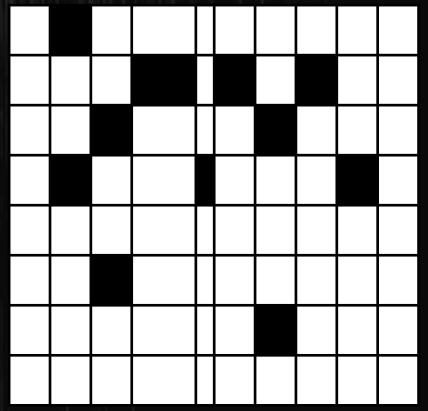


特征集2 Import table （导入表 ）

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 Ransom-Tescrypt.H
- Size: 396384 bytes

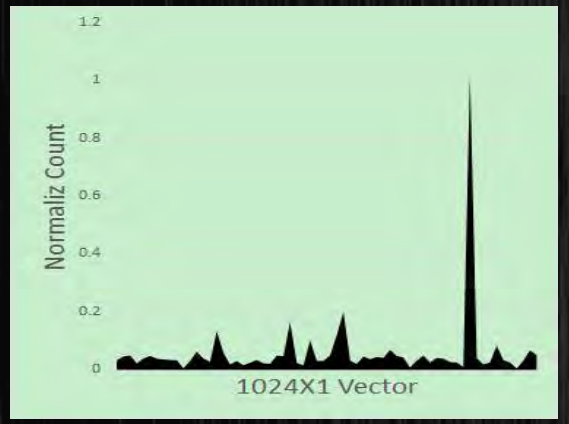
机器学习文件特征示列训练样本特征可视化后对比

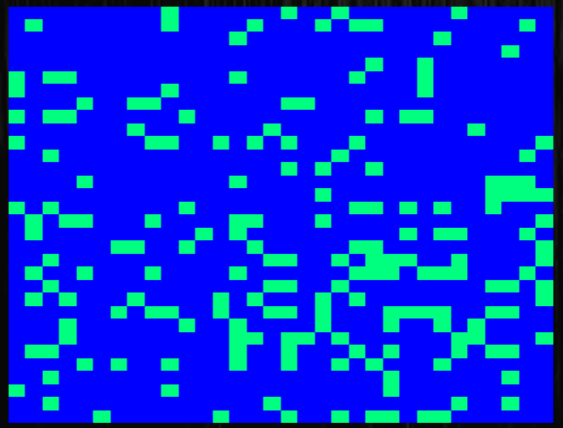
Opcode

Import Table

Ransom-Tescrypt

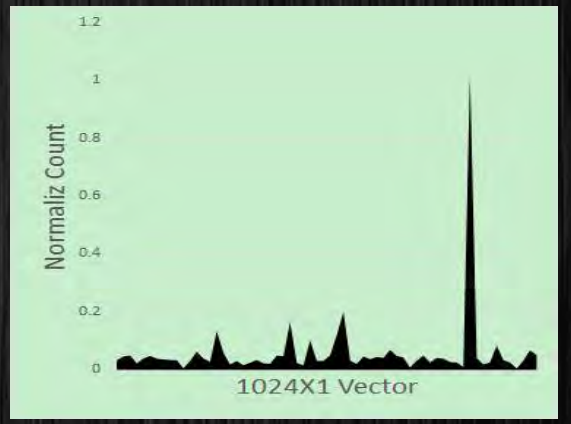
Size: **326144** bytes

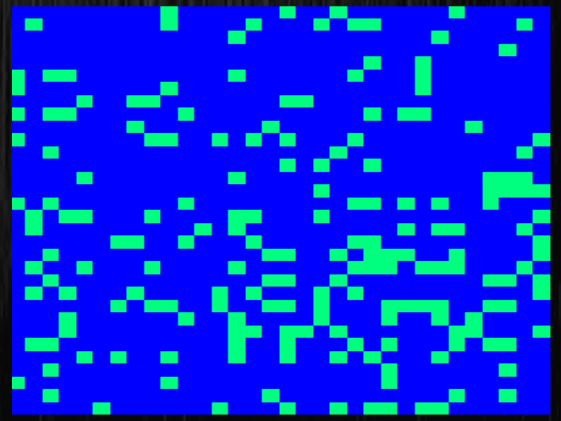




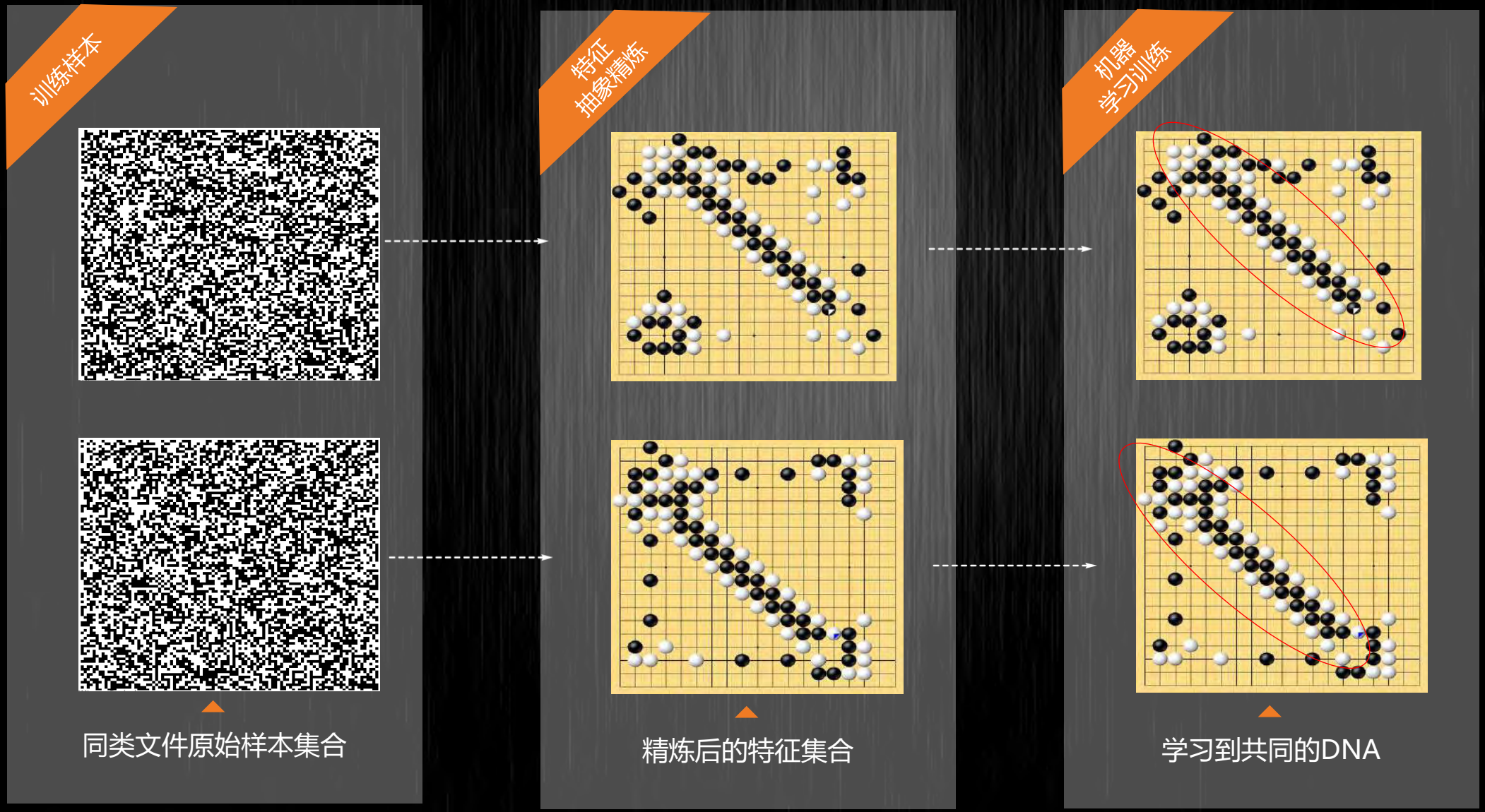
Ransom-Tescrypt.H

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

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:

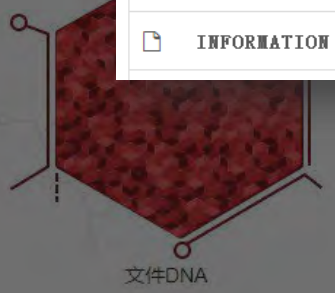
威胁指示器

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。



文件DNA

- CreateProcessA
- CreateServiceA
- DeleteCriticalSection

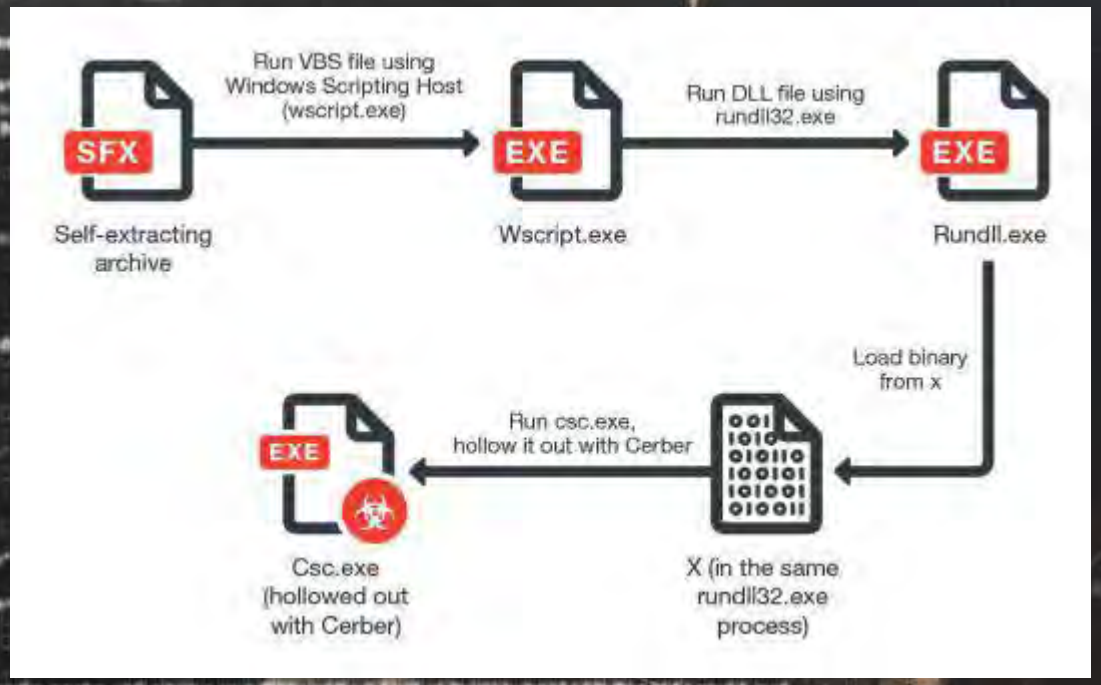
WannaCry存在可疑行为的系统接口调用列表

类似已知威胁

Ransom_HPCRYPTESLA.SM2

相似已知恶意程序列表

Cerber勒索病毒逃避机器学习检测



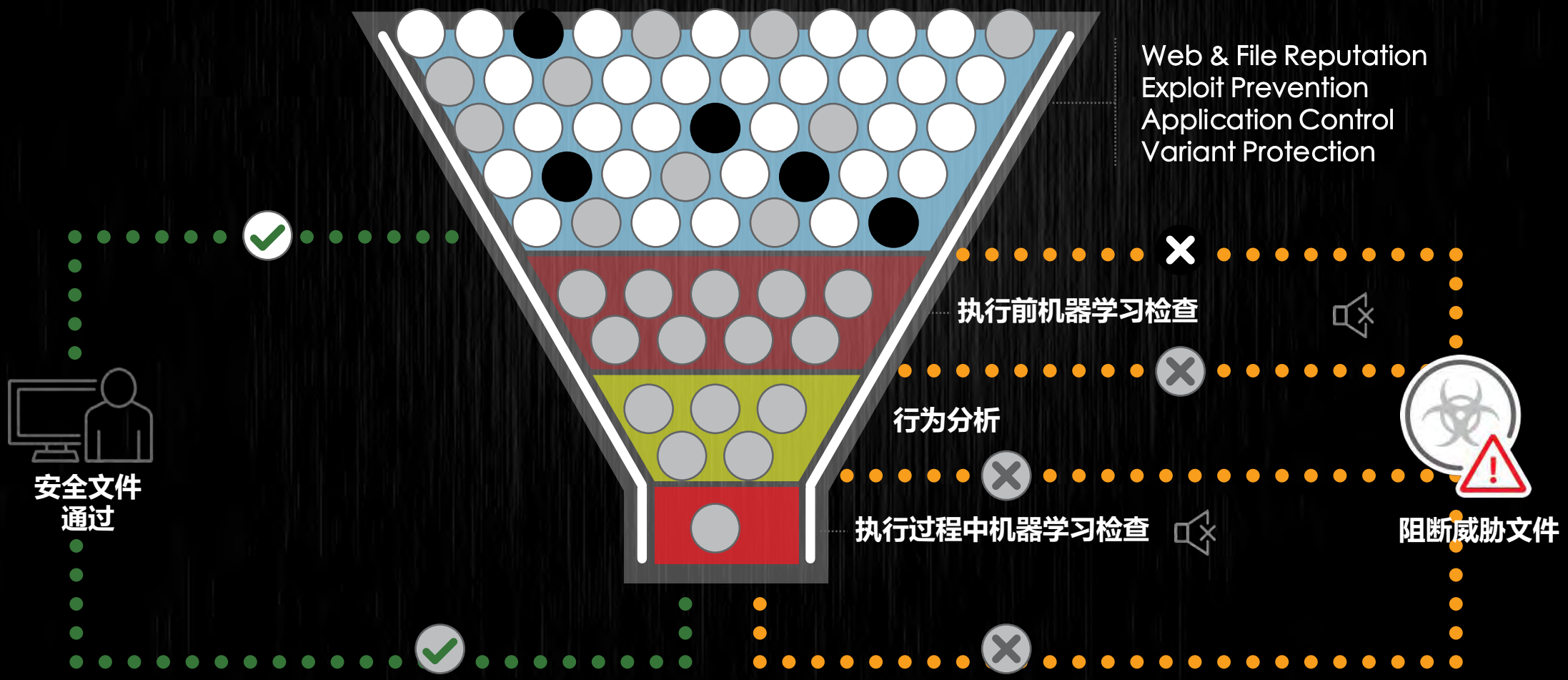
对于企业安全,历史已经清楚的证明,不存在任何单一的方法能够阻止所有类型的恶意软件攻击,企业和安全方案提供商必须使用自适应方案和策略来进行保护.

---Gartner EPP Magic Quadrant 2016

跨代融合的安全防护方案

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



THANKS