

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

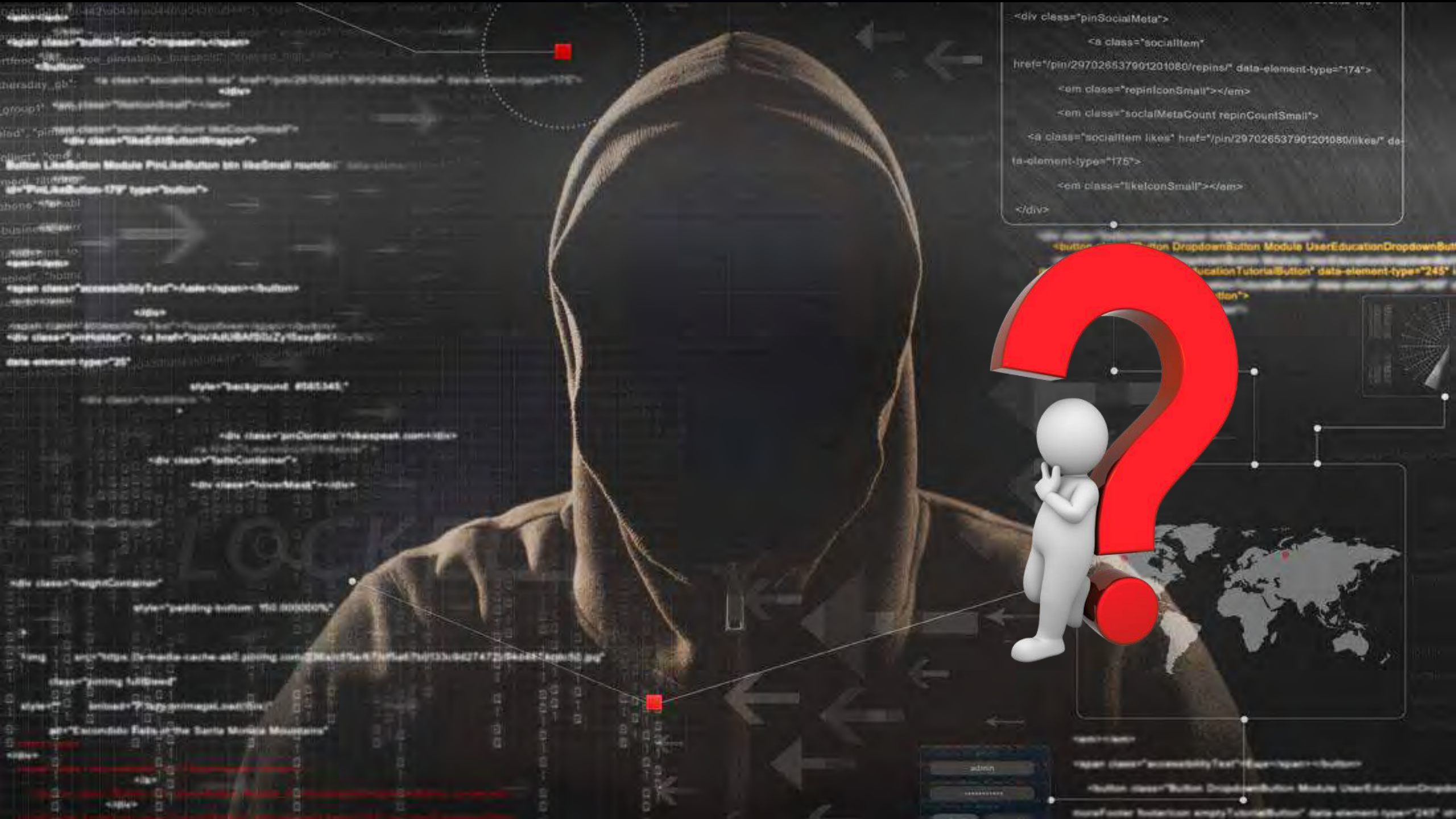


2017年5月12日

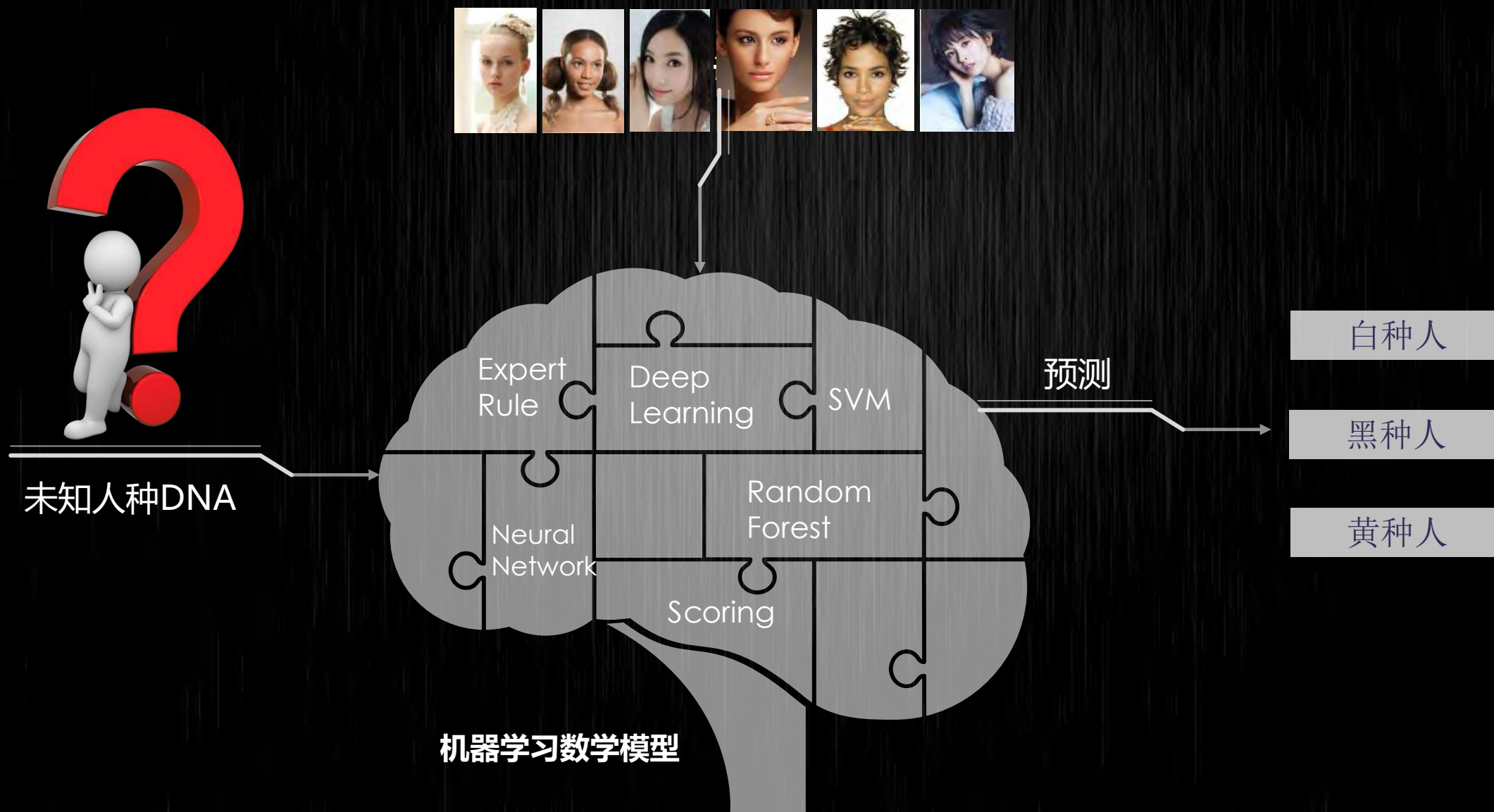
WannaCry 病毒爆发

192个国家
30万台 Windows机器



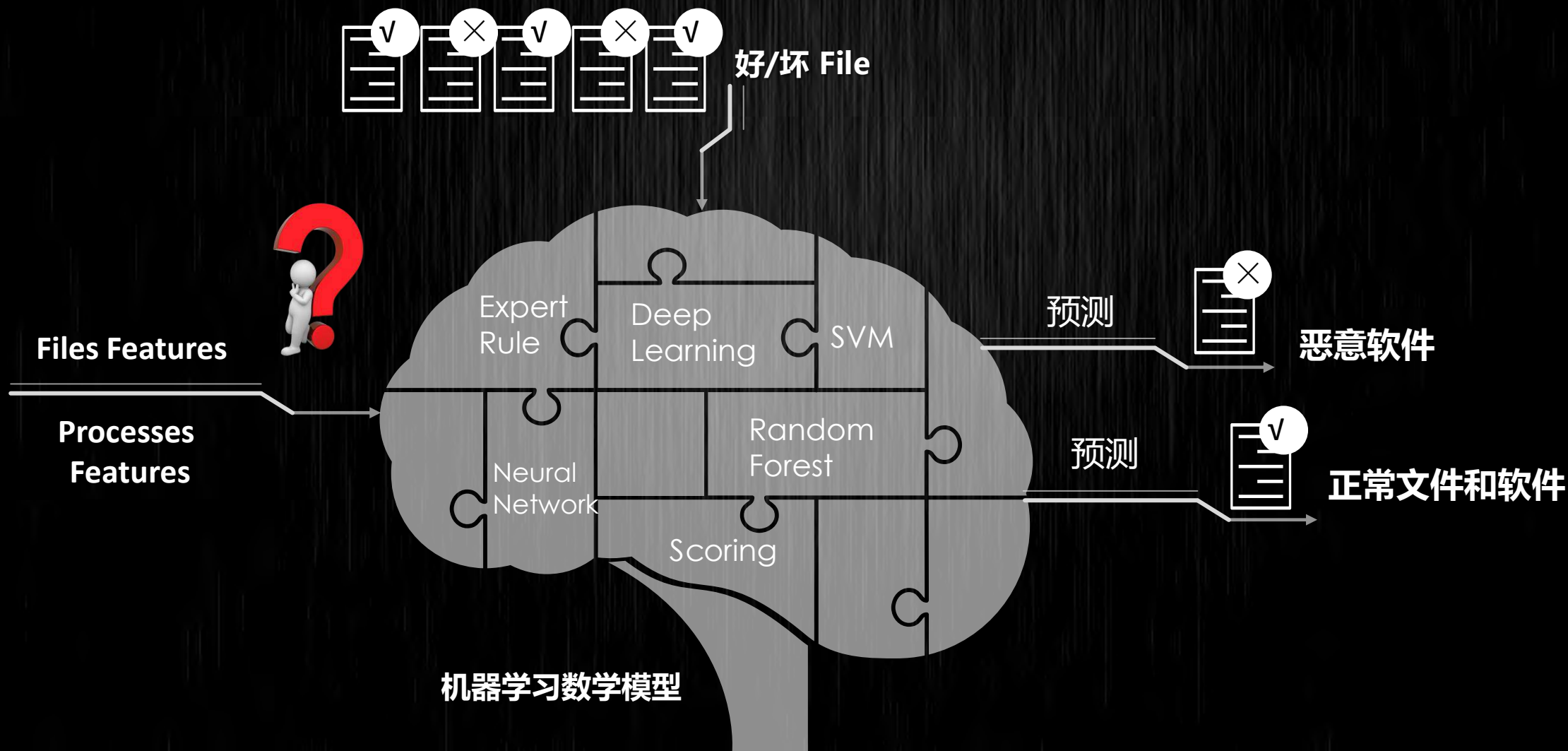


AI引擎使用的机器学习技术介绍



AI引擎使用的机器学习技术介绍

「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

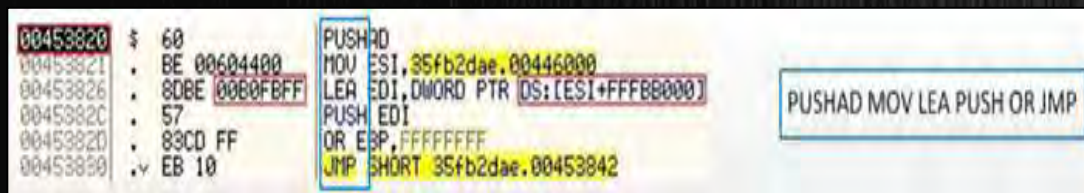
轻简

模型

高精度,低功耗双重机器学习威胁检测模型

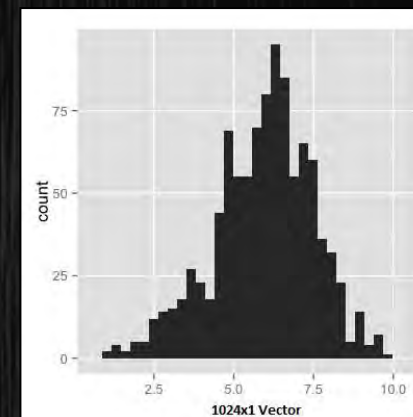
机器学习文件特征示例-特征可视化处理

特征集1 Opcode (CPU操作码)



归一化处理

可视化特征

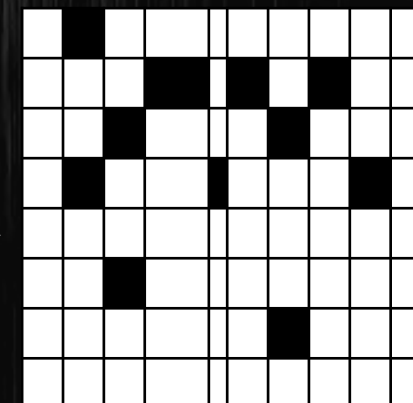


特征集2 Import table (导入表)

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

- 测试样本A Ransom-Tescrypt.H
- Size: 326384 bytes



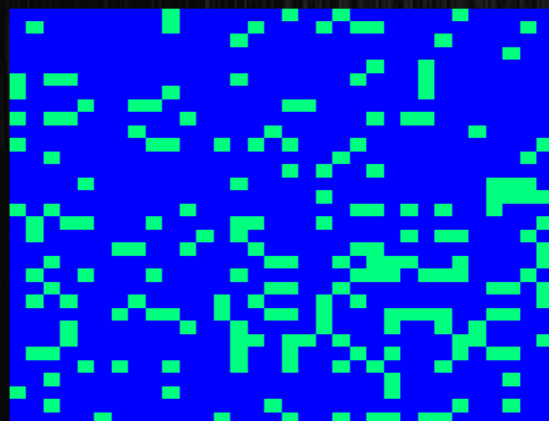
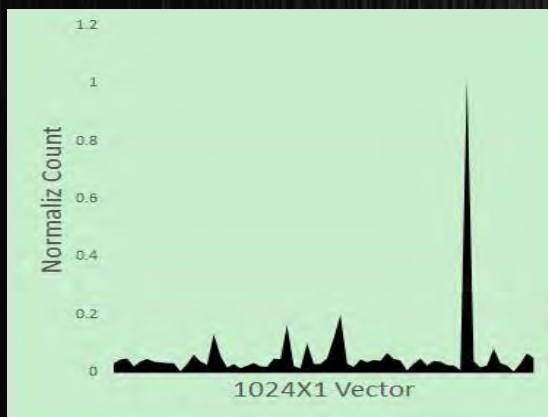
机器学习文件特征示例训练样本特征可视化后对比

Opcode

Import
Table

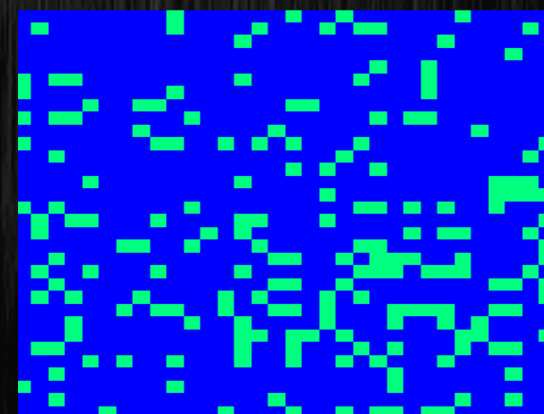
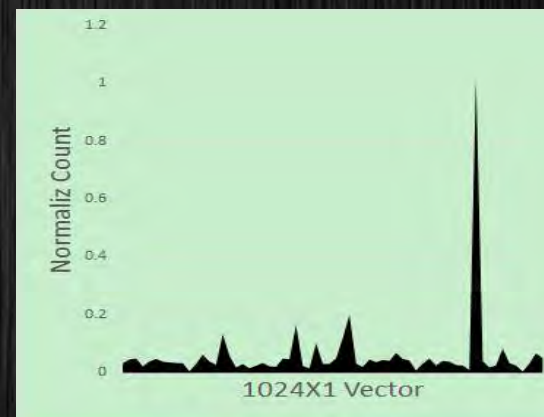
Ransom-Tescrypt

Size: 326144 bytes

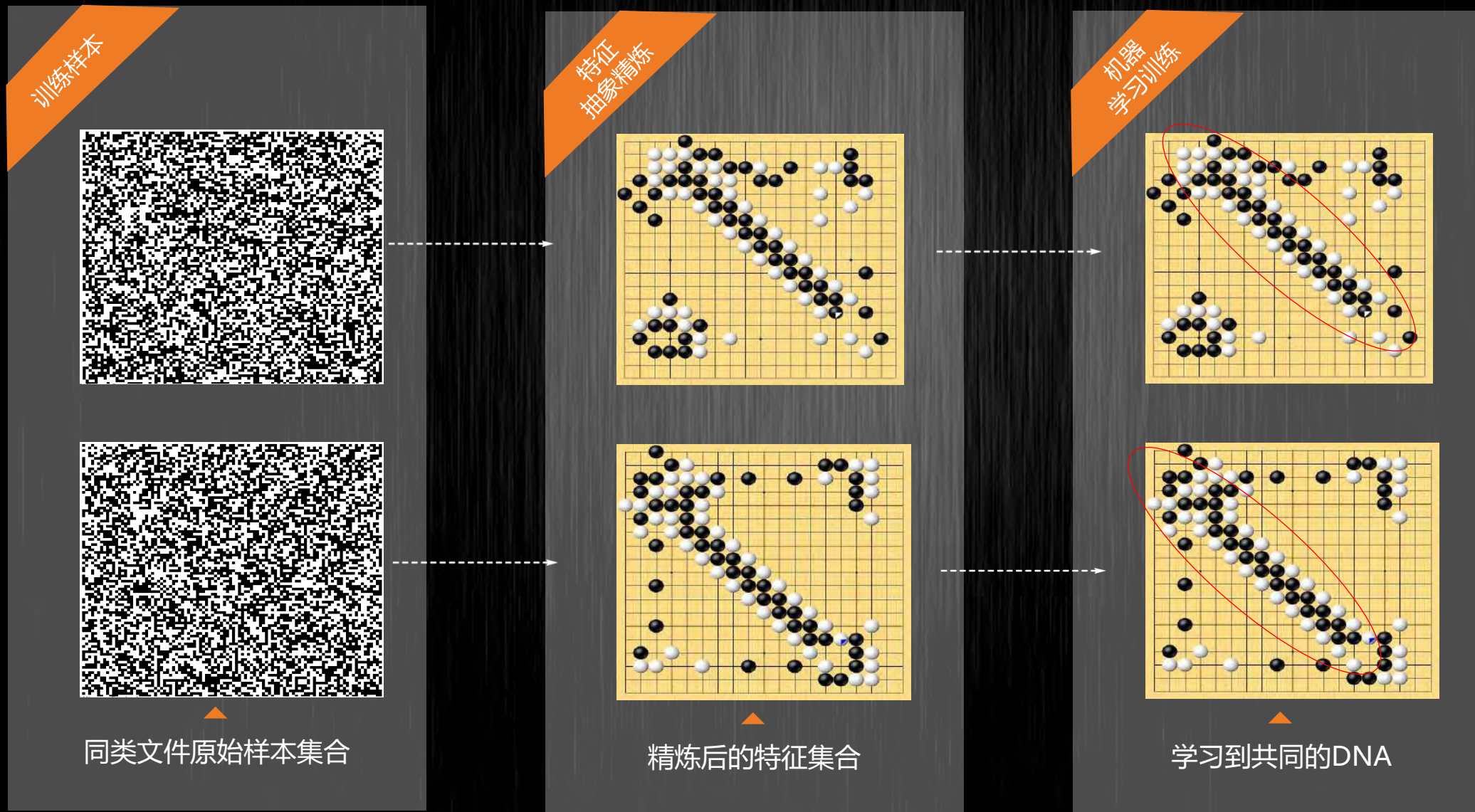


Ransom-Tescrypt.H

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

什么时间 When

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:

威胁指示器

威胁概率

100%

亚信安全预测

文件DNA

WannaCry存在可疑行为的系统接口调用列表

- CreateProcessA
- CreateServiceA
- DeleteCriticalSection

Web

C:\Users\aaa\Downloads\

什么位置 Where

文件功能检测新兴未知安全风险。

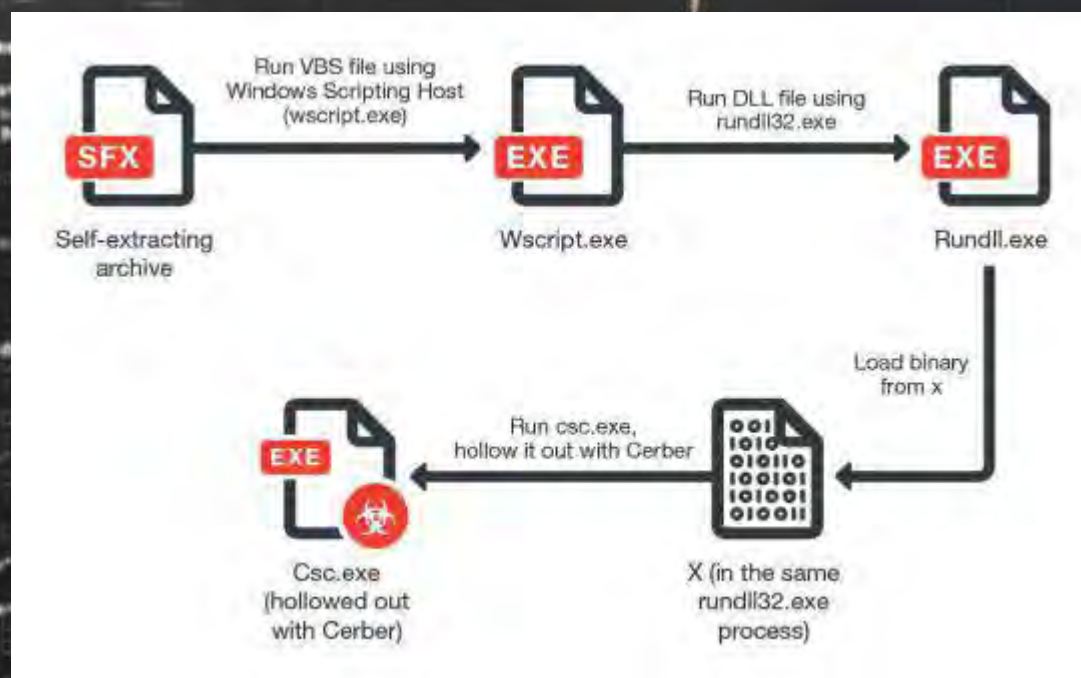
类似已知威胁

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

Cerber勒索病毒逃避机器学习检测



There is no silver bullet...

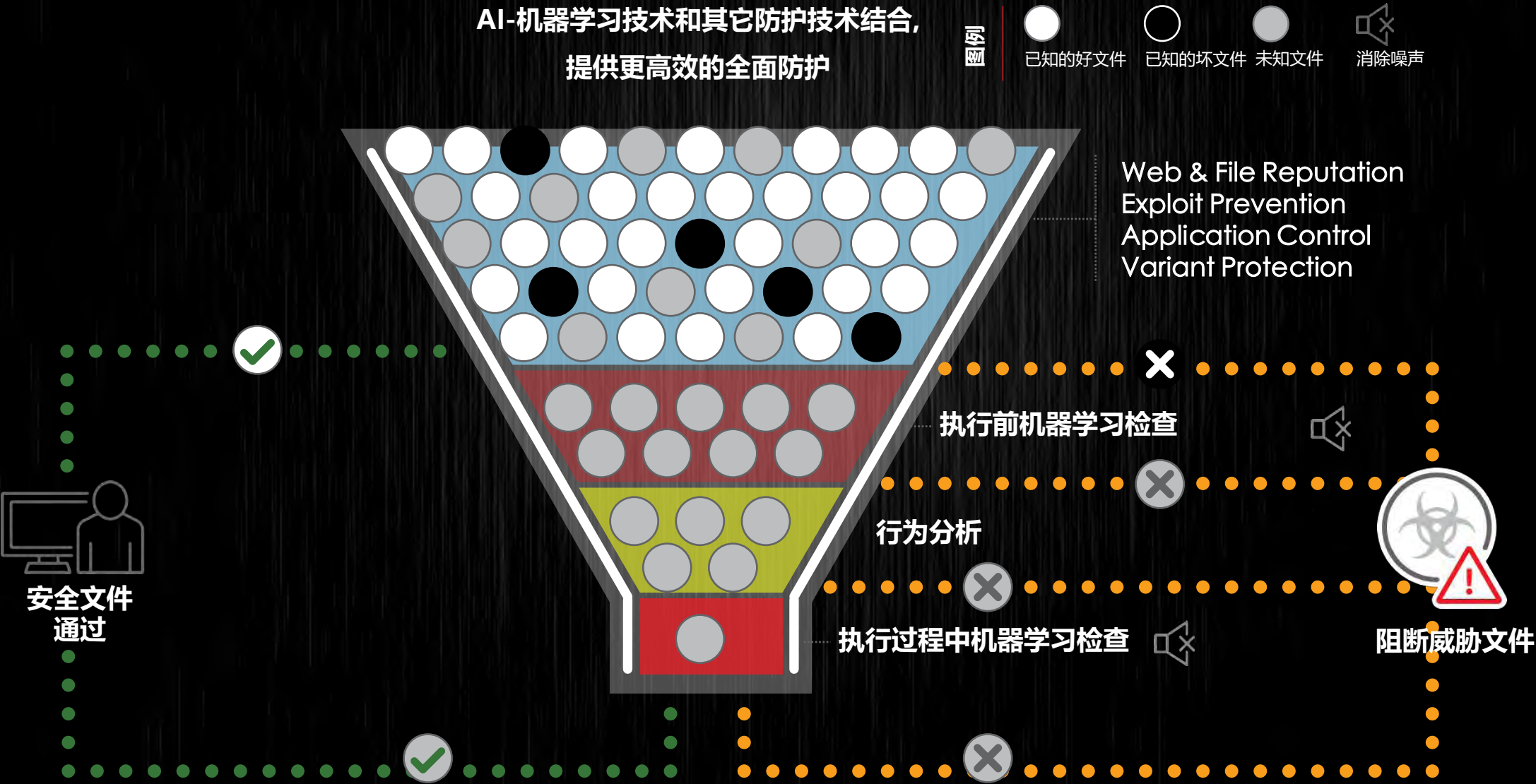


从来就没有什么灵丹妙药!

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



THANKS