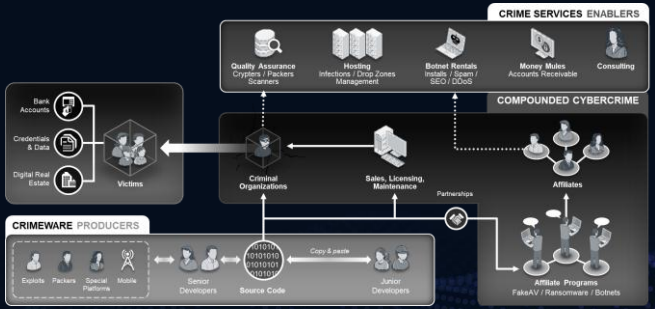
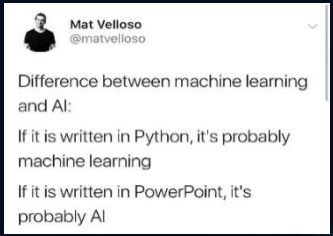
威胁与安全AI战场上的决斗

张略　Fortinet中国技术总监

不断进化的网络犯罪组织



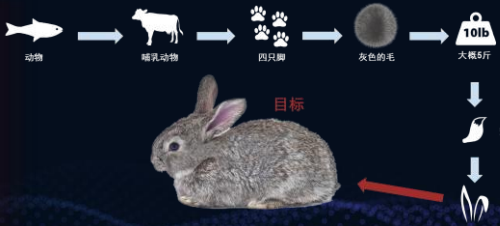
AI? 机器学习？


Mat Velloso
@matvelloso
Difference between machine learning and AI:
If it is written in Python, it's probably machine learning
If it is written in PowerPoint, it's probably AI


Mat Velloso
Technical Advisor to the CEO
Redmond, Washington | 计算机软件
目前就职 Microsoft
上一个 Microsoft, Microsoft New Zealand, Gen-I\Telecom
教育背景 National University
推荐信 6 位会员推荐了Mat Velloso
网站链接 博客

AI? 机器学习？深度学习？


人工
智能
机器
学习
深度
学习
可用的感知信息
专家系统


动物
哺乳动物
四只脚
灰色的毛
10lb
大概5斤
短尾巴
长耳朵
目标

AI在恶意软件制作中的案例

早在2003年，Swizzor Trojan horse就已经自动的每分钟变种一次，几乎每一个中毒者都有独一无二的变种。这使得检测和防御变得困难。

AI被用于恶意软件的最早的尝试？还是只是简单的自动化？

还是Swizzor Trojan horse，为了检测它，我们必须分析出它变种的模式。

人工 还是 AI ？

AI在威胁中的进化

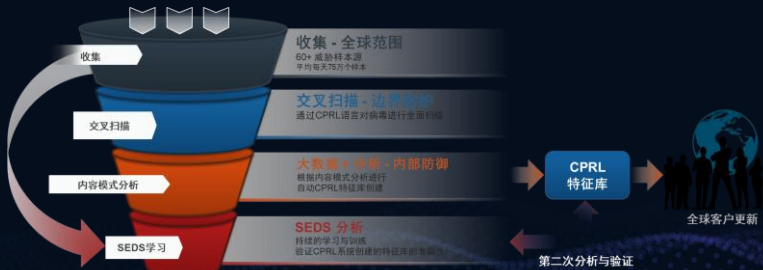
- 自动识别出变种模式被发觉，并自动改变变种模式
- 自动发现并攻击高价值目标（震网病毒）
- 自动躲避疑似蜜罐，并释放假病毒，迷惑防御者
- 自动撰写，并发送给高价值目标钓鱼邮件
- 自动识别防御体系，并采用绕过策略和变种
- .....

AI和自动化显著降低了攻击时间

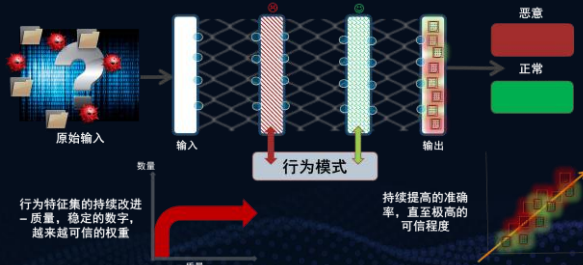
FortiGuard的数字...

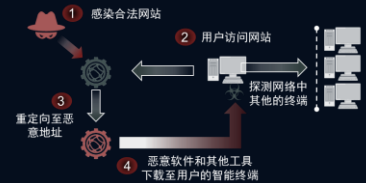
AI的基础：大数据和机器学习

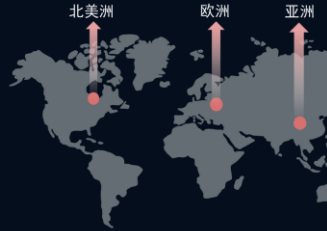
自主进化的检测系统（SEDS）



FortiGuard自主进化的检测系统（SEDS）







FIT 2019

Fortinet的AI技术在一个复杂的响应网络中分析数百万个文件，发现新的0-day恶意软件和变种

Fortinet的AI系统自主发布了一个动态的算法
(W32/Generic.AC.39AB6D!tr)

Trend Micro发现了RATANKBA病毒，但是Fortinet的客户们已经早在2016年10月就得到了保护

Symantec发布了针对RATANKBA的新的特征库，然而Fortinet早在2016年10月就已经能防护了

Fortinet自动发现了几个恶意网站，通过网页过滤和DNS查询引擎，客户得到了保护

几个新的域名被公布为RATANKBA的恶意域名，然而Fortinet早在4天前就发布了

事件发生前

Oct 29th 2016

Feb 8th, 2017

Feb 9th ,2017

Feb 10th ,2017

Feb 14th, 2017

2018 Fortinet Security Fabric

Security Fabric安全架构能够提供:

无缝 安全可视化，并且保护来自任意攻击平面的的威胁

协同 通过多个安全技术之间的互动，检测和防御高级可持续性威胁

智能 自动响应安全事件，并持续性的进行安全评估

安全架构支持如下形式的部署:

下一代Web应用防护


FW/IPS
FortiGate 和竞争对手
100% 基于特征
优势
• 独立设备
• 已知攻击特征检测
• 简易部署
劣势
• HTTP 的理解有限
• 无会话意识
• 无法感知应用层交付
• 无法感知用户层交付
• 没有误报的调优
• 有限的 WAF功能防护
WAF
FortiWeb 和竞争对手
自动学习
优势
• 特征 + 自动扫描
• 应用感知
• 已知正常的流量模型
• 异常检测
劣势
• 较高的误报率
• 频繁的防护策略调整
• 自动学习不是100%可靠
• 应用数据的变化需要重新学习
AI
机器学习

传统的WAF应用学习防护

多种机器学习来解决


异常检测
威胁检测
应用数据流
异常
威胁
阻断
SECURED BY FORTIGUARD.
基于学习到的web应用流量进行统计概率分析
基于FortiGuard和威胁模型分析
= 正常请求
= 合理的异常
= 威胁
正常的数据流
正常和合理的数据流

多种机器学习来解决


https://www.example.com/insert?firstname=Mark&lastname=Smith
用户在NAME的表单字段中输入 "Mark Smith"
FortiWeb 通过机器学习，学习到只有这个表单需要输入字符.
FortiWeb 的机器学习将此视为正常应用流量
允许
正常流量
通过Forti/Web 机器学习学习到这个表单需要输入的字符和长度等
异常
攻击
SECURED BY FORTIGUARD.
支持向量机(SVM)模式，FortiGuard通过该模式将威胁与异常分离开来
https://www.example.com/insert?firstname=Janette&lastname=Smit&
用户无意中在NAME的表单字段中输入 "Janette Smit&"
FortiWeb通过机器学习预测，这是来自通常预期的字段条目的异常，但不是威胁
允许
用户在NAME的表单字段中输入"SELECT * FROM CUSTOMER"
FortiWeb机器学习与FortiGuard SVM模型预测这是一个异常和攻击
阻断
https://www.example.com/insert?firstname="SELECT * FROM CUSTOMER"


闪电战:
ARTIFICIAL
INTELLIGENCE
FORTINET


FREEBUF | FIT
THANKS