In the Boxing Ring 2023年8月

Network Box 技术新闻

Mark Webb-Johnson
CTO,, Network Box

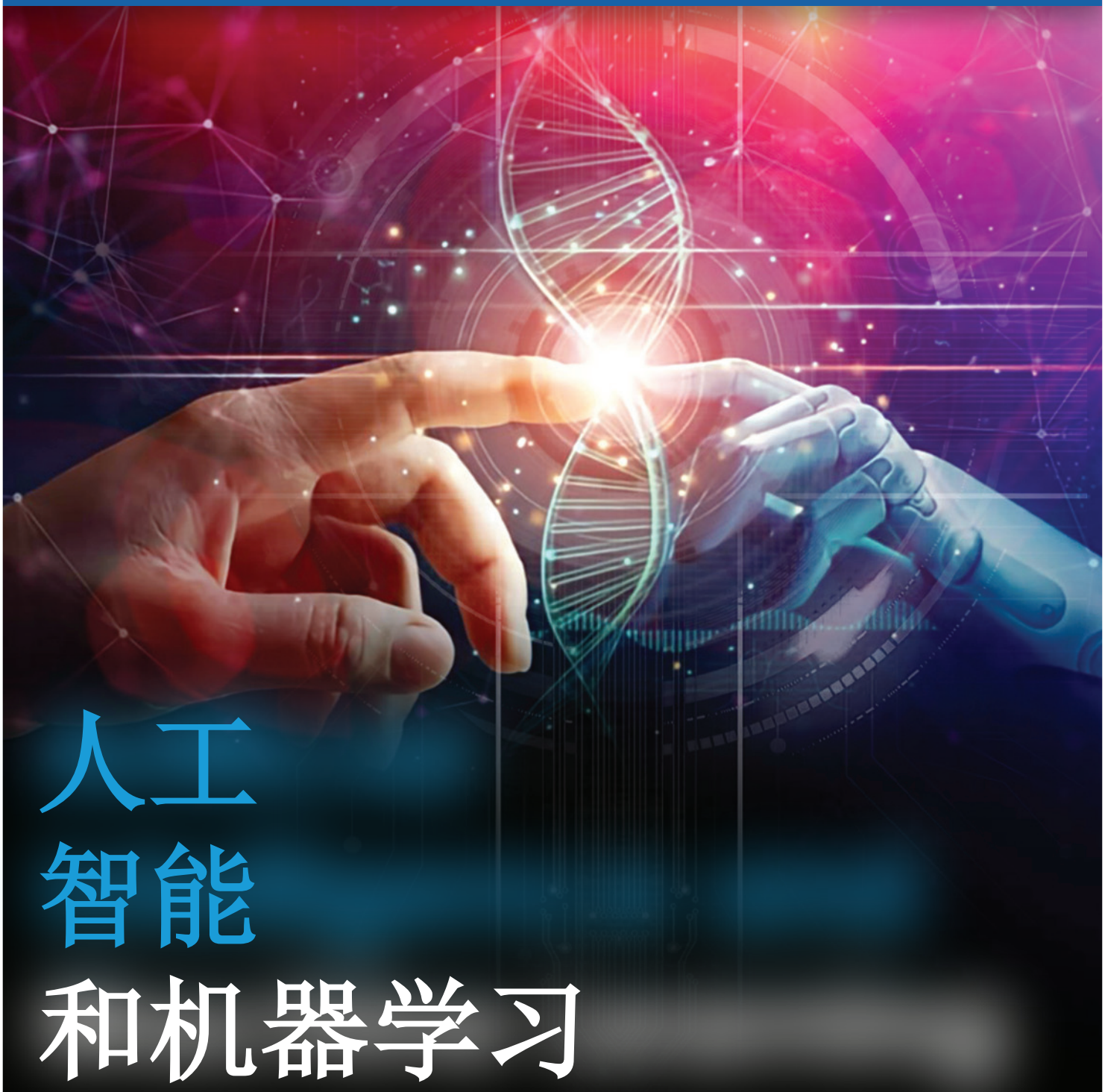
欢迎阅读2023年8月份的 In the **Boxing Ring**

本月，我们将讨论人工智能和机器学习（AI/ML）。近年来，我们看到人工智能/机器学习技术逐渐进入我们的日常生活。这些新技术不再按程序 "编程"。取而代之的是，它们被 "教授 "或 "训练 "预期的内容，并由机器模型本身决定 "如何 "完成。与所有此类工具一样，该技术也有好坏两面。在第 2 页至第 3 页，我们将通过提供三个如何将AI/ML 用于计算机安全的实例来谈谈AI/ML 的积极方面。

此外，Network Box 香港 出席了在香港會議展覽中心舉行的 Business GoVirtual 博览会。此外，Network Box Germany 的 Dariush Ansari 接受 it-daily.net 訪問，談及保安意識的好處，以及如何衡量成功與否。此外，在本月的全球安全头条新闻中，微软、苹果、思科和 Fortinet 都出现了安全问题。最后，最新一期的 HPCC Hackpod 现已发布。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2023

本月摘要:



人工智能和机器学习

近年来，人工智能和机器学习（AI/ML）技术逐渐进入我们的日常生活。从与 Siri/Alexa/Google Home 设备对话，到自动聊天应答系统、计算机视觉和自动驾驶汽车--这些新系统不再是按程序 "编程 "的。取而代之的是，它们被 "教授 "或 "训练 "预期的内容，并由机器模型本身决定 "如何做"。

我们已经习惯了计算机化系统的可预测性--给定相同的输入，就会一次又一次地得出相同的输出。2+2 永远等于 4。但是，这些新的AI/ML的行为却更加随机，它们能够适应不断变化的输入，有时能理解我们的要求，给人留下深刻印象，但有时也会以奇异的方式出现重大失误。

与所有此类工具一样，该技术也有好坏两面。在本月的文章中，我们将通过三个当今计算机安全领域使用人工智能/ML 的实例，来谈谈AI/ML 的积极意义。

1. 拒绝访问安全事件分析

几十年来，我们一直使用启发式方法来分析拒绝访问的安全事件。例如，设定每分钟拒绝网络端口访问的阈值，并在超过该阈值时发出警报/阻断。这就是经典的"端口扫描"拒绝。

这种方法有两个问题：

1. 阈值必须根据个别网络配置进行手动设置和调整
2. 慢速扫描（攻击者故意扫描得很慢）不会被检测到。

这些启发式方法是程序设计的典型例子--如果这样，那么那样。

AI/ML 模型提供了另一种方法。在这里，我们用正常的拒绝访问流量和目标攻击流量的示例来训练模型。我们通过实例对模型进行教学，并让它根据训练结果自动设置阈值。就像孩子一样，计算机也在学习--我们并不告诉它如何检测有针对性的攻击，而只是训练它这种攻击可能是什么样子的。训练完成后，我们就可以向模型输入真实网络事件流，它就会告诉我们它是否发现了值得应对的攻击行为（以便我们进行适当的更改/阻止/应对）。

这种方法不仅可用于端口扫描检测，还可用于更一般的高级访问拒绝，如应用程序登录、检测暴力或用户枚举类型的攻击。

2. 行为分析

虽然启发式方法在处理拒绝访问安全事件方面效果显著，但在网络行为分析方面并不好用。这里的要做的是为正常的网络流量设置阈值和标准，这样我们就能对任何异常情况发出警报。在协议执行方面已经取得了一些成功（如定义特定协议的特定数据包类型），但这种白名单方法非常费力，而且必须针对每个协议和应用程序进行定制。

人工智能/人工智能在这方面大有可为。我们只需用已知的良好行为来训练模型，然后让它对任何不同的行为发出警报，而不是对每个协议的行为和阈值进行程序化编程。

3. 元分析

一般行为分析关注协议和应用程序，而元分析则关注网络流量属性（如源和目标 IP 地址、授权用户、国家、网络、时间等）。在这里，人工智能/人工智能可以通过正常的网络流量进行训练，并对任何异常情况发出警报。例如，通常在周一至周五工作的用户在周日登录网络。

尽管 ChatGPT 如雨后春笋般崛起，但AI/ML 仍处于起步阶段，尤其是在计算机安全方面的应用。从历史上看，计算机在输入、输出和程序过程定义明确的情况下最为有用，但在处理模式匹配等较为模糊的问题时却举步维艰。AI/ML 更为 "模糊"，要求也不那么明确，主要问题是误报。AI/ML 的准确性往往给人留下深刻印象，但同样也经常会因不明原因而出现重大失误。

目前，Network Box Security Response 正在继续部署 AI/ML 模型，主要用于我们的 NBSIEM+ 事件分析和事故响应系统。在未来数月和数年内，我们预计这一工具将变得更加有用，并开始部署到外围网关保护和终端。

Network Box HIGHLIGHTS

Network Box 香港 Business GoVirtual博览会

Network Box 香港參加了在香港會議展覽中心舉行的 Business GoVirtual 博览会。在为期三天的展览中，参观者了解了 Network Box 屡获殊荣的安全技术和管理服务。此外，Network Box 董事总经理 Michael Gazeley 发表了题为 "万物的脆弱性 "的演讲。

月刊主办	联系方式
Mark Webb-Johnson 主编	Network Box CNNOC cnnoc@network-box.cn
Michael Gazeley **Kevin Hla** 产品支持	或者上门到: 深圳市福田区深南大道 竹子林求是大厦西座 920
Network Box HQ **Network Box USA** 贡献者	+86 (755) 3336 1581 www.network-box.cn

媒体报道和 安全头条新闻

it-daily.net
安全意识培训的成功是可以衡量的
LINK: https://bit.ly/43KB4jT

HPCC Hackpod Club
第 20 集：
网络安全作为横向入口
LINK: https://anchor.fm/hackpodclub

GB Hackers
微软消息队列服务漏洞允许 DoS 和 RCE 攻击
LINK: https://bit.ly/3KkoXDb

Bleeping Computer
拉扎罗斯黑客劫持微软 IIS 服务器传播恶意软件
LINK: https://bit.ly/3YcZMYW

Dark Reading
苹果零日漏洞影响 iPhone 内核
LINK: https://bit.ly/3OfusED

Security Week
思科企业交换机存在漏洞，攻击者可修改加密流量
LINK: https://bit.ly/43NsT6o

Bleeping Computer
300,000多台Fortinet防火牆易受關鍵FortiOS RCE漏洞影響
LINK: https://bit.ly/3Kk60kj