ivanti

机器学习在全面防范移动网络钓鱼中的作用

Ivanti Mobile Threat Defense 如何在设备上实现移动网络钓鱼攻击零日检测能力

目录

前言

网络钓鱼成为威胁至少有四分之一个世纪了，但移动设备的兴起使网络钓鱼变得更加有效和复杂，更难防范。

移动设备的使用现在超过了桌面设备的使用，特别是在企业用户中，于是网络犯罪分子将移动设备视为钓鱼攻击的主要目标。而移动设备让网络钓鱼攻击更有可乘之机，带来了全新的威胁途径和必须加以解决的独有技术问题。

在检测移动网络钓鱼攻击时，Ivanti Mobile Threat Defense (MTD) 知道保护必须落实到攻击实际发生 之处：设备上。而且这种保护必须利用机器学习，以防范零日威胁。

网络钓鱼攻击日益猖獗

网络钓鱼攻击的数量正在迅速增加。Verizon 的 2021年 Verizon 数据泄露调查报告 (DBIR) 发现，网络钓鱼连续第三年成为数据泄露事件中使用的首要手段。这一趋势没有停止的迹象，据 DBIR 数据显示，从 2019 年到 2020 年，牵涉网络钓鱼的数据泄露事件的比例上升了 25%（从 11% 到 36%）。这种增长有很多原因，包括对攻击者来说门槛较低。

网络犯罪分子能在几分钟内策划网络钓鱼攻击，并使攻击极难得到规模化检测。虽然网络攻击不保证一定成功，但许多网络犯罪分子发现，网络钓鱼是他们能做的并且最有把握的事情。

移动网络钓鱼要有新的应对方法

企业 IT 和安全团队使用各种反钓鱼对策来保护传统端点，其中大部分都集中在企业电子邮件上（例如电子邮件和网络网关、下一代防火墙）。即便所有这些保护措施都落实到位，也仍有很大的改进余地。II

而从安全角度来看，移动设备使事情变得更加具有挑战性。移动设备使网络钓鱼攻击更有可能得逞，它带来了全新的威胁途径和必须加以解决的独有技术/用户问题。

网络钓鱼攻击类型：

凭证式网络钓鱼使用大规模垃圾电子邮件广告活动。

鱼叉式网络钓鱼的针对性更强，包括利用付款通知、发票或 W-2 税表等附件发起攻击。

短信钓鱼使用短信。

鲸钓以企业高管为目标。

语音钓鱼是利用语音或电话的诈骗方式。

自动网络钓鱼攻击使用中间人 (MITM)漏洞来击败双因素验证。

十大原因使得移动设备更容易遭受网络钓鱼攻击

01 户自有设备

用户通常自行管理这类设备，缺乏企业台式机和笔记本电脑的自动化补丁和安全流程。

02 屏幕太小。

屏幕尺寸小，使其更难访问和查看关键信息。

03 操作系统和应用 = 极好的藏匿地点。

操作系统和应用制约用户获得正确评估电子邮件、网页等真实性所需的信息。

04 用户太信赖

用户跟自己的移动设备关系太亲近，形成了对该设备及其中内容的无脑信任。

05 无法并行查阅

很难或无法并排查看网页和其他数据。

06 先看清再点击。

用户界面限制了可用信息量，同时促使用户快速作出决定。

07 切换麻烦

在网页或应用之间切换很麻烦。

08 短信 = 急事。

用户觉得短信都是比较急的事，因此不太会去核实别人通过短信发来的请求。

09 不问就说。

GUI 设计鼓励诸如接受、回复、发送、点赞等操作，这促使用户回应请求。

10 一心两用。

用户边走路、说话、开车边使用移动设备，在这种一心两用的情况下可能收到请求就回应 了，不会费心去看发出请求的应用，这使得他们更有可能接受请求。

移动设备独有的技术/用户问题

移动设备常被认为是个人设备，不管它是归组织还是用户所有。即使移动反网络钓鱼解决方案能够保护企业，但其最终能否成功与用户对各种技术因素的态度密切相关，包括：

- **耗电。**
  如果用户认为该方案太耗电，他们可能卸载该保护方案。
- **内存。**
  如果用户认为该解决方案太占内存（例如带有一个很大的已知不良网址数据库），那么他们可能卸载该保护方案。
- **数据用量/成本。**
  如果用户认为该解决方案使用了太多他们的数据流量（例如对每个可疑网址都要进行云查找），那么他们可能卸载该保护方案。
- **用户隐私。**
  如果用户认为该解决方案正在将个人信息（包括他们正在浏览的内容）从设备上发送出去（例如通过云查询功能），那么他们可能会卸载保护方案。

新的移动网络钓鱼途径能绕过现有解决方案

企业电子邮件是传统端点上网络钓鱼的主要攻击途径。由于三分之二的电子邮件是在移动设备上阅读的，而且大多数企业移动用户没有对所有流量使用永远在线的 VPN，因此该途径在移动设备上非常危险。移动设备还带来了一些现有解决方案无力防范的新攻击途径，包括：

- **个人电邮。**
  当用户在移动设备上访问其个人电子邮件时，企业电子邮件网关检测网络钓鱼攻击的功能就派不上用场。
- **短信和消息应用（例如微信）。**
  虽然电子邮件账户可能有保护措施，但短信和消息应用则没有
- **恶意应用（例如BankBot）。**
  传统反钓鱼技术没有能力检测恶意应用模仿合法应用来窃取凭证的钓鱼行为。

移动设备反网络钓鱼之关键：基于机器学习的设备内置检测功能

虽然网关和防火墙可以保护传统端点免受基于电子邮件的网络钓鱼攻击，但移动设备存在我们前面讨论到的所有新途径/问题，而且大部分时间都在企业网络之外。此外，虽然已知威胁网址列表可以帮助保护电子邮件（例如提取尚未查看的电子邮件），但它们并不能防范移动设备可能通过短信等途径实时访问的零日钓鱼网站。

在检测移动网络钓鱼攻击时，Ivanti 知道保护必须落实到攻击实际发生之处：设备上。而且这种保护必须利用机器学习，以打击零日威胁。

MTD 成熟可靠的机器学习方法非常适用于在无处不在的工作空间保护企业移动安全。我们的机器学习引擎分析系统数据并从中识别恶意行为，然后创建复杂的数学模型以实现设备本地检测。MTD 不是在寻找与已知攻击之间的特定或部分匹配（如网络钓鱼案件中的网址）；它是通过那些表明威胁正在发生或即将发生的示警行为来识别攻击，甚至是那些从未见过的攻击。

MTD 基于机器学习在设备上检测设备、网络、钓鱼和恶意应用攻击。

虽然创建一个基于机器学习的高效检测引擎（比如 MTD 所用的这个）很复杂，而且需要多年的数据收集和训练，但通过参照其他生活领域的简单类比，可以更好地理解这一概念。

例如，凭借多年训练，然后问患者几个关键问题，心脏外科医生就可以查看心电图读数并立即做出诊断。她不需要事先知道患者有某种病症；她通过了解哪些数据是相关的（以及哪些数据应该被忽略）对其加以确定并做出准确诊断。机器学习也是同样道理，只不过是自动的。

对于针对性攻击，黑客……

1. 使用未知或变异攻击，旨在避免简单的确定性检测。
2. 专注于侵害设备，这是持久利用并且未来对该设备加以掌控/劫持的主要方式。
3. 利用中间人 (MITM) 攻击或网络钓鱼技术来提供侵害设备所需的漏洞。在大多数情况下，他们不会在 App Store 或 Google Play 上投放应用并寄望目标组织的人会下载它。

因此，企业移动安全解决方案必须……

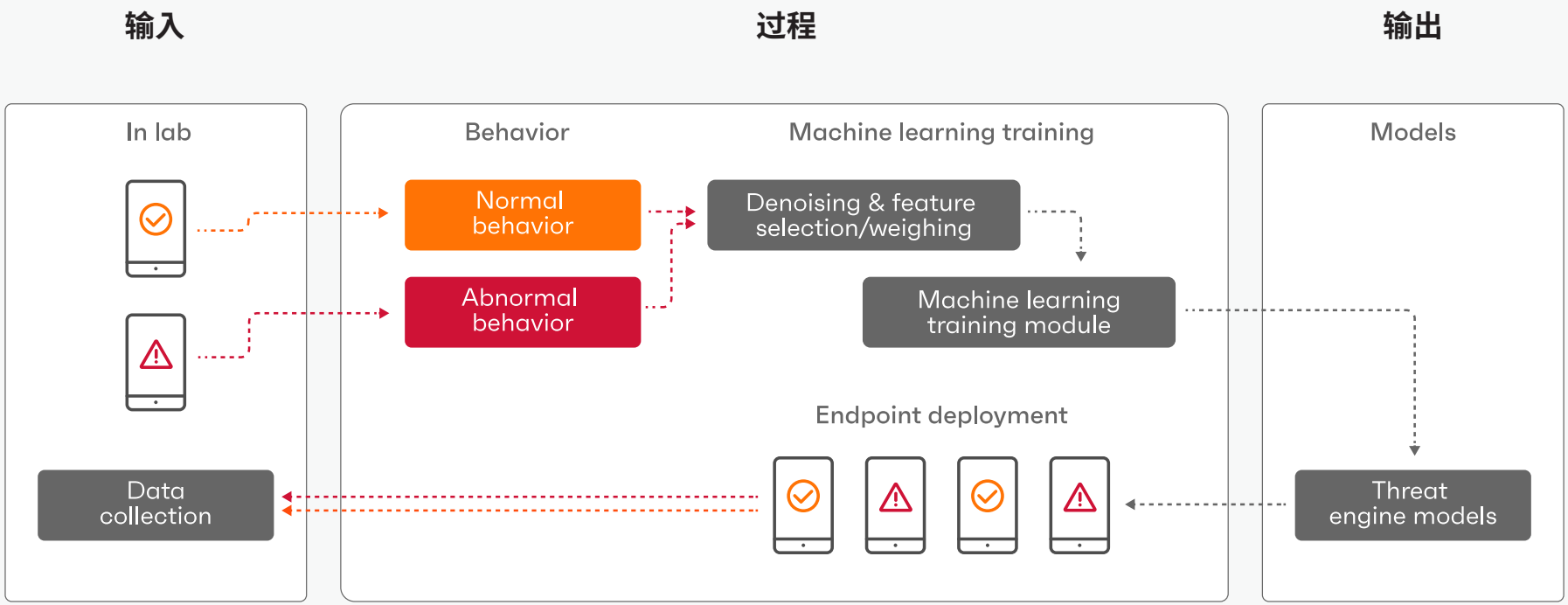
1. 用基于机器学习的检测来增强任何确定性方法，以阻止针对目标的未知/变形攻击。
2. 同时覆盖整个设备的所有攻击途径。单一的故障点就足以完全破坏一个设备。
3. 在设备上检测威胁，不需要基于云的查询。如果攻击者使用 MITM 或恶意接入点，他就会控制网络，不会将设备连接到任何基于云的检测解决方案。
4. 因地制宜解决问题，例如：
   a. **训练。**鉴于有数十亿的数据点需要分析，机器学习训练应该在云端离线进行。
   b. **检测。**为了防止 MITM 规避和其他与基于云的方法相关的风险，实际检测必须在设备上就地进行。

Ivanti 坚信关于企业移动安全的几个基本事实

秉持以上这些原则，接下来内容将阐述 MTD 如何实现和执行基于云的机器学习训练和基于设备的钓鱼网站检测。我们相信这个组合是提供有效的企业移动安全的唯一途径。

训练：基于云的机器学习

为了创建高度准确的移动威胁预测器，像 MTD 使用的这类机器学习引擎必须分析（并反复重新分析）数以十亿计的数据点。为了处理如此大量的数据，Ivanti 利用云端数十个高性能计算集群来建立其机器学习模型。然后在设备上评估这些模型，以即时检测哪怕是之前未知的威胁——甚至在断开连接的情况下。



D检测：在设备上并且基于机器学习

秉持“因地制宜解决问题”的理念，繁重的机器学习任务放在云端进行。但在模型被交付给设备后，所有的实际检测都在设备上实时进行。

以下是这种在设备上基于机器学习的检测方法的优点：

- **检测未知威胁。**
  与确定性解决方案不同，机器学习甚至可以检测之前未知的威胁或零日威胁。
- **机器速度检测。**
  由于移动攻击是以机器速度发生的，防护方案必须能够以同样速度做出响应。只有实时、设备本地检测才能与机器速度相匹配。云端查询不能匹配这种速度，因为它们存在与网络延迟等因素相关的各种可能。
- **最高程度的隐私保护。**
  通过在设备上执行所有检测，可能有敏感性的数据就不需要外流到云端。
- **断网保护。**
  设备本地检测可以即时防范 MITM 这类网络攻击，而它们可以使基于云的检测失去作用。只有设备本地检测能在断网时继续提供保护。

分清炒作与真相

如今，大多数移动安全供应商都声称自己用了机器学习方法。要确定任何供应商（包括 MTD）所用方法的真实性，请问这些问题：

1. 所谓机器学习功能是否不需要零号病例或牺牲品就能发挥作用？
2. 机器学习数学模型的广泛性如何，它在现实世界中测试了多少年？
3. 解决方案多久需要更新一次，添加新的网址（用于网络钓鱼检测），以检测最新的威胁？
4. 机器学习功能是否在连网和断网环境下都能发挥作用？
5. 保护方案能否在几毫秒内发挥作用，并且对CPU 和电池使用的影响很小？

以隐私为中心的网址评估机制

为了开展移动网络钓鱼检测，必须为解决方案提供可疑网址。这里使用的主要机制有两种。

1. **手动提交。**大多数解决方案为用户提供了手动提交网址供测试的功能，但这需要用户有这方面的意识和培训，不仅是网络钓鱼方面的知识，还要知道如何长按并提交给网络钓鱼解决方案。
1. **自动评估。**为了监测所有流量以识别恶意网 址，解决方案通常使用 VPN 来自动实现网址评估。

对于每一种机制，MTD 的设备本地检测方案都有胜过基于云的解决方案（如果它们有这些机制的话）的关键优势：

- **手动提交。**由于 MTD 在设备上执行所有检测，用户的隐私得到保护。可能有敏感性的数据（包括正在浏览的网站）不需要外流到云端。
- **自动评估。**除了上述手动提交中提到的隐私优外，MTD 的设备内 VPN 在耗电量上远低于基于云的解决方案所需的设备外 VPN，因为它不必建立和加密发往云端的出站会话

全面防范移动网络钓鱼攻击

在“无处不在的工作空间”中，企业数据在设备和云 端服务器之间自由流动，Ivanti 使您的员工能够随时随地安全地工作，即使移动钓鱼攻击日益猖獗。Ivanti 面向 iOS 和 Android 设备的多途径移动网络钓鱼防护方案可以检测并修复当今复杂的移动网络钓鱼攻击。

多层次安全战略：

- **消除密码。**
  减少因凭证失窃而导致的数据泄露风险。
- **针对移动威胁的设备本地检测及修复。**
  基于机器学习，防范设备、网络、应用层面和网络钓鱼攻击 (DNAP)。无需 Wi-Fi 或蜂窝网络连接。
- **多途径反钓鱼攻击。**
  设备内置机器学习和钓鱼网址查询经扩展后可添加云端查询功能，进一步提高防范效果。
-

  制定并执行合规策略以保护无处不在的工作空间。

实现反钓鱼方案 100% 的用户采用率

MTD 实现了反钓鱼方案的无缝部署，以及对设备、网络和应用层面钓鱼攻击的防护和修复。激活不需要用户互动，因此管理员可以确保 100% 采用。可以利用分层合规行动来帮助推动和保持采用率，以改善组织的整体安全态势。

部署多途径网络钓鱼防护及修复

MTD 反钓鱼软件可以检测和修复所有移动威胁途径上的钓鱼攻击，包括文本和短信、即时讯息、社交媒体和其他通信方式，而不仅仅是企业电子邮件。多途径网络钓鱼防护功能利用设备本地机器学习和数据库查询。经扩展后还可包括基于云的网络钓鱼网址数据库查询功能，以获得更好的效果。此外，网络钓鱼分析功能可以快速简单地为您提供洞见，让您更好地了解组织反网络钓鱼覆盖情况。

控制企业安全和用户隐私之间的平衡

MTD 反钓鱼方案使您的组织能够完全掌控，在企业安全和用户隐私之间保持平衡，以最好地满足您的需求和舒适度。利用 MTD 高效的设备本地网络钓鱼检测功能，或者轻松地将检测扩展到云端。选择权在您手中！

关于 Ivanti

Ivanti让无处不在的工作空间成为可能。在“无处不在的工作空间”，员工使用各种各样的设备访问IT网络、应用和数据，以便能随时随地保持工作效率。Ivanti自动化平台连接业界领先的统一端点管理、零信任安全和企业服务管理解决方案，通过单一管理界面让企业实现设备的自我修复和自我保护，让终端用户实现自我服务。已有超过40,000家客户，包括78家财富百强企业，选择了Ivanti来为他们发现、管理、保护和服务从云端到边缘的IT资产，并为员工提供卓越的终端用户体验，无论他们在哪里、以什么方式工作。更多信息请访问 www.ivanti.com.cn

www.ivanti.com.cn
8610 8541 2999
ContactChina@ivanti.com

I. Verizon: 2021 Data Breach Investigations Report. - https://enterprise.verizon.com/resources/reports/dbir/
II. NewsWise: Tech companies not doing enough to protect users from phishing scams. - https://www.newswise.com/articles/tech-companies-not-doing-enough-to-protect-users-from-phishing-scams/sc-rsbn