Robust Intelligent Malware Detection Using Deep Learning

> 使用深度学习进行稳健的智能恶意软件检测

Abstract

- 当前的恶意软件检测解决方案采用静态和动态分析恶意软件签名和行为模式，这在识别未知恶意软件方面既耗时又无效。
- 新的恶意软件主要是现有恶意软件的变种，因此最近使用机器学习算法 (MLA) 来进行有效的恶意软件分析。这需要大量的特征工程、特征学习和特征表示。
- problems:
  - 通过使用深度学习等高级 MLA，可以完全避免特征工程阶段。尽管最近在这个方向上存在一些研究，但算法的性能会受到训练数据的影响。需要减少偏见并独立评估这些方法，以便获得有效的零日恶意软件检测的新增强方法。
- 这项工作评估了经典 MLA 和深度学习架构，用于使用公共和私有数据集进行恶意软件检测和分类。
- 提出了一种新颖的图像处理技术，具有用于 MLA 和深度学习架构的最佳参数。
- 提出了使用可扩展和混合深度学习框架进行实时部署的恶意软件的有效视觉检测。
- 大数据环境中基于静态、动态和图像处理的混合方法的可视化和深度学习架构是一种有效的零日恶意软件检测的新增强方法。

1.Introduction

> 恶意软件是一种旨在对操作系统 (OS) 造成损害的计算机程序。恶意软件根据其目的和行为获得不同的名称，例如广告软件、间谍软件、病毒、蠕虫、特洛伊木马、rootkit、后门、勒索软件和命令与控制 (C&C) 机器人。

Introduction Background

- 防病毒软件程序旨在通过与不时更新的病毒定义数据库匹配来检测此类恶意软件的存在。这称为基于签名的恶意软件检测，它也可以执行启发式搜索来识别恶意软件的行为。
  - 这种经典方法的主要挑战是恶意软件的新变种使用防病毒规避技术，例如代码混淆。
  - 基于签名的恶意软件检测系统需要广泛的域级知识来使用静态和动态分析对恶意软件进行逆向工程并为其分配签名。

    - 基于签名的系统需要更长的时间来对恶意软件进行逆向工程，在此期间攻击者会侵入系统。
    - 基于签名的系统无法检测新型恶意软件。
    - 介绍了一些前人相关的研究工作，构成了研究动机。

Need for study

- 机器学习算法 (MLA) 依赖于特征工程、特征选择和特征表示方法。具有相应类的一组特征用于训练模型，以便在良性和恶意软件之间创建分离平面。该分离平面有助于检测恶意软件并将其分类为相应的恶意软件系列。
- 各种特征可以通过静态和动态分析获得。静态分析是一种在不执行的情况下从二进制程序中获取信息的方法。动态分析是在隔离环境中在运行时监控恶意软件行为的过程。
- 存在的问题：
    - 动态分析无法部署在端点实时恶意软件检测中，因为分析其行为需要花费大量时间，在此期间可以交付恶意负载。
    - 与静态收集的数据相比，基于动态分析的恶意软件检测方法对混淆方法更加稳健。
    - 基于经典机器学习的恶意软件检测系统的主要问题是它们依赖于需要广泛领域级知识的特征工程、特征学习和特征表示技术。此外，一旦攻击者了解这些特征，就可以轻松绕过恶意软件检测器。
    - MLA 需要包含各种恶意软件模式的数据。由于安全和隐私问题，用于恶意软件分析研究的公开可用基准数据非常少。
    - 尽管存在用于抓取恶意软件数据集的公开可用资源，但为研究准备合适的数据集是一项艰巨的任务
- 深度学习是一种改进的神经网络模型，在多个领域存在的许多任务中，其性能优于经典 MLA。在训练过程中，它试图捕获深层隐藏层中特征的更高级别表示，并具有从错误中学习的能力。
- 当 MLA 看到越来越多的数据时，他们会经历输出减少，而深度学习捕获新模式并与已经捕获的模式建立关联，以提高任务的性能。

Contributions

> 提出了一种称为 ScaleMalNet 的用于恶意软件检测的可扩展深度学习网络架构，该架构能够利用大数据技术的应用来处理不同数量的恶意软件样本。

- 一个可扩展和混合框架的新提议，即 ScaleMalNet，它有助于以分布式方式从不同来源收集恶意软件样本，并以分布式方式应用预处理。该框架能够实时和按需处理大量恶意软件样本。
- 一种用于恶意软件分类的新型图像处理技术的提议。
- ScaleMalNet 采用两阶段方法:
    - 第一阶段使用静态和动态分析将可执行文件分类为恶意软件或合法文件。
    - 第二阶段将恶意软件可执行文件分类为相应的恶意软件家族。
- 对经典 MLA 和深度学习架构的独立性能评估，对各种恶意软件分析模型进行基准测试。

本文结构分布

- 第二节回顾了关键的恶意软件分类模型，考虑了传统上用于恶意软件分析的各种方法。
- 在第三节中，引入了深度学习架构以深入了解这一研究背景。
- 第四部分介绍了本研究中深度学习的实现架构以及用于评估分类器性能的统计措施。
- 第五部分描述了使用基于静态分析的深度学习进行恶意软件分类的实验和观察。
- 第六节讨论了使用基于动态分析的深度学习进行恶意软件分类的实验研究和结果。
- 第七节展示了我们基于
- 用于恶意软件分类的新型图像处理技术的深度学习架构的实验结果。
- 第八节提供了 ScaleMalNet 的详细信息。
- 最后，提供了本研究的结论和未来的工作。

2.恶意软件分类模型

> 在本节中，我们将讨论一些流行的恶意软件检测分类模型的优缺点，传统上使用静态和动态分析，以及它们近年来的变化。

使用静态分析的恶意软件分类

> 一些安全研究人员已将可移植可执行文件 (PE) 的域级知识应用于静态恶意软件检测。目前，字节 n-gram 和字符串的分析是两种最常用的静态恶意软件检测方法，无需域级知识。

- problems:
  - n-gram 方法的计算成本很高，而且性能相当低。
  - 在构建机器学习模型以区分恶意软件和良性文件时，通常很难应用领域级知识来提取必要的特征。这是因为 Windows 操作系统并没有始终如一地强加自己的规范和标准。
  - 由于规范和标准不时不断变化，恶意软件检测系统需要进行修订以满足未来的安全要求。
- solutions:
  - 应用了机器学习算法 (MLA)，其特征是从 PE 文件的解析信息中获得的。
- 传统上采用深度学习的经典全连接网络和循环神经网络 (RNN) 模型来检测具有来自 PE 头文件的 300 字节信息的恶意软件。
- 本文提出了应用 Windows-StaticBrain-Droid (WSBD) 模型来整合深度学习。

使用动态分析的恶意软件分类

> 与静态分析相比，基于动态分析的恶意软件分析方法对混淆方法更具鲁棒性。

- 介绍了一些前人的研究成果

- 在这项工作中，我们提出了 Windows-Dynamic-Brain-Droid (WDBD) 模型，该模型评估各种经典机器学习算法 (MLA) 和深度学习架构的有效性，以了解哪种算法最适合 Windows 恶意软件分类。我们使用两个不同的数据集，其中包含不同数量的恶意软件和在不同执行时间捕获的良性样本。

使用图像处理技术的恶意软件分类

> 恶意软件攻击呈上升趋势，最近几天，新的恶意软件很容易生成为已知恶意软件家族中现有恶意软件的变体。为了克服这个问题，了解恶意软件的相似特征很重要，这有助于将其归入其家族。

- 图像处理技术既不需要反汇编也不需要代码执行，与静态和动态分析相比，它更快。这种方法的主要优点是它可以处理打包的恶意软件，并且可以在不考虑操作系统的情况下处理各种恶意软件。
- 介绍了前人的一些研究成果
- 在本文的工作中，我们在同一数据集上应用深度学习架构，旨在提高恶意软件识别性能。详细的实验分析是在 Malimg 数据集上进行的，以了解每个恶意软件家族的特征。最后，我们提出了 DeepImageMalDetect (DIMD)，它利用深度学习和图像处理方法进行恶意软件分类。所提出架构的性能与其他深度学习架构和经典机器学习分类器进行了比较。所有这些方法都在基准数据集上进行评估，并且这些方法的性能也显示在最近收集的私人恶意软件样本上。
- 我们提出了一种名为 ScaleMalNet 的混合恶意软件分析系统，它由 Windows-Static-Brain-Droid (WSBD)、Windows-Dynamic-Brain-Droid (WDBD) 和 DeepImageMalDetect (DIMD) 组成。这可以更准确地实时检测恶意软件。深度学习架构的细节、实现架构和不同方法的分析如下。

3.深度学习架构

> 深度学习体系结构的主要优势是，当数据量很大时，能够理解数据的含义，并自动调整新数据的派生含义，而不需要领域专家知识。

- 卷积神经网络 (CNN) 和循环神经网络 (RNN) 是两种主要应用于现实生活场景的深度学习架构。
- 通常，CNN 架构用于空间数据。
- RNN 架构用于时间数据。
- CNN 和 LSTM 的组合用于空间和时间数据分析。

深度神经网络(DNN)

- 前馈神经网络 (FFN) 创建一个有向图，其中一个图由节点和边组成。
- FFN 沿边缘将信息从一个节点传递到另一个节点，而不形成循环。
- 多层感知器 (MLP) 是一种 FFN，它包含 3 层或更多层，特别是一个输入层、一个或多个隐藏层和一个输出层，其中每一层都有许多神经元，在数学符号中称为单元。
- 通过遵循超参数调整方法来选择隐藏层的数量。信息从一层向前转换到另一层，而不考虑过去的值。而且，每一层的神经元都是全连接的。

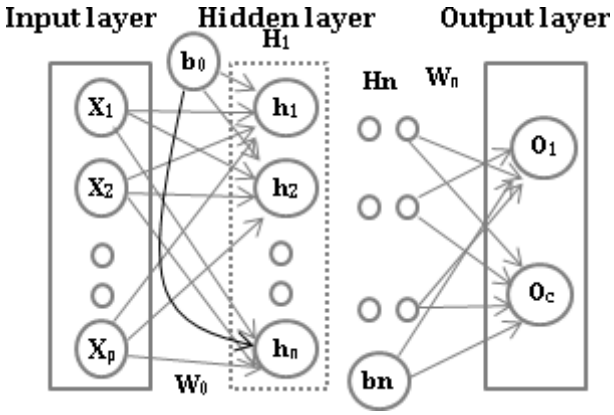

图 1：具有n个隐藏层的 DNN 架构。

卷积神经网络(CNN)

> 卷积网络或卷积神经网络或CNN 是对经典前馈网络(FFN) 的补充，主要用于图像处理领域。

- 在本文中，CNN 网络由卷积一维层、池化一维层和全连接层组成。一个 CNN 网络可以有多个卷积 1D 层、池化 1D 层和全连接层。
- 在卷积 1D 层中，过滤器在 1D 序列数据上滑动并提取最佳特征。从每个过滤器中提取的特征被分组到称为特征映射的新特征集中。过滤器的数量和长度是通过遵循超参数调整方法来选择的。这反过来在每个元素上使用非线性激活函数 ReLU。
- 使用最大池化、最小池化或平均池化的池化一维层来减少最优特征的维度。由于在最大池化中选择了选定区域内的最大输出，因此我们在这项工作中采用了最大池化。
- 最后，CNN 网络包含用于分类的全连接层。在全连接层中，每个神经元都包含与其他每个神经元的连接。除了将池化一维层特征传递到全连接层之外，还可以将其传递给循环层、LSTM 以捕获序列相关信息。
- 最后，LSTM 特征被传递到全连接层进行分类。

循环结构

> 循环结构具有学习数据中序列信息的能力。众所周知的循环结构是循环神经网络(RNN)和长短期记忆(LSTM)。