基于大数据的混合恶意软件检测系统

□曾睿昊　福建师范大学海外教育学院

【摘要】　近年来，由于恶意软件的日益扩散，人们期望采用先进的机器学习算法来及时检测其产生的新威胁。基于云的方法允许利用客户端代理产生的大数据来训练这些算法，但另一方面，这对算法的可扩展性和性能构成了严峻的挑战。本文提出了一种基于云的混合恶意软件检测系统，将静态分析和动态分析相结合，在响应时间和检测精度之间找到了一个较好的折衷。我们的系统通过利用客户提供的不断增长的数据，基于深度网络执行其模型的持续学习过程。初步的实验评估证实了本文提出的方法的适用性。
【关键词】　大数据　恶意软件检测　深度学习　云计算

引言：如今，来自不同通信渠道的恶意软件的意外执行使 IT 系统不断暴露在风险之中。因此，恶意软件检测是计算机安全科学家面临的最关键问题之一。即使在威胁不断增加的情况下，要保证高检测率，最有希望的方法之一就是采用基于云的解决方案。这种方法允许通过能够分析大量潜在感染文件的机器学习技术来远程执行恶意软件检测。

一、系统结构

本文提出了一种基于云的恶意软件检测系统，该系统将静态分析和动态分析相结合，如图 1，以提供对超大规模可执行文件的快速分类。我们的系统基于大数据管理基础设施，能够实时摄取数据，并支持利用这些数据来完善底层模型的持续学习过程。客户端将待分析的可执行文件发送到请求管理器 (RM)(1)，请求管理器 (RM)(1) 是负责驱动整个恶意软件检测过程的云代理。Request Manager 通过应用简单的散列过滤器来区分新文件和已收到的副本。每个以前未见过的可执行文件被存储为未分类数据的新样本，并将在后续学习阶段 (2) 中使用。恶意软件检测由静态分析子系统 (SA)(3) 执行，该静态分析子系统 (SA)(3) 基于能够通过轻量级处理通过处理文件的一小部分来获得良好分类精度的深层网络。然后，大数据基础设施 (BDI) 将通过动态分析获得的分类结果与分析的文件 (5) 相关联，从而构建用于持续学习过程的新的标签文件集。最后，将分类结果传送给客户端 (6)。

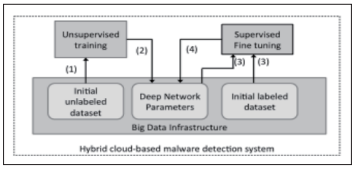

图 1　基于云的恶意软件检测系统 .

在第一步，不是随机初始化模型参数，而是对未标记的数据集执行无监督的预训练，以便获得隐藏层的权重和偏差的第一估计。第一个学习阶段通过堆叠去噪自动编码器来实现。根据这种模型，借助于由输入层、被破坏层、编码器和解码层组成的支持网络分别对每个隐藏层进行预训练，其中编码层对应于待预训练的隐藏层。相反，输入层、被破坏层和解码器层具有相同的节点数，这等于要预训练的隐藏层的输入数 ,。这种方法可以克服深度网络设计中最相关的问题之一，即可利用大量数据进行培训。此外，利用不同时间间隔收集的数据集，允许网络动态跟踪软件的不断演化。

二、实验结果分析

首先，我们想要调查用于训练深层网络的历元数与整个系统的性能之间是否存在联系。为此，我们比较了通过改变预训练阶段的最大训练周期阈值 (即 600、800 和 1000) 获得的性能。第二个评估旨在评估训练前阶段的有效性，将我们的系统与具有相同拓扑结构的深层网络进行比较，但只通过第二个训练阶段进行训练。最后，我们打算验证我们的深层分类器的分层对恶意软件检测系统整体性能的影响。为此，我们将我们的系统与一个经典的神经网络进行了比较，该神经网络是通过去除分类器中最后两个隐含层而得到的，从而分别得到了 636、256 和 1 个节点的三层。评估是通过分层抽样的 K 倍交叉验证来执行的，以便在 K=5 的情况下保持每类样本的百分比。

表 1　性能指标的平均值

Classifier	Loss	Accuracy (%)	Precision (%)	TPR (%)	FPR (%)	AUC (%)
Deep model (600)	0.075	97.39	97.48	**97.33**	2.55	97.39
Deep model (800)	**0.074**	**97.48**	**98.09**	96.88	**1.91**	97.48
Deep model (1000)	**0.074**	**97.49**	97.92	97.08	2.09	**97.49**
Deep model (*fine tuning* only)	0.087	96.73	96.69	96.82	3.37	96.73
Classic-623-256	0.095	96.48	95.98	97.10	4.15	96.47

在表 1 中，显示了所考虑的性能指标的平均值。我们可以观察到，使用预先训练的分类器可以获得更高的准确值，这证实了两阶段训练的有效性。然而，增加训练前时段的数量 (例如，从 600 个增加到 800 个或 1000 个) 不会显著提高精度，也不会降低损失值。

总结：在这项工作中，我们提出了一个基于云的恶意软件检测系统，能够面对网络上产生的大数据量。我们的系统基于深度网络执行静态分析，以提供对潜在恶意软件文件的快速分类，而只有当检测不确定性超过给定阈值时，才会进行更繁琐的动态分析。利用客户端代理产生的连续数据流和动态分析的分类结果来细化连续学习循环中的深层网络。这样的机制使得系统对于新的恶意软件版本总是最新的。

参 考 文 献

[1] J. H. Abawajy, A. Kelarev, and M. Chowdhury, “Large iterative multitier ensemble classifiers for security of big data,” IEEE Trans. on Emerging Topics in Computing, vol. 2, no. 3, pp. 352–363, 2014.
[2] L. Xu, D. Zhang, N. Jayasena, and J. Cavazos, “Hadm: Hybrid analysis for detection of malware,” in Proc. of the SAI Intelligent Systems Conf.,2016, pp. 1037–1047.