**一种融合了efficient-net和1d-cnn的恶意代码分类方法**

**摘 要**

近几年来，恶意代码的数量在不断上升,恶意代码的溯源问题日益凸显。而目前主流的将恶意代码转换成图片,进而使用图像分类的对恶意代码进行分类的方法，需要对恶意代码进行裁剪以及变换，从而将恶意代码转换为二维的图像。这种方法会损失恶意代码作为一维数据本身的部分信息，并且可能会增加恶意代码本身并不存在的空间特征。针对以上问题，本文提出了一种方法，将efficient-net和1d-cnn相融合的恶意代码分类模型，将恶意代码的二进制文件分别转换为1维矢量和图像后，分别输入两个网络，在反向传播时对两个网络同时进行修正。这种方法既保存了恶意代码的纹理特征，同时也让恶意代码本身的一维特征得以保存，从而在爬取的38个类别的数据集上表现出了更好的性能，本文的平均分类准确率达。

**一 研究背景**

在计算机历史上，最早记录的恶意软件出现在20世纪70年代。后来，在80年代早期，出现了elk克隆，它是一种针对Apply II型电脑的启动区病毒[1]。之后，恶意代码的编写者和安全人员之间便开始了一场无止休的军备竞赛，一方面，安全人员在不断寻找新方法去提高恶意代码的检测能力，另一方面，恶意软件编写者也在不断提高代码的混淆能力以试图躲过检测。

为了有效的抵抗恶意软件的攻击，安全人员研究了一系列对抗恶意软件的方法。最早的方法是基于签名的启发式的方法，通过签名来识别特定的恶意代码，但这种方法很容易受到混淆、加密等恶意代码形变技术的攻击。而随着深度学习技术的不断发展，越来越多的研究开始集中在使用深度学习检测恶意代码中。网络安全专家普遍认为，人工智能支持的反恶意软件工具有助于检测新型恶意软件攻击，并改进扫描引擎[1]。深度学习在恶意代码检测领域在重现它在其他领域的成功。例如，[2]和[3]提出的建立一个卷积神经网络来从文件的原始字节确定PE是否为恶意可执行文件。

为了更好的研究恶意代码的动机以及采取更有效的应对措施，研究人员将恶意代码分为不同的家族，并以此产生了对恶意代码家族分类的研究。当前对于恶意代码的分类主要有提取静态特、动态特征以及混合特征三种方法，在提取特征后，使用不同的机器学习模型或者深度学习模型进行训练，得到一个恶意代码的家族分类模型给。一种主流的方法是将恶意代码先转换为图像，然后用CNN对其进行建模，论文[]最早提出了这种方法。随后，越来越多的学者开始集中于对恶意代码的图像分类的研究中。

然而，在这些研究中，存在着一个明显的问题，恶意代码本身为一维数据，如何转换为二维数据？目前的方法在将恶意代码转换为图像后，它的宽度，高度都被设置为一个固定值，这是及其不合理的，因为恶意代码的大小是不一样的。其次，为恶意代码设置一个宽度将它截断可能会导致其语义上的不连贯性。

为了解决这个问题，本文主要做出了以下几点贡献：

1. 首次将efficient-net和1d-cnn网络结合，既保留了恶意代码的空间特征，也最大限度地保留了恶意代码地语义完整性，从而提取出更加具有代表性地恶意代码家族特征。
2. 对单纯使用恶意代码图像和将本文提出的方法进行了对比，验证了单纯的将恶意代码转换为图像后，会丢失掉恶意代码原有的部分语义信息。
3. 使用openmax层替换softmax层，提出一种解决恶意代码的开放集识别问题的方法。