 DOI: https://doi.org/10.12349/iser.v4i5.1729

Analysis of Mobile Internet Malicious Code Monitoring Technology

Bo Lu Shicong Song Yan Yang Ruipeng Zhou

Xinjiang Information Industry Co., Ltd., Urumqi, Xinjiang, 830000, China

Abstract

With the rapid development of mobile Internet, the threat of malicious code to mobile devices is also increasing. Malicious code refers to the computer system or mobile devices can destroy, steal information or against user will of software program, mobile Internet malicious code is divided into many types, including viruses, worms, Trojan, spyware, etc., if not timely processing, is likely to cause a series of danger to user information. Based on this, this paper mainly to mobile Internet malicious code not core, introduces the common types and transmission routes of mobile Internet malicious code, as well as the development and application of monitoring technology, and analyzes the main monitoring technology and its advantages and disadvantages, points out that the future should strengthen the mobile Internet research and application of malicious code monitoring technology.

Keywords

mobile Internet; malicious code; detection technology

移动互联网恶意代码监测技术浅析

鲁博 宋仕聪 杨艳 周瑞鹏

新疆信息产业有限责任公司，中国 · 新疆 乌鲁木齐 830000

摘 要

随着移动互联网的快速发展，恶意代码对移动设备的威胁也日益增加。恶意代码是指能够给计算机系统或移动设备带来破坏、窃取信息或违反用户意愿的软件程序，移动互联网恶意代码分为多种类型，包括病毒、蠕虫、木马、间谍软件等，若未及时对其进行处理，很可能对用户信息造成一系列危险。基于此，论文主要以移动互联网恶意代码为核心，介绍移动互联网恶意代码的常见类型和传播途径以及监测技术的发展和应用，并针对目前主要的监测技术及其优缺点展开分析，指出未来应加强移动互联网恶意代码监测技术的研究和应用。

关键词

移动互联网；恶意代码；监测技术

1 引言

随着移动互联网的快速发展，移动设备在日常生活中扮演着主要角色。然而，由于移动设备的开放性和全球化互联网的便利性，移动互联网用户面临大量的恶意代码威胁，这些恶意代码可通过手机应用程序、短信、邮件、蓝牙等多种途径传播，并带来一系列的安全和隐私问题。

2 移动互联网恶意代码的类型和传播途径

2.1 移动病毒

主要通过手机应用程序传播，一旦感染，会破坏系统文件、数据文件或其他应用程序。

2.2 蠕虫

主要通过短信、邮件、蓝牙等途径传播，一旦感染，会自动复制并传播到其他设备。

2.3 木马

通过伪装成正常应用程序或通过欺骗用户获取权限，一旦感染，会窃取用户的个人信息或控制设备。

2.4 间谍软件

通过监控用户的通话记录、短信、位置等信息，隐私信息会被传输到黑客的服务器。

移动互联网恶意代码的传播途径多种多样，用户要增强安全意识，不随意下载不明应用程序，不点击不明链接，不随便连接公共 Wi-Fi 等 [1]。

3 目前主要的移动互联网恶意代码监测技术

3.1 基于特征的监测

基于特征的监测技术通过监测恶意代码的特征判断是否存在恶意代码。这些特征可是病毒的病毒特征库或木马的行为特征。当应用程序被安装或执行时，监测系统会进行扫

【作者简介】鲁博（1987–），男，中国新疆乌鲁木齐人，本科，助理工程师，从事电力系统相关系统开发及运维研究。

描并与已知的恶意代码特征进行匹配。如果匹配成功，则判定该应用程序为恶意代码。

举例如下：基于特征的简化监测案例代码如图 1 所示。

```python
def detect_malware(app):
    malicious_signatures = get_malicious_signatures() # 获取已知的恶意代码特征
    app_signatures = get_app_signatures(app) # 获取待检测应用程序的特征
    for signature in app_signatures:
        if signature in malicious_signatures:
            return True
    return False
```

图 1 特征简化监测案例代码

其中 detect_malware() 函数接收一个应用程序作为输入，并调用 get_malicious_signatures() 函数获取已知的恶意代码特征，调用 get_app_signatures() 函数获取待监测应用程序的特征。使用循环遍历待监测应用程序的特征，并与已知的恶意代码特征进行匹配。如果找到匹配的特征，则判定该应用程序为恶意代码，返回 True；否则，返回 False。基于特征的监测技术具有快速识别已知恶意代码的优势，可及时阻止这些恶意代码的传播和影响。然而，该技术的缺点是对于未知的恶意代码无法进行监测。并且，恶意代码的变种可能会绕过已知特征的监测，导致漏报或误报的情况。因此，基于特征的监测技术通常需要与其他监测技术结合使用，以提高恶意代码的监测率和准确性 [2]。

3.2 行为分析

行为分析技术通过分析恶意代码的行为模式判断是否存在恶意代码，该技术可监测到未知的恶意代码，因为恶意代码的行为模式基本相似。然而，恶意代码的行为可能隐蔽，并且对恶意代码进行行为分析也需要消耗较大的计算资源，可能影响设备的性能。举例如下：基于行为的简化监测案例代码如图 2 所示。

以上代码简单地检查文件是否包含恶意代码特征，当发现匹配的特征时，会输出相应的提示信息。其中特征列表是一个简化的示例，实际上可根据实际情况，结合恶意代码的行为模式和已知特征，构建更加细致准确的特征列表。

3.3 机器学习

机器学习技术是一种常用的恶意代码监测方法，通过对大量样本数据的训练，建立恶意代码的特征模型，判断是否存在恶意代码。该技术可监测到未知的恶意代码，并且能够不断进行模型更新以适应新的恶意代码。举个例子，可使用机器学习技术训练一个恶意代码监测模型。首先，收集大量的恶意代码样本和正常代码样本，并对其进行特征提取。这些特征可包括文件的哈希值、API 调用序列、静态特征等，使用这些特征训练一个机器学习模型，如支持向量机（SVM）或深度神经网络（DNN）。

在实际监测过程中，可将待监测的文件提取相同的特征，并将其输入到训练好的模型中，通过模型判断文件是否为恶意代码。如果模型输出的概率值高于一个设定的阈值，则可判断该文件为恶意代码。

```python
# 导入必要的库和模块
import os
import re
# 恶意代码特征列表
malicious_features = [
    'secret_file.exe',
    '/root/.ssh/authorized_keys',
    'rm -rf /',
    'exploit'
]
def analyze_behavior(file_path):
    # 读取文件内容
    with open(file_path, 'r') as file:
        file_data = file.read()
    # 判断文件是否包含恶意代码特征
    for feature in malicious_features:
        if re.search(feature, file_data):
            print(f"恶意代码特征 '{feature}' 在文件 '{file_path}' 中被发现！")
# 遍历指定目录下的所有文件
def analyze_directory(directory):
    for root, dirs, files in os.walk(directory):
        for file in files:
            file_path = os.path.join(root, file)
            analyze_behavior(file_path)
# 示例：分析当前目录下的文件
analyze_directory('.')
```

图 2 行为的简化监测案例代码

然而，机器学习技术对于样本数据的质量和数量有一定要求。样本数据需要尽可能全面且代表性，以保证模型的准确性和泛化能力。为解决这个问题，可采取以下措施：

一是定期更新训练数据：及时收集新的样本数据，并将其包含在训练集中，以保证模型的更新速度。可通过监测恶意代码数据库、恶意行为分析和用户反馈等方式获取新的样本数据。

二是增加一定的人工干预：如果机器学习模型的判断结果不确定或与真实情况相悖，可人工介入进行确认或修正，以提高监测的准确性。

三是结合其他技术与方法：可将机器学习与传统的规则引擎、行为分析等技术相结合，形成多层次的监测体系，提高恶意代码的监测能力。

4 移动互联网恶意代码监测技术的发展和应用

4.1 基于特征的监测

该方法会监测应用程序在设备上的行为，以识别是否存在恶意行为。例如，恶意应用程序可能会试图获取用户敏感信息、未经用户授权的访问设备的各种功能、在后台执行恶意操作等。基于行为的监测技术能够识别出这些恶意行为，从而保护用户的隐私和设备安全。随着移动互联网的发展和恶意代码的不断演变，传统的基于特征和基于行为的监测技术已经不再足够应对各种新型的恶意代码。因此，研究人员和安全公司开始探索新的监测技术和方法。一种新兴的移动互联网恶意代码监测技术是基于机器学习的监测。该方法通过对已知恶意代码和正常代码进行训练，构建模型自动识别未知的恶意代码。机器学习技术可通过分析大量的数据

和特征，发现隐藏在其中的模式和规律，从而能够准确地识别恶意代码。已经有许多研究者和安全公司使用机器学习技术监测移动互联网恶意代码，并取得显著效果。

此外，研究人员还在探索使用深度学习监测移动互联网恶意代码。深度学习是一种特殊的机器学习方法，通过构建多层神经网络模拟人脑的工作原理。深度学习技术可更好地处理非线性、高维和复杂的数据，能够更准确地识别恶意代码。一些最新的研究表明，使用深度学习技术可显著提高移动互联网恶意代码的监测准确率和效率。

4.2 行为分析

行为分析是一种非常重要的移动互联网恶意代码监测技术，该技术通过监测应用程序在设备上的行为，如访问权限、网络通信、文件操作等，识别恶意代码。行为分析可快速监测到未知的恶意代码，因其关注的是应用程序的行为模式而不是特定的代码签名或特征，使行为分析能够有效应对恶意代码的变种和新型的攻击方式。恶意代码的作者会不断修改和变异代码，以逃避传统基于特征的监测技术，但行为分析能够通过分析行为模式发现恶意代码的活动轨迹，从而保护用户的设备安全。行为分析技术通常结合人工智能和机器学习技术，以提高监测的准确性和效率。

通过分析大量的数据和特征，机器学习模型可发现隐藏在恶意代码行为中的模式和规律，并将其与正常的行为进行区分，以此，对未知的恶意代码进行监测和识别 [3]。

除了基本的行为模式监测，行为分析还可通过建立行为模型预测恶意代码的行为。模型可根据历史数据和学习算法自动学习和更新，随时适应新的威胁和攻击方式。例如，若某个应用程序突然开始访问用户的联系人信息并发送大量的短信，则行为分析可通过行为模型识别出这是一种恶意行为，并进行相应的处理和防护措施，从而提供给用户更安全可靠的应用。

4.3 机器学习

机器学习是一种可应用于移动互联网恶意代码监测的重要技术，通过建立恶意代码的特征模型，利用机器学习算法对恶意代码进行分类和监测，可在一定程度上提高监测的准确性和效率。机器学习技术可通过学习大量的数据和特征，从中发现恶意代码的隐藏模式和规律。通过训练一个机器学习模型，将已知的恶意代码和正常代码进行区分，使用这个模型对未知的恶意代码进行监测。机器学习模型可自动识别恶意代码，并通过不断更新模型适应新的恶意代码。在机器学习中，特征是一种描述恶意代码的属性或属性组合。这些特征可是恶意代码的二进制指纹、API 调用序列、权限请求、代码执行路径等等。通过分析这些特征，机器学习模型可对恶意代码进行分类和监测。

机器学习算法是机器学习技术的核心，常见的机器学习算法包括决策树、朴素贝叶斯、支持向量机、随机森林等。这些算法可根据训练数据的特征和标签，自动学习和调整模型的参数，从而实现对恶意代码的分类和监测。选择合适的机器学习算法对于恶意代码监测的准确性和效率非常重要。

然而，恶意代码的演化速度很快，需要及时更新机器学习模型以适应新的恶意代码。为克服这些挑战，研究人员和工程师们不断探索新的机器学习方法和技术。例如，深度学习是一种特殊的机器学习方法，可通过构建多层神经网络模拟人脑的工作原理，能够更好地处理复杂的数据和特征。深度学习在移动互联网恶意代码监测中已经开始得到应用，并取得一些有希望的结果。机器学习是一种重要且有效的移动互联网恶意代码监测技术，通过建立恶意代码的特征模型，并利用机器学习算法对恶意代码进行分类和监测，可提高监测的准确性和效率。

5 结语

综上所述，移动互联网恶意代码的监测技术至关重要，可保护用户的移动设备免受恶意代码的威胁。目前主要的监测技术包括基于特征的监测、行为分析和机器学习。这些技术各有优缺点，需要根据实际情况选择合适的方法。未来，应加强对移动互联网恶意代码的监测技术的研究和应用。同时，还需要加强与移动设备厂商和应用开发者的合作，共同推动移动互联网安全的发展。只有不断提升监测技术和加强合作，才能有效地应对移动互联网恶意代码的威胁，保护用户的安全和隐私。

参考文献

[1] 杨倩倩,王龙,张晓娜.基于数据挖掘的移动互联网数据包安全监测技术分析[J].电子技术与软件工程,2022(11):1-3.

[2] 张亦弛.互联网和移动互联网领域新媒体技术研究和应用浅析[J].科学与信息化,2021(16):39-40.

[3] 晁楠.浅谈移动互联网技术在科技管理信息化中的应用[J].中国宽带,2022(1):115-116.