doi 10.3969/j.issn.1671-1122.2011.07.005

# 基于行为分析的黑客攻击软件自动化分析工具的设计与实现

刘恒[1]，文伟平[1]，万正苏[2]

（1. 北京大学，北京 102600；2. 湖南理工学院数学学院，湖南岳阳 414006）

摘 要：静态分析和动态分析是两种主流的恶意代码分析技术。随着反调试、程序补丁、代码混淆、多态和变型等技术的出现，静态分析技术的局限性越来越明显。该文设计了一种基于内核调用和正则表达式技术的恶意软件自动化分析工具，并用熊猫烧香病毒进行了验证，此工具提高了自动化分析的效率。

关键词：行为分析；恶意软件；动态分析

中图分类号：TP393.08 文献标识码：A 文章编号：1671-1122（2011）07-0010-03

## Design and Implementation of Malware Automated Analysis Tool Based on Behavior Analysis

LIU Heng[1], WEN Wei-ping[1], WAN Zheng-su[2]

( 1.*Peking University, Beijing* 102600, *China;*

2. *Hunan Institute of Science and Technology of Mathematics,Yueyang Hunan* 414006, *China* )

**Abstract:** Static analysis and dynamic analysis are the two common analysis methods in malware analysis. With the anti-debugging, program packers, code obfuscation, polymorphism and variants such technologies coming out, the limitations of static analysis methods become more and more. Here is a tool to dynamic analysis Malware Code based on kernel callback and Regular Expressions, demonstrate it's capabilities by analyzing the Fujacks .As a result ,improved the efficiency of the tool in the automating analysis.

**Key words:** Behavior analysis; Malware; Dynamic analysis

## 0 引言

随着互联网技术的日益普及，互联网安全问题也变得越来越突出 ，虽说近年来政府不断加大投入对网络安全问题的治理，但是安全形式依然严峻。互联网的开放性为病毒、木马的传播提供了便利，各项新技术的出现也为病毒、木马的推陈出新提供了技术条件，如何有效、及时地检测并处理这些恶意程序一直是信息安全领域研究的重要课题。在和恶意代码长期的斗争过程中，研究人员通过对各种样本的分析总结，提出了多种检测分析手段，这些检测手段也随着恶意代码的变化而不断发展变化。行为分析是逆向工程中用于检测应用程序对它所运行的系统的影响的一个重要步骤。很多时候，我们无法获取应用程序的源代码，行为分析就成了我们掌握软件做了什么和怎样操作数据的利器。行为分析出现在计算机安全领域有很长时间了，Foorest 在 1996 年基于入侵检测系统创造了应用程序在正常运行时反常的行为的系统调用指纹，这些指纹使得那些系统调用顺序异常的攻击能被检测到。Willems 在沙箱环境下利用行为分析来自动分析恶意软件，生成的报告大大简化和自动化了恶意软件分析任务。现在越来越多的杀毒软件厂商也开始使用行为特征进行恶意软件检测。在复杂的操作系统环境下确定软件的行为是比较困难的，即使是空闲的操作系统，也会有很多事件发生，监听所有的事件是费时费力的，有时也会干扰我们的分析。分析工具在分析系统状态时需要确定状态的变化的只来源于被分析的软件，同时软件的系统环境和配置会随着应用环境的变化而不断改变，这就要求分析软件的可移植性。本工具对不同的监控功能配置不同的排除列表，这种基于正则表达式的排除列表从一定程度上降低了非系统目标事件的干扰，极大的方便我们进行系统行为分析，同时也增加了软件的可移植性。

收稿时间 2011-06-10

作者简介 刘恒（1984-），男，湖北，硕士研究生，主要研究方向：软件测试与质量保证；文伟平（1976-），男，湖南，副教授，博士，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等；万正苏（1976-），男，湖南，副教授，博士，主要研究方向：微分方程数值解等。

## 1 恶意代码分析

### 1.1 恶意代码定义

关于恶意代码的定义没有明确的统一说法。《Malware: Fighting Malicious Code》中给出的恶意代码定义为：运行在目标计算机上，使系统按照攻击者意愿执行任务的一组指令。在维基百科里，恶意代码的英文是 Malware，恶意代码定义被描述为 :恶意代码是在未被授权的情况下，以破坏软硬件设备、盗取用户信息、干扰用户心理、扰乱用户正常使用为目的而编制的软件或者代码片段。相对而言，这个定义涵盖的范围非常广泛，它包含了所有带有恶意目的的程序或者源代码片段，使得识别恶意代码不再以恶意代码本身的特征来判断，而是主要依据软件制作者的意图。

### 1.2 恶意代码的分析技术

对恶意代码进行分析一方面是为了研究恶意代码所使用的技术手段，识别恶意代码的类型和种类，搞清恶意代码的结构；另一方面，根据分析的结果，可以为恶意代码的进一步检测和清除打下良好的基础，这也是进行分析的最终目的。

恶意代码分析技术的分类标准有多种。传统的恶意代码分析技术按照分析方式的不同，一般可以分为静态分析和动态分析两类，这是按照分析过程中恶意代码是否正在执行所进行的分类。静态分析技术，就是在不运行代码的方式下，通过词法分析、语法分析、控制流分析等技术对程序代码进行扫描，验证代码是否满足规范性、安全性、可靠性、可维护性等指标的一种代码分析技术，近年来反反编译、变型代码、代码混淆等技术的出现使得静态分析技术面临较大挑战，常见的特征码分析和反汇编分析都属于静态分析的范畴；动态分析是通过监视恶意代码运行过程来分析恶意代码的方法。它需要在一个可控的环境中运行恶意代码，全程监控代码的所有操作，观察其状态和执行流程的变化，获得执行过程中的各种数据，分析恶意代码与主机系统之间的行为特征。

### 1.3 恶意代码行为分析

恶意代码的行为分析是一种动态分析技术，由于行为分析能够检测和识别未知的恶意代码，已经成为信息安全领域的研究热点。使用行为分析技术的安全软件通常具备自我学习的能力，因此可以提高自身对未知恶意代码的识别能力。程序在运行期间所进行的操作被称为“ 程序行为 ”，一般泛指程序运行时表现的相对明显的操作，例如创建文件、删除文件、修改注册表、创建进程、连接网络等。行为分析工具通过内核 API hook 或者 用户级的 API hook、内核调用等方式捕获恶意代码运行时 API 调用序列或者引起操作系统状态变化的系统事件，将统一处理后的系统事件或者 API 调用序列通过模式匹配、数据挖掘等算法进行分析，进而得出恶意软件类别或者威胁级别等结论。

## 2 工具设计

恶意软件自动化分析工具采用了内核调用而不是 API hook 的方式捕获系统事件进而分析恶意软件的行为。工具主要由三个部分组成：行为监控、行为审计、报告输出。工具的系统结构如图 1 所示：

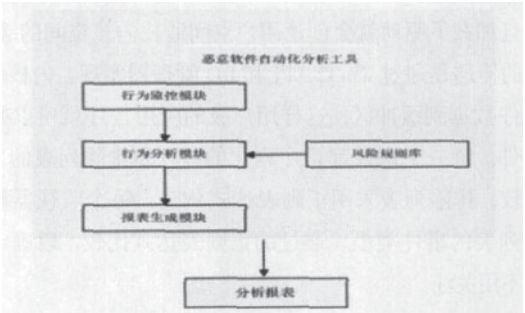


图1 系统结构图

### 2.1 主要实现技术

工具对恶意软件行为的捕获主要是通过内核驱动和用户空间进程的通信实现。内核驱动工作在内核空间，利用基于事件的监测机制监控恶意软件运行后系统状态的变化。用户空间的进程，通过缓冲区获取排除列表过滤后的系统事件，并将它们传递给行为分析模块。

1) 内核驱动。

分析工具使用内核驱动监视系统，利用内核中已经存在的内核调用机制，当一个事件发生时通知已经注册的驱动。这些内核调用内核驱动中的函数，放过实际发生的事件信息，这样就可以捕捉到系统事件。本工具注册了 CmRegisterCallback、PsSetCreateProcessNotifyRutine、FilterLoad、FltRegisterFilter 等系统调用函数。CmRegisterCallback 函数允许注册表监控驱动可以监视 Windows 系统注册表，注册表管理器在每次注册被修改时触发这个函数，一旦创建或者删除事件发生，这个函数就会在事件被提交到注册表之前或者之后被关联，以便分析工具可以监测注册表的创建或者删除事件 , 这些事件包含注册表上的动作、执行这个动作的进程、注册表键值的路径等信息；利用 PsSetCreateProcessNotifyRutine 函数使进程监控驱动可以观察到正在运行的进程的变化，以了解进程的创建、结束以及父进程等信息；文件监控的工作方式稍微有些不一样 , 和前面提到的在内核上注册一个调用直接接收系统事件的方式不同，文件监控驱动是一个位于 Windows 内核的 I/O 管理器和基本的文件系统之间的小型过滤驱动。当某种文件事件发生时，一个 Windows 过滤管理器管理这些驱动和这些将要注册的系统调用的调用。工具利用过滤管理器调用 FilterLoad 函数加载文件过滤驱动，在驱动被加载后，迷你过滤驱动在过滤管理器上注册以方便侦听它所想监听的事件，当文件读或者写时就能收到通知了，然后通知进程发生事件的

原因以及事件文件的路径。将内核驱动收集到的事件信息先放到一个等待队列中，然后通过一个从用户空间指向内核空间的缓冲区将这些信息送往用户空间，便于用户空间的进程进行处理。

2）用户空间进程。

主要负责加载驱动、处理从内核空间收集到的事件信息、将收集到的各种类型事件信息的结果进行输出。用户空间进程一旦加载了驱动就会创建用户空间通往内核空间的缓冲区，信息的传递是通过 win32 API 和 I/O 管理器实现。内核驱动复制事件数据到缓冲区，这样用户级的应用程序就可以处理系统事件，每一个事件都是序列化的并且和排除列表的条目进行比较，排除列表采用正则表达式构建，每个监视器都要和排除列表的事件类型、通过的正则表达式比较，以确定哪些事件不用关注。

## 2.2 行为分析实现

行为分析是将监控模块收集到的信息进行处理，是分析结果的重要依据。系统事件是系统行为的反映，在本文中，首先将监控模块获取的监控事件信息转化成软件行为特征，利用已有的风险规则库，提取出恶意软件行为特征的威胁程度的权值，某种行为特征出现的越多其权值越高，越具有危害性。同时结合文件创建、网络端口等信息进行关联分析，以此作为分析的依据对恶意软件进行判别。

行为分析模块的功能主要是分析捕获模块传递过来的参数信息，将其与风险规则库中的行为规则进行匹配，如果能够匹配，则确定该行为是恶意行为，进而确定该行为的恶意级别，输出恶意行为的相关信息 ;否则，结束对该事件的分析。

## 3 实验结果

为了验证自动化分析的工具能力，选取了近几年比较盛行的熊猫烧香病毒样本进行自动化分析，实验平台使用 VMware Station , 测试用操作系统使用 Windows XP professional sp2。实验前需要配置文件、进程、注册表、网络排除列表，通过排除列表过滤掉一些系统事件，如图 2 所示 ：

图2 排除列表

运行行为分析工具 , 在虚拟机中解压恶意软件样本 , 运行样本 , 自动化分析工具实时捕获系统行为，根据行为进行分析，得出恶意软件风险级别。实验结果如图 3 所示 ：

图3 自动化分析报告

## 4 结论

本文设计实现了一种基于行为分析的恶意软件自动化分析工具。工具采用基于内核调用和正则表达式的方式，借助排除列表一定程度上减轻了行为分析的工作量，避免了静态分析的局限性，增强了工具的移植性，提高了自动化分析的效率，通过实验验证了工具在自动化行为分析上的表现。在行为分析的评审阶段只简单与风险规则库进行匹配，在未来的研究中，将考虑通过机器学习和数据挖掘等相关技术提高行为分析的准确性。（责编 杨晨）

参考文献：
[1] Willems C, Holz T, and Freiling F. CWSandbox: Towards auto - mated dynamic binary analysis[C]. IEEE Security and Privacy, 2007, 5(2).
[2] Sharif M I, Lee W, Cui W, and Lanzi A. Secure in - VM monitoring using hardware virtualization[C]. Proceedings of the 16th ACM Conference on Computer and Communications Security. CCS, 2009.
[3] Dinaburg A, Royal P, Sharif M, and Lee W. Ether: Malware analysis via hardware virtualization extensions[C]. Proceedings of The 15th ACM Conference on Computer and Communications Security. CCS 2008.
[4] Carsten Willems, Thorsten Holz, Felix Freiling, Toward Automated Dynamic Malware analysis Using CWSandbox[C]. IEEE Security and Privacy, vol. 5, no. 2, pp. 32 - 39, Mar./Apr. 2007.
[5] Bayer U, Kruegel C, and Kirda E. TTAnalyze: A Tool for Analyzing Malware[C]. 15th European Institute for Computer Antivirus Research (EICAR 2006) Annual Conference, April 2006.
[6] 许敏，赵天福 . 基于行为特征的恶意程序检测方法 [J]. 网络与信息，2009，(06) ：6.