作品文档

2022年全国大学生信息安全竞赛

作品报告

作品名称：基于DetoursWinAPI拦截技术的安全小卫士

电子邮箱：

提交日期：

摘要

随着互联网的蓬勃发展，网络与我们的生活关系越来越密切，网络极大地便利了我们的生活，却也无形中带来了各种各样的安全问题。各式各样的计算机病毒层出不穷，无孔不入地寻找着我们计算机上程序的弱点，进行侵入，获取、修改我们计算机一些重要的数据，严重时甚至会使我们的系统瘫痪。因此，在享受互联网便利的同时，安全人员的工作是必不可少的，计算机病毒检测技术应运而生。

如何判断一个程序是不是病毒？一种方法是分析它的行为。软件行为分析技术发展迅速，现阶段已有很多成品，各有利弊。本作品利用微软开发的Detours库中的WinAPI函数拦截功能，截获一些常见的API函数，进而对软件行为进行分析。软件分析思路大体为：首先编写生成dll文件，包含需要Hook的函数和替换函数，替换函数要可以显示截获的函数信息；编写注射器程序，将生成的dll文件注入到检测程序中；编写图形化界面程序，将截获的API函数信息显示在屏幕上；编写测试程序对工具经行测试，主要包含一些常见的API函数和异常。作品主要工作流程为：由图形化界面程序创建两个进程，其中一个进程用于显示检测结果，线程1到共享内存中获取截获的API信息，反馈给线程2，刷新到界面上；另一个进程启动注射器程序，将dll文件注入到测试程序中，并将截获的API信息写入共享内存。关键在于对API函数的拦截。本作品尝试用Detours技术对WinAPI函数进行拦截替换，达到分析函数信息的目的。Detours是微软提供的一个开发库，使用它可以简单、高校、稳定地实现API HOOK的功能。Detours库对windows系统的高度适配性使得它可以以极小巧的体积完成API HOOK功能，占用空间和速度都远远优于其他API HOOK技术。

未来，我们将持续优化我们的作品，在此基础上研究二进制代码插桩、重写技术，加深对某些病毒加壳机制的研究，实现去壳分析，深度检测，提高分析的准确性，在windows病毒分析领域走的更远。

关键词：Detours技术 API函数 dll文件 消息拦截 分析

1作品概述

1.1背景分析

随着互联网时代的到来，网络与我们的关系越来越密切。而在使用网络的过程当中，软件安全则显得越来越重要。在编写代码的过程中，我们可能会出现各式各样的问题，这些问题使得我们的代码出现安全的缺陷，并且正常情况下这些缺陷通常都难以定位与修复。正因为此，我们给了计算机病毒侵入计算机的机会，计算机病毒会趁机获取、修改我们计算机一些重要的数据，严重时甚至会使我们的系统瘫痪。所以，计算机病毒的检测显得尤为重要。

而检测病毒，避不开软件行为分析技术，了解软件都干了什么。了解一个软件中的函数信息，就可以大体理解软件的功能，所以需要HOOK技术对函数进行勾取。

本项目基于Detours技术，未来将研究一种二进制代码插桩和重写的新方法，对计算机病毒的执行过程实现动态监控，并对其自我保护机制进行对抗，例如加壳、加密、反虚拟机等机制，提升对计算机病毒分析的准确性，为杀毒软件和沙箱等检测工具对抗计算机病毒的保护机制提供一种新的解决思路。

1.2相关工作

1.2.1计算机病毒

随着计算机病毒越来越猖獗，计算机安全越来越受到人们的重视，计算机反计算机病毒技术也发展得越来越快。当今最新的计算机反计算机病毒技术有实时扫描技术、启发式代码扫描技术、虚拟机技术和主动内核技术等。这些技术各有特点，但是应用起来仍然不够成熟。现有计算机反计算机病毒软件虽然在对抗计算机病毒方面发挥了巨大作用，但是仍有不尽人意之处，尤其是对付未知计算机病毒缺乏足够有效的方法。

目前常用的检测计算机病毒的方法有：比较法、校验和法、行为检测法、感染实验法、软件模拟法、分析法等，这些方法依据的原理不同，实现时所需开销不同，检测范围也不同。

随着计算机技术的不断发展，网络上出现了许多极具隐蔽性和破坏性的计算机病毒，如CIH计算机病毒、熊猫烧香、红色代码、灰鸽子、LOVE BUG、梅利莎、Windows勒索计算机病毒等，这使得计算机病毒技术与计算机反计算机病毒技术的对抗性也越来越尖锐，计算机病毒分析检测到目前依旧是亟待深入发展的。

1.2.2 Detours技术

Detours是一个微软开发的用于拦截机器上的二进制函数的库，其发展已经相对成熟，一直以来都有很好的应用前景。Detours最常用于拦截应用程序中的 Windows API 调用，例如添加调试检测，拦截代码等。具体实现原理是将目标函数的前几条指令替换为无条件跳转到用户提供的Detours函数，并在蹦床中放置来自目标函数的指令，蹦床的地址放置在目标指针。Detours 可以通过为目标函数重写在内存中的代码而达到拦截Win32函数的目的。

除了基本的Detours功能外，Detours还包含了编辑任何二进制文件的DLL导入表、将任意数据段附加到现有二进制文件以及将DLL加载到新进程的功能。一旦加载到进程中，检测DLL可以拦截绕开执行目标函数进程中的任何函数，无论是在应用程序中还是系统库中，比如Windows API。

1.2.3发展趋势

计算机病毒的检测分析方法随着时间不断的迭代，目前包括比较法 、特征代码法 、校验和法 、行为监测法 、感染实验法、软件模拟法 、分析法等,基于此的检测杀毒工具也层出不穷。但与之对应的是计算机计算机病毒的保护机制也在不断发展进化，以对抗或者绕过现有的检测方法和工具。如何有效的去除这些计算机计算机病毒的保护机制是计算机计算机病毒分析遇到的难题。一种可能存在的解决方式是利用二进制代码插桩技术向计算机计算机病毒中注入探针监控其运行，然后利用重写技术去除保护机制以实现计算机计算机病毒的查杀。微软开发的针对Windows系统的Detours库提供给了我们实现这一技术的工具，我们将基于这样的思路和技术实现计算机计算机病毒的深入分析。

1.3作品特色

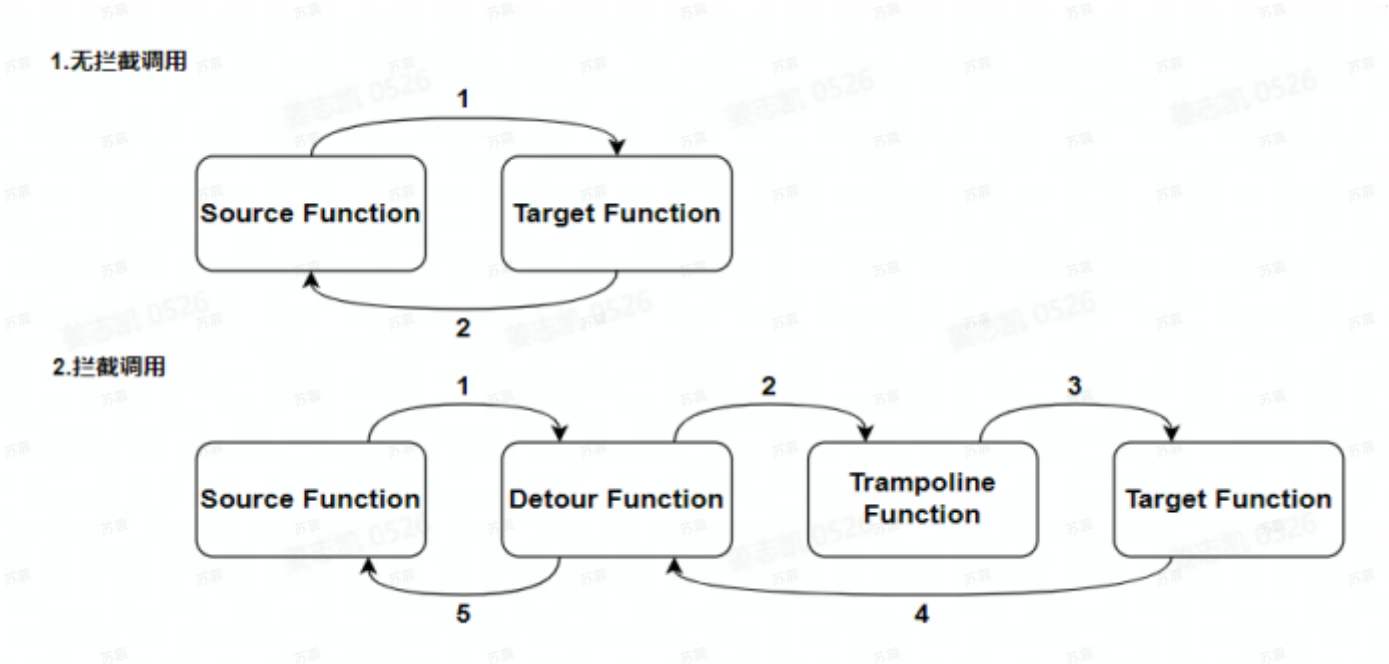
利用Detours实现对计算机病毒行为的监控、跟踪，相比于传统的计算机病毒检测方法，该方法更高效，并且能获得更多的计算机病毒内部信息。

2作品设计

2.1 Detours技术

Detours是一个微软开发的用于拦截机器上的二进制函数的库，其发展已经相对成熟，一直以来都有很好的应用前景。Detours最常用于拦截应用程序中的 Windows API 调用，例如添加调试检测，拦截代码等。具体实现原理是将目标函数的前几条指令替换为无条件跳转到用户提供的Detours函数，并在蹦床中放置来自目标函数的指令，蹦床的地址放置在目标指针。Detours 可以通过为目标函数重写在内存中的代码而达到拦截Win32函数的目的。

除了基本的Detours功能外，Detours还包含了编辑任何二进制文件的DLL导入表、将任意数据段附加到现有二进制文件以及将DLL加载到新进程的功能。一旦加载到进程中，检测DLL可以拦截绕开执行目标函数进程中的任何函数，无论是在应用程序中还是系统库中，比如Windows API。



Detours工作流程图

2.2 HOOK技术

对于Windows系统，它是建立在事件驱动机制上的，说白了就是整个系统都是通过消息传递实现的。hook（钩子）是一种特殊的消息处理机制，它可以监视系统或者进程中的各种事件消息，截获发往目标窗口的消息并进行处理。所以说，我们可以在系统中自定义钩子，用来监视系统中特定事件的发生，完成特定功能，如屏幕取词，监视日志，截获键盘、鼠标输入等等。

钩子的种类很多，每种钩子可以截获相应的消息，如键盘钩子可以截获键盘消息，外壳钩子可以截取、启动和关闭应用程序的消息等。钩子可以分为线程钩子和系统钩子，线程钩子可以监视指定线程的事件消息，系统钩子监视系统中的所有线程的事件消息。因为系统钩子会影响系统中所有的应用程序，所以钩子函数必须放在独立的动态链接库(DLL) 中。

所以说，hook（钩子）就是一个Windows消息的拦截机制，可以拦截单个进程的消息(线程钩子)，也可以拦截所有进程的消息(系统钩子)，也可以对拦截的消息进行自定义的处理。Windows消息带了一些程序有用的信息，比如Mouse类信息，就带有鼠标所在窗体句柄、鼠标位置等信息，拦截了这些消息，就可以做出例如金山词霸一类的屏幕取词功能。

2.2.1分类

HOOK分为线程钩子和系统钩子：线程钩子监视指定线程的事件消息；系统钩子监视系统中的所有线程的事件消息。因为系统钩子会影响系统中所有的应用程序，所以钩子函数必须放在独立的动态链接库(DLL)中。

2.2.2工作原理

创建一个代理对象，然后把原始对象替换为我们的代理对象，这样就可以在这个代理对象为所欲为，修改参数或替换返回值。

·寻找Hook点，原则是静态变量或者单例对象，尽量Hook public的对象和方法，非public不保证每个版本都一样，需要适配；

·选择合适的代理方式，如果是接口可以用动态代理；如果是类可以用静态代理；

·用代理对象替换原始对象。

2.3 Detours技术实现HOOK

由于Detours库是微软开发库，很多windows的补丁都是通过它实现的，所以Detours技术对于windows系统的适配性非常高，实现HOOK非常简单。不需要各种类、函数，只需要调用Detours库中的相关函数即可实现简单的HOOK。函数的参数一般为需要HOOK的API函数和替换函数，而替换函数就可以用来实现我们想要的功能。

2.4