**Ransomware分析与检测**

**1、Introduction**

（1）ransomware的发展历史

（2）对ransomware的进行分析检测的重要意义

（3）ransomware的特点

（4）我们所做的工作以及我们系统的特点

介绍Ransomware是什么，ransomware对我们造成的威胁越来越大，引出对ransomware进行分析检测的重要意义。介绍ransomware的特点，如大量的加密用户文件并生成具有特定扩展名的文件、可能会通过网络来传递密钥、为了躲避反病毒引擎可能会尝试获取系统管理员的权限等等。从ransomware的特点和云计算的广泛使用入手，引出我们的方法：在虚拟机外部，通过VMI技术，对系统的文件系统和网络系统进行监控，实现对ransomware进行动态的分析检测， 并且通过静态的方法进行辅助分析。

**2、Related work**

介绍之前的工作，他们系统的特点以及每个系统的不足之处。抛砖引玉，引出我们系统的优点和价值所在。

**3、系统设计及实现**

（1）分析与检测ransomware的方法

使用动态分析和静态分析相结合的方法。以动态分析为主，静态分析为辅。静态分析是动态分析的一个补充。

1. 动态分析的方法。利用VMI技术，捕获虚拟机中进程的系统调用，对进程发生的系统调用的参数进行解析。监控ransomware的行为，主要包括2个方面：首先对文件相关的系统调用进行解析，监控ransomware的文件活动；其次是对网络相关的系统调用进行解析，监控ransomware的网络活动。对大量的ransomware进行测试，得到监控结果进行分析，总结ransomware的文件和网络行为特点。
2. 静态分析。利用反编译工具，对每个ransomware进行初步的分析。首先，对动态分析中的网络活动进行补充验证，分析网络活动具体完成了一个什么功能。利用vmi虽然能够检测到网络活动，但却无法获悉网络活动的具体意义，因此可以对ransomware进行反编译，查找一些与网络相关的函数或者得到执行流程，明确ransomware网络行为的具体作用，并给出几个典型的例子进行具体的说明；其次，检测ransomware中是否存在进行系统权限提升的API，给出具体数据统计结果，验证大部分ransomware是否会尝试去提升系统权限。
3. 检测方法

待补充…….

（2）系统实现

分为ransomware分析和检测两大模块

1. VMI的原理
2. 解析文件相关系统调用和网络系统调用的方法
3. 解析日志得到ransomware行为模式的方法
4. 静态分析是如何实现的
5. 如何实现对ransomware的检测

**4、实验及评估**

应该分为两个部分：首先，先测试大量的ransomware，进行分析，得到ransomware的文件和网络的行为特点；然后，在找一些ransomware和一些良性的软件，进行测试，分析系统的性能。

**5、局限性**

介绍我们系统的不足之处