基于API短序列的勒索软件早期检测方法

2024-09-27 10:55:05

# 摘要

传统的勒索软件动态检测方法需要收集较长时间的软件行为，难以满足勒索软件及时检测。

该文从勒索软件及时检测的角度出发，提出了“勒索软件检测关键时间段（CTP）”的概念，并基于CTP的要求提出了一种基于应用程序编程接口（API）短序列的勒索软件早期检测方法（REDMS）。

该方法能够以高准确率检测出已知和未知的勒索软件样本。

# 引言

勒索软件与传统的窃密类恶意软件的行为表现有较大的差别，勒索软件感染主机后会尽快地加密被感染主机中文件，故在短时间内勒索软件会执行大量的操作。

该文通过分析多个不同家族的勒索软件运行过程，从勒索软件及时检测的角度提出了“勒索软件检测关键时间段”（CTP）的概念，并进一步提出了一种基于应用程序编程接口（API）短序列的勒索软件早期检测方法（REDMS）。

总而言之，本篇论文贡献如下： - 分析多个不同家族的勒索软件和多种类型的正常软件的运行过程，从勒索软件及时检测的角度提出CTP的概念，明确了勒索软件早期检测需要满足的时间要求。 - 基于检测时间少于CTP的要求提出一种勒索软件早期检测方法REDMS。该方法采集各软件在CTP内调用的API序列，运用n-gram、TF-IDF和分类算法对勒索软件进行早期检测。 - 利用来自24个不同家族的78个勒索软件以及40个多种类型的正常软件对REDMS进行实验测试。实验结果表明，REDMS能够在软件开始运行后数秒内高准确率地检测出已知和未知的勒索软件。

# 相关工作

## 静态检测方法

* 通过反汇编提取操作码序列作为特征训练模型检测。
* 基于可视化的勒索软件检测以及分类方法。
* 基于纹理的勒索软件分类方法

总之，虽然不需要运行程序，但此类方法难以应对使用了混淆技术的勒索软件。

## 动态检测方法

* 运行后统计API调用，根据API调用情况判断是否为勒索软件。
* 通过监控软件的IO缓冲区的熵值变化、文件访问模式以及文件系统活动来实现对勒索软件的检测。
* 通过检测诱导文件是否被加密来检测勒索软件。（不同勒索软件加密行为不同，适用范围局限）
* 关注潜在的勒索软件加密行为的检测方法。（误报率高）

总之，大部分现有的动态检测方法在检测出结果之前需要收集较长时间的软件行为，难以满足勒索软件及时检测的要求。

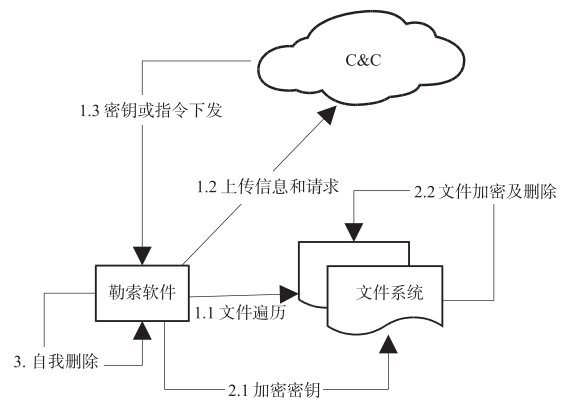
## 早期检测方法

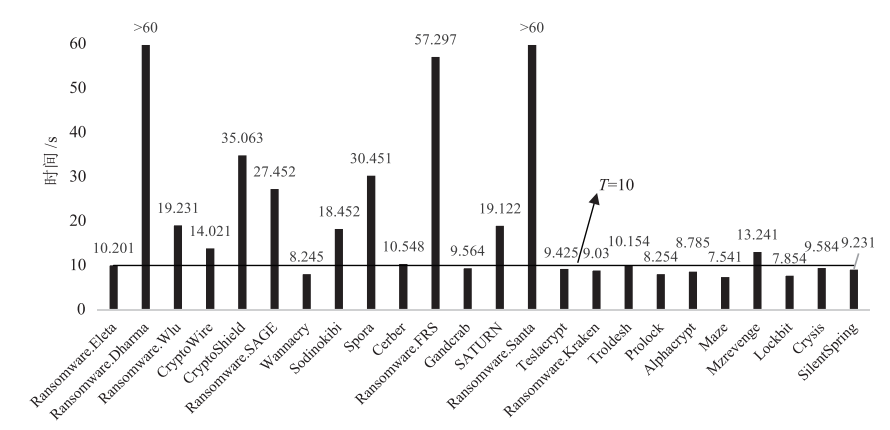
* Crypto-Drop通过检测文件类型和文件熵的变化来快速检测勒索软件。（未给出检测勒索软件所需的具体时长）
* 通过网络共享卷中的SMB流量来对勒索软件进行早期检测。（最佳检测效果需要花费20秒监控流量）

总之，现有的早期检测方法并未详细分析其所提出的方法的检测时间是否为真正意义上的’早期’。

# 勒索软件行为分析

勒索软件的攻击过程可分为系统感染、文件遍历和加密、索取赎金和文件解密四个阶段。

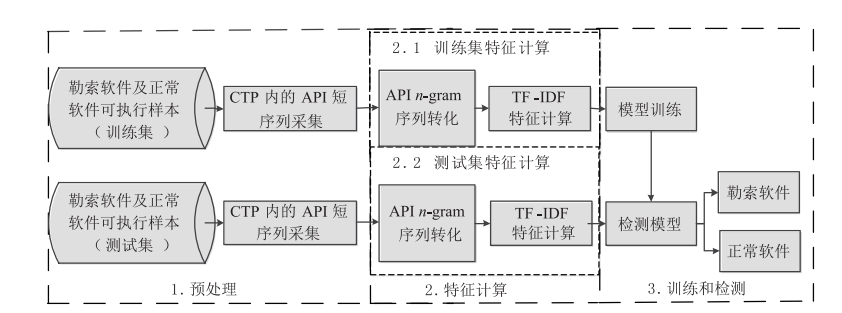
文件遍历和加密的一般执行过程： 

下图统计了不同勒索软件从运行到弹出勒索告知文本所需要的时间： 

该文将这段时间区间定义为CTP,由上图可知大部分勒索软件在其运行后10秒左右弹出勒索告知文本。因此，该文的CTP被设置为10秒。

除此之外，该文还通过实验发现大部分勒索软件在弹出勒索告知文本前的API调用数量远大于弹出勒索告知文本后的。因此，该文认为在CTP内执行的API数量可以用于区分正常软件和勒索软件。

# 基于API短序列的勒索软件早期检测方法

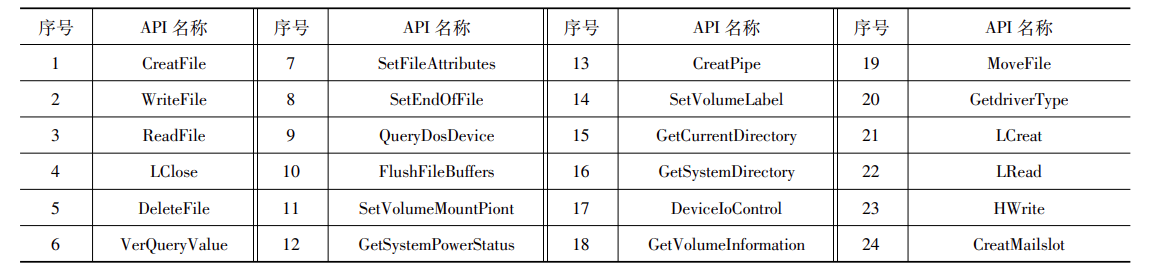
该文针对检测时间少于CTP的要求，提出了一种基于API短序列的勒索软件早期检测方法REDMS，框架如下： 

该方法重点关注软件开始运行后初期的API调用，通过CTP内各软件调用的API短序列判别该软件是否为勒索软件。REDMS包含预处理、特征计算、训练和检测三个阶段。

## 预处理

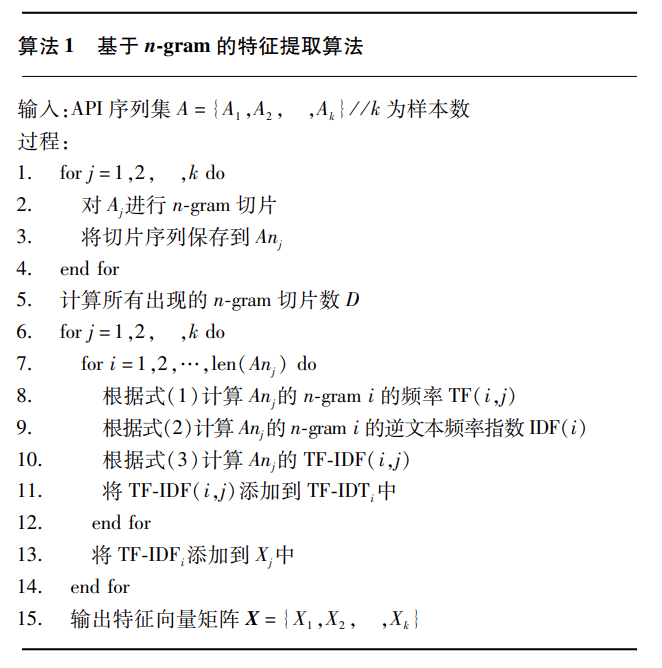
REDMS在预处理阶段采集勒索软件与正常软件CTP内的API短序列，并将其作为下一个阶段的输入。

下图给出了该文分析勒索软件运行时所统计的24个API，包含文件系统API、进程间通信API等。



该文监控的API

## 特征计算

伪代码如下： 

公式一：

公式二：

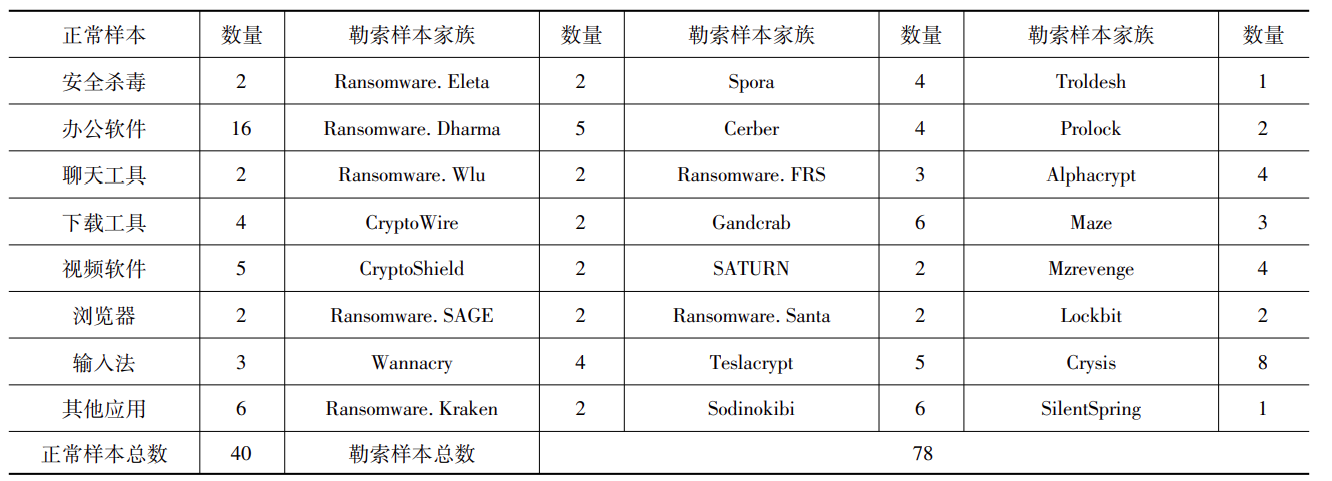
公式三：

## 训练与检测

REDMS在本阶段将基于特征计算阶段所得的特征向量构建一个勒索软件检测模型，用于区分勒索软件和正常软件。通过将上一阶段提取的特征向量添加类别标签（正常软件和勒索软件分别标记为-1和1），构建训练集。之后运用分类算法结合训练集建立一个勒索软件检测模型。

# 实验及结果

## 实验环境和样本



实验样本种类与数量

## 评估指标

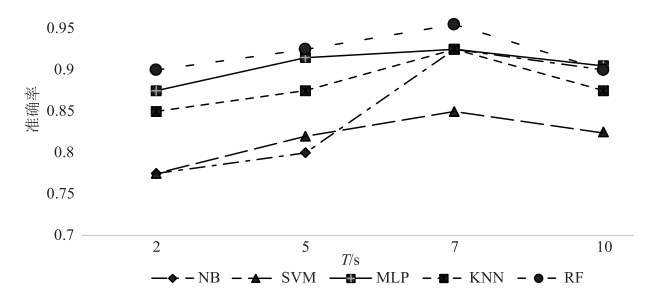
该文使用恶意软件检测领域常用的准确率（Accuracy）、精确率（Precision，P）、召回率（Recall，R）以及F1-score（F1）作为REDMS的性能评估指标。

## 实验结果

### 已知勒索软件样本检测

该文将78个勒索软件及40个正常软件运行时调用的API短序列所计算出的特征向量作为训练集，将新采集的来自其中24个不同家族的24个勒索软件以及16个来自8种类型的正常软件在CTP内所调用的API短序列所计算出的特征向量作为测试集。

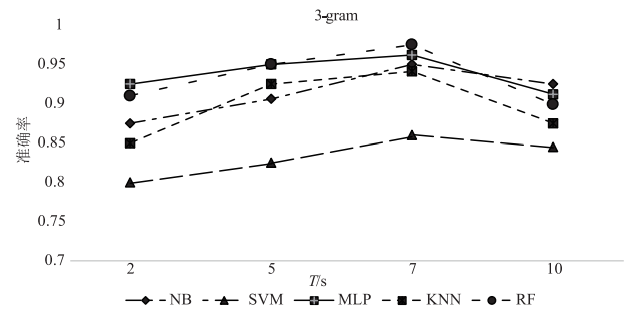
2-gram：



不同T下使用2-gram及不同算法的准确率

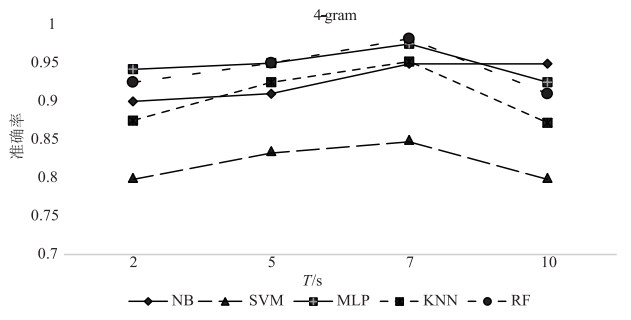
T为前2秒时，模型准确率较低，原因是勒索软件和正常软件在运行前2秒的API序列中有较多相似的部分。

3-gram：



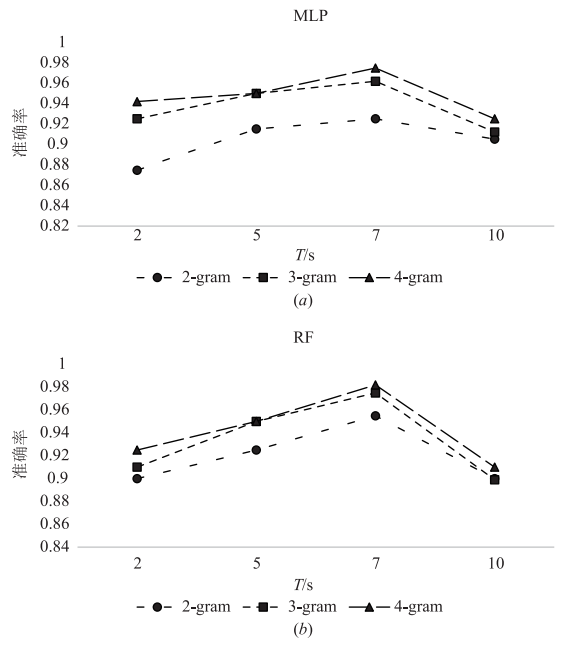
不同T下使用3-gram及不同算法的准确率

4-gram：



不同T下使用4-gram及不同算法的准确率

综上，REDMS使用RF和MLP所获得的检测结果优于其他算法。

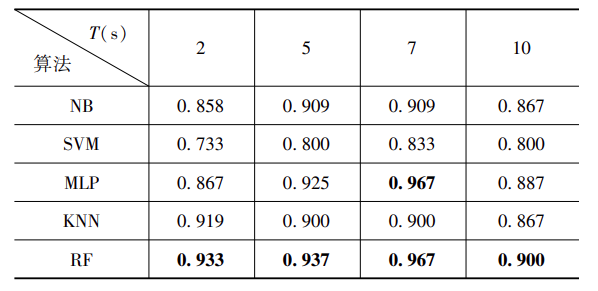
下面对比RF和MLP在不同n-gram下的准确率： 

可以发现： - 当使用MLP和RF时,REDMS在T为前2s、前7s和前10s下使用不同n-gram所得到的准确率均满足4-gram>3-gram>2-gram。经分析发现，原因是勒索软件的一次文件操作经常需要调用四个API。 - REDMS使用五种算法均在T为前7s时获得最佳检测结果并且在各采集时段上所获得的检测结果基本满足 7s > 5s > 2s 的关系。当T为前10s时REDMS使用五种分类算法获得的准确率均不是很高。经分析发现，这是因为勒索软件在完成文件加密并弹出勒索文本之后,其所执行的操作及对应的API调用数量将大大减少，而该文实验中有部分勒索软件样本在10s前已经完成了文件加密及弹出勒索文本。

### 未知勒索软件样本检测

该文将78个勒索软件样本中来自16个家族的64个勒索软件样本和40个正常软件样本在CTP内调用的API短序列所计算出的特征向量作为训练集,将16个正常软件样本和未包含在训练集中的8个家族共 14个勒索软件样本在CTP内调用的 API短序列所计算出的特征向量作为测试集。

REDMS在不同T下使用4-gram及五种算法对未知勒索软件测试集的准确率:



REDMS在不同T下使用4-gram及五种算法对未知勒索软件测试集的准确率

# 评价

## 创新点

* 使用n-gram+TF-IDF算法提取API段序列中的文本特征，用于构建模型。
* 证明了API短序列能够用于区分正常软件和勒索软件。
* 从勒索软件早期检测的角度提出了CTP概念，明确了勒索软件早期检测的时间要求。

## 新点子

* 该文使用n-gram+TF-IDF算法提取API段序列中的特征，使用其他文本处理方法提取特征效果会不会更好？
* 根据处理API短序列的n-gram+TF-IDF方法，提取出来的API短序列应该是只包含API名，如果提取出来的API短序列还包含API参数、API调用者和API调用时间等信息，效果会不会更好？