专家：刘旭 王江民 张波云 Dengguo Feng，Jiwu Jing，Dongdai Lin

肖国镇、王新梅、王育民 杨义先 张焕国

可切入点：启发式扫描

IBM：神经网络 引导型病毒

Schultz M：数据挖掘算法如朴素贝叶斯算法 检测未知恶意代码

SVM支持向量机的病毒检测模型

论文比较多的是张波云….

张波云系列：

总共方法的集合：

\*\*\*\*\*\*计算机病毒智能检测技术研究\_张波云(2007 国防科大博士论文)：

3种动态监测方法，2种静态检测方法，1种动静态结合方法。参考性很大，参考文献几乎全英文，可以参考下载。

1）\*\*\*基于K\_最近邻算法的未知病毒检测\_张波云（2005 国防科大期刊）：

提供了一种算法，后期可以参考

2）\*\*\*基于模糊模式识别的未知病毒检测\_张波云(2005 计算机应用)：

依然是模糊模式识别

\*\*\*一种未知病毒智能检测系统的研究与实现\_张波云(2006 计算机工程与设计期刊)：

提出了模糊检测模型，特征向量是API调用序列

3）\*\*\*基于多重朴素贝叶斯算法的未知病毒检测\_张波云(2006 计算机工程)：

贝叶斯算法

4）\*\*\*基于SVM的计算机病毒检测系统\_张波云（2007 计算机工程与技术期刊）：

提出了另一种模型

5）\*\*\*基于集成神经网络的计算机病毒检测方法\_张波云(2007计算机工程与应用)：

神经网络

以上共提出了5种方法:

K-最近邻算法，模糊模式识别，朴素贝叶斯算法，SVM自动向量机，神经网络

与PE文件结构有关的：

\*\*\*基于分类的未知PE病毒检测技术的研究\_洪群业（2010 重庆大学硕士论文）：

也是根据PE文件，检测未知病毒，使用了weka工具，分析了好几种分类算法，

特征是PE文件托壳后的反汇编字符串，然后继续提取。

\*\*\*基于PE文件结构异常的未知病毒检测\_樊震(2009 计算机技术与发展)：

根据PE文件得出特征向量，是根据PE文件的异常结构得出的特征向量，用了贝叶斯分类算法和支持向量机模型（SVM）

\*\*基于PE文件的启发式特征码自动提取的研究\_陈晋福（2010 电子科大硕士论文）：

特征码自动提取技术，根据PE文件的，还没仔细看

\*\*一种对Windows中PE文件进行启发式病毒扫描的算法\_何志永(2013 科技通报)：

对于特征码的选择，其实也是根据PE文件的异常结构，然后进行扫描算法

\*\*\*基于分类的未知病毒检测方法研究\_熊俊(2012 电脑开发与应用)：

基于PE文件的K-means算法，基于静态PE文件，但可以根据未知PE文件检测是否是病毒。

特征的选取是PE文件中体现出的dll,api,关键注册表，系统路径，代码相似度，我在想这些信息是不是也得通过反汇编看到？

\*\*\*基于分类的未知病毒检测技术研究与实现\_余晓姿（2012 中国邮电大学硕士论文）：

分析了PE文件，然后提出的是改进的K-mens算法

根据PE文件进行特征向量的提取，设计了一个特征向量的数据库，好多，还包括对字符串的分析等等。

\*\*基于数据挖掘技术的病毒主动防御系统\_叶艳芳（2005 福州大学硕士论文）：

也是基于PE文件，特征序列式api调用序列，使用的是数据挖掘的关联规则，没仔细看

\*\*\*\*行为分析算法综述\_谷军霞（2009 期刊）：

高质量论文，清华大学的….就是不一样，参考文献全部是英文的！！！（参考文献可以查阅）

\*\*\*\*基于关联规则的未知病毒检测方法研究\_赖英旭(2008 计算机工程与应用)：

关联规则的 静态的分析未知病毒的技术，根据PE文件的字符串和数据挖掘中关联规则的算法（没有用分类算法），特征码的提取是根据PE文件的字符串得出的，本文相当于提出了一个新的思路

\*\*基于特征码病毒扫描技术的研究\_关欣(2013 技术研究)：

现有的特征码的扫描技术的研究，一个二叉树，一个hash表

\*\*几种检测计算机病毒的方法研究\_姚学武（2011 专题研究期刊）：

简单介绍病毒检测方法。

\*\*\*\*基于病毒行为序列的未知病毒分析技术研究\_郑重(2009 国防科大学术技术)：

提出了基于虚拟机技术和病毒行为序列的病毒检测方法。具有可参考性，并且最后的参考文献有英文的，回来可以下载，参考文献可参考

\*\*\*面向未知病毒检测方法与系统实现技术研究\_张凡（2003 西北工业大学硕士论文）：

粗看，写论文时可以参照，包括特征码提取，与病毒分类，特征码提取包括了对PE文件格式，二进制文件格式，宏病毒的特征

\*静态和动态相结合的病毒检测方法研究\_黄馥妃（2012 大家谈）：

怀疑是抄袭张波云博士论文提出的动静病毒扫描模型，静态的特征码提取采用n-gram算法，分类采用KNNP神经网络，动态采取API特征序列，分类采用SVM

\*计算机病毒的传播模型及其求源问题研究\_韩兰胜（2006 华中科大博士论文）：

如题，研究的是传播模型和求源问题，似乎不太相关，没仔细看

\*浅析杀毒软件的现状及趋势\_曹丽萍（2008以后）：

内容如题，常识性了解吧

\*\*浅析360安全卫士及360杀毒软件机制及漏洞\_陈素霞(2010 信息技术期刊)：简单分析了360,360杀毒软件是一种启发式杀毒、

\*浅析计算机病毒类型及其防护措施(2009以后 信息产业)：简单介绍了下计算机病毒及其分

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

启发式扫描：

\*\*一种对Windows中PE文件进行启发式病毒扫描的算法\_何志永(2013 科技通报)：

对于特征码的选择，其实也是根据PE文件的异常结构，然后进行扫描算法

\*\*一种启发式反病毒技术的研究\_谭云松（2006 网络安全技术与应用）：

启发式扫描介绍，对病毒指令序列进行反编译，每个异常的指令有不同的权重，并且定义一个界限值，然后将这个检测病毒得出的权重跟这个值进行比较判断是否是病毒

\*\*\*基于虚拟机的启发式扫描反病毒技术\_曾宪伟(2005 计算机应用与软件):

对虚拟机进行了分类介绍 启发式扫描，没说具体的判断规则，

\*\*基于启发式算法的恶意代码检测系统研究与实现\_雷迟骏（2012 南京邮电大学硕士论文）:

内容很多，包括模式匹配，虚拟机技术，PE文件，云防御等，基于语义的启发式扫描技术，

仔细看也许能有想法

\*\*二进制病毒的启发式扫描技术\_张青霞（2006 农业信息网络）：

基于指令序列的判断方法，在虚拟机中运行可疑程序，根据权值判断是否为病毒

\*\*虚拟机在反病毒实验中的应用\_彭安杰（2010 计算机光盘软件与应用）：

实验环境的搭建

\*\*\*\*基于语义的启发式病毒检测引擎研究\_崔鹏（2008 常熟理工学院学报）：

改进基于虚拟机的扫描引擎，且设计了基于语义的，可以仔细看看。

\*\*基于多态病毒行为的启发式扫描检测引擎的研究\_王振海（2006 实验室研究与探索）：

虚拟机加启发式扫描，可以仔细看，也是设定阈值的判断方法，但是最后写了一些改进，特征的选取也是一大堆。

\*\*\*虚拟机查毒技术的实现\_刘勇（2008 科技创新导报）：

介绍了一个虚拟机技术，以32位自含代码虚拟机的具体事例，讲解具体的实现过程

\*一种启发式宏病毒扫描技术\_孙伟（2007 长春大学学报）：

针对宏病毒的，也是权值的设定，很多的特征，有抄袭，

看了这么多，抄袭很多，谁抄袭谁的还不知道，唉

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

分类算法：

\*\*\*基于分类的未知病毒检测方法研究\_熊俊(2012 电脑开发与应用)：

基于PE文件的K-means算法，基于静态PE文件，但可以根据未知PE文件检测是否是病毒。

特征的选取是PE文件中体现出的dll,api,关键注册表，系统路径，代码相似度，我在想这些信息是不是也得通过反汇编看到？

\*\*\*基于分类的未知病毒检测技术研究与实现\_余晓姿（2012 中国邮电大学硕士论文）：

分析了PE文件，然后提出的是改进的K-mens算法

根据PE文件进行特征向量的提取，设计了一个特征向量的数据库，好多，还包括对字符串的分析等等。

\*\*\*基于改进的K\_最近邻算法的病毒检测方法\_谢金晶（2007 现代电子技术）：

对分类算法的改进，特征的提取也是静态特征。

BP神经网络：

\*\*\*基于BP神经网络的病毒检测方法（2005 计算机工程期刊）：

提出了BP神经网络的算法，以后可参考

SVM自动向量机

\*\*\*\*基于主动学习的计算机病毒检测方法研究\_张勇（2011 计算机与数字工程）：

提出了基于主动学习的模型，特征码提取采用n-gram,分类采用SVM向量机，可以在新加入特征向量之后主动学习，形成新的训练集，而对特征码是将PE文件转换成ASCII的十六进制代码形式。

贝叶斯算法：

\*\*\*未知病毒检测技术的研究\_赖英旭（2006 计算机科学）：对朴素贝叶斯算法、复合贝叶斯算法进行研究，提出了种增量贝叶斯算法，带有自学习的能力，另外可以参考特征码的提前方法

以下为之前木马的有些相关的内容：

\*\*\*基于行为特征库的木马检测模型设计\_李焕洲（2011 四川师范大学学报）：

可以参考该检测模型，模糊模型

\*\*\*\*用于行为分析反木马的模糊分类算法研究\_顾雨捷（2008 浙江工业大学硕士论文）

可以参考本文写，这个可以好好读一下，包括参考文献等，很多英文的文献，可以读一下，

这篇细读。

\*\*木马攻击防范理论与技术研究\_宋海涛（2004 南京师范大学硕士论文）：

可参考决策树模型，里面提到了人工神经网络

\*\*基于行为分析的木马检测系统\_颜会娟(2010 网络安全)：

梳理了行为分析检测系统的过程，可以仔细参考。

\*\*采用行为分析的单机木马防护系统设计与实现\_王泽东(2011 计算机工程与应用)：

项目参照的论文，可以再看。贝叶斯算法

还没看 基于行为序列灰色模糊判定的计算机木马检测方法\_胡光俊（2011 北京理工大学学报）：

用于木马的模糊算法

以下三篇是实验室论文，提出的两个模型也可参考：

\*\*\*基于行为分析的特种木马主动防御技术研究\_李春晓（2012 实验室论文）：

针对项目写的一篇论文，其中提到了一个贝叶斯分类算法，讲诉了查杀方法还包括云查杀

\*\*\*木马行为特征及防护策略的研究\_胡中雨（2012 实验室论文）：

里面提出了一种攻击树模型，可参考

\*\*基于动态链接库的摆渡木马设计方法研究\_胡俊夫（2012 实验室论文）:

设计了摆渡木马，可以根据这个了解摆渡木马，和木马的具体的行为特征