可参考度：按\*\*多少确定

以下三篇与项目有关，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（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（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（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

以下两篇提出的模型可参考，

\*\*\*\*\*基于行为特征库的木马检测模型设计（期刊）：

可以参考该检测模型

\*\*\*木马攻击防范理论与技术研究（硕士论文）：

可参考决策树模型，里面提到了人工神经网络

\*\*\*\*\*\*用于行为分析反木马的模糊分类算法研究\_顾雨捷（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。

以下三篇为监控部分

\*\*\*基于行为分析的主动防御技术及其脆弱性研究\_罗晓波（期刊）：

分析了主动防御技术，即下面的监控内容，一般是监控程序对下面那些行为的监控，有助于理解项目。

\*木马的攻击及新型的木马检测技术的研究（硕士论文）：

参考第五章

\*基于木马行为特征的检测报警系统的设计和实现（硕士论文）:

可以参考实时监控部分，相当于项目的文件、注册表、进程、网络监控部分。

\*木马行为特征检测技术研究（硕士论文）：

也是关于文件、注册表、进程、网络监控部分，帮助理解项目，这就是动态行为检测吗？

\*\*基于特征码技术的攻防策略（期刊）：

可以了解一下静态特征码技术，提取方法等。

\*木马病毒分析及其检测方法研究（期刊）：

可参考提出的多agent模型，还没具体看