1

第一代：手工杀毒软件
病毒表征诊断

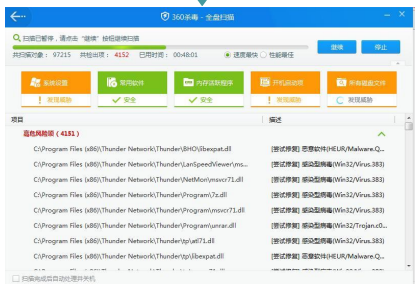
√ 为恶意软件检测奠基

× 仅判断文件是否被感染
× 不具备自动病毒清除能力
× 大多产生于纯 DOS 年代

提出时间：1970s，主流时间：1990s

2

第二代：杀毒软件
广谱特征码扫描与比对技术



√ 比对特征值
√ 病毒特征库完整时可达 100% 识别

× 特征的提取速率远不及变异速率
× 难以防范未知病毒

提出时间：1990s，主流时间：2005~2015

3

第三代：主动防御软件
主动防御技术

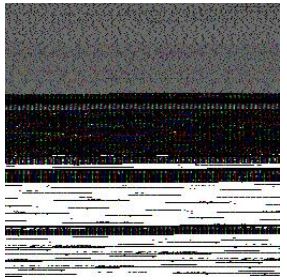
√ 颠覆传统反病毒理念
√ 从行为入手，以防为主
√ 从病毒特征库升级为行为特征库

× 易忽略行为动作小的病毒
× 易误报行为动作大的正常文件

提出时间：2000s，主流时间：2015~2020

4

第四代：人工智能防御软件
机器学习/深度学习技术



检测结果

ML.Attribute.HighConfidence

√ 模型训练提高准确度
√ 有效辅助主防判断
√ 模型迁移容易
√ 能够等效归化为其它问题

× 模型训练周期长
× 识别过程资源消耗大

提出时间：2010s，预计主流时间：2025后