反病毒引擎

产品简介

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

产品简介
产品概述

最近更新时间：2021-08-02 10:23:57

什么是反病毒引擎

腾讯云反病毒引擎（Antivirus）是腾讯反病毒实验室独立研发的反病毒产品，运行于终端的判毒程序，其包含腾讯反病毒本地引擎和腾讯反病毒云两大功能模块，开放多个功能性接口 SDK，可支持多种平台使用且无需联网。反病毒引擎具备完善的海量样本运营体系和专业级安全支撑团队，适用于断网或隔离网环境下的终端产品集成场景，同时拥有十余年反病毒技术经验以及海量的数据积累，可广泛应用于各类涉及判定文件是否安全的场景，也可以快速集成到各类相关产品。

产品功能

反病毒引擎拥有多个功能性接口，可帮助您判断文件是否安全，并提供清除修复文件的功能。

- **文件扫描**
  通过接口上传文件或本地下载安装客户端后，反病毒引擎可以对指定文件进行扫描，判端文件是否存在安全隐患。文件扫描支持多种文件格式，可以精准识别恶意文件。
- **文件修复**
  反病毒引擎扫描文件后，将根据判定结果，针对性地为您提供修复方案。
- **MD5 云查**
  通过接口上传 MD5 信息，反病毒云将根据云查返回该 MD5 的安全判定结果。

产品优势

最近更新时间：2021-08-02 10:23:24

反病毒引擎的产品优势如下：

- **优秀的病毒检测能力**
  反病毒引擎集成于腾讯电脑管家英文版和腾讯手机管家 WeSecure 中，其中，电脑管家在赛可达 PC 安全评测中，多次获得动态扫描和静态测试第一名。腾讯手机管家 WeSecure 在国际权威 AV-TEST 移动安全测试中，凭借反病毒引擎的安全能力，连续取得了17次满分。
- **完整的格式识别体系**
  反病毒引擎有一套完整的格式识别体系，可以精准的识别 PE 文件、加密壳、Linux 文件、APK 文件、压缩包、复合文档、各类脚本如 JS、VBS 等。
- **强大的脱壳解密功能**
  反病毒引擎有强大的格式拆析、脱壳解密的功能，可以通过静态解析、动态执行等技术手段将压缩包、复合文档以及各类加密壳进行拆解，暴露出更多的子文件，方便检测查杀。
- **高性能低占用**
  在效率和内存占用等性能方面，反病毒引擎也有很好的把控，扫描单文件的时间平均控制在1ms，内存占用均值控制在15MB。
- **易于集成扩展**
  引擎设计架构基于平台无关性设计，可运行于 Windows、Linux、Mac 等多平台操作系统，轻量化设计充分保证 反病毒引擎易于集成和扩展，方便应用到更多的场景中。
- **本地通杀特征**
  反病毒引擎输出了方便分析人员添加通杀特征的接口，如模糊搜索、静态跳转、算术运算、逻辑运算、虚拟地址转换、文件数据结构定位等功能，大大提升了通杀特征的效果。
- **虚拟动态执行代码**
  在动态执行方面，反病毒引擎有 PE 动态执行虚拟机、Android 执行虚拟机和 JSVM 脚本执行虚拟机，可进行动态脱壳解密、动态行为检测，可有效处理复杂的病毒木马。
- **深度机器学习**
  近年反病毒引擎将文件的行为特征检测与 AI 深度学习结合，对新病毒和变种病毒有了更强的泛化检测能力，能够及时发现未知病毒和变异病毒，将机器学习技术和病毒检测技术完美结合。

应用场景

最近更新时间：2021-08-02 10:22:35

联网公有云查

- **可疑文件公有云查**
  对可疑文件进行 Hash 计算，通过反病毒引擎公有云查询服务查询文件黑白属性。
- **可疑文件云端扫描**
  将可疑文件通过 API 接口上传至云端扫描服务器进行样本扫描，服务器将返回样本黑白属性。

断网私有云查

可疑文件私有云查：在企业内部搭建私有云服务器，对可疑文件进行 Hash 计算，通过私有云查询服务查询文件黑白属性。

本地引擎扫描

- **可疑文件本地黑白鉴定**
  可直接使用腾讯反病毒引擎或集成有反病毒引擎（SDK）的软件进行本地文件扫描，直接判断样本黑白属性。
- **被感染文件修复**
  可直接使用腾讯反病毒引擎 或集成有反病毒引擎（SDK）的软件对被病毒感染过的重要文件进行修复，还原母本文件，保护文件数据。