ThreatBook Public API 说明文档

一、Public APIs

1.1 扫描文件

提交文件进行扫描。

URL: https://x.threatbook.cn/api/v1/file/scan

POST/GET? POST

输入：

输入	说明
apikey (string)	用户专属 apikey
file	要用 multipart/form-data 方式提交

输出：

输出	说明
response_code (int)	可为以下值： 1: 上传成功，正在排队 -1: 出错，具体看 verbose_msg 的返回
verbose_msg (string)	response_code 相应的 Verbose 信息
resource (string)	文件的 sha256
scan_id (string)	用于后面取扫描报告用
permalink (string)	查看本次扫描报告的 URL
sha256 (string)	文件的 sha256 值
sha1 (string)	文件的 sha1 值
md5 (string)	文件的 md5 值
is_white(boolean, optional)	为 true 表示是白名单文件，如 Windows 操作系统文件。
white_desc(string, optional)	如果是白名单文件，这里是一个关于是哪种白名单文件的描述。

1.2 获取文件扫描结果

获取之前提交的文件的扫描结果或根据文件 HASH 得到最近的一次结果。

URL: https://x.threatbook.cn/api/v1/file/report

POST/GET? POST

输入：

输入	说明

apikey (string)	用户专属 apikey
resource (string)	可为以下值： ● 文件的 md5/sha1/sha256，获取的是这个文件的最近的扫描结果。 ● 之前提交的文件时返回的 scan_id。 ● 批量操作，CSV 格式的多个（最多 4 个）的哈希值或 scan_id。

输出：

输出	说明
response_code (int)	可为以下值： 0: 请求的文件没有结果 1: 扫描已经完成，返回结果 3: 有部分扫描结果 -1: 出错，具体看 verbose_msg 的返回
verbose_msg (string)	response_code 相应的 Verbose 信息。
resource (string)	和传入的 resource 一致
scan_id (string)	这次扫描的 id
permalink (string)	查看扫描报告的 URL
sha256 (string)	文件的 sha256 值
sha1 (string)	文件的 sha1 值
md5 (string)	文件的 md5 值
scan_date (string)	扫描时间
positives (int)	共有多少引擎返回有毒
total (int)	共有多少引擎返回扫描结果
total2(int)	当前后台共部署了多少扫描引擎
scans(array)	所有引擎的扫描结果，每个 item 是一个引擎的结果，包括： 引擎名 detected: boolean, 为 true 表示有毒，为 false 表示没毒或没有检测 version: 引擎的版本 result: 查到恶意软件名或 safe 表示没毒，或 timeout 表示超时. update: 引擎的病毒库的最后更新时间 例： "NOD32": {"detected": true, "version": "5115", "result": "a variant of Win32/Qhost.NTY", "update": "20100514"}, "F-Prot": {"detected": false, "version":"4.5.1.85", "result": null, "update": "20100514"},

is_white(boolean, optional)	为 true 表示是白名单文件，如 Windows 操作系统文件。
white_desc(string, optional)	如果是白名单文件，这里是一个关于是哪种白名单文件的描述。

1.3 重新扫描已经提交过的文件

重新扫描已经自己或其他用户提交过的文件。

URL: https://x.threatbook.cn/api/v1/file/rescan

POST/GET? POST

输入：

输入	说明
apikey (string)	用户专属 apikey
resource (string)	md5/sha1/sha256 或 CSV 格式的多个（最多 25 个）这三种 HASH 值的组合

输出：

输出	说明
response_code (int)	可为以下值： 0: resource 对应的 hash 值在我们的库中没有 1: 成功进入扫描队列 -1: 出错，具体看 verbose_msg 的返回
verbose_msg (string, optional)	response_code 相应的 Verbose 信息,当调用成功时，没有此输出选项。
resource (string)	文件的 sha256
scan_id (string)	用于后面取扫描报告用
permalink (string)	查看扫描报告的 URL
sha256 (string)	文件的 sha256 值
sha1 (string)	文件的 sha1 值
md5 (string)	文件的 md5 值
is_white(boolean, optional)	为 true 表示是白名单文件，如 Windows 操作系统文件。
white_desc(string, optional)	如果是白名单文件，这里是一个关于是哪种白名单文件的描述。