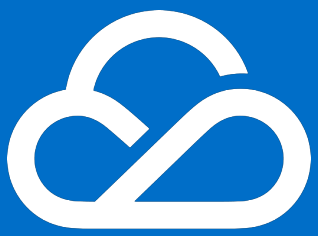
腾讯云网络安全（大禹）

DNS劫持检测

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

DNS劫持检测产品简介

Local DNS劫持是一种通过改变指定域名在运营商侧Local DNS配置的正确解析指向，将该域名的解析结果重定向到劫持IP的劫持行为。

Local DNS劫持类型可大致分为运营商缓存，广告，恶意劫持等类别。

其中运营商缓存是运营商侧为了降低跨网流量及用户访问速度进行的一种良性劫持；广告劫持是运营商或恶意团体将用户正常页面指向到广告页面或在正常页面中插入第三方广告的劫持行为；恶意劫持是指通过改变域名指向IP，将用户访问流量引到挂马，盗号等对用户有害页面的劫持。

DNS劫持检测操作指南

为当要对新的域名进行劫持检测时，点击DNS劫持检测页面右上角“添加记录”进行添加。

第一步首先添加需要监控的主域名（主域名的形式例如qq.com），可以添加新的域名，也可以从已有的域名中进行选择。

添加完域名之后进行DNS记录配置，点击“新增一行”后依次添加“记录类型”，“主机名”和“记录值”。记录类型包括A和cname，当该域名直接指向一个IP地址时，选择A，当该域名直接指向另一个域名时，选择cname。“主机名”处填写需要监测的具体子域名，例如www.qq.com，“记录值”处填写该子域名指向的IP或域名，如果记录类型是A，则填写该子域名指向的IP地址，如一个子域名指向多个IP地址，则依次点击“新增一行”，每次添加一个IP地址。如果记录类型是cname，则填写该子域名指向的新域名，如一个子域名指向多个域名，则依次点击“新增一行”，每次添加一个新域名。