

腾讯云大禹网络安全

DNS劫持检测

产品文档



腾讯云

【版权声明】

©2013-2017 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【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

文档声明.....	2
DNS劫持检测.....	4
DNS劫持检测产品简介	4
DNS劫持检测操作指南	5

DNS劫持检测

DNS劫持检测产品简介

Local DNS 劫持

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

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。

相关概念

- 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

第一步：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。

第二步：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。

第三步：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。