DNS外带查询怎么防。。。

jfeiyi / 2018-01-13 12:52:51 / 浏览数 2300 安全技术 技术讨论 顶(0) 踩(0)

求问大佬。。。。DNS这方面怎么防，最近在看各种技巧，感觉不好防啊。

点击收藏 | 0 关注 | 1

上一篇：Misc 总结 ----隐写术之多... 下一篇：Misc 总结 ----流量分析 ...

1. 1 条回复

 hades 2018-01-14 11:01:23

@安全小飞侠 检测的话可以利用pdns数据来分析恶意dns
可以是从企业内部去dns数据中分析恶意dns，也可以是从外部pdns威胁分析服务中获取恶意的dns，如思科的opendns服务；防御方法一般可以采用DNS RPZ来sinkhole/blackhole dns请求(前者是返回无害的dns答复给请求，后者是不返回dns答复给请求，从而阻断恶意dns的请求),
或者采用外部的具备安全能力的DNS服务器，如IBM的9.9.9.9DNS服务。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录