

[🏠 首页](#)[🏷 标签](#)[📁 分类 ▾](#)[📖 日志](#)[🔧 工具 ▾](#)[📌 关于 ▾](#)

CS新特征

BlueTeam

🛡 安全

📅 发布日期: 2022-01-10

📄 文章字数: 69

🕒 阅读时长: 1分

👁 阅读次数:

基本描述

CobaltStrike的HTTP(S)监听器对请求URL未进行"/"开头验证, 攻击者可通过指定URL获取相关信息。

有效载荷



GET stager HTTP/1.1

Host: x.x.x.x

User-Agent: Mozilla/5.0

测试过程



🏠 首页

🍃 标签

📁 分类 ▾

📖 日志

🔧 工具 ▾

📍 关于 ▾





🏠 首页

🍃 标签

📁 分类 ▾

📖 日志

🔧 工具 ▾

📍 关于 ▾





🏠 首页

🍃 标签

📁 分类 ▾

📖 日志

🔧 工具 ▾

📍 关于 ▾





🏠 首页

🍃 标签

📁 分类 ▾

📖 日志

🔧 工具 ▾

📍 关于 ▾





🏠 首页

🍃 标签

📁 分类 ▾

📖 日志

🔧 工具 ▾

📍 关于 ▾





🏠 首页

🏷 标签

📁 分类 ▾

📅 日志

🔧 工具 ▾

📌 关于 ▾



影响范围

CobaltStrike <= 4.5

👤 文章作者: DongHuangT1

🔗 文章链接: <https://DongHuangT1.com/writings/Stager/>

📄 版权声明: 本博客所有文章除特别声明外, 均采用 CC BY-NC 4.0 许可协议。转载请注明来源 DongHuangT1 !

💬 评论



Nickname

Required

Email

Required

Website

Optional

[🏠 首页](#)[🏷 标签](#)[📁 分类 ▾](#)[📅 日志](#)[🔧 工具 ▾](#)[📌 关于 ▾](#)[Preview](#)[Send](#)

Powered by [Twikoo](#)

[← 上一篇](#)

MarkHacker

MarkHacker是一个用于标记Hacker的JS脚本，它通过请求资源文件判断客户端使用的Hacker工具。

🕒 2022-03-29

📁 推荐

BlueTeam

[下一篇 >](#)

[🏠 首页](#)[🏷️ 标签](#)[📁 分类 ▾](#)[📖 日志](#)[🔧 工具 ▾](#)[📌 关于 ▾](#)

信息收集

|| “复制粘贴” 之信息收集 ||

🕒 2021-03-10

🛡️ 安全

RedTeam

📖 目录

基本描述

有效载荷

测试过程

影响范围

Copyright © 2020 DongHuangT1
本站已运行 1061 天 9 小时 29 分钟 0 秒

