|  |
| --- |
| 【文档编号：2020020401】 |
| 四川省生态环境厅安全报告  宜宾市生态环境局  Webshell命令控制安全事件分析 |
| 二〇二〇年二月 |

# 基本信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **资产IP** | 10.0.8.20 | | | **隶属** | 宜宾市生态环境局 |
| **发现时间** | 2020年2月1日 | **处理期限** |  | **事件类型** | 恶意文件 |
| **事件名称** | Webshell命令控制 | | **事件级别** | □I级 □II级 ☑III级别 □IV级 | |
| **危害表象** | □网络中断  □系统瘫痪  ☑数据毁坏  ☑数据泄密  ☑其它危害 | | | | |

# 事件综述

## 事件概述

通过AiLPHA大数据平台分析发现，2020年1月20日-2020年2月1日，发现Webshell命令控制攻击共计4条，请求响应码为200。

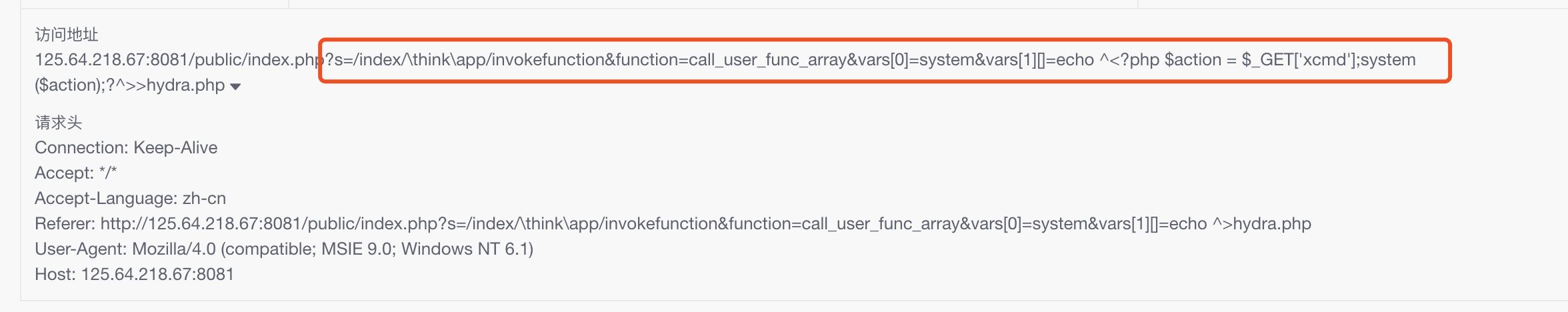


## 事件定位分析

外部IP：125.64.223.48向宜宾市生态环境局IP：10.0.8.20的8081端口发送Get请求，状态响应码为200。



在请求信息中，我们发现是典型的“一句话木马”注入，并且响应码是200，疑似注入成功。



外部IP：112.60.90.3向宜宾市生态环境局IP：10.0.8.20的8081端口发送POST请求，状态响应码为200。



在请求的body中我们可以看到，这是明显使用“中国菜刀”连接的痕迹，攻击者可能连接之前已经上传的webshell。



# 建议与措施

1、检查IP对应的主机中是否存在来历不明的文件。  
2、一旦发现被入侵，查看服务器是否有来历不明的文件，如无法判断需删除所有可访问文件，并重新上传。

3、对于来自外部的攻击行为，务必配置好服务器权限。最小的权限=最大的安全。防范webshell的最有效方法就是：可写目录不给执行权限，有执行权限的目录不给写权限