

正面测试未形成突破后，攻击路径转向同源资产检索，并连续命中应用、消息组件和业务接口三层暴露。

01

IOT 未授权

可直接查看遥控配置与设备清单，控制入口已暴露。

02

RabbitMQ 默认凭据

guest / guest 可登录管理端，队列与运行通道可被查看。

03

业务接口直出配置

节点、站点、通道、驱动类型和串口配置可被批量枚举。

这不是三个孤立问题，而是一条从应用入口延伸到消息组件和设备配置的供应链风险链。

ATTACK PATH

正面测试无果后，icon\_hash 打开了供应商侧入口

关键转折不是增加攻击强度，而是改变资产发现方法。



关键转折 从“攻目标”切换为“找供应商同源资产”。

# 三类薄弱点串成一条可扩展攻击链

| 已验证证据            | 直接后果       | 系统性影响         |
|------------------|------------|---------------|
| 01 IOT 未授权访问     | 进入设备与遥控配置  | 控制面与业务面失去边界   |
| 02 RabbitMQ 默认凭据 | 查看队列与运行通道  | 消息层成为横向扩展点    |
| 03 业务接口鉴权不足      | 枚举站点、通道与设备 | 供应商系统拓扑可被批量获取 |

风险判断

攻击链具备可重复、可扩展并影响终端控制面的条件。

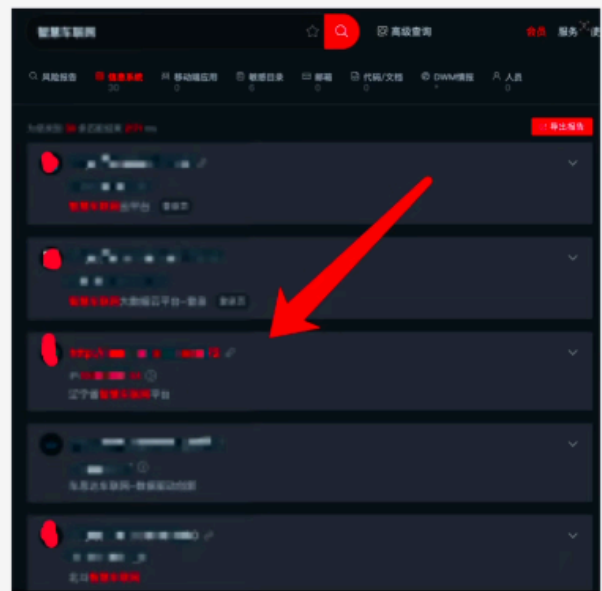
## 1、供应链事件背景



### 3、通过系统关键词定位测试系统

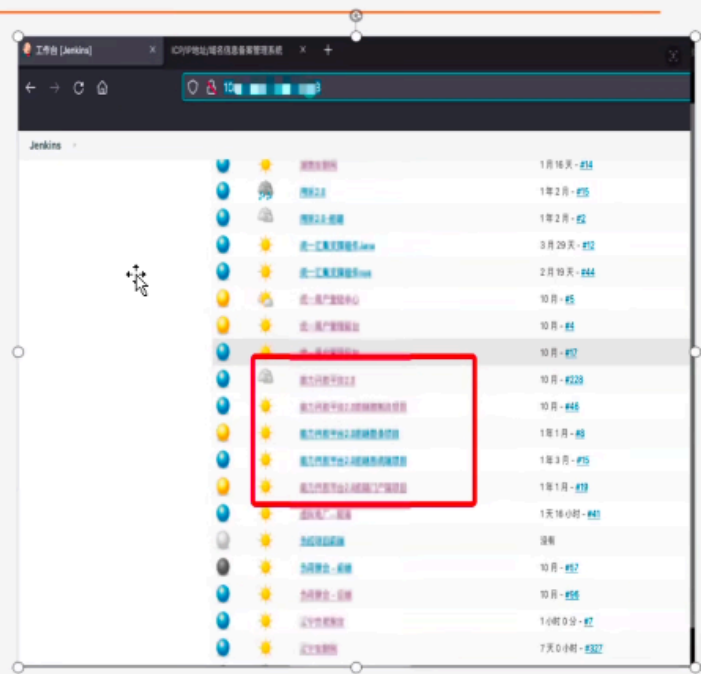
如右图，通过“\*\*\*\*\*”关键词，定位到带有客户资产图标的信息资产，且该资产的出口IP并非客户的出口网段，故怀疑是测试环境或者私搭环境，当时该资产已经无法访问，但IP仍然存活，因此对该IP进行了全端口扫描。

备注：信息收集过程中，不要忽略了那些已经关闭的系统，可以通过历史快照或端口探测等方式对该资产进行深入测试，该资产无法访问不代表该IP没有使用。



### 4、全端口探测，发现Jenkins平台，获取敏感代码

如右图，通过全端口探测，发现该历史IP的其中一个端口，存在Jenkins平台未授权访问漏洞，并且发现了大量的代码，其中包括\*\*\*\*的核心系统-能力开放平台





## 7.1、重大突破，获取数据桶权限

对Jenkins平台的代码进行初步分析，发现了AccesskeyID和AccessKeySecret，并成功登录了该数据桶

```
public class OSSUtil {
    //测试环境

    private final String bucketName = "hltoss";
    private final String endpoint = "http://oss-cn-beijing.aliyuncs.com";
    private final String accessKeyId = "AKIAJ44K44K44K44K44K44";
    private final String accessKeySecret = "*****";

    /*
    //正式环境
    private String bucketName="hlhtoss";
    private String endpoint="http://*****.cloud.echarge.net.com/hlhtoss";
    private String accessKeyId="*****";
    private String accessKeySecret="*****";
    */

    private static final Logger log = Logger.getLogger(OSSUtil.class);
}
```

## 8、再次突破，获取阿里云控制台

对获取的AccesskeyID和AccessKeyS进行深入利用，成功获取到了阿里云控制台的控制权限。

```
2022-07-20 10:37:07] 配置完成，配置文件路径 (Configure done, Configuration file path): C:\Users\Mr. Zhong\...
2022-07-20 10:37:14] WARS 需要配置访问凭证 (Access Key need to be configured first)
2022-07-20 10:37:14] WARS 需要配置访问凭证 (Access Key need to be configured first)

用户名称      密码      控制台登录地址
-----
admin@aliyun.com      *****      https://*****.aliyun.com
```

