## 附件： 网络安全专项行动事件记录表

|  |  |
| --- | --- |
| 填表人：陈翔 日期：2024年8月 02日 | |
| 防守成果名称 | 有限天津蜜罐系统捕获攻击地址主机 |
| 攻击源IP | 122.228.200.194 |
| 被攻击  系统1 | 被攻击系统URL：无  被攻击系统IP：60.30.184.48  网络层级：  ☑互联网 □办公网 □业务内网 □生产网 |
| 监测  发现 | √及时性  攻击时间：08月01日13:47:46-20:32:19  √采用工具或手段  □安全设备 □态势感知平台  □流量分析 ☑其他： 蜜罐诱捕系统 |
| **攻击行为描述：**  尝试sql注入、远程命令执行等、SSH连接、zmap连接、尝试FTP登录等高危攻击  **监测截图：** |
| 分析  研判 | **分析研判：**  **1、研判攻击的影响范围**  60.30.184.48  **2、分析研判采用的工具或手段**  蜜罐诱捕系统、fscan、威胁情报平台等 |
| 应急  处置 | √抑制攻击的能力  √阻断有效攻击源  时间：  攻击时间：08月01日13:47:46-20:32:19  发现时间：08月01日14:12:11  阻断时间：08月01日20:35:22  阻断方式：拦截、阻断  √阻断IP：  122.228.200.194 |
| 协同  联动 | ☑单位内部各部门之间的联动  有限天津网络安全专项行动防守指挥部通过邮件统一上报集团公司监测预警组，集团公司监测预警组将攻击IP封堵处理，防止该攻击IP对海油内网的攻击,有效阻止攻击蔓延。 |
| 追踪  溯源 | 防御过程描述：  **追踪溯源**  通过蜜罐诱捕系统，捕捉到国内互联网地址IP：122.228.200.194,尝试对蜜罐系统sql注入、远程命令执行、ssh、telnet、ftp连接等高危攻击。  通过威胁情报分析平台得知这是一个未知的恶意ip：      安全工程师使用fscan对该ip：122.228.200.194做进一步溯源信息获取：    其中该恶意主机存在redis未授权漏洞：  1、122.228.200.194:6379 redis未授权漏洞，使用redis-tool工具直接连接     1. http://122.228.200.194:3000 yapi接口管理平台，存在NoSQL注入导致远程命令执行漏洞     进一步溯源到ip对应的域名信息：quickapp.uochen.com    对应的公司：深圳市优辰科技有限公司    恶意IP的地址信息（仅供参考）： |