## 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 15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 | 117.33.169.73 |
| 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15日05:54:27-06:30:24  √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：**  使用zmap扫描端口、尝试SSH连接、尝试FTP登录等高危攻击  **监测截图：**  1  1.1  （这里只列举出3条尝试ftp登录的攻击事件，类似的事件共有927条） |
| 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15日05:54:27-06:30:24  发现时间：08月15日10:12:11  阻断时间：08月15日10:35:21  阻断方式：拦截、阻断  √阻断IP：117.33.169.73 |
| 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：117.33.169.73尝试对蜜罐系统进行zmap端口扫描、尝试SSH连接、尝试FTP登录等高危攻击。  安全工程师使用fscan对该IP：117.33.169.73进行溯源获取信息：  2  发现117.33.169.73存在路径 /Account/Login?ReturnUrl=%2f ，访问网页如下：3  使用密探工具发现 IP 117.33.169.73 对应域名为 pecofirst.cn，并且该域名有网站备案号：**陕ICP备2023006308号**。  4  查询ICP备案主体信息， 发现 **陕ICP备2023006308号** 对应的主办单位是一家企业——朋成科仪（西安）智能科技有限公司。  6  百度搜索朋成科仪（西安）智能科技有限公司，发现公司的法定代表人是**郭常春**。  7  分析发现 117.33.169.73 是腾讯云服务器，**域名 pecofirst.cn 的注册人**是 **郭常春**。  5 |