故障类型： 外部分布式攻击ddos and cc

故障描述： 用户打开网站缓慢，甚至打不开

预计影响时间：10分钟-2小时

处理步骤：

1. 联系机房要求机房协助清洗流量。排除80端口以外的流量. 18969103581通北机房 15158117685销售总监马丽清
2. 进入系统利用top命令查看系统的基本状况，判断出是系统负载问题，IO问题，内存问题，并且查看是那个程序导致，如果是流量问题利用iftop，iptraf等命令判断哪些主机有异常流量的传送，且判断是哪些程序引起这些流量。
3. 通过第二部分析各个程序的日志，判断问题所在，做相应的处理。
4. 80端口流量过大.启用nginx防护.iptable防护
5. 限制并发请求数量一个ip1次.
6. 客户端设置cokkie 机器人攻击无法返回cokkie.被排除
7. Iptable规则设定 并发大于50次的iptable屏蔽.
8. 如果经过以上步骤后流量还是过大.启用cdn.网站停止https解析.https无法做cdn分流.
9. 500m以内用电信线路用百度云免费cdn.联通线路用加速乐www.jiasule.com
10. 1g的流量清洗费用  921.6元/日联系财务付款{提前告知公司后可通知财务付款}2g以上做乘法.
11. 如果想节省费用就按照省ip来关闭经济发达的省份先开放.其余关闭比如(广东 浙江 江苏 北京 上海 成都开放其余关闭)
12. 如果是数据库出现io，负载，内存占用率高的情况：
13. 分析mysql的慢日志，看是有那些sql拖死mysql，提交程序优化sql.
14. 分析数据库的错误日志查看数据库是否有异常。
15. 进入数据库利用show processlist，查看数据库执行状态做相应处理
16. 1.只允许中国ip 2.只允许浙江ip