|  |  |
| --- | --- |
| **故障标题** | **机房出口被攻击，催收系统各业务线密集卡顿，对业务正常作业造成较大影响** |
| **故障级别** |  |
| **申报人员** |  |
| **发现时间** | **2017-11-14 日10:40~10:50，11:10~11:20，11:40~11:50，13:10~13:20，14:20~14:30，每次卡顿时间为数十秒到几分钟不等** |
| **描述信息** | **催收系统访问异常的情况，具体表现为“功能模块访问白屏”、“加载速度十分缓慢”、“系统服务失联”等** |
| **受影响产品线** | **快信催收、利信催收、快闪催收** |
| **责任部门** | **北京研发中心-资产系统部门-催收组** |
| **故障影响** | **导致1300+业务员频繁卡顿，影响正常工作** |
| **处理人员** | **shehe.li、yingfei.wan** |
| **处理进度** | **【2017-11-14 10:40~10:50】业务群反馈异常**  **【2017-11-14 10:41】开始时间：2017-11-14 10:41:00**  **1：先将报错信息和地区出口ip、CDN信息汇总提报给运维和CDN**  **2：这个过程中CDN定位问题时间也是有点长，最后给的是502异常码**  **3：根据异常信息和系统中唯一的随机生成的时间戳，通过cdn反馈信息，并找运维同事进行线上nginx请求上是否有该日志信息，主要是来判断是否网络有问题**  **4：根据服务器上nginx和tomcat服务器请求日志没有发现502的请求过来，初步判断cdn到机房网络不通造成**  **5：再次和运维沟通确定机房是否网络正常，根据运维监控机房其他业务线主站等各个流量没有太大的增幅，暂时以为网络没有问题，同时通过查询催收监控访问的监控日志发现，在爆发10点40之前出问题前一段时间访问流量特别低，再次确定较大可能应该还是机房网络问题**  **6：万老板和机房多次多人沟通交流后，确认机房端口攻击，催收系统被波及影响**  **总结：催收各业务线之前碰到较多的问题是CDN节点不稳定影响，但是北京访问正常。处理流程是把异常截图、出口信息、汇总发至cdn群，由他们协助查找问题，据cdn人员反馈多次都是因为节点配置有问题、边缘节点访问有问题和这次的cdn到机房网络不同造成**  **【2017-11-14 13:00:00】结束时间：2017-11-14 13:00:00**  **【2017-11-14 13:01:00】引起故障原因：机房端口被攻击，催收系统被波及影响，机房加急解决中** |
| **开始时间** | **2017-11-14 10:41:00** |
| **结束时间** | **2017-11-14 13:00:00** |
| **故障时长（分钟）** | **50（间断异常）** |
| **处理时长（分钟）** | **140** |
| **发现类型** | **人工通知** |
| **业务影响描述** | **系统间歇性卡顿，影响业务员大概1300+，累积时长50分钟，不能正常作业** |
| **业务处理负责人** | **Ming.yang** |
| **业务解决方案** | **及时和技术反馈，沟通评估影响范围，异常的特点** |
| **故障原因分类** | **第三方导致** |
| **故障原因** | |  |  | | --- | --- | | **导致故障的问题** | **1.机房端口被攻击，催收系统被波及** | | **导致发现过晚的问题** | **1. 没有及时第一时间报警提醒，而是通过业务反馈有些被动，信息滞后 2.没有相应网络异常的报警监控** | | **恢复过慢的问题** | **1.运维和机房多次沟通确认为该为网络攻击，这个过程中和多个人沟通，存在信息不一致，最终方案是需要机房采取措施来恢复** | |
| **改进计划** | **改进措施[1](http://pmo.corp.qunar.com/browse/PAY-17001" \t "_blank)：通过系统增加一个监控页面供运维和网络同时时刻监控机制检测是否从CDN到机房网络正常，可以第一时间了解线上的情况**  **完成日期：2017-11-20**  **所属项目组：催收组、运维组、网络组**  **经办人：shehe.li、yingfei.wan**  **改进措施2:为催收系统建立灾备机制，和运维、架构组沟通后计划在成都添加nginx反向代理北京机房节点走专线到北京机房，这条链路打通后采用CDN容灾模式，通过不同的权重来实现自动容灾，保证系统的可用性**  **完成日期：待定**  **所属项目组：催收组、基础架构组、运维组**  **经办人：shehe.li、yantao.yin、yingfei.wan** |
| **review应用负责人** | **shehe.li** |
| **review时间** |  |