中国联通官网被发现含木马脚本，可向用户推广色情APP

小小莫理 莫理

关注莫理！每天获取稀奇古怪的好东西

前言

联通官网携带木马脚本 可向用户推广色情APP

最新资讯 2020-11-12 9642次阅读

11月12日，据火绒安全实验室官网公告，近期发现中国联通官方网站的业务办理页面携带木马脚本。

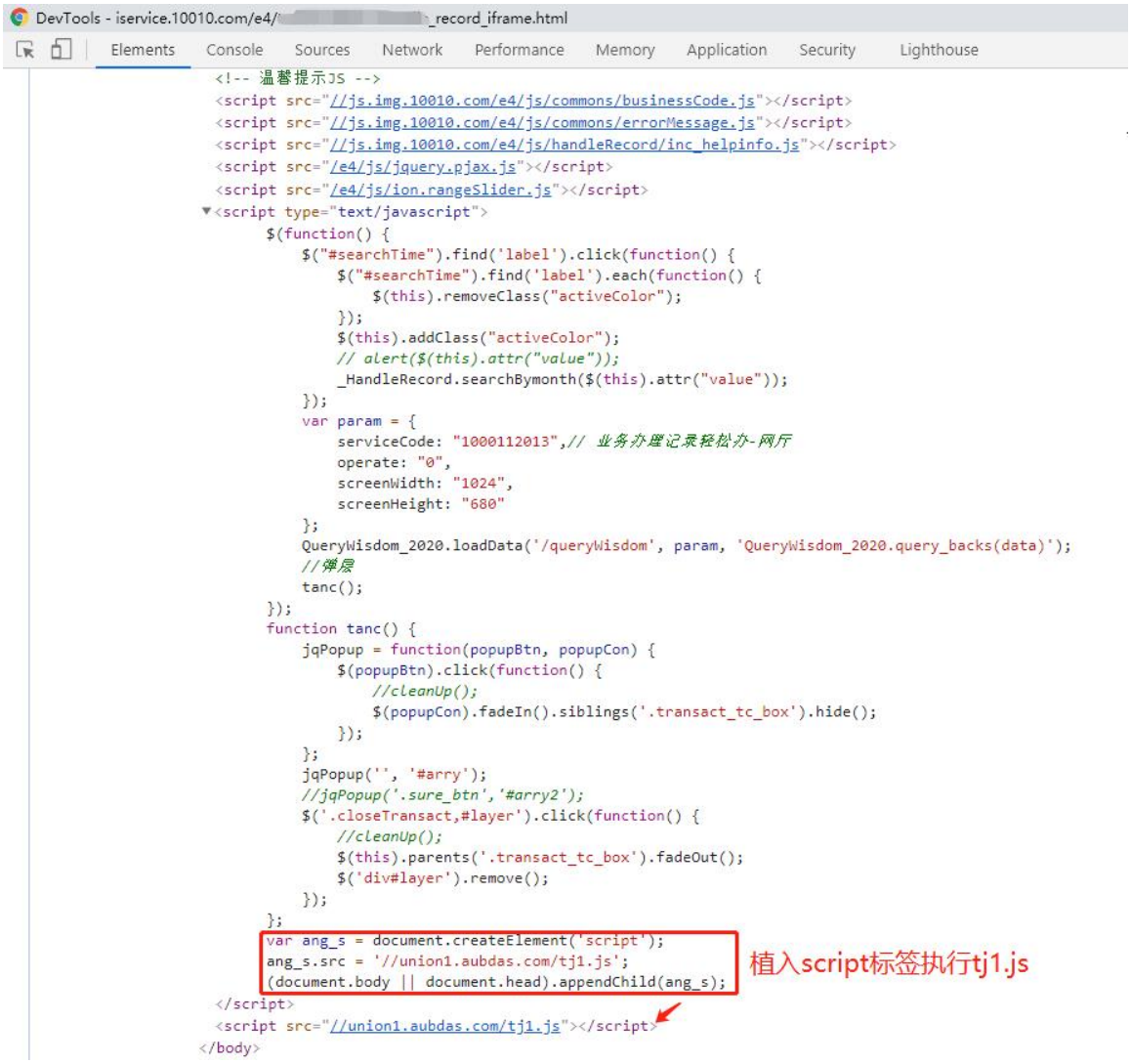
可用于向用户推广色情APP和游戏，此外检测到这些域名服务器均托管在境外。

公告原文

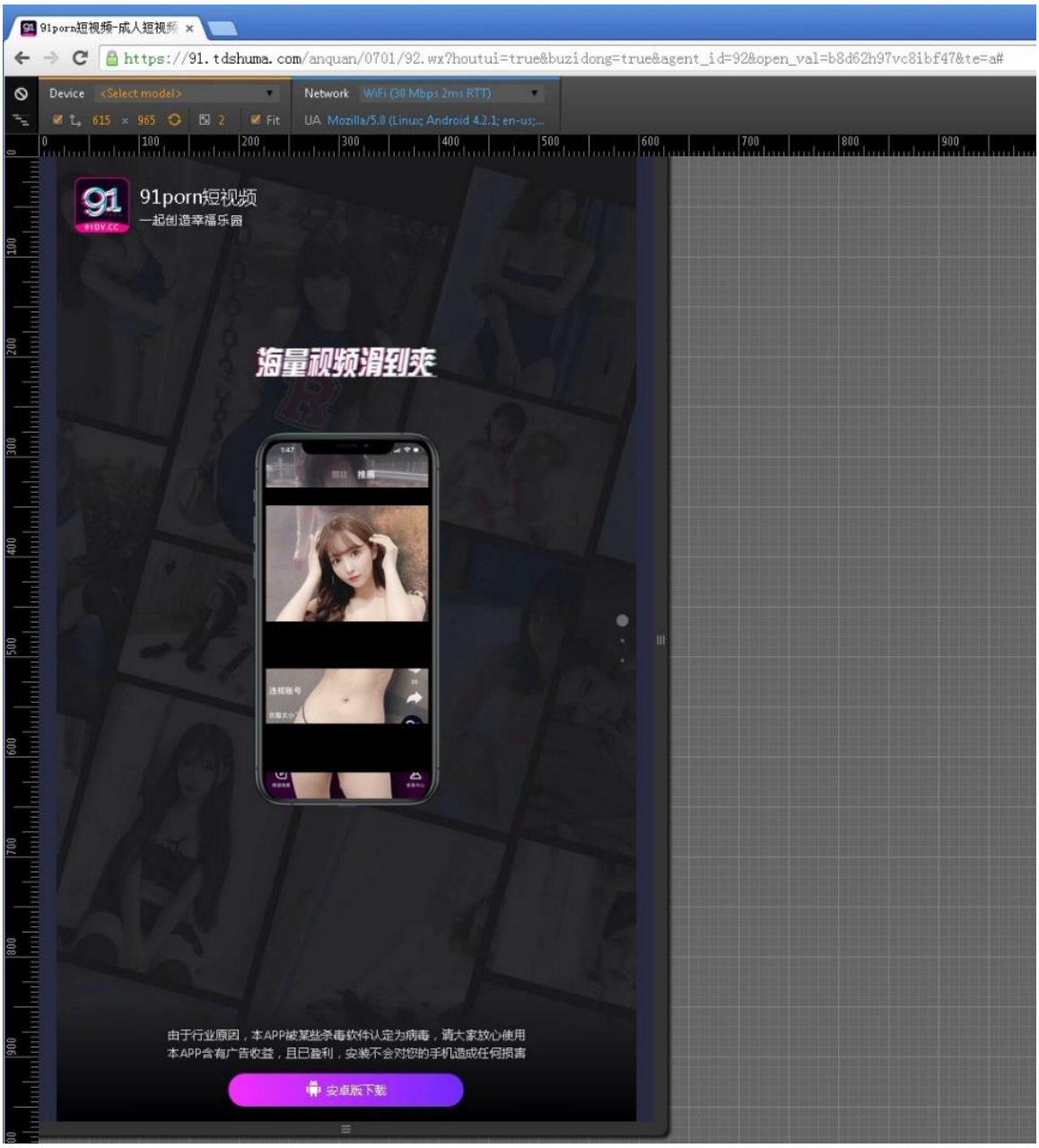
近期，火绒接到用户反馈，称在登录中国联通官网办理业务时被火绒报毒。

火绒工程师查看后，发现中国联通官网携带木马脚本Trojan/JS.Redirector

当用户访问其中某“业务办理记录”页面时，即会激活木马脚本，导致用户被强行跳转到其他推广页面上，推广内容涉及色情、游戏等。



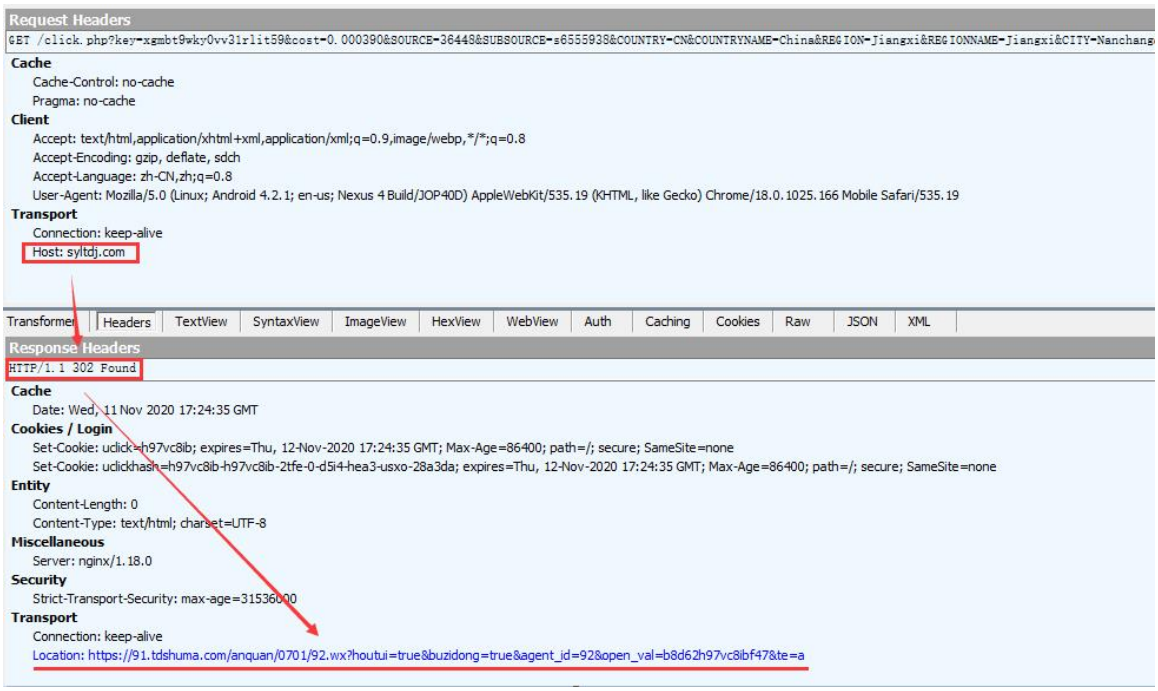
不仅如此，该木马脚本还被设定为一天只跳转一次，降低用户警惕性，以便长期存留于该页面。



不过火绒用户无需担心，火绒安全软件可拦截该木马脚本和网页。

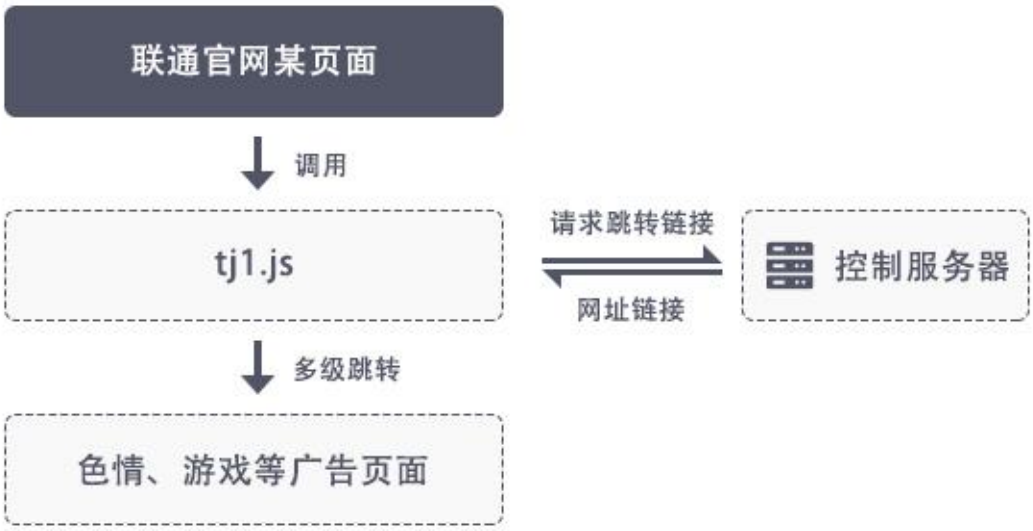
最后，为避免更多用户受该木马脚本影响，我们建议中国联通官方尽快排查上述问题。

通过此次事件反映出内容审查和安全检测对官方平台的重要性，我们也希望能通过此次报告，引起相关平台开发人员、管理人员的重视，及时加强安全审查力度，保障广大用户安全。

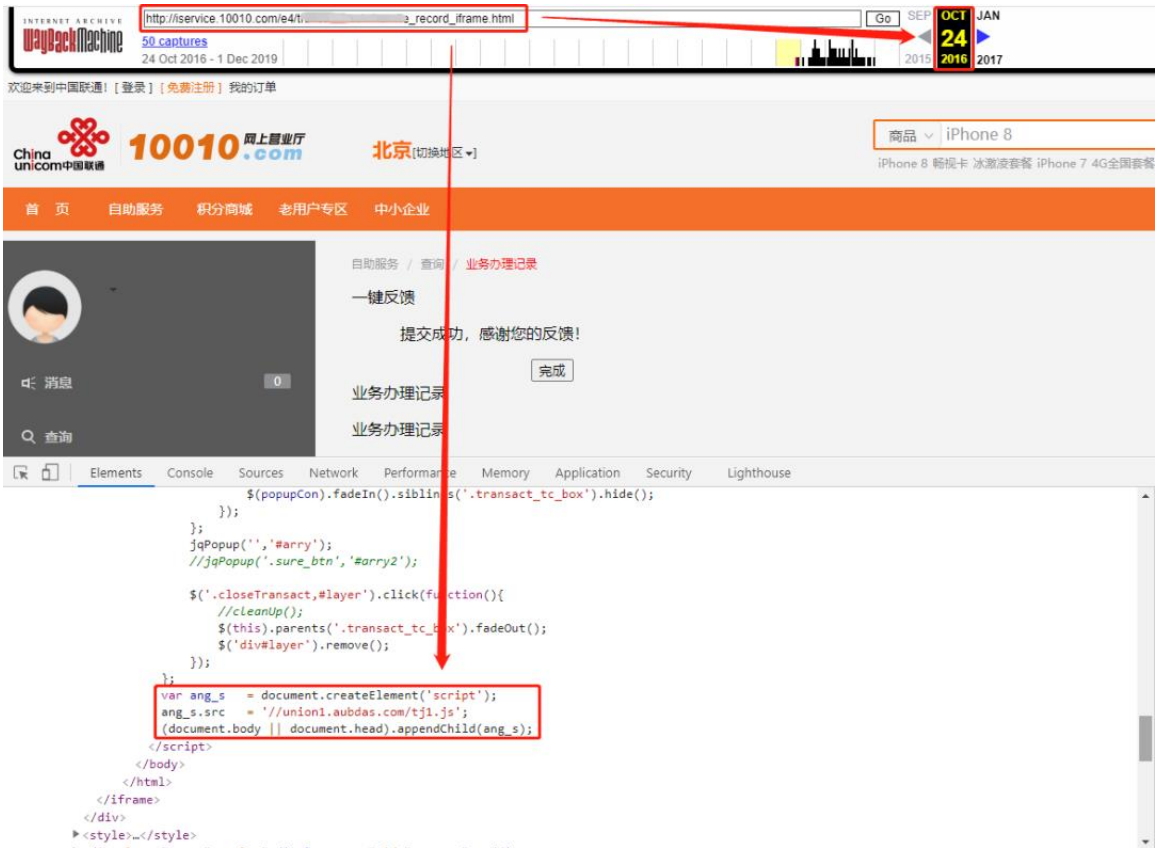


现阶段我们发现，在被植入相同代码的情况下，只有手机端浏览器可以复现跳转过程，控制服务器可能针对浏览器UA进行了判断。

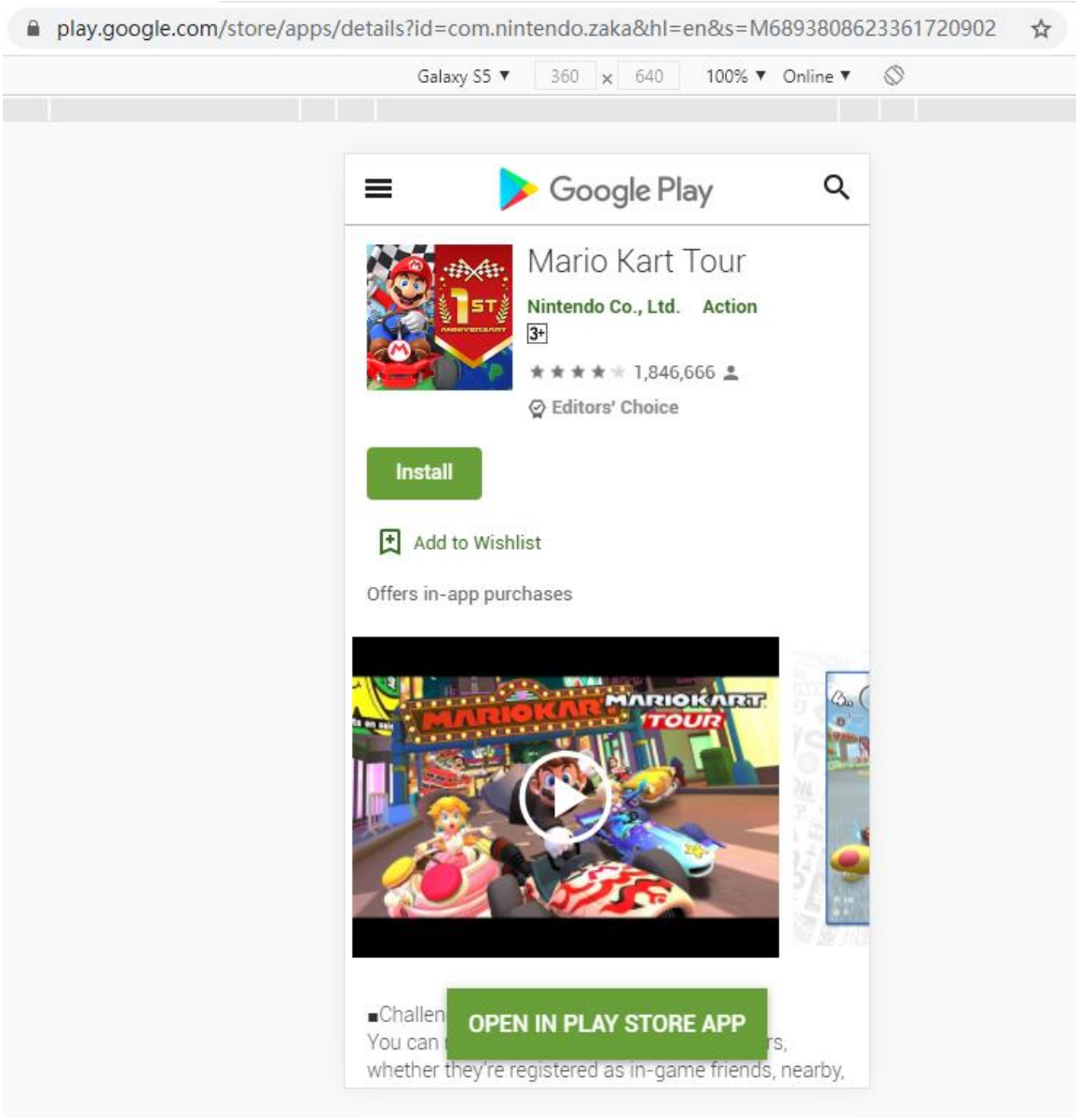
但是不排除PC端浏览器也会出现相同跳转行为的可能性。跳转流程如下图所示：



另外，经过火绒工程师进一步溯源发现，上述木马脚本早在2016年10月份就已经在联通官网页面中出现过。



除前文中提到的色情广告外，现阶段监测到的部分其他被推广链接，如下图所示：



如果大家将来在打开某些官方网站时发现被跳转到奇奇怪怪的页面，也请务必提高警惕。

原文地址：

https://www.huorong.cn/info/1605176406524.html

歌事故里

陈奕迅《我什么都没有》

由网友“Ther”点歌

视频来源：腾讯视频

可能喜欢

X浏览器拦截优酷广告被索赔100万

刚淘到的国外神器，仅302KB！

想要一些设计类神仙网站？满足你！

360 的这款“三无产品”，真的良心！

国外无损万能录制神器，全兼容！

IE浏览器终于"挂了"，撰文纪念！

戳戳留言区上方卡片