UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Mr. Kaiser Kuo
Director of International Communications, Baidu
Email: kaiser.kuo@baidu.com

February 16, 2016

Dear Mr. Kuo,

Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, is currently researching the security and privacy features of Baidu Browser (Android and Windows versions). As you know, on November 26, 2015, we notified Baidu of the security vulnerabilities we discovered in the browser. We followed up by email regarding Baidu's progress toward completion of fixes on January 5, 2016, and spoke via Skype with a Baidu security engineer on January 14, 2015, to discuss the scope of the vulnerabilities and a timeline for rectification. We write now concerning the status of the fixes, as well as broader issues of user privacy and access to information implicated in the browser's design.

We would appreciate your timely response to the following questions:

1. Baidu Browser (Android version 6.2.18.0 and Windows version 7.6.100.2089) collects detailed and extensive user data, as documented in our correspondence. For example, the Windows version of Baidu Browser collects and transmits -- unencrypted -- the URL and title of all websites visited by a user, as well as the user's hard drive serial number and MAC address. Why is this sensitive user data collected in the first instance? Why is it transmitted insecurely?

2. Which laws, regulations, or policies (internal or external) govern Baidu's collection of user data? What user data is Baidu required to collect pursuant to such law, regulation, or policy?

3. Does Baidu intend to alter its collection through its browser of certain types and amounts of user data? If so, what changes will be made, and when?

4. For how long does Baidu retain the user data that it collects through its browser? How is that data stored, and what security measures are in place to protect that data at rest? Does Baidu share that data with third parties? and if so, with whom?

5. What if any laws, regulations, or policies (internal or external) guide Baidu's approach to the use of encryption in transmitting or storing user data?

6. Why was Baidu Browser designed to transmit certain sensitive user data, such as GPS coordinates and browser search queries, in an unencrypted format?

7. Why was Baidu Browser designed to use symmetric encryption and hard-coded keys, rather than asymmetric encryption?

8. What entities -- within or outside Baidu -- were involved in creation of the analytics software development kit (SDK) used in Baidu Android apps? Does Baidu subject its SDKs to any form of security audit or testing? Please describe that process.

9. Why does the Windows version of Baidu Browser contain a feature to automatically proxy requests to certain websites hosted outside of China? Is this feature related to the partnership between Baidu and CloudFlare announced in September 2015?

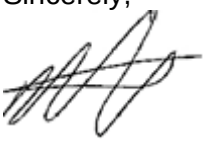
10. Did Baidu seek the approval of the Chinese government in order to enable the aforementioned proxy request feature of the browser? Is Baidu required by authorities to collect any user data as a condition to providing uncensored web access through its proxy feature? What data related to the proxy feature is Baidu required to share with the Chinese government?

11. Why do the Baidu proxy servers allow access to domains that are additional to those for which the browser uses the proxy? Does this disparity serve a particular technical or other function?

12. Please provide a current timetable reflecting actual or estimated dates of completion of fixes for each of the vulnerabilities we reported to you. Additionally, how does Baidu intend to address the use by third-party apps of vulnerable versions of its SDK?

We plan to publish a report reflecting our research on February 22, 2016. We would appreciate a response to this letter from your company as soon as possible, which we commit to publish in full alongside our research report. Thank you.

Sincerely,



Professor Ronald J. Deibert
Director of the Citizen Lab
Munk School of Global Affairs
University of Toronto