# Researchers identify major security and privacy issues in popular china browser application, QQ

March 29 2016, by Dena Allen

A new study from the University of Toronto's Citizen Lab identifies security and privacy issues in QQ Browser, a mobile browser produced by China-based Internet giant Tencent, which may put many millions of users of the application at risk of serious compromise.

Citizen Lab researchers identified problems in both the Android and Windows versions of the application. The Android version of the browser transmits personally identifiable data, including a user's search terms, the URLs of visited websites, nearby WiFi access points, and the user's IMSI and IMEI identifiers, without encryption or with easily decrypted encryption. Similarly, the Windows version sends personally identifiable data, including the URL of all pages visited in the browser, a user's hard drive serial number, MAC address, Windows hostname, and Windows user security identifier, also without encryption or with easily decrypted decryption.

The transmission of personally identifiable user data without properly implemented encryption leaves this data vulnerable to surveillance by a number of intermediaries, including a user's ISP, wireless network operator, mobile carrier, a malicious actor with network visibility, and/or a government agency with access to any of those intermediaries.

"QQ Browser phones home information on your device's hardware serial numbers and tracks your location and every page you visit. Even the

person you trust most does not have access to this amount of information on you and yet QQ receives it from everyone who uses their browser," said Jeffrey Knockel, Senior Researcher at the Citizen Lab at the University of Toronto's Munk School of Global Affairs

In addition, both the Windows and Android versions of the application did not adequately protect the software update process, which leaves the application vulnerable to the execution of arbitrary code. This means that a user could be deceived by a malicious actor into installing malware without their knowledge during the QQ Browser update process.

Citizen Lab researchers disclosed these vulnerabilities to Tencent on February 5, 2016. Tencent security engineers acknowledged these security concerns and released updated versions of both the Windows and Android versions of the application in March 2016. Analysis by Citizen Lab researchers showed that some of the problems identified were resolved, while others remain.

The Citizen Lab's Director, Ron Deibert, also sent questions to Tencent seeking comment on the reasons for the vulnerabilities and data collection issues, specifically requesting comment on whether the company is following state directives. China maintains one of the world's most extensive censorship and surveillance regimes and all companies are required by law to follow state regulations. China's anti-terrorism law, which came into effect on January 1, 2016, includes requirements for telecommunications operators and Internet service providers to "provide technical interfaces, decryption, and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law". As of the date of publication, however, Tencent has not replied to the Citizen Lab letter.

"Most users would likely be surprised to discover the extent of

personally identifiable data that the application is collecting, and would likely be troubled to find it is being transmitted in an insecure manner. If developers are going to be collecting this data, it is imperative that they use widely-accepted methods of transmitting the data in a more secure way," said Adam Senft, Researcher at the Citizen Lab at the University of Toronto's Munk School of Global Affairs.

This is the third web browser produced by a China-based company that Citizen Lab researchers have identified security issues with. In May 2015, Citizen Lab research identified similar security concerns with UC Browser, a popular mobile web browser owned by China-based e-commerce giant Alibaba. In February 2016, Citizen Lab published a report describing similar security concerns with Baidu Browser, a web browser produced by China-based Baidu.

"The collection of such sensitive information about a user, and its insecure transmission across networks, is disturbing regardless of where it takes place. But the fact that this is being undertaken in a context like China—where there is extensive surveillance, companies are required by law to share user data with authorities on demand, and dissidents are routinely incarcerated for opposition to the government—is a serious matter of personal security and human rights," said Ron Deibert, Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs.

Provided by University of Toronto