China propaganda app fraught with security concerns: report

17 October 2019, by Eva Xiao

Some experts say the 'Xuexi Qiangguo' app, meaning 'Study to make China strong', could actually be monitoring users

A widely downloaded Chinese propaganda app that quizzes users on Communist Party heroes and military achievements may be "studying them right back" through data collection and potential security breaches, an internet freedom campaign group says.

The app—called "Xuexi Qiangguo" or "Study to make China strong"—has accumulated 130 million users since its launch by the Communist Party's propaganda arm in January, according to state media in August.

Marketed as an education tool, it awards points for sharing articles and watching videos such as speeches by Chinese President Xi Jinping.

But the Open Technology Fund (OTF)—a US government-funded group that campaigns for internet freedom—says users also provide a plethora of data to the app, including location and emails.

OTF contracted the independent German tech firm Cure53 to study the app.

While the Communist Party advertises it as "a way for citizens to prove their loyalty and study their country, the app's maintainers are studying them right back", OTF wrote on its website.

The app's terms and conditions also say users may have to hand over more personal information—such as fingerprints and ID numbers—depending on the features or third-party tools they want to access.

The Chinese government has come under increasing scrutiny for high-tech surveillance—from facial recognition-enabled security cameras to apps used by police to extract personal information from smartphones at checkpoints.

And though "Study to make China strong" is an education app, Cure53 said it contains code that could run "arbitrary commands"—reminiscent of a backdoor—on certain phones.

The app "maintains a level of access that no app would normally have over a user's device", said OTF.

'Intrusive app'

The investigation, which was conducted in August, only looked at the Android version of the app, partly because of its market dominance, said Sarah Aoun, the group's director of technology.

OTF is considering tackling the iOS version—which runs on Apple iPhones—next, Aoun told AFP.

"This is just another way of expanding that digital control through a very intrusive app that is being pushed onto its citizens," said Aoun.

The Communist Party's propaganda arm, which is responsible for the app, did not respond to AFP's request for comment.

Dozens of provincial and county governments across the country reportedly held workshops to promote the app earlier this year.

Chinese journalists will also have to use the app for online press accreditation exams later this month and November, said a notice last week from the State Council, China's cabinet.

"It is unusual to see so much data gathered for an education app," said Jane Manchun Wong, who reverse-engineers apps for security vulnerabilities and unreleased features.

"It's like reading a book about the great nation but the book somehow searches your home," she told AFP.

The app also scans for 960 applications—including gaming, travel and chat apps—appearing as if "attempting to find which popular apps are installed on the phone", said Cure53's report.

'Creepy code'

A spokesperson at DingTalk, an enterprise chat platform that was used to build the app, told AFP that it had "no 'backdoor code' or scanning issues".

But OTF said users' data and their phones could be further jeopardised if the code that "amounts to a backdoor" runs successfully.

Currently, this code only affects phones where users have installed software that gives them "superuser" privileges—such as the ability to modify the device's code.

But apps can also abuse this level of privilege to take over a user's device.

"The code they found is creepy", Baptiste Robert, a French security researcher, told AFP—but cautioned against the use of the word backdoor.

The investigation also found "no evidence" that the code was used during testing, with Cure53 concluding that "further investigation" was needed to determine how it was used.

The code "can raise suspicion," Robert said, but to conclude that there is "vast espionage from China is complicated".

APA citation: China propaganda app fraught with security concerns: report (2019, October 17) retrieved 19 January 2022 from https://techxplore.com/news/2019-10-china-propaganda-app-fraught.html