UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 44 – July 2014

Asia Chats: Update on Line, KakaoTalk, and FireChat in China

Media coverage: CBC News, TechPresident, and Slate.

On July 10 we reported that messaging applications LINE and KakaoTalk were being disrupted in China as a result of DNS tampering and HTTP request filtering. We also found that Flickr and Microsoft OneDrive were blocked in the country.

Since that time we have done daily tests of these domains from servers in China. We find that Flickr and OneDrive remain consistently blocked, but LINE and KakaoTalk show inconsistent fluctuation between accessibility and inaccessibility.

We also analyze security and privacy issues in the mobile app FireChat and test accessibility of the service in China.

ACCESSIBILITY OF KAKAOTALK, LINE, FLICKR, ONEDRIVE IN CHINA

In our previous post, we established that injected DNS replies was the primary mechanism by which KakaoTalk and LINE was being blocked in China. We test the domains that we investigated in our previous post twice daily from July 12 – 23, 2014 to measure the consistency of the blocks. We resolved the DNS records of the following domains in China:

Domain Tested	Service
flickr.com	Photo sharing service
kakao.com	KakaoTalk – Cross platform messaging app
line.naver.jp	LINE – Cross platform messaging app
onedrive.live.com	Cloud file sharing service

Our tests return known fake DNS replies that have been previously observed in China, as noted in a presentation from John-Paul Verkamp at the CAIDA Active Internet Measurements Workshop (see slide 6).

These possible fake response addresses are summarized below:

IP	Network
8.7.198.45	LEVEL3 – Level 3 Communications, Inc.,US
78.16.49.15	AS-BTIRE BT Communications Ireland Limited,IE
37.61.54.158	BAKINTER-AS Baktelekom,AZ
93.46.8.89	FASTWEB Fastweb SpA,IT
46.82.174.68	DTAG Deutsche Telekom AG,DE
159.106.121.75	
59.24.3.173	KIXS-AS-KR Korea Telecom,KR
203.98.7.65	CLIX-NZ TelstraClear Ltd,NZ
243.185.187.39	
127.0.0.1	Localhost

We tested the domains to see whether or not they would return these known bad DNS responses. We found that onedrive.live.com and flickr.com consistently returned false DNS replies, while kakao.com and line.naver.jp had sporadic fluctuations in the DNS reply given, occasionally giving a legitimate response.

Figure 1 summarizes our results; a red block is a known false DNS reply and a green block is a correct DNS reply.

Figure 1: Accessibility of domains from July 12 to 23 2014. Click to enlarge

We do not have an explanation for the inconsistent results we observe with Kakao and LINE. However, our findings are correlated with recent reports from Korean media that cite a diplomat in the South Korean Embassy in Beijing who explained "The Chinese side tells us that the blockages will not last for a long time, and I expect services to return to normal by the end of this month". The unnamed diplomat also noted that the Chinese government gave a "brief" reason for the blocking, but he could not share the information.

SECURITY AND PRIVACY ISSUES IN FIRECHAT

We also analyzed the mobile messaging application FireChat, which is advertised as enabling "off-the-grid" chatting, to users nearby, even without a mobile or wireless Internet connection. Using Bluetooth and Apple's Multi peer Connectivity it claims to be able to connect users off-the-grid who are up to 200 feet away.

This app recently saw a spike in download rates in Iraq, Taiwan, and elsewhere. Open Garden, the developer of FireChat appears particularly interested in growing Chinese speaking user bases, as evidenced by a recent update to their website that promotes the app in Chinese and provides link to Chinese app stores. The Tencent App store currently reports 3.8 million downloads of the application.

Figure 2: Screen shot of Open Garden website advertising FireChat in Chinese

FireChat has three chat modes: "everyone", a semi-global chat room where up to 80 individuals are sorted broadly based on their geographic location; "nearby", mode that pairs users who are in close geographic proximity to each other using Wi-Fi, Bluetooth, or Apple's Multipeer Connectivity functions; and "firechat", Internet based chat rooms organized around a single theme word.

Through these features FireChat enables open broadcast communication channels. Given the nature of this functionality one would not necessarily expect robust security features. Indeed, our analysis shows that the application does not encrypt any communications, or user data stored on the device. Messages sent in any of the application's three messaging modes are sent in the clear without encryption. All messages sent and

received, as well as a list of chat channels the user has joined, are stored unencrypted on the device. It is also possible for anyone (regardless of whether they have installed the app or not) to visit an IP address associated with the service in a web browser to see the most recent messages sent by users of the application. Finally the application does not perform any user authentication, so a user cannot be certain who is using a given username at any given time.

Full technical details on our analysis are available in a post here.

In media reports FireChat's developers have acknowledged the potential security risks of using the application for sensitive communications:

"People need to understand that this is not a tool to communicate anything that would put them in a harmful situation if it were to be discovered by somebody who's hostile," he said. "It was not meant for secure or private communications."

While the developers have been clear on this point in some media reports, the App store descriptions and developer's website do not include similar warnings as of July 23.

FireChat does not advertise itself as a secure communications tool, but that has not stopped it from being picked up by users in at risk environments such as Iraq. Given that security and privacy are not goals of the open broadcast channel implemented by FireChat, users should carefully assess if using FireChat is safe for their specific context and avoid sharing sensitive information through the service.

ACCESSIBILITY OF FIRECHAT IN CHINA

We ran tests to determine the accessibility of the FireChat service in China. We tested the website of the developers (opengarden.com) as well as the site of the FireChat program (opengarden.com/firechat) and were able to retrieve the content in full from a network vantage point in Hangzhou, China. The application is also available in a variety of Chinese app stores such as the one operated by Tencent.

We also tested the connection that the FireChat program uses in the "Everyone" mode of chatting. We tried to initiate a connection to FireChat's server IP address 209.237.236.194 on port 4175 from a server in Hangzhou and Beijing. When we attempt this connection, we consistently receive spoofed RST segments, which is indicative of blocked content in China.

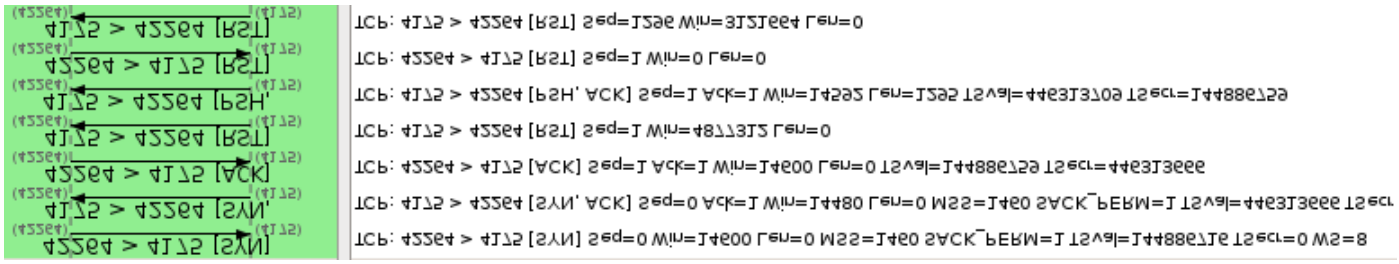

Figure 3: TCP flow diagram of the connection to FireChat server showing an RST response

These results mean that while the website of the application developers is accessible, the chatroom functions of the app are blocked in our tests. However, blocking the connection to the FireChat server does not affect chat modes that rely on Bluetooth and Apple's Multipeer Connectivity.

CONCLUSION

We will continue to monitor accessibility of LINE, KakaoTalk and other chat applications in China and post updates as they are available.

DATA

Updated DNS and HTTP request data for Line, KakaoTalk, Flickr, and OneDrive domains on Github

ACKNOWLEDGEMENTS

Jakub Dalek, Philipp Winter, Andrei Dranka, Masashi Crete-Nishihata, and Adam Senft undertook the research and writing of this post. This research is supported by the John D. and Catherine T. MacArthur Foundation.