UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 16 – April 2013

Permission to Spy:

An Analysis of Android Malware Targeting Tibetans

KEY FINDINGS

- A compromised version of Kakao Talk, an Android-based mobile messaging client, was sent in a highly-targeted email to a prominent individual in the Tibetan community.
- This email message repurposed a legitimate private email message sent by an information security expert in the Tibetan community to a member of the Tibetan parliament-in-exile.
- This malware is designed to send a user's contacts, SMS message history, and cellular network location to attackers.
- The cellular network information gathered by this malware would only be useful to actors with detailed knowledge of the cellular communication provider's technical infrastructure.
- The compromised application was not detected as malware by any of the three mobile malware scanning applications we tested.

BACKGROUND

This blog post is part of a series documenting the use of information operations against Tibetans and others who advocate for Tibetan rights and freedoms. This research is part of the Citizen Lab's ongoing study of targeted cyber threats against human rights organizations. Prior research by the Citizen Lab has documented targeted malware sent to a Tibetan organization by the APT1 group, malware that repurposes privately-held content of Tibetan groups, and malware that leverages the issues of self-immolations amongst Tibetans and a European Parliament resolution on the human rights situation in Tibet.

The incident described in this post stands out from our past reports given its use of malware designed for the Android platform. The attack repurposed a genuine private email message containing a legitimate Android Application Package File (APK) that was sent from an information security expert in the Tibetan community to a member of the Tibetan parliament-in-exile. It is likely that the attacker obtained the original message and attachment through a compromised email account of the parliament member. The attacker then sent the same message to another prominent member of the Tibetan community, but this time with a compromised version of the same Android APK containing malicious code.

Malware targeting the Tibetan community has utilized a variety of platforms over time. The majority of targeted malware campaigns against the Tibetan community focus on Windows platforms. However, we have also seen attacks targeting Macs and the emergence of mobile malware. Additionally, during investigations of command and control (C2) servers associated with the Luckycat campaign [PDF], Trend Micro [PDF] found two malicious Android APKs in early stages of development that could collect device information and download and upload files by remote command. Based on the available information, it was not clear to Trend Micro how the attackers intended to deliver the mobile malware to targets.

On March 26, 2013, researchers at Kaspersky reported on a compromise of an email account of a high-profile Tibetan activist, which was used by attackers to send targeted malware to the activist's contact list. The targeted attacks leveraged email content about the World Uyghur Congress and included a malicious APK file purporting to be an app with information on the event. That malware allowed attackers to collect data from infected devices including contacts, call logs, SMS messages, geo-location, and phone data (phone number, OS version, phone model, SDK version).

ATTACK OVERVIEW

In January 2013, a Tibetan source provided the Citizen Lab with a forged email containing a compromised software installation package, in the form of an Android APK, for a mobile application called Kakao Talk. Kakao Talk is an application developed by a South Korean company that "allows its users to send and receive messages including photos, videos and contact information, both on a one-to-one basis and in groups, all for free." Members of the Tibetan community have used Kakao Talk and other applications as alternatives to WeChat (a chat client rapidly rising in popularity) after concerns were raised regarding that application's general security and the potential for Tencent (the Chinese company that provides the application) to monitor users at the behest of the Chinese government.

On December 4, 2012, an information security expert who works within the Tibetan community sent a private email to a member of the Tibetan parliament-in-exile, based in Dharamsala, India. That email attached a genuine version of Kakao Talk and Tunein (an online radio application) as .apk files.

On January 16, 2013, an email purporting to be from this same information security expert was sent to a high profile political figure in the Tibetan community. The email contained the same text as the message from December 4, but attached a compromised version of the same Kakao Talk Android APK, as seen below in Figure 1.

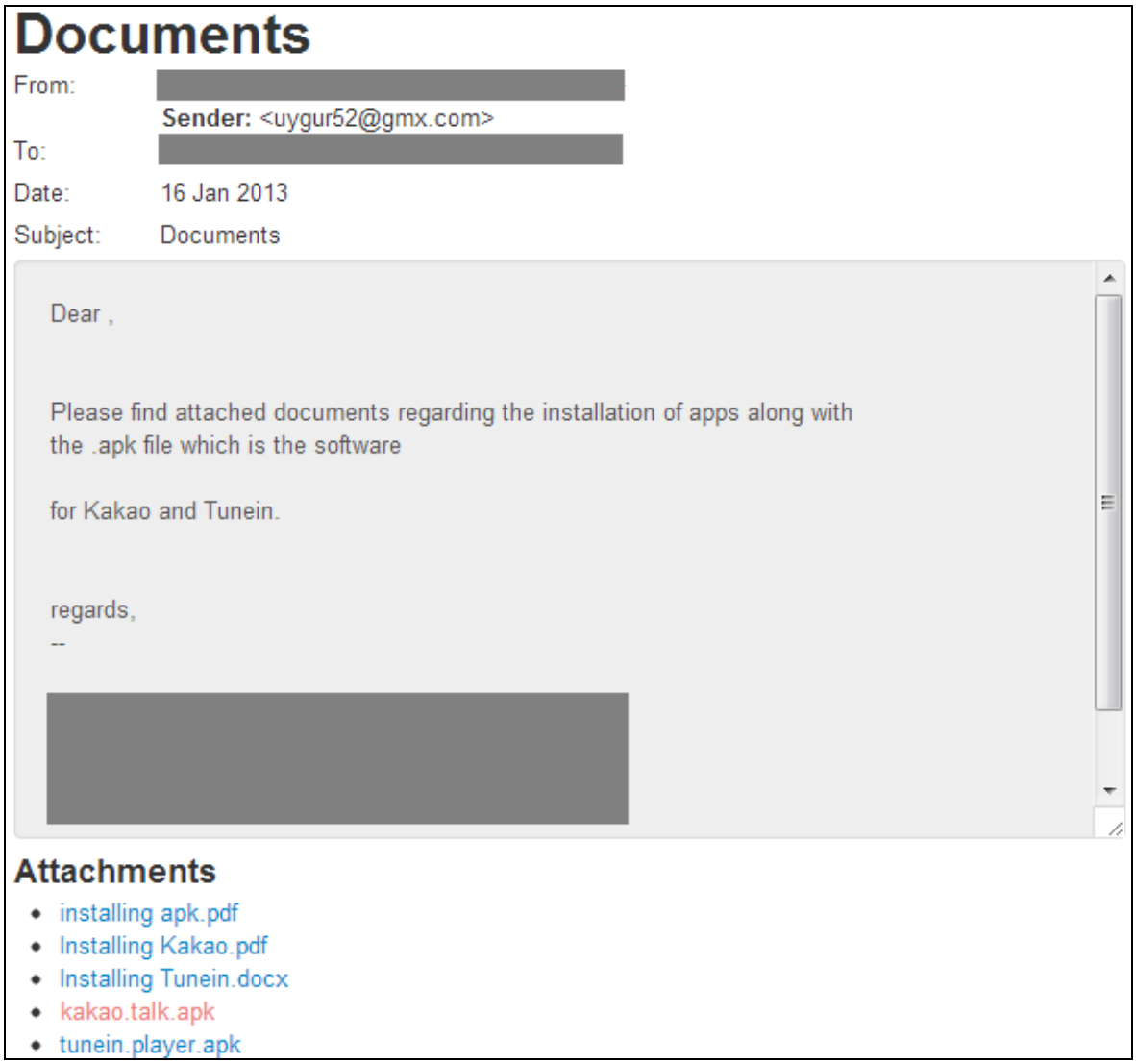

Figure 1: Forged email containing compromised version of Kakao Talk APK (highlighted in red). The email spoofed the real address of the security expert who originally sent the legitimate message. The actual sender email address used by the attackers was *uygur52@gmx.com*.

TECHNICAL ANALYSIS

Our analysis reveals that the legitimate Kakao Talk application was modified to include additional permission requests while preserving the core chat functionality and user interface of the application. (Hereafter this added functionality will be referred to as the "malware.") In order for the malware to be installed, the user must permit applications to be installed from sources other than the Google Play store. This permission is not enabled by default in Android. However, as many members of the Tibetan community (particularly those inside Tibetan areas) have access to the Google Play service restricted, they are required to permit applications to be installed from outside sources, and circulating APKs outside of Google Play is common. In addition to permitting the "allow from unknown sources" option, the user must also must permit the additional permissions requested by the application. Users may be duped into accepting these permissions by assuming

they are required for the regular functionality of the application or by not reviewing them carefully and approving. Once these permissions are approved, they are used to authorize the additional data-gathering capabilities of the malware, which is configured to autostart on device boot.

The Kakao Talk application and malware were repackaged into the modified APK and signed with an illegitimate certificate. Both the original and illegitimate certificates are reproduced below. Notice that fields in the illegitimate certificate have been populated with what appears to be an assortment of nonsensical characters from a QWERTY keyboard:

Original legitimate certificate:

Owner: OU=kakaoteam, O=kakao, C=ko
Issuer: OU=kakaoteam, O=kakao, C=ko
Serial number: 4c707197
Valid from: Sat Aug 21 20:38:47 EDT 2010 until: Mon Jul 28 20:38:47 EDT 2110
Certificate fingerprints:
MD5: 70:D4:94:75:18:38:25:BE:88:A1:BA:9A:50:30:DA:E3
SHA1: EC:C4:5B:90:2A:C1:E8:3C:8B:E1:75:8A:25:7E:67:49:2D:E3:74:56
Signature algorithm name: SHA1withRSA
Version: 3

Illegitimate certificate:

Owner: CN=qwe, OU=asd, O=zxc, L=rty, ST=fgh, C=vbn
Issuer: CN=qwe, OU=asd, O=zxc, L=rty, ST=fgh, C=vbn
Serial number: a3e5475
Valid from: Tue Jan 08 22:45:49 EST 2013 until: Wed Oct 12 23:45:49 EDT 2067
Certificate fingerprints:
MD5: BC:04:8C:12:93:39:BE:B7:72:B3:62:E0:9C:B3:03:0B
SHA1: A6:41:78:7B:93:FC:00:77:ED:61:AC:B9:10:9B:07:48:46:9A:76:EB
Signature algorithm name: SHA1withDSA
Version: 3

The following permissions are added by the malware and do not exist in the legitimate version:

android.permission.GET_ACCOUNTS
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_SMS
android.permission.INTERNET
android.permission.ACCESS_FINE_LOCATION
android.permission.WRITE_SETTINGS
android.permission.WRITE_SECURE_SETTINGS
android.permission.WRITE_APN_SETTINGS
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.PROCESS_OUTGOING_CALLS
android.permission.DEVICE_POWER
adnroid.permission.ACCESS_CHECKIN_PROPERTTES
android.permission.INTERNET
adnroid.permission.CHANGE_WIFI_STATE
android.permission.MODIFY_PHONE_STAT
android.permission.BLUETOOTH_ADMIN
android.permission.BLUETOOTH
android.permission.BIND_DEVICE_ADMIN
android.permission.USES_POLICY_FORCE_LOCK
android.permission.CHANGE_CONFIGURATION

Figure 2 below shows the difference in permissions between the legitimate and modified Kakao Talk software package. Users can display the permissions granted to an application by selecting ‘Apps’ from the settings menu. The sections highlighted in red show differences between the legitimate and illegitimate version of the application:

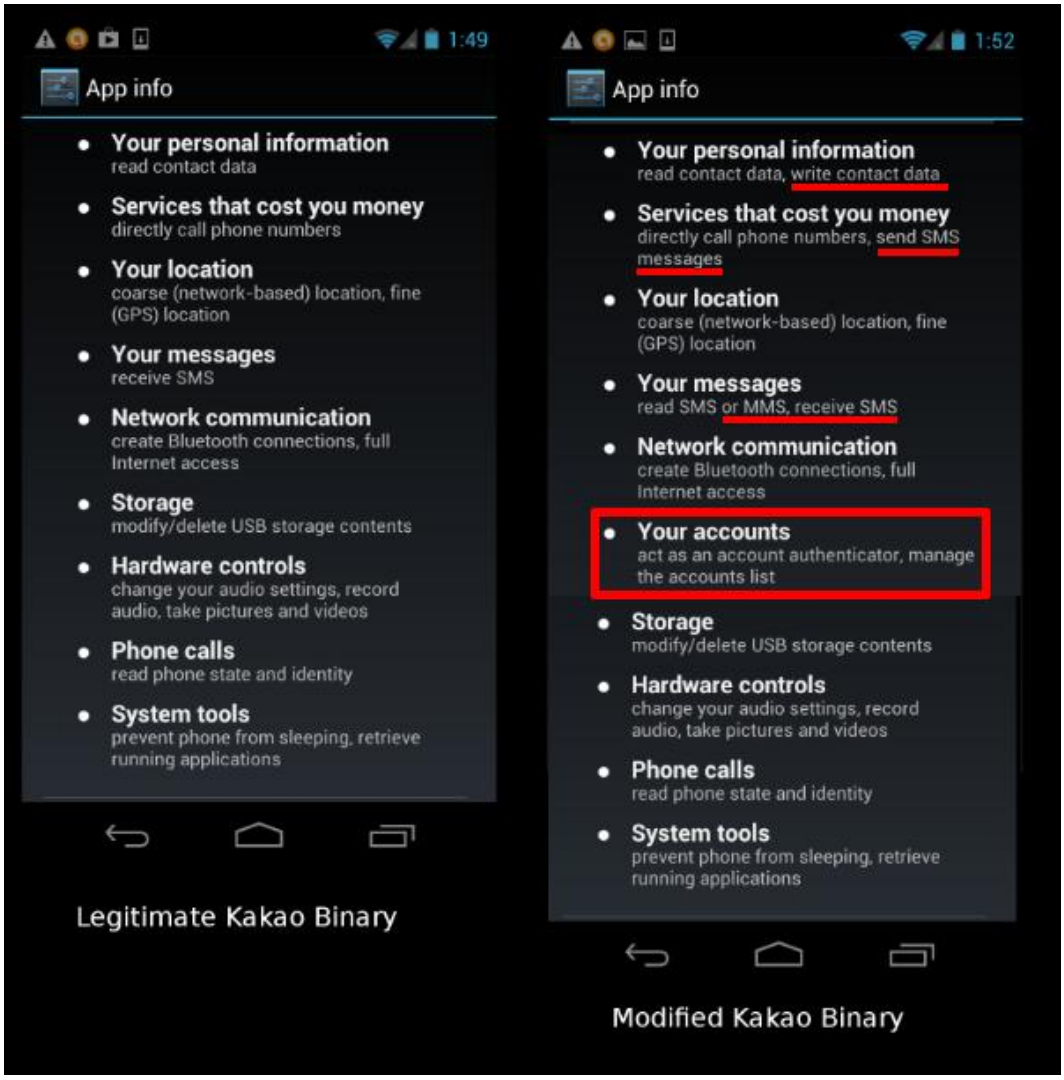

Figure 2: Comparison of permissions between legitimate and illegitimate versions of Kakao Talk.

Using these permissions, the malware performs the following actions of significant concern:

1. On a periodic basis the user's contacts, call history, SMS messages and cellular network configuration are written to an encrypted file called info.txt.

2. Periodically contacts a command and control server (C2) "android.uyghur.dnsd.me" to retrieve updated configuration information such as URLs and login credentials. This configuration information directs the malware where to upload the info.txt file. The site hosting the C2 appears to emulate the appearance of the Baidu website (a Chinese search engine), but includes encrypted configuration data hidden in the comments. By masking the C2 as a seemingly innocuous website, requests would appear to be legitimate on casual inspection. The configuration data contained in the comments direct the malware to upload captured data from the device to an FTP server and contain a pointer to a new C2 that would allow the attackers to change the C2 should that need arise.

3. Intercepts SMS messages and searches for a special code sent by a malicious actor, which if detected responds to the sender with the base station ID, tower ID, mobile network code and mobile area code of the phone in question. This message is not displayed to the user and they are never made aware of it.

The fact that the malware silently responds to the SMS with such detailed technical information on the cellular phone network and topology is both troubling and curious.

An unsophisticated actor would have little or no use for this information if they were simply interested in exfiltrating data from the user for purposes such as fraud, spam or identity theft. Nor can this information be easily used to place a person's physical location — the malware is not responding with a convenient longitude and latitude. Detailed knowledge of the cellular network topology and configuration would be required to determine a user's location, something unlikely to be in such an actor's possession.

This information is only useful to actors with access to the cellular communications provider and its technical infrastructure, such as large businesses and government. It almost certainly represents the information that a cellular service provider requires to initiate eavesdropping, often referred to as "trap & trace." Actors at this level would also have access to the data required to perform radio frequency triangulation based on the signal data from multiple towers, placing the user within a small geographical area.

However, it is also possible that this data is being gathered opportunistically by an actor without access to such cellular network information. We can only speculate on what may be done with the data that is collected.

Of the additional permissions requested by the malware, some do not appear to be used, including GPS location, Bluetooth radio access, and phone sleep state. While these features are not currently being utilized, exploiting them could have serious consequences. For instance, Bluetooth functionality could potentially be used to enumerate devices (and through this other individuals) in close proximity to the compromised phone. The fact that these features are not currently utilized may indicate that the malware is still undergoing development.

Further evidence suggests that the malware may be in the process of development. Two of the additional permissions requested by the malware are misspelled, rendering these permissions unusable:

adnroid.permission.ACCESS_CHECKIN_PROPERTTES
adnroid.permission.CHANGE_WIFI_STATE

We ran three popular mobile antivirus scanners (provided by Avast, Lookout, and Kaspersky) on an Android handset with the compromised application installed. As seen in Figure 3, none of the three scanners detected the applications as malicious on two separate days of testing: February 6, 2013 and March 27, 2013. Therefore, at this time manual inspection of the applications permissions is required to detect the compromised application.

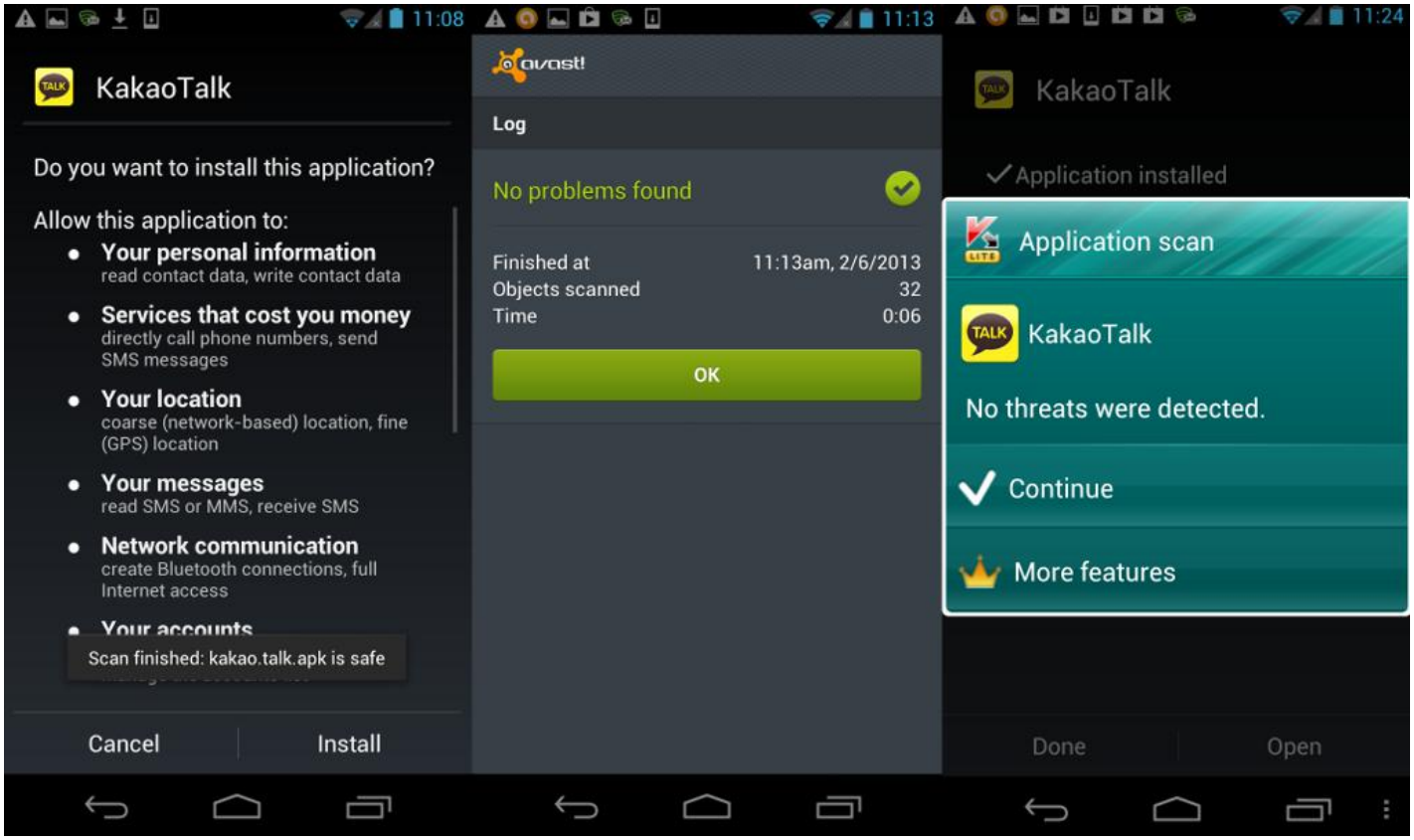

Figure 3: Screen captures of three mobile malware scanning applications (from left to right, Avast, Lookout and Kaspersky) failing to detect the compromised version of Kakao Talk.

The identifiers for the sample are listed below and further information is available on VirusTotal.

MD5	cbc474e34f26b4afd02932d8cae9e401
SHA-1	495b622d8209820022fe743c340b39e6e9313cd9
SHA-256	9390a145806157cadc54ecd69d4ededc31534a19a1cebbb1824a9eb4febdc56d

CONTEXTUAL ANALYSIS

While groups advocating for Tibetan rights have been the targets of persistent malware campaigns for many years, this attack stands out for a number of reasons. First, it targets a prominent member of the Tibetan community and leverages legitimate emails that attempt to encourage the use of alternatives to applications with security issues like WeChat when communicating with individuals in the Tibetan community. WeChat has been rapidly gaining popularity amongst Tibetans, including those in exile communities and individuals communicating sensitive information inside Tibetan areas.

In addition, the discovery of this malware comes at a particularly sensitive time for Tibetans and those working on issues related to Tibetan human rights. The wave of self-immolations amongst Tibetans has led to an increasingly severe response from Chinese authorities. The practice of self-immolation among Tibetans has intensified significantly since Citizen Lab first examined information controls in Tibet in the wake of self-immolations over a year ago. As of April 1, 2013, 112 Tibetans have self-immolated. The Chinese government's response to such practice has become increasingly hardline, with officials explicitly characterizing measures employed to maintain stability in Tibetan regions as a "crackdown" in March 2013. This hardening policy is perhaps an indication of the government's view of the severity of the threat to its control presented by events in Tibet.

The government and official media have characterized the underlying causes of self-immolation differently over time, gradually moving to the position that the practice is the result of the influence of "foreign hostile forces," coordinated and encouraged by overseas Tibetan organizations as well as the Dalai Lama. The crackdown in Tibet against self-immolators and those who are alleged to incite them has already resulted in severe criminal sentences for some individuals, based in part on "evidence" of their digital contact with overseas groups.

With official reliance on "evidence" of overseas contact as a basis for conviction and crackdown, it appears that Chinese authorities are specifically targeting mobile devices in China as a perceived means of communicating and organizing self-immolations. In March 2013, reports emerged from Lhasa that Chinese authorities had introduced restrictions against the use of mobile phones and had conducted a security sweep of mobile devices in the city's monasteries in an attempt to limit the dissemination of images and text. Although we have no specific evidence linking these new restrictions to the targeted malware we found, the timing is certainly suggestive and warrants further exploration.

CONCLUSION AND RECOMMENDATIONS

This incident demonstrates the capacity of attackers to rapidly adapt their techniques in response to changes in the communication methods used by targeted communities. In this case, Tibetan community members began discussing alternative applications to WeChat following concerns raised about its security. In a tit-for-tat response, attackers quickly leveraged this change, duplicating a legitimate message and producing a malicious version of an application being circulated as a possible alternative.

The malicious APKs linked to the Luckycat campaign [PDF], the recent Android malware attacks reported by Kaspersky and the example presented here demonstrate that the Tibetan community is being actively targeted by mobile malware.

The attack we analyzed and the malware reported by Kaspersky are not technically related. The malware binaries and command and control infrastructure are different and there is no clear indication from technical comparison of the two samples that the attacks were conducted by the same attacker(s). However, both attacks leveraged compromised email accounts of high profile members of the Tibetan community and also included reference to the Uyghur community (in the email lure of the sample reported by Kaspersky, and in the actual sender email "uygur52@gmx.com" and C2 domain "android.uyghur.dnsd.me" used in the attack we

analyzed). Notably, authorities in China have also targeted use of the "'Internet, mobile phones and digital storage devices'" by Uyghurs in the government's campaign against the "three evils" of terrorism, separatism and extremism. These similarities are inconclusive, but suggest that mobile malware campaigns against these communities are likely to continue.

These examples demonstrate the risks communities face from targeted mobile malware. Attackers will continue to adopt new methods and widen targeting of platforms. For communities under persistent threat from targeted malware campaigns, user vigilance and education are essential for reducing risk.

The Citizen Lab recommends:

- That users exercise caution in opening unexpected or unsolicited attachments or opening unverified links. See Citizen Lab's Recommendations for defending against targeted cyber threats for additional information, and Tibet Action Institute's Detach from Attachments campaign.
- That users be aware of mobile malware and exercise caution when installing mobile applications. Users should pay close attention to the permissions requested by the malware, and should avoid installing applications that request permissions they do not need. The Guardian Project and other initiatives are developing secure mobile applications to help users protect their communications and personal data from intrusion and monitoring.
- That users consult the Tibet Action Institute's Mobile Security resources, which are aimed at Tibetan audiences.

ACKNOWLEDGEMENTS

This report is by the Citizen Lab Targeted Threats team. We are grateful to Dylan Neild for analysis and our Technical Advisory Group members, Morgan Marquis-Boire and Nart Villeneuve, for review and comments.