1. BACKGROUND

1.1 About TibCERT

The Tibetan Computer Emergency Readiness Team (TibCERT) is a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community, as well as to expand Tibetans' technical research capacity on threats in the diaspora and surveillance and censorship inside Tibet, ultimately ensuring greater online freedom and security for Tibetan society as a whole.

1.2 Purpose

The purpose of the TibCERT quarterly bulletin is to share updates about TibCERT, advisory on threats that were seen in the community and issues inside Tibet related to cybersecurity issues.

1.3 Summary

Tibet Action Institute has been doing numerous workshops and trainings in Tibetan diaspora communities. However, it was not enough to reach all the communities so TibCERT program was started with the Digital Security Team (located in Dharamsala) while also recruiting four additional staff as Digital Security Ambassadors ("DSA") for four major Tibetan settlements (Dharamsala, Dehradun, Mundgod and Bylakuppe).

Launched in November 2018, TibCERT was joined by 25 organizations/institutions (NGOs, Institutions, offices) as of March 2019. TibCERT provides services such as Timely Security Audits, creating and implementing Digital Security. TibCERT also has a support helpdesk where anyone can send an email to support@tibcert.org, state their issue and TibCERT will get back within 24 hours.

TibCERT has two sections: TibCERT Response and TibCERT Recon. TibCERT Response includes all the Digital Security Ambassadors along with the training and response work they do. TibCERT Recon is a research based collaboration between Tibetan communities and global researchers. TibCERT has begun working on a few of these research projects.

1.4 TibCERT Launch

TibCERT was launched on November 5th 2018 at Dharamshala, India with attendees from Bylakuppe, Mundgod and Dehradun Lhakar Tech Week, people from different NGOs, monasteries and offices from Dharamsala, school computer teachers. The first two days of the conference focused on TibCERT Response Network and the other two days for TibCERT Recon.

2. DIGITAL SECURITY UPDATES

2.1 Phishing Attacks and Email attachment

The diaspora Tibetan communities has witnessed many cyber security attacks over the past years. Initially, these cyber attacks had a pattern where they used decoy email attachments to send malicious software. Over time, they switched to malicious links to steal the user credentials or to infect the system.

Recently, these attackers have begun to use both malicious attachments and links to cyber espionage the Central Tibetan Administration (CTA) and other offices. Some examples of these cyber security attacks in Tibetan communities were:

- There was a malware campaign to deliver a malicious Microsoft PowerPoint document to users of a mailing list run by the CTA. Researchers dubbed it ExileRAT and discovered it was a 2017 malware which abuses a known vulnerability in Microsoft Office, CVE-2017-0199, an arbitrary code execution that resides in the "slide1.xml.rels" file.
- There was malicious links circulating through There was malicious links circulating through Whatsapp. The malware was targeting high profile Tibetans in few offices. A collaborative research on this is currently in process and

TibCERT will send out more details in the coming weeks. The same concept that attachments or links which could compromise your computer can also compromise your mobile phone if you click on links sent from unknown users or download attachments from unknown senders.

2.1.1 TibCERT solutions

Title	Instruction videos
Detach from attachments	https://www.youtube.com/watch?v=v4E1SRDmtZE https://www.youtube.com/watch?v=Op3rV7ReNIk
Don't be a Phish	https://www.youtube.com/watch?v=gNRzivSBonQ&t=16s
Don't wait Update:	https://www.youtube.com/watch?v=2PALi87h6yM&t=168s
Turn of 2-step verification	https://www.youtube.com/watch?v=4jak_bWV5BU
Strong password	https://www.youtube.com/watch?v=qAend7JaNFU

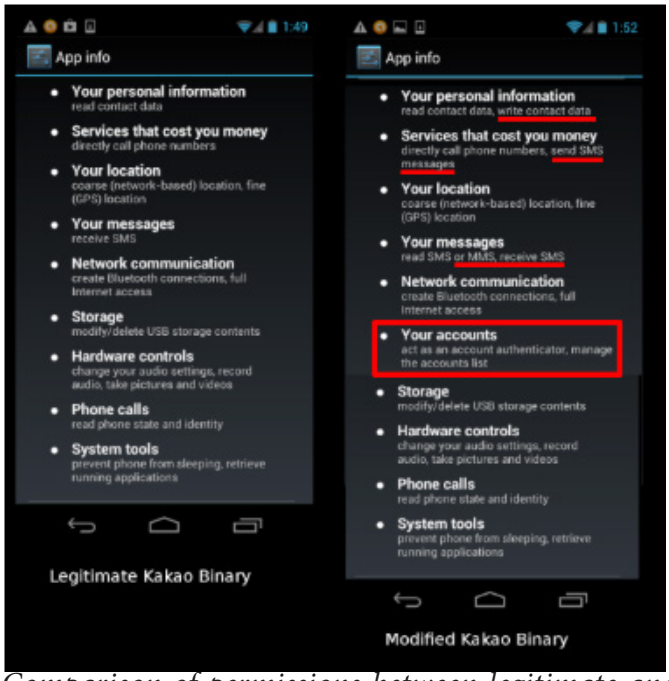
Cyber criminals spends a lot of time and resource in making malwares and infiltrating it in the community. However, it is easy to prevent and mitigate the threat if we followed some of the best practices listed above. For mobile, please follow the solutions in the infographic below

2.2 Mobile based attacks

In addition to email phishing attacks, the diaspora Tibetan community has also witnessed mobile based attacks. A 2013 report published by Citizen Lab shared these 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.

This report is also available in Tibetan here. Note that the compromised APK files (both Kakao Talk and Tunein) was modified to ask for additional permissions (as shown in the screenshot below).



Comparison of permissions between legitimate and illegitimate versions of Kakao Talk
Source: https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

Similarly, a year later, Citizen Lab researchers found that messaging applications such as LINE and KakaoTalk were being disrupted in China as a result of DNS tampering and HTTP request filtering.

Recently, there have also been additional reports in regards to Whatsapp and WeChat where clicking on a link shared in these platforms or answering a call (Whatsapp only) can compromise your system. We will be sharing additional details around this security vulnerability in the next bulletin.

3. TIBET - TECHNOLOGY INSIDE

3.1 Updates to Cyber Law China

The cyber security law is a broad cyber legislation passed by Chinese government in the 2016. The law aims to strengthen the security and privacy within the nation by having strict controls around online activities and provisions around storing data locally, having joint venture partners, and in some cases, registering cyber network assets. It also has mandatory requirements around breach notification, appointing a head of cybersecurity, incident response plans, and more.

In 2017, a new provision called Regulations on Internet Security Supervision and Inspection by Public Security Organs was added to the cyber security law and would come into effect on November 1, 2018. This gave Chinese authorities the right to analyze the source code of technologies used by foreign companies in China, all under the guise of identifying vulnerabilities during "national security reviews" to ensure national security. In addition, this new provision gave the Ministry of Public Security to conduct the following activities as well:

- Conduct in-person or remote inspections of the network security defenses taken by companies operating in China
- Check for "prohibited content" banned inside China's border
- Log security response plans during on-site inspections
- Copy any user information found on inspected systems during on-site or remote inspections
- Performing penetration tests to check for vulnerabilities
- Perform remote inspections without informing companies
- Share any collected data with other state agencies
- The right to have two members of the People's Armed Police (PAP) present during on-site inspection to enforce procedures

3.2 Huawei

Huawei is a telecom giant with the world's biggest manufacturer of telecommunications equipment and its second-biggest smartphone maker. It is outlawed in many countries and has also been a center of controversy for the past few months.

In January 2018, Huawei was accused of sending data from servers of African Union ("AU") headquarters in Addis Ababa to Shanghai for five years. This AU headquarters was built by the Chinese along with the building's network and computer system. However, there was no evidence of Huawei did it under the influence of China.

Another high profile Huawei case took place where telecom giant was accused of breaking the trade sanctions with Iran and Syria. More specifically, the US government believes that Meng Wanzhou lied

to U.S. banks in order to clear financial transactions with Iran, thus violating the current trade sanctions. Meng Wanzhou is the Chief Financial Officer of Huawei and the daughter of the founder of Huawei. She claimed that the two companies were not subsidiaries of Huawei, when in fact, their senior executives were picked by Huawei.

There was also one indictment against Huawei, which involved criminal charges including obstruction of justice and the attempted theft of trade secrets. Last year, Australia went a step further and banned equipment suppliers "likely to be subject to extrajudicial directions from a foreign government". Huawei was not mentioned by name, but Danielle Cave of the Australian Strategic Policy Institute says the company posed a national security risk because of its government links. She cites an article in Chinese law that makes it impossible for any company to refuse to help the Chinese Communist Party in intelligence gathering.

"Admittedly, what is missing from this debate is the smoking gun," she says. Over the last few months, with a number of countries banning the use of Huawei's networking equipment. That's why it's smartphones are virtually invisible in the US despite its massive presence around the world.

3.3 Surveillance cameras

China has reportedly equipped about 200 million surveillance cameras around the nation, amounting to approximately one camera per seven citizens. Surveillance cameras in China are mostly used for security and traffic control purposes, as well as for catching criminals through AI technologies.

In February, it was revealed that a facial recognition database containing information on about 2.6 million users owned by Shenzhen-based SenseNets had been left open on the internet for months. The facial recognition database had been utilised by the Chinese government to track the Uyghur Muslim population in the Xinjiang region via surveillance cameras.

Hangzhou based Hikvision, a company controlled by the Chinese government, is now the world's largest supplier of video surveillance equipment, with internet-enabled cameras installed in more than 100 countries.

Capable of capturing sharp images even in fog, rain or darkness, Hikvision claims its most advanced technologies can recognize license plates and tell if a driver is texting while behind the wheel. They can also track individuals with unrivaled "face-tracking" technology and by identifiers such as body metrics, hair color and clothing.

The Trump administration is considering a US export ban on Hikvision and it would be the same ban as the one applied to Huawei, which has been included in the US government's Security Entity List.

3.4 5G News in Tibet

China Mobile's Tibet has launched 5G in Tibet with equipment provided by controversial Chinese Tech giant Huawei. There are a total of three 5G bases in Tibet:

1. Company's building the Lhasa post,
2. Telecommunication school
3. The Tibet Post Group office in Lhasa (said to have download speed of upto 530 mbps)

The Chinese government believes that these network improvements can support many things such as the faster and more efficient internet, development of businesses, serve a wide range of military purposes, including monitoring the mountainous border. However, these network upgrades is also being used for increased surveillance and spying operations such widespread application of facial recognition technology.

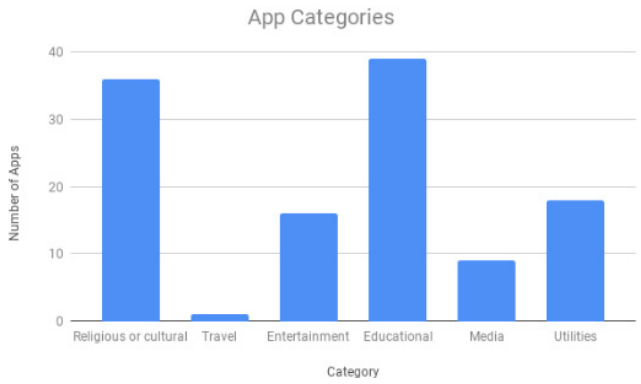
Reports says that the next step for China Mobile's Tibet office will be to accelerate the testing of the 5G application and promote the development of the big data industry and innovation of 5G technology in Tibet, which will enable residents living in farming areas in Tibet to enjoy advanced modern communication services.

3.5 App Censorship

There are many apps either made by Tibetans or for Tibetans and Apple is censoring many of these

apps in the China App Store. It is important to understand how and why certain apps are blocked and the rationale behind these decisions. To understand this, TibCERT conducted an analysis of Tibetan apps being censored in the Chinese App Store. The research was conducted using keyboards to search for Tibetan apps and then using the app censorship platform provided by GreatFire. The detailed report is shared on TibCERT blog (https://blog.tibcert.org/apple-app-censorship/). Finally, a proposed solution to bypass the App Store censorship would be to create an Apple ID with a different geographical region (Taiwan or India, etc.).

All 119 apps were tested on https://applecensorship.com/ to see if they are blocked/censored in China. It has been determined that 29 iOS apps have been censored in China. Among the censored apps, seven are "Religious or Cultural" and five are "Media/Political".



By looking at which apps have been censored, it is possible to identify some of the censorship criteria. If the name of the app contains the Dalai Lama's name then the app is likely to be censored. All media apps are censored. The only game that has been censored prominently features the Tibetan National Flag in its logo.

Given Apple's lack of transparency about which apps it censors, many developers may be unaware that their app is blocked from the China App Store. However, one Tibetan App developer, who wishes to remain anonymous, reported: "I am not allowed to publish apps when I select China. A message appears saying that I have violated the cyber rules of the country (China)". This vague message offers no explanation for how the developer's app violates cyber rules, and what those rules are, and offers no option for redress. Given the overall lack of transparency about its censorship policies, it is unclear how many apps Apple prevents from being published in the first place.

Some Tibetan Buddhist-themed apps are censored while others are not, and the reasons for these discrepancies are unclear. TibCERT continues to conduct more analysis to understand why certain apps are available and why certain apps are banned. In some cases, apps may be available in the China App Store (VOA Tibetan, for example), but the websites that they rely on to feed information to the apps are blocked in China, rendering the apps useless. The methodology that TibCERT used to find Tibetan apps was through keyword search. However, this methodology has its own limitations and TibCERT is continuing to explore other ways to expand its research in understanding how Apple censors apps related to Tibet. Finally, as mentioned earlier, an interesting tactic to bypass this censorship requires creating an Apple ID from a different geographical region (say Taiwan or India or Japan, etc.). TibCERT has tested this approach and were able to access and download the censored apps.