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, expanding Tibetans' technical research capacity on threats in the diaspora, surveillance, and censorship inside Tibet, and 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, advise on threats observed in the community, and report on issues inside Tibet related to cybersecurity. As we enter the new year, we believe we should keep ourselves abreast of the "best practices" to protect against digital threats, ensuring that in the coming years, we can all build the capacity to keep ourselves and our communities safer online.

1.3 TibCERT Updates

It has been just a little over a year since TibCERT was launched and there are now 43 TibCERT members, including stakeholders from institutions, organizations, monasteries, and schools. We have successfully drafted digital security policies with 38 of our members, as well as conducted 30 one-on-one training on these policies through our Digital Security Ambassadors based at major Tibetan settlements in India.

1.4 Summary

This third edition of the Bulletin features:

Overview of the Year
: TibCERT has published two comprehensive reports on the malicious links shared by fake personas via WhatsApp, each targeting senior staff of Tibetan rights groups and containing malware for both iOS and Android devices. We have also carried out research on the number of apps that have been blocked in Apple's Chinese App Store. In addition, in the past year, we conducted more than 47 one-on-one trainings on digital security, including many with TibCERT members.

Predictions and Solutions
: The Tibetan community has been under constant threat of digital attack. To ensure each of us are aware of and utilizing the best precautionary methods, this year TibCERT published a list of the most common forms of digital attack, as well as a compilation of "best practices" and solutions to secure ourselves and our networks from these frequent attacks.

Digital Security Updates
: China's production of technologies geared towards censorship and surveillance are both longstanding and received with much controversy. There are multiple cases, for example, of WeChat censoring information and its exchange even beyond China's borders. The Chinese government has also adopted facial recognition systems for social control and surveillance. Finally, a satellite image (see below) shows a tethered aerostat in the South China Sea that is raising concerns over increased surveillance capabilities by the Chinese government.

2. YEAR IN REVIEW

2.1 TibCERT Completes One Year

2.1.1 Apple Censorship in Chinese App Store

TibCERT has now conducted an analysis of Tibetan apps censored in Apple's Chinese App Store to understand how and why certain apps are blocked and the rationale behind it. The research was conducted on a platform provided by GreatFire at https://applecensorship.com/. We found 119 Tibetan-themed

iOS apps and categorized them into topics, such as religious, cultural, media, political, entertainment, utilities, and educational. Among the 119 apps, we found that 29 so far have been censored. In a detailed report shared on the TibCERT blog https://blog.tibcert.org/apple-app-censorship/, we summarized our understanding of why these apps were blocked. The solution, as proposed in the first issue of our TibCERT Bulletin, is to bypass the Chinese App Store censorship by creating an Apple ID with a different geographical region (Japan or India, etc.).

2.1.2 WhatsApp Attack

From November 11-14, 2018 through April 22, 2019, Tibetans reviewed 15 attempts to steal information from high profile personalities working at human rights groups in Dharamshala, India. These attacks targeted both iOS and Android devices in which malicious links were shared via WhatsApp from fake personas claiming to be "Jason Wu," head of the "Refugee Group" at Amnesty International's Hong Kong branch, as well as a New York Times Reporter. The attacks were manipulated in such a way by just clicking on the link would steal all the information from the iOS device (with the vulnerability of iOS version 11 to 11.4). In the case of Android, the malware would grant access to the device's Gmail accounts. This attack was discovered by TibCERT in collaboration with The Citizen Lab based in Toronto, Canada. This attack appears to be carried out by a single operator that The Citizen Lab called POISON CARP. A detailed report is shared on the TibCERT blog *https://blog.tibcert.org/tibetans-targeted-by-spyware-for-iphone-and-android/*

2.1.3 Trainings and Workshops

So far, we have 43 TibCERT members and have successfully drafted digital security policies with 38 of them, providing tech support and incident response to many organizations and institutions over the past year. In particular, we have conducted a total of 45 training sessions with 680 participants, 37 of which were one-on-one trainings given by our Digital Security Ambassadors. We also organized three intense, multi-day trainings called the "Lhakar Tech Week" in which we trained communicators (Tibetans who are the conduit for information from inside Tibet) and staff from different Civil Society Organizations (CSOs) and institutions on topics such as how the internet works, what kinds of cyberthreats our community faces, how to defend ourselves from these threats, and how to keep our devices clean, etc. At the request of other CSOs, we also conducted additional workshops, including at an Action Camp organized by Students for a Free Tibet, a Youth Leadership training held by Tibetan Youth Congress, and a training for staff and students at TCV Selakui.

2.1.4 Future Plans

In the coming months, our Digital Security Ambassadors will begin sharing endpoint security tools, software that can hunt potential threats in an operating system. We have also built a malware intake system and are working on implementing it in the coming year. This will allow us to analyze and set up firewalls in our stakeholders network systems, helping keep them safe from potential attacks. We are also aiming to strengthen the security and capacity within the Tibetan community by continuing to build up the skill sets of CSOs and individuals on issues like data encryption, device and system security, and best practices to protect against threats, etc.

3 PREDICTIONS FOR THE COMING YEAR

For more than a decade now, the Tibetan community in diaspora has been a target of the Chinese government to test their malware and steal our information. Throughout the years, we have faced all sorts of attacks, including socially engineered malware, phishing attacks, and the most recent one-click-mobile exploit via WhatsApp. While it's always hard to know exactly what kinds of attacks we might face in the future, judging from the past and the kinds of vulnerabilities we currently have in our community, the following are some predictions for the coming year.

3.1 PC Predictions

Our community has endured many attacks on our PCs or Macs over the years and it is predictable that

we will continue to face such threats. These attacks can even be sent using the name of a person we know. Computer attacks can be sent in the form of malware in email attachments or links that infect the user when opened or clicked. There can also be more phishing attacks in the coming year as it's one of the easiest and most efficient ways of stealing someone's credentials.

Many people in our community are still using outdated software and operating systems on their computers. This puts themselves and their networks very much at risk of being compromised by an exploit kit—a tool used by cybercriminals to gain access to devices and steal confidential data. However, these potential digital threats listed here can be prevented and mitigated through the solutions and practices provided below.

3.2 Mobile Phone

Most mobile phones nowadays have the same capability as that of a computer and, due to convenience, more and more people tend to use their mobile phones rather than a computer. However, many people only think about keeping laptops and computers secure, putting us at great risk when using our phones if we are not running the most recent updates and security provisions. Since we keep our personal, financial, and official information on our mobile devices, it is just as important to keep them as secure as our computers and laptops.

As has been well documented, there is a rise in mobile phone attacks globally like the WhatsApp attacks we have reported on extensively. Another example is the recent attack by Saudi-linked Pegasus spyware on a New York Times journalist. This particular malware was sent as an SMS containing a hyperlink to a website of a Pegasus operator called KINGDOM. When clicked, the link gave the operator access to all the information stored on the targets' phone. Given this alarming trend, we believe in the coming years the Tibetan community may be the target of more mobile phone-based attacks like this one and others, sent through links and attachments via messaging apps.

In addition, since most Chinese apps are not open-source and are being surveilled by the Chinese government, we also predict that using such apps on our devices will keep putting us at risk. How the app works, how the data is being transferred, how the app uses the phone's permissions are information that we need to be aware of. How many of us are aware of the fact that the mobile version of *"Pubg" is owned by Tencent Games, the same company which owns "Wechat".*

3.3 Disinformation Campaigns

An unusually active social media campaign was observed during the Tibetan elections of 2011 and 2016. In the midst of the political campaigning on social media platforms such as Facebook and WeChat, there was a concern that the Chinese government and Chinese trolls were using fake accounts to spread disinformation via fake news, sharing disturbing content and doctored images.

In order to secure our community from such disinformation and enable a healthy environment for the coming 2021 elections, we advise all social media users to report such content and fake profiles, as well as block all fake personas. The steps for reporting disruptive content and fake profiles being used on Facebook is posted on our Knowledge Base at: https://learn.tibcert.org/knowledge-base/how-to-report-content-or-fake-profile-in-facebook/

3.4 Solutions by TibCERT to Stay Safe Online

Attackers use resources to create malware and other methods for stealing information. However, adopting the following simple and easy "best practices" can help you keep your data secure and stay safe online and at the same time, raise the cost for the attackers.

3.4.1 Don't Wait, Update

Updating the software on your devices is one of the most effective ways of preventing your system from getting compromised. Over time, security vulnerabilities are discovered by software manufacturers and they will periodically send updates over the internet that act as security patches. Updating your software removes its vulnerabilities so it can no

longer be used by attackers to exploit the system. Therefore, updating your software as soon as it becomes available is one of the best ways to help you stay safe online. You can even set your system to update automatically so you won't forget.

3.4.2 Think Before You Click

"Did you know this funny video of you is posted online?"

"Click here to read the latest breaking news on the situation inside Tibet."

"An important message from the Dalai Lama."

It is tempting to click on these links, isn't it?

This is because the messages are designed to take advantage of things we care about. Unfortunately, these links are often malicious and will take you to a website where your computer or phone can get infected with a virus. Don't just open attachments or click on the links you receive in your email, Facebook, WhatsApp, and other communication apps. Unless you were expecting it, there's a strong chance that the attachment or link contains a virus that will dangerously infect your computer or phone as soon as you open it.

3.4.3 Detach from Attachments

If you are someone who thinks, "I have nothing to hide. Why should I be afraid?" then think again. Many attacks are designed to steal information. For most people, this includes everyday items like credit cards and banking information. However, for us in the Tibetan community, what we also often fail to recognize as information is the human networks we have online and on our devices. The Tibetan community is small and incredibly connected and with the majority of us living under direct threat from China, our responsibility to protect each other through staying secure on our devices is much higher. Any time our systems are infected through a targeted attack, we put everyone we are in communication with at risk of having their information stolen too, which could have real-life consequences. Although everyone everywhere has this responsibility to their networks, with attacks from the Chinese government commonplace in Tibetan communities, we must be continuously vigilant.

3.4.4 Strong Password

Passwords are key to your life. Whether for your computer, your email account, or your Facebook account, make your passwords long, complex, and unique. Using a password that is a phrase is one of the most secure methods, such as "!TheSkyIsSoBeautifulToday514!" Or, you can make a password of words that are irrelevant to each other with spaces in between, such as "Flower Chair Surprising Pens +19%" For any strong password, you must have:

Lowercase and uppercase letters
Numbers
Symbols
Be at least 16 characters long
Should not have names or dates related to you (eg., Tenzin1985 or Rangzen59)

3.4.5 Turn on 2-Step Verification

Have you ever feared your Facebook or email account might get hacked?

Do you ever worry that you don't have the knowledge to protect yourself online?

The good news is you can easily protect yourself by turning on your 2-step verification (also called two-factor authentication).

If someone is able to crack your password, 2-step verification will block them from logging in to your accounts. It is an extra layer of protection—a code sent by text, through an app, or via push notification on your phone—that only you can get.

There are many other "best practices" which can be further used to strengthen the security of your devices. You can visit our website https://tibetaction.net/digitalsecurity/ to find out more information on digital security, including videos and infographics on pressing topics.

4. Digital Security Updates

4.1 Chinese Censorship:

Chinese censorship policy for WeChat is now extending beyond its border. Recently, a Chinese-American information security analyst named Bin Xie had his account shut down after he wrote on WeChat about the recent Hong Kong election, saying, "The pro-China candidates totally lost." Later, he joined a group chat of Chinese Americans who have been censored on WeChat.[1]

Also, information related to the coronavirus outbreak in China is being censored and surveilled online by the Chinese government. According to online news app Quartz, "Earlier this month, a timeline of developments in the coronavirus outbreak was being widely shared on WeChat but then began to be censored, according to users Quartz spoke to. Quartz on Jan 22 tried and failed to send the image via a private chat between a user in the US and one in the UK. There was no notification to the sender that the picture had not been sent, which often happens when people try to send "sensitive" content on the app. However, the person in the UK never received the picture on her end. After rotating the photo, it went through."[2]

On the sender's side, left, the picture, sent twice in a WeChat message, looks like it was sent successfully. However, on the receiver's end, the two pictures never showed up.

In addition, on 23 January, Chinese social media platform Weibo blocked/censored a photo displaying the front page of the People's Daily (China's state media) which was fully dedicated to Xi Jinping and had inadequately covered the national crisis of the coronavirus. The image wasblocked even though it was simply showing the newspaper and did not include any additional commentary as is usually shared on Twitter.[2]

The front page of People's Daily never fails to surprise you. Amidst one of the most serious public health crises, there's NO mention of the Wuhan coronavirus

4.2 Privacy & Security Implications of Facial Recognition in Authoritarian Regimes Like China

In November 2019, local officials in eastern China were authorised to use facial recognition software to trace any kind of "uncivilised behavior" depicted by its citizens. Later, the surveilled photos from street

1 https://www.dailywire.com/news/chinese-communist-party-is-censoring-people-in-america-for-talking-about-hong-kong
2 https://qz.com/1790719/china-coronavirus-outbreak-unfolds-in-a-new-age-of-information/

cameras of seven residents wearing pajamas in public were published along with their names, government identification numbers, and location where they had displayed their "uncivilized behavior" of wearing pajamas in public areas. This sparked outrage in Anhui Province. The urban management department of Suzhou later apologized and took down the original post. However, the act clearly shows that Chinese officials are using such a powerful tool to control their citizens and shame them publicly.

China's use of facial recognition and surveillance software has become widespread, unlike other countries where such software is often banned and highly debated. The police authorities in China are using these tools to create a powerful surveillance dragnet and racially profile minorities. Such acts of the Chinese government are giving rise to a fear that the Chinese Communist Party (CCP) will rule via Digital Authoritarianism,[3] i.e., state-led mass surveillance using a new form of credit scoring to influence the behavior of citizens.

4.3 Tethered Aerostat Image from South China Sea

A tethered aerostat is a type of unmanned airship which is lighter than a regular aircraft. Towards the end of 2019, satellite imagery confirmed the presence of a tethered aerostat floating in the air above one of China's man-made islands in the South China Sea. The aerostat is almost certainly carrying a sensor system such as radar which may help provide relatively low cost early warning capabilities—especially against low flying cruise missiles—as well as provide the Chinese government with improved general situational awareness throughout the region.

From the imagery, it is unclear what type of sensor is being used or if it's working. However, it is believed that this technology may provide China with other security services and more opportunities to challenge American ships patrolling in the South China Sea and prevent them from reaching their intended destination.

This new surveillance blimp is likely just the beginning. "Whatever China's aerostat plans in the South China Sea turn out to be, these platforms are certainly well suited to expanding the country's already significant anti-access and area denial capabilities in this heavily disputed region."[4]

3 https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html

4 https://www.thedrive.com/the-war-zone/31279/chinas-new-surveillance-blimp-in-the-south-china-sea-is-likely-just-the-beginning