National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

BND

Bundesamt für Verfassungsschutz

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre | PART OF THE GCSB

Advisory

BADBAZAAR and MOONSHINE: Spyware targeting Uyghur, Taiwanese and Tibetan groups and civil society actors

9 April 2025

BADBAZAAR and MOONSHINE: Spyware targeting Uyghur, Taiwanese and Tibetan groups and civil society actors

The NCSC and partners publish new information and mitigation measures for those at high risk from two spyware variants.

Summary

With support from the UK Cyber League, this advisory has been jointly produced by the National Cyber Security Centre (NCSC UK) and international partners:

- **The Australian Cyber Security Centre, part of the Australian Signals Directorate**
- **The Canadian Centre for Cyber Security, part of the Communications Security Establishment**
- **The German Federal Intelligence Service**
- **The German Federal Office for the Protection of the Constitution**
- **The New Zealand National Cyber Security Centre, part of the Government Communications Security Bureau**
- **The United States Federal Bureau of Investigation**
- **The United States National Security Agency**

Its purpose is to raise awareness about the growing threat that malicious cyber actors pose to individuals connected to topics including Taiwan, Tibet, Xinjiang Uyghur Autonomous Region, democracy movements and the Falun Gong.

This advisory includes two case studies detailing techniques used by malicious cyber actors using spyware known as BADBAZAAR and MOONSHINE to target data on mobile devices including smartphones that could be of interest to the Chinese state. It also signposts to guidance to help individuals protect themselves, their devices and their data.

Alongside this advisory, the NCSC has published full technical detail with separate guidance.

Who is at risk?

The authoring agencies and industry partners have observed BADBAZAAR and MOONSHINE specifically targeting individuals connected to topics considered by the Chinese state to be a threat to their domestic authority, ambitions and global reputation. Those most at risk include, but are not limited to, anyone connected to:

- **Taiwanese independence**
- **Tibetan rights**
- **Uyghur Muslims and other ethnic minorities in or from China's Xinjiang Uyghur Autonomous Region**
- **democracy advocacy (including Hong Kong)**
- **the Falun Gong spiritual movement**

This includes non-governmental organisations (NGOs), journalists, businesses and individuals who advocate for, identify with, or otherwise represent these groups. The indiscriminate way this spyware is spread online also means there is a risk that infections could spread beyond intended victims.

This advisory aims to help those at risk respond effectively to the specific threat from BADBAZAAR and MOONSHINE spyware. The suggested mitigations complement broader cyber security advice and should not be considered in isolation.

By following the guidance referenced in this advisory, users can reduce the risk of infection of their mobile devices and data.

The threat

MOONSHINE and BADBAZAAR are examples of trojans; they have malicious functions hidden inside an otherwise functioning app that can be downloaded from app stores or online file-sharing services.

These apps are designed to trick a user into downloading and installing them on a device. Once an app is installed, it uses vulnerabilities on the device to perform unauthorised functions, or it may rely on a user granting app permissions to access and download information from the device, including:

- **location data including real time tracking**
- **access to microphone and camera**
- **messages, photos and other files stored on the device**
- **device information and more**

The actors then exploit the legitimate interests of at-risk groups, to identify and infect as many victims as possible, and gain access to their data. One way they do this is by designing apps they know will appeal to their victims, such as apps which support their native languages, or contain content specific to locations such as Tibetan regions of China or Xinjiang.

The case studies in this advisory provide some examples of this, including the TibetOne and Uyghur Quran apps.

The actors are active in online forums where there is a user base of their intended victims, which maximises their chance to infect victims. They have been observed deliberately sharing spyware in Tibet-related Telegram channels and Reddit forums. The case studies in this advisory also give examples of these methods.

Malicious apps are often shared as standalone files, such as APK files on Android, which users are required to download and install. The actors try to make their spyware appear more legitimate by uploading it to official app stores such as the Google Play Store and the Apple App Store or by adding malicious code to previously benign apps, although official stores have security features and vetting processes which make this tactic less successful. This makes apps from official stores safer, but as demonstrated in the case studies and the NCSC's App Store Threat Report, these processes are not perfect.

Following these four tips can help protect you from the threats outlined in this advisory. For more detailed advice, see the mitigations section.

National Cyber Security Centre
a part of GCHQ

Four tips to stay secure on your smartphone

Reduce the risk from malicious apps with good cyber hygiene, by following these four principles:

Stay mainstream

Don't root or jailbreak devices, and only use apps from trusted stores

Stay organised

Review installed apps and permissions regularly

Stay in touch

Report suspicious messages and files

Stay alert

Stay vigilant on social media and check shared files and links

Case studies

These two case studies illustrate how MOONSHINE and BADBAZAAR work, and how malicious cyber actors are targeting those most at risk.

Case study one: MOONSHINE

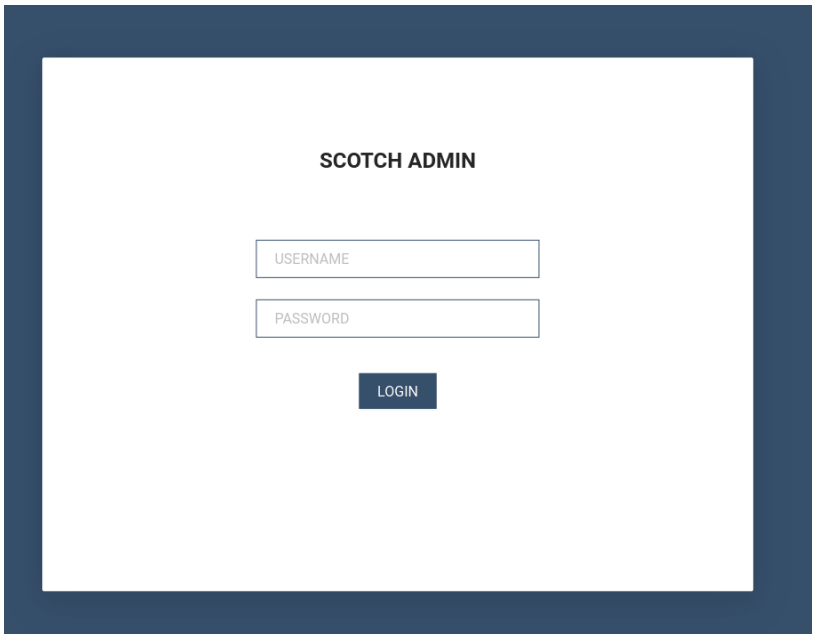
MOONSHINE is an Android spyware reported in 2019 by Citizen Lab as targeting Tibetan groups. MOONSHINE masquerades as a legitimate app to lure victims into installing it. It has been shared via Telegram channels and links sent via WhatsApp.

MOONSHINE has extensive surveillance capabilities, such as:

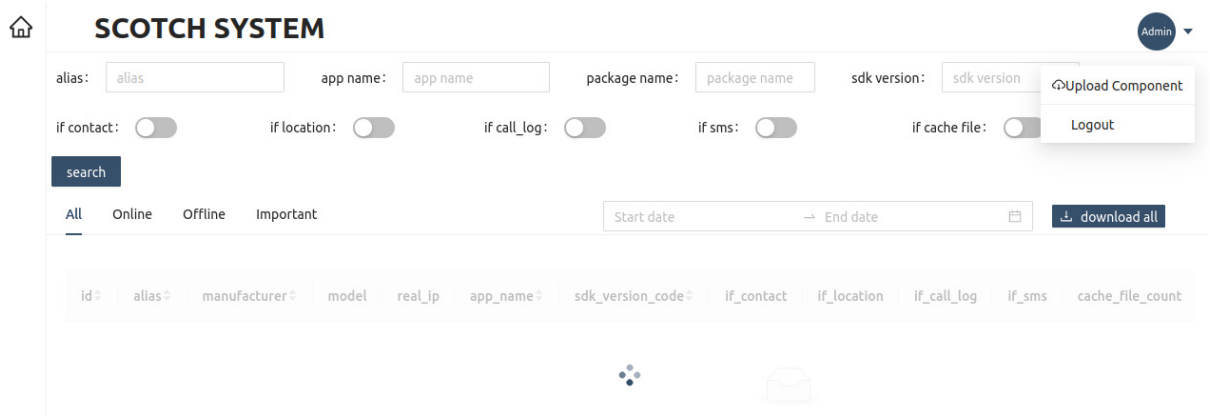
- **location data including real time tracking**
- **live audio and photo capture**
- **downloading files from device**
- **retrieving device information**
- **playing audio on the device**

The application '**ئاۋازلىق قۇرئان.apk**', which translates as '**Audio Quran.apk**', is an example of how MOONSHINE is used to target Uyghurs. The use of the Uyghur language in the file name, indicating a Quran application, was likely designed to appeal to Uyghur Muslims.

Once installed, the malicious cyber actors can collect information from victims' devices. This information is accessed via the 'SCOTCH ADMIN' panel.



Once logged in, the actors can access the page shown in the screenshot below. This page would display details of infected devices and the level of access the actor has to infected devices:



The malware management panel, showing the data collected, would include:

- **level of access to device**
- **SMS messages**
- **call logs**
- **location data**
- **device information**

In collaboration with Cyber League, the NCSC has built on industry reporting from Trend Micro to find overlaps between the MOONSHINE exploitation kit and login

panels containing 'UPSEC' in the HTML title. Full details are in the accompanying technical advisory.

According to Intelligence Online, UPSEC is a reference to 'Sichuan Dianke Network Security Technology Co. Ltd'. The authoring agencies have not verified this statement.

Case study two: BADBAZAAR

BADBAZAAR is a mobile malware with iOS and Android variants that has targeted Uyghurs, Tibetans and Taiwanese individuals. This malware has been spread via social media platforms and official app stores.

BADBAZAAR has been used to target Tibetans via the app '**TibetOne**', as reported by Lookout and Volexity. **TibetOne** is an iOS app created by the malicious actors, with the capability to access device information and location data. It was uploaded to the Apple App Store in December 2021 but is no longer available. To spread the malware further, the actors also advertised the app in a Telegram channel called '**tibetanphone**'.

TibetOne

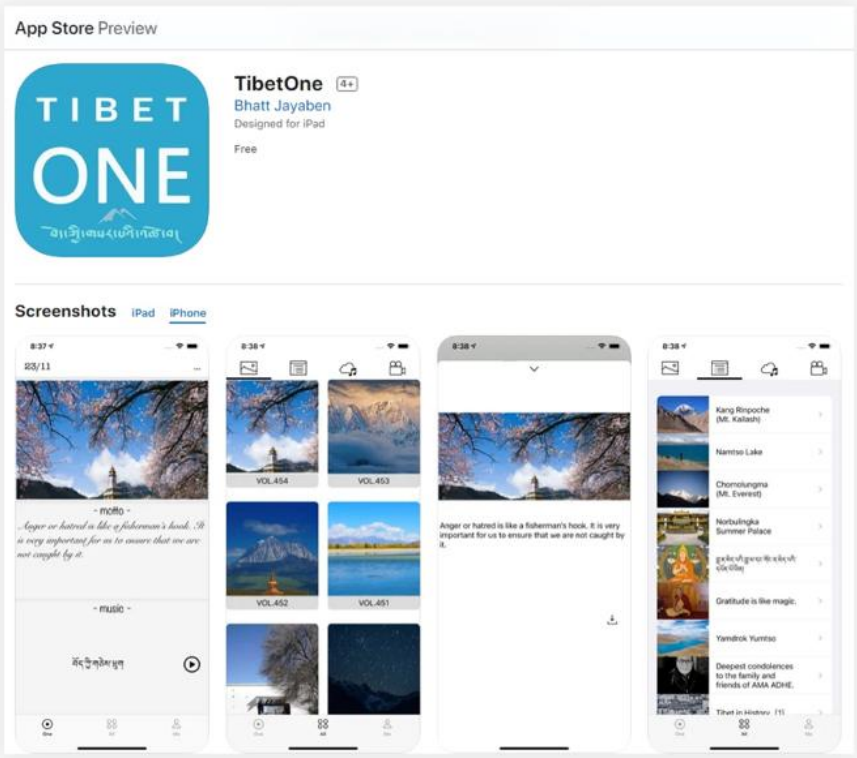


Figure 1: TibetOne app page on the Apple App Store. The app has since been removed.

Figure 2: TibetOne as shared in Telegram channels.

To add legitimacy to the app, the actors also developed a website called '**tibetone[.]org**', which described itself as '*bring[ing] rich and high-quality works to people who love Tibetan culture and make reading a new way of life*'.

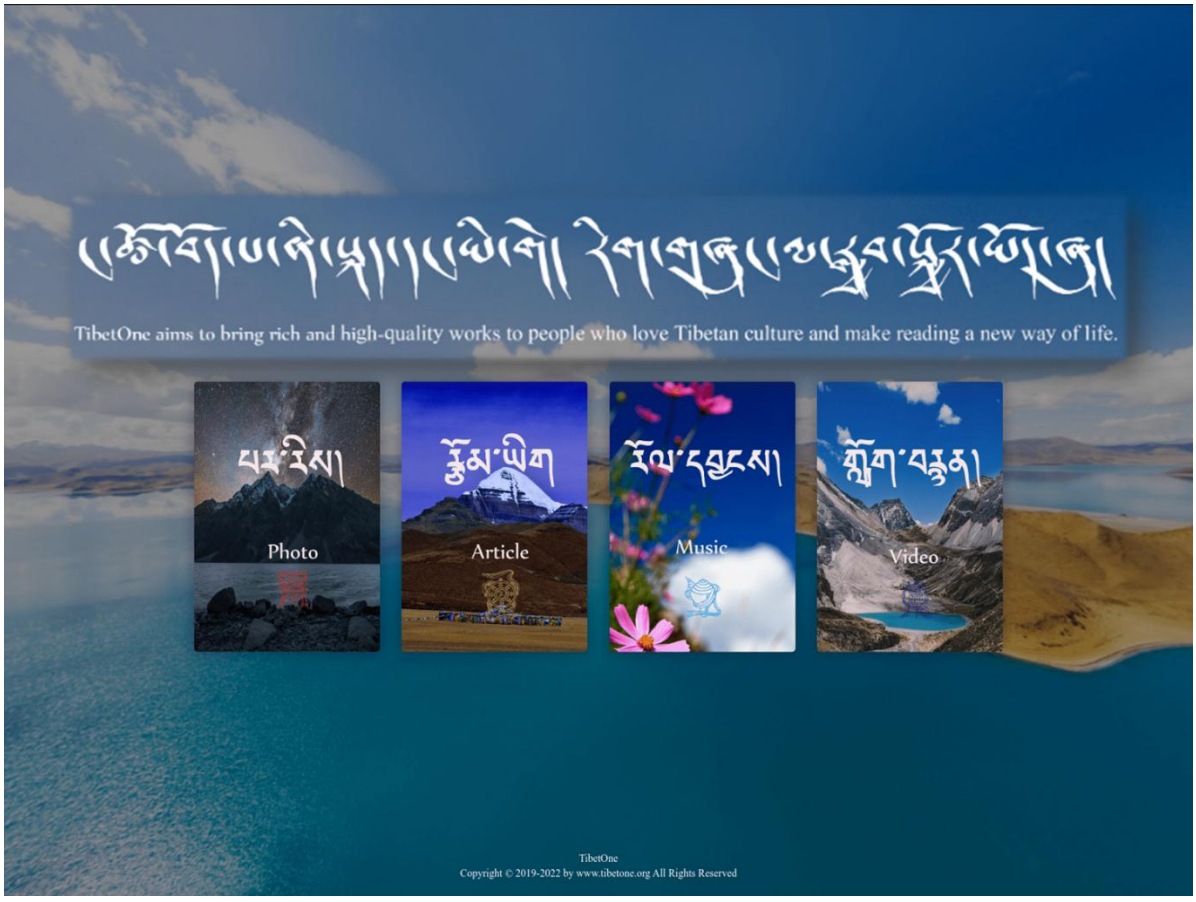


Figure 3: Homepage of 'tibetone[.]org'.

This image has been edited to make relevant sections clearer.

This website had a page for articles which allowed users to leave comments. A comment left by email address '**choekyi.wangmo@ignitetibet.net**', is believed to be controlled by the malicious actor and is likely to impersonate '**Choekyi Wangmo**' who the Tibetan Centre of Human Rights and Democracy lists as a pro-Tibet protestor. This is likely to be another attempt to give the impression that the app genuinely advocates for Tibetan independence.

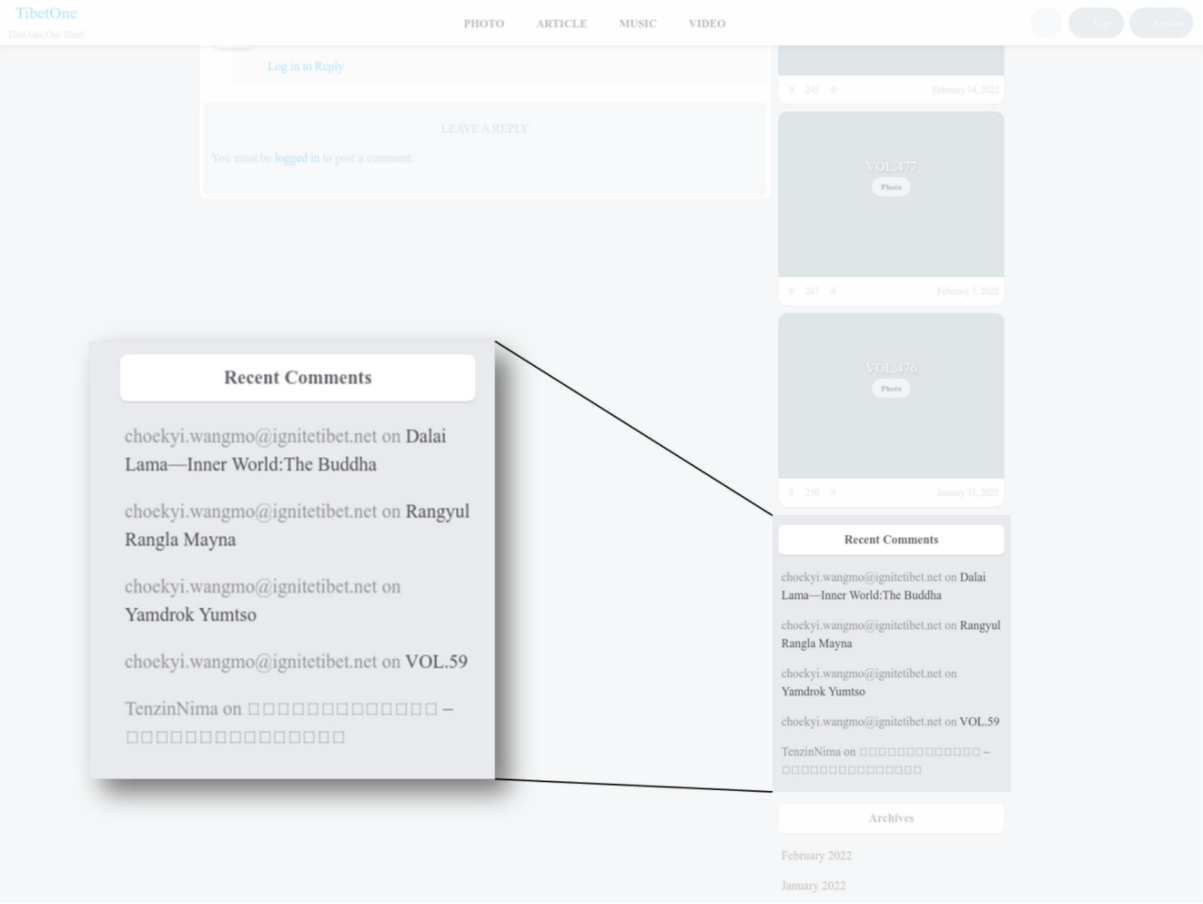


Figure 4: 'tibetone[.]org' page showing comments from users believed to be controlled by the malicious actor.

This image has been edited to make relevant sections clearer.

'**TenzinNima**' is another username that has added comments on this site. Volexity has reported that this username is also used on Reddit to advertise the Telegram channel '**Tibetanmaptalk**'. It includes a link to download a malicious sample of '**AlpineQuest**', a navigation app available on Android devices. The download link provided is for a third-party file-sharing service called Mega.

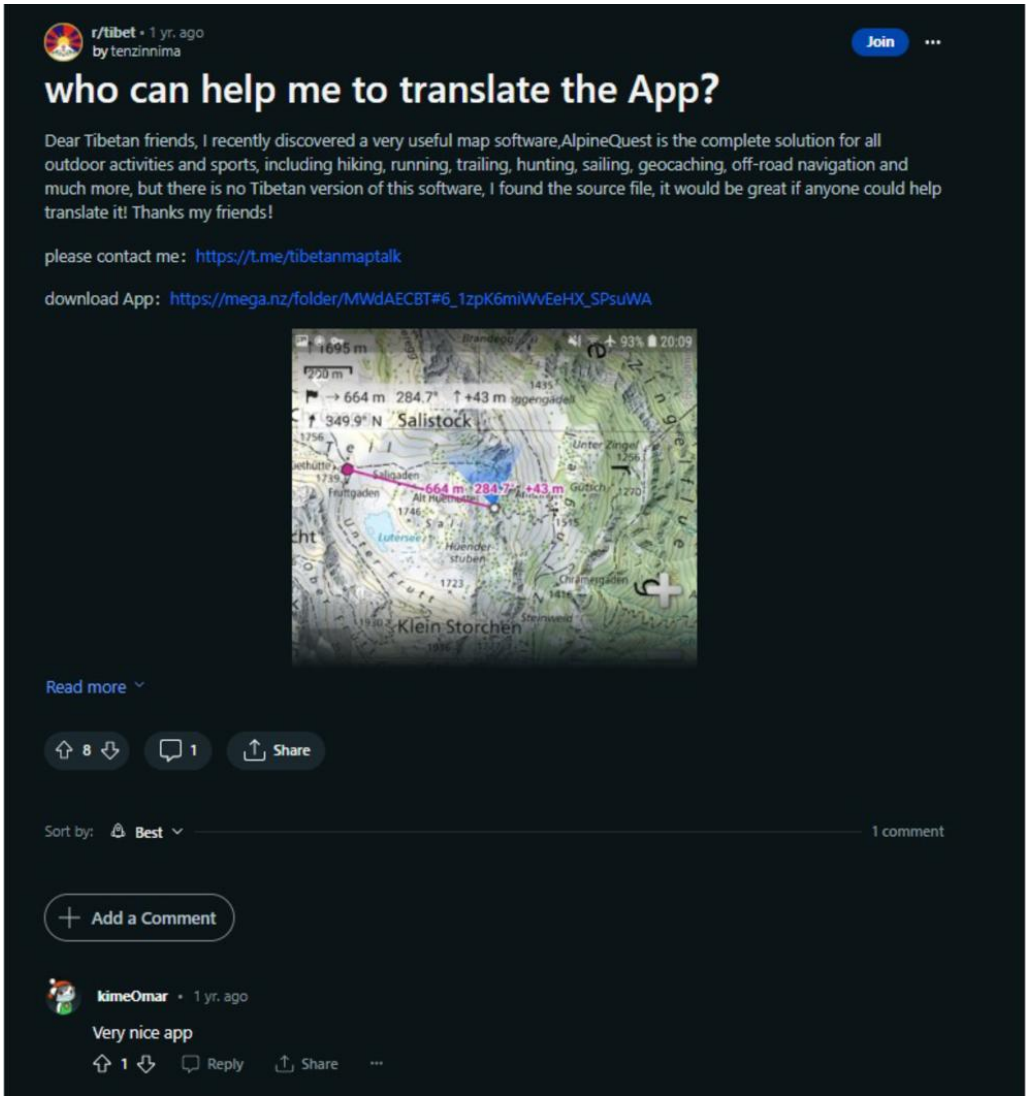


Figure 5: Reddit post advertising malicious application by account believed to be malicious actor controlled.

Volexity also notes that a user known as '**KimeOmar**' who commented on the post has also been observed sharing malicious apps on another sub-Reddit forum. This could indicate that the malicious actors use multiple social media profiles to make their posts appear legitimate.

Assessment

BADBAZAAR and MOONSHINE use several social engineering methods to specifically target Uyghur, Tibetan and Taiwanese communities, namely:

- the trojanisation of apps of interest to these communities, such as a Uyghur language Quran app, is almost certainly tailored to the target victim base
- the adding of these trojanised apps to official app stores highly likely lends a sense of legitimacy, and the sharing in group chats is highly likely intended to exploit trusted relationships within these communities

BADBAZAAR and MOONSHINE collect data which would almost certainly be of value to the Chinese state. Although BADBAZAAR and MOONSHINE have been observed targeting Uyghur, Tibetan and Taiwanese individuals, there are other malwares that target other minority groups in China. Citizens from the co-sealing nations, in China and abroad, who are perceived to be supporting causes that threaten regime stability, are almost certainly under threat from mobile malware such as BADBAZAAR and MOONSHINE. The capability to capture location, audio and photo data almost certainly provides the opportunity to inform future surveillance and harassment operations by providing real-time information on the target's activity.

Mitigation measures for mobile app users

The authoring agencies encourage the following security practices to protect against the threats described in the case studies. These recommendations are underpinned by best-practice NCSC guidance. See the 'further reading' section for links to best-practice guidance for readers in Australia and the US.

Keep your device secure

- **Only download apps from official app stores, such as Google's Play Store or Apple's App Store.** Google's Play Store and Apple's App Store scan software for viruses before making it available, giving you more assurance that what you're downloading is safe. Apps from trusted stores may still carry a risk, but downloads from other sources may have no protections at all. The NCSC has a threat report on app stores: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Keep your device and apps up to date.** Install updates to your apps and device software as soon as they are available. Turn on 'automatic updates' in your device's settings if available so you don't need to remember to do it. See NCSC guidance about staying secure online, to protect against known viruses and other kinds of malware. Updates often include improvements and new features: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Do not 'jailbreak' or 'root' your device;** that is, modify your device in an attempt to bypass the security controls put in place by the manufacturer. As this uses unpatched vulnerabilities, this leaves the device more vulnerable to attacks. See NCSC guidance: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Manage your apps

- **Review your apps and their permissions.** If you no longer need an app, delete it. Where you can, restrict app permissions to minimise data exposure, as malware is often designed to access protected files or peripherals, such as cameras and microphones.
    - How to check app permissions for Apple users: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
    - How to check app permissions for Android users: https://support.google.com/android/answer/9431959?hl=en-GB

- **Automatically send unknown apps to Google**. If you are an Android user and have downloaded an app that isn't from Google's Play Store, you can send it to Google by enabling 'Improve harmful app detection' in Google's Play Store app settings under 'Play Protect'. This will scan the app for malware detection helping protect users. Information on how to set this up: https://support.google.com/android/answer/2812853?hl=en-GB

Utilise cyber services

- **Use URL reputation services before clicking on a link**. You can check if a link from an email, text message or elsewhere is safe by scanning it first using services such as Google's Safe Browsing tool or Virus Total. You can also upload suspicious files and apps to a malware analyser, such as Virus Total which can help detect if a file is malicious. Be aware that scanning services can produce false negatives.

- **Enrol in the Google Advanced Protection programme.** This is a free service designed to safeguard individuals who use Google services (Gmail, Play Store, etc) who are at risk of being targeted. This service provides heightened security when using Google services: https://landing.google.com/advancedprotection/

- **Enrol in additional resilience services, where they are available.** For example, high-risk individuals in the UK may be eligible for extra defensive services to help with their cyber security. Check eligibility and find out more: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Report threats

- **Identifying and reporting fake accounts**. Malicious cyber actors create fake accounts or hack real accounts to further their aims. If you suspect an account is fake or compromised, report it to the platform and block it. Many services have a process to verify accounts, such as 'verified badges' for Instagram and Facebook. This can help identify that an account is genuine. The NCSC has guidance on using social media safely which includes details of how to verify and report compromised accounts: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Phishing using scam emails, SMS and links**. The NCSC can investigate suspicious email addresses and websites. If you think a site, email or message is suspicious, you can report it: https://www.ncsc.gov.uk/collection/phishing-scams

NCSC Glossary

- **Android**

Google's mobile operating system, used by several smartphone and tablet manufacturers.

- **App**

An application, or app, is a software package that users can install or are pre-installed on a device to provide extra functionality or content to their device.

- **Cyber Security**

The protection of devices, services and networks - and the information on them - from unauthorised access, theft or damage.

- **Device**

Computer-based hardware that physically exists, such as a desktop computer, smartphone or tablet.

- **iOS**

Apple's mobile operating system used on its suite of mobile devices.

- **Malware**

Derived from 'malicious software', malware is any kind of software that can damage computer systems, networks or devices. Includes viruses, ransomware and trojans.

- **Operating system**

The basic software running on computers, tablets and smartphones, required to run additional applications and hardware.

- **Phishing**

Scam emails or text messages that contain links to websites which may contain malware, or may trick users into revealing sensitive information (such as passwords) or transferring money.

- **Spyware**

A type of malware that installs on a device without the user's consent, collecting data and then sending it to a third party.

- **Social media**

Websites and apps, such as Facebook, X and Instagram, that allow people to share and respond to user-generated content (text posts, photos and video).

- **Smartphone**

Modern mobile phones that perform complex functionality including those with Android and iOS operating systems.

- **Trojan**

A type of malware, disguised as legitimate software, that is used to gain unauthorised access to a victim's device.

- **URL**

Uniform Resource Locator. An address on the world wide web such as a domain name (for example www.bbc.co.uk).

- **Virus**

A type of malware that is designed to infect legitimate software programs and replicates across networks when those programs are activated.

Further reading

Guidance from the Australian Cyber Security Centre

- Report a cybercrime, incident or vulnerability
- How to secure your devices
- Secure your mobile phone
- Phishing
- Scams
- Secure your social media
- Security tips for social media and messaging apps

Guidance from the UK NCSC and NPSA

- Defending Democracy
- Social Media: how to use it safely
- Device Security Guidance for organisations including mobile
- Threat report on application stores.
- Personal safety and security for high-risk individuals
- Phishing: Spot and report scam emails, texts, websites and calls

Guidance from the US NSA

- Mobile Device Best Practices

Disclaimer

Please note that this advisory provides information that is validated at the time of publication.

This report draws on information derived from authoring agency and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

In the UK, this information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.ukAll material is UK Crown Copyright ©

Annex: MOONSHINE & BADBAZAAR samples observed

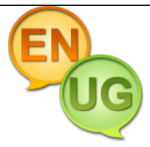
This table lists the apps used in MOONSHINE and BADBAZAAR campaigns in the past two years.

Many of these apps show a clear similarity to established apps. This is likely to be a deliberate actor technique to 'spoof' well-known brands.

It's important to note, the name of the app, package name, and icon can all imitate or match the real application and should therefore not be used exclusively to identify if a device is infected.

As included in the mitigations section, you can send apps on your Android device to Google by enabling 'Improve harmful app detection', which will scan apps on your device that were installed from outside the Play Store.

App title	Package name	App icon
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	

FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

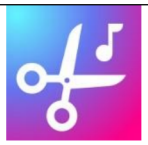
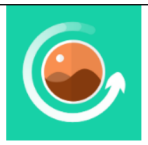
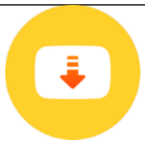
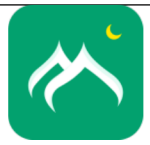
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitc h.san.basicpdfviewer	

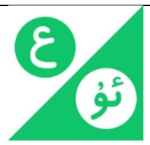
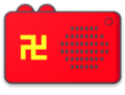
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	

SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	
Tibetan Divination System MO	net.rhombapp.mo	

Tibetan Prayer	com.chorig.tibetanprayer	
Translator AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Video Converter	com.inverseai.video_converter	
Video Cutter	com.naing.cutter	
Video Downloader	downloader.video.download.free	
Video Maker	com.bstech.slideshow.videomaker	

Video Player for Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Voice Recorder	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	

WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
WiFi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
YouTube Downloader	dentex.youtube.downloader	
Zom	im.zom.messenger	
iQuran Lite	com.guidedways.iQuran	

ئاۋازلىق ئەسەرلەر	com.ewlat.eserler	
ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
ئۇيغۇرچە قۇرئان	com.c9.uyghurquran	
القرآن الكريم	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	
نۇر كىرگۈزگۈچ	com.nur.ime	
《心灵法门》念佛机	com.guanyincitta.chant	

汉藏英辞典	com.dacd.dictionary	
藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate