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

Pabatid

BADBAZAAR at MOONSHINE: Spyware na tumatarget sa Uyghur, Taiwanese at Tibetan na mga grupo at mga civil society actor

ika-9 ng Abril 2025

BADBAZAAR at MOONSHINE: Spyware na pumupuntirya sa Uyghur, Taiwanese at Tibetan na mga grupo at mga civil society actor

Ang NCSC at mga kasosyo ay naglathala ng bagong impormasyon at mga hakbang sa mitigasyon para sa mga nasa mataas na panganib mula sa dalawang variant ng spyware.

Buod

Sa suporta mula sa UK Cyber League, ang pabatid na ito ay magkasamang ginawa ng National Cyber Security Center (NCSC UK) at mga internasyonal na kasosyo:

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

Ang layunin nito ay upang itaas ang kamalayan tungkol sa lumalaking banta na dulot ng mga malicious cyber actor sa mga indibidwal na konektado sa mga paksa na kinabibilangan ng Taiwan, Tibet, Xinjiang Uyghur Autonomous Region, mga kilusang demokrasya at ng Falun Gong.

Kasama sa pabatid na ito ang dalawang case study na nagdedetalye ng mga diskarteng ginagamit ng mga malicious cyber actor na gumagamit ng spyware na kilala bilang BADBAZAAR at MOONSHINE para mag-target ng datos sa mga mobile device kabilang ang mga smartphone na maaaring mahalaga sa estado ng China. Nagpapakita rin ito ng patnubay upang matulungan ang mga indibidwal na protektahan ang kanilang sarili, kanilang mga device at kanilang datos.

Kasabay ng pabatid na ito, ang NCSC ay naglathala ng buong teknikal na detalye na may hiwalay na gabay.

Sino ang nasa panganib?

Napagmasdan ng mga ahensya ng pag-akda (authoring agencies) at mga kasosyo sa industriya ang BADBAZAAR at MOONSHINE na partikular na nagta-target sa mga indibidwal na konektado sa mga paksang itinuturing ng estado ng China na banta sa kanilang domestikong awtoridad, ambisyon, at reputasyon sa buong mundo. Kabilang sa mga nasa panganib, ngunit hindi limitado dito, ang sinumang konektado sa:

- **Kalayaan ng Taiwan**
- **Mga karapatan ng Tibet**
- **Mga Uyghur Muslim at iba pang etnikong minorya sa o mula sa Xinjiang Uyghur Autonomous Region ng China**
- **nagtataguyod ng demokrasya (kabilang ang Hong Kong)**
- **espirituwal na kilusang Falun Gong**

Kabilang dito ang mga non-government organization (NGOs), mga mamamahayag, mga negosyo at mga indibidwal na nagtataguyod, kumikilala sa, o kung hindi man ay kumakatawan sa mga grupong ito. Ang walang pinipiling paraan ng pagkalat ng spyware na ito sa online ay nangangahulugan din na may panganib na ang mga impeksiyon ay maaaring kumalat nang higit pa sa mga nilalayong biktima.

Nilalayon ng pabatid na ito na tulungan ang mga nasa panganib na tumugon nang epektibo sa partikular na banta mula sa BADBAZAAR at MOONSHINE spyware. Ang mga iminungkahing mitigasyon ay umaakma sa mas malawak na payo sa seguridad sa cyber at hindi dapat isaalang-alang nang nakahiwalay.

Sa pamamagitan ng pagsunod sa gabay na binanggit sa pabatid na ito, mababawasan ng mga user ang panganib ng impeksyon sa kanilang mga mobile device at datos.

Ang pagbabanta (threat)

Ang MOONSHINE at BADBAZAAR ay mga halimbawa ng mga trojan; mayroon silang mga malicious function na nakatago sa loob ng dapat sana ay gumaganang app na maaaring ma-download mula sa mga app store o online na mga serbisyong file-sharing.

Ang mga app na ito ay idinisenyo upang linlangin ang isang user na i-download at i-install ang mga ito sa isang device. Kapag na-install na ang isang app, gumagamit ito ng mga kahinaan sa device upang magsagawa ng mga hindi awtorisadong function, o maaari itong umasa sa isang user na nagbibigay ng mga permiso sa app na mag-access at mag-download ng impormasyon mula sa device, kabilang ang:

- **datos ng lokasyon kabilang ang real time tracking**
- **access sa microphone at camera**
- **mga message, photo at iba pang mga file na nakaimbak sa device**
- **device information at marami pa**

Pagkatapos ay sinasamantala ng mga actor ang mga lehitimong interes ng mga grupong nasa panganib, upang matukoy at mahawahan ang pinakamaraming biktima hangga't maaari, at makakuha ng access sa kanilang datos. Ang isang paraan para gawin nila ito ay sa pamamagitan ng pagdidisenyo ng mga app na alam nilang makakaakit sa kanilang mga biktima, tulad ng mga app na sumusuporta sa kanilang mga katutubong wika, o naglalaman ng content na partikular sa mga lokasyon gaya ng mga rehiyon ng Tibet ng China o Xinjiang.

Ang mga case study sa pabatid na ito ay nagbibigay ng ilang halimbawa nito, kabilang ang TibetOne at Uyghur Quran apps.

Ang mga actor ay aktibo sa mga online na forum kung saan mayroong user base ng kanilang mga nilalayong biktima, na nagpapalaki ng kanilang tsansa na hawahan ang mga biktima. Napagmasdan silang sadyang nagse-share ng spyware sa mga channel ng Telegram na nauugnay sa Tibet at mga forum ng Reddit. Ang mga case study sa pabatid na ito ay nagbibigay din ng mga halimbawa ng mga pamamaraang ito.

Kadalasang ibinabahagi ang mga malicious app bilang mga standalone na file, gaya ng mga APK file sa Android, na kinakailangang i-download at i-install ng mga user. Sinisikap ng mga actor na gawing mas lehitimo ang kanilang spyware

sa pamamagitan ng pag-upload nito sa mga official app store gaya ng Google Play Store at Apple App Store o sa pamamagitan ng pagdaragdag ng malicious code sa mga dating benign app, bagama't ang mga official store ay may mga security feature at mga proseso ng pag-vet na ginagawang hindi gaanong matagumpay ang taktika na ito. Ginagawa nitong mas ligtas ang mga app mula sa mga official store, ngunit tulad ng ipinakita sa mga case study at sa Ulat ng Banta sa App Store ng NCSC, hindi perpekto ang mga prosesong ito.

Ang pagsunod sa 4 na tip na ito ay makakatulong na protektahan ka mula sa mga banta na nakabalangkas sa pabatid na ito.

Mga case study

Inilalarawan ng dalawang case study na ito kung paano gumagana ang MOONSHINE at BADBAZAAR, at kung paano tina-target ng mga malicious cyber actor ang mga nasa panganib.

Case study one: MOONSHINE

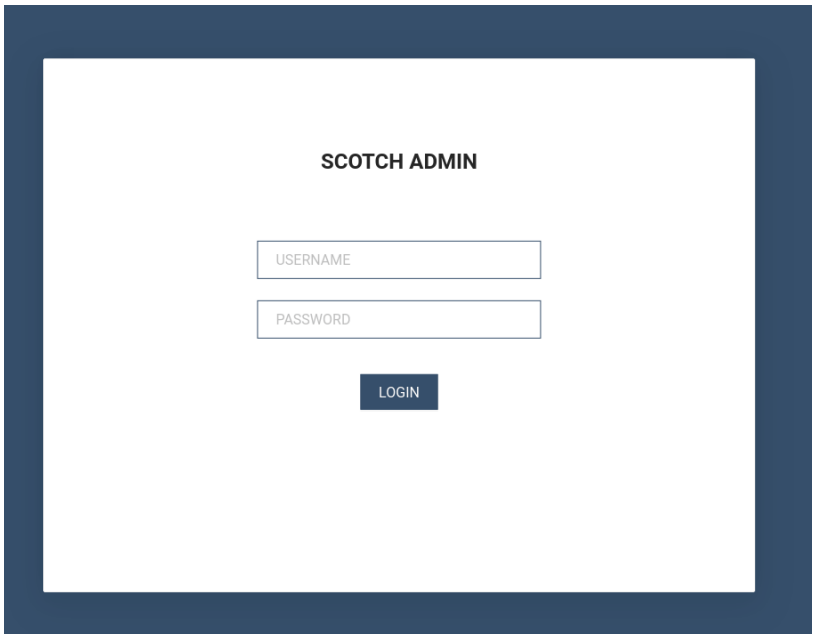
Ang MOONSHINE ay isang Android spyware na iniulat noong 2019 ng Citizen Lab bilang nagta-target ng mga Tibetan group. Ang MOONSHINE ay nagpapanggap bilang isang lehitimong app upang akitin ang mga biktima na i-install ito. Ibinahagi ito sa pamamagitan ng mga channel sa Telegram at mga link na ipinadala sa pamamagitan ng WhatsApp.

Ang MOONSHINE ay may malawak na kakayahan sa pagsubaybay, tulad ng:

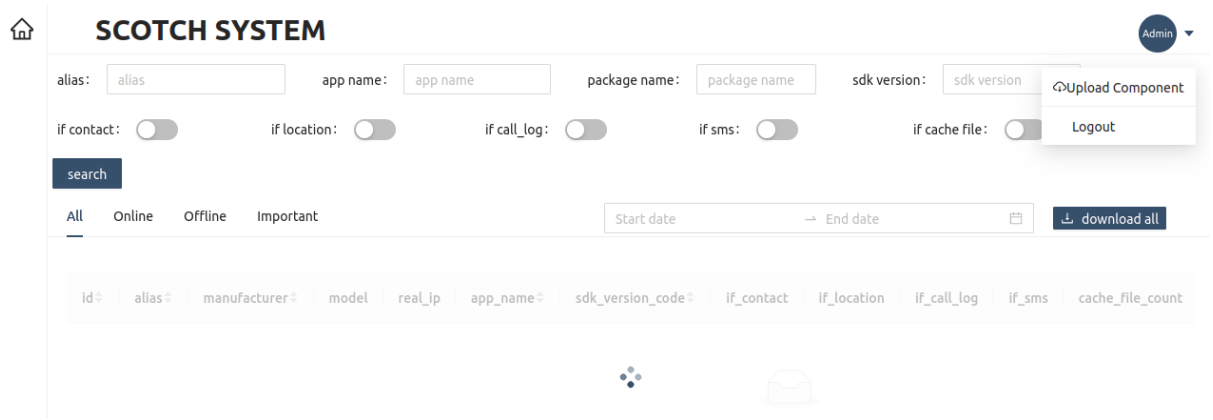
- **datos ng lokasyon kabilang ang real time tracking**
- **live audio at pag-capture ng photo**
- **pag-download ng mga file mula device**
- **pagkuha ng impormasyon sa device**
- **nagpe-play ng audio sa device**

Ang application na ‘ئاۋازلىق قۇرئان**.apk**’, na isinasalin bilang **'Audio Quran.apk'**, ay isang halimbawa kung paano ginagamit ang MOONSHINE upang i-target ang mga Uyghurs. Ang paggamit ng wikang Uyghur sa pangalan ng file, na nagpapahiwatig na isang Quran application, ay malamang na idinisenyo upang umapela sa mga Muslim na Uyghur.

Kapag na-install na, maaaring mangolekta ng impormasyon ang mga malicious cyber actor mula sa mga device ng mga biktima. Ang impormasyong ito ay ina-access sa pamamagitan ng panel ng ‘SCOTCH ADMIN’.



Kapag naka-login, maa-access ng mga actor ang page na ipinapakita sa screenshot sa ibaba. Ang page na ito ay nagpapakita ng mga detalye ng mga nahawaang device at ang antas ng pag-access ng actor sa mga nahawaang device:



Ipinapakita ng malware management panel ang datos na nakolekta, kabilang ang:

- **antas ng pag-access sa device**
- **mga mensaheng SMS**
- **mga call log**
- **datos ng lokasyon**
- **impormasyon sa device**

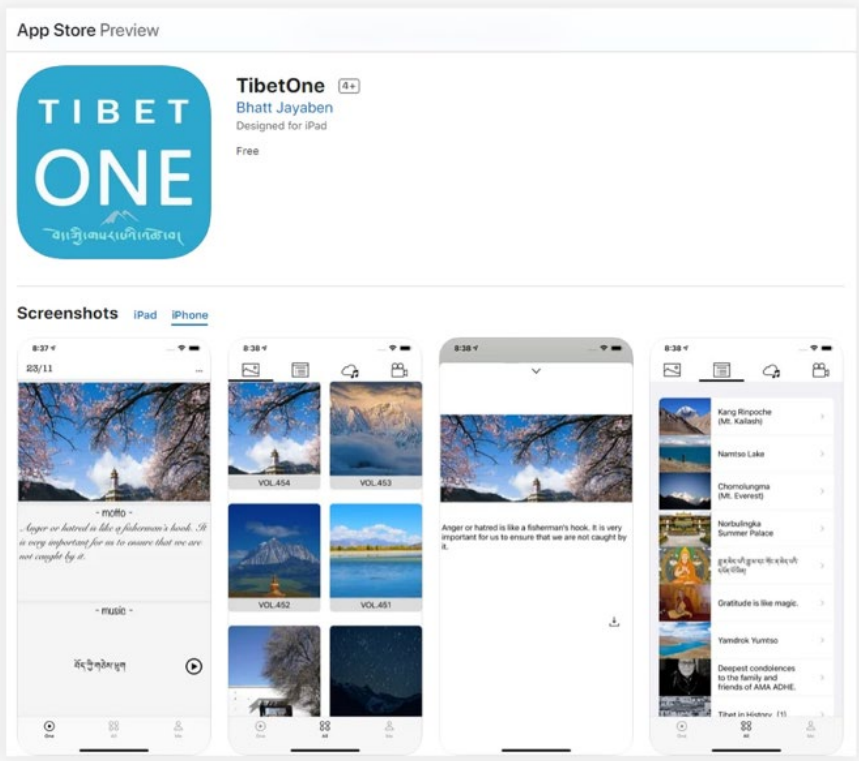
Sa pakikipagtulungan sa Cyber League, binuo ng NCSC ang industriya pag-uulat mula sa Trend Micro upang makahanap ng mga overlap sa pagitan ng MOONSHINE exploitation kit at mga login panel na naglalaman ng 'UPSEC' sa HTML title. Ang buong detalye ay nasa kasamang teknikal na pabatid.

Ayon sa Intelligence Online, ang UPSEC ay isang reference sa 'Sichuan Dianke Network Security Technology Co. Ltd'. Hindi pa napatunayan ng mga ahensyang may akda ang pahayag na ito.

Case study two: BADBAZAAR

Ang BADBAZAAR ay isang mobile malware na may mga variant ng iOS at Android na naka-target sa mga indibidwal na Uyghurs, Tibetans at Taiwanese. Ang malware na ito ay kumalat sa pamamagitan ng mga platform ng social media at mga official app store.

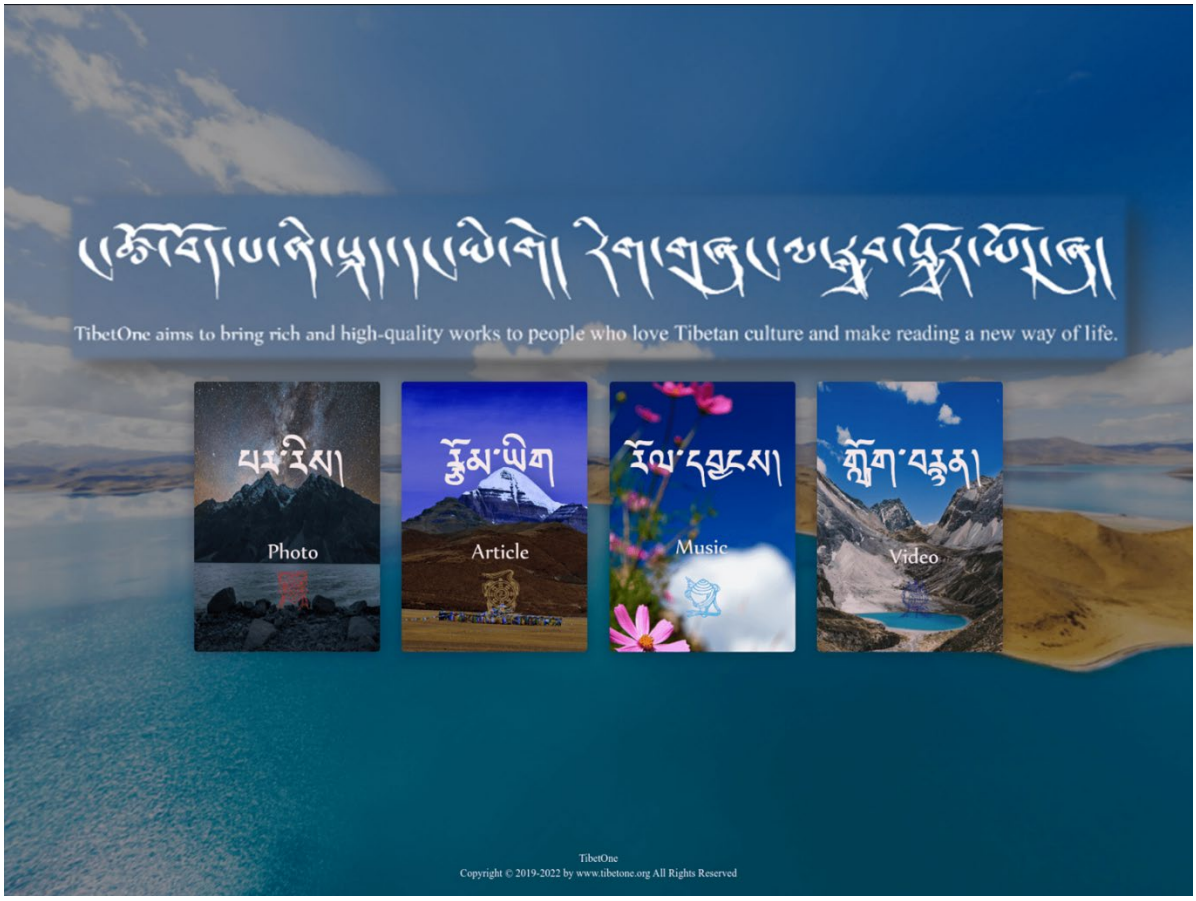
Ginamit ang BADBAZAAR upang i-target ang mga Tibetan sa pamamagitan ng app na '**TibetOne**', gaya ng iniulat ng Lookout at Volexity. Ang **TibetOne** ay isang iOS app na ginawa ng mga malicious actor, na may kakayahang ma-access ang impormasyon sa device at datos ng lokasyon. Na-upload ito sa Apple App Store noong Disyembre 2021 ngunit hindi na available. Upang higit pang maikalat ang malware, in-advertise din ng mga actor ang app sa isang Telegram channel na tinatawag na '**tibetanphone**'.



Larawan 1: TibetOne app page sa Apple App Store. Ang app ay tinanggal na.

Larawan 2: TibetOne gaya ng pagka-share sa mga Telegram channel.

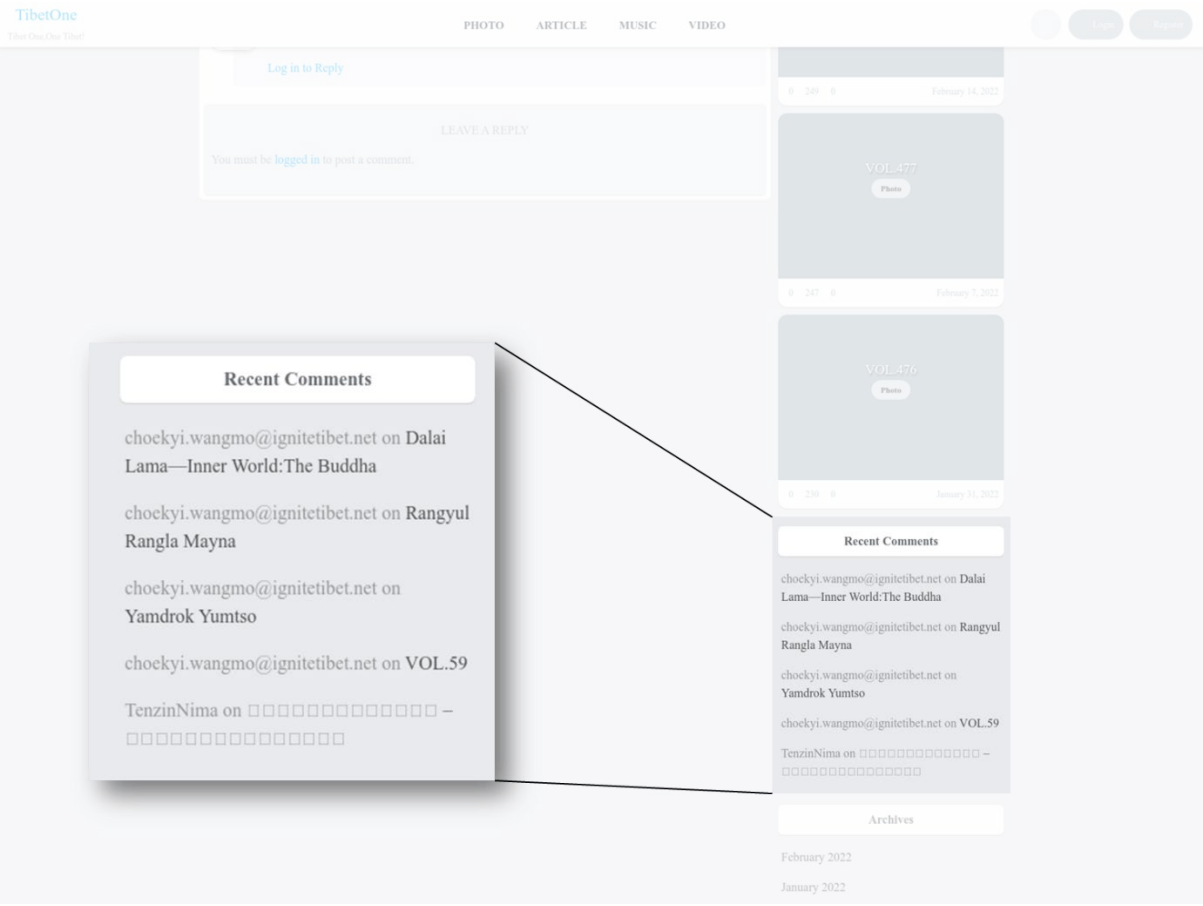
Upang magdagdag ng pagiging lehitimo sa app, bumuo din ang mga actor ng website na tinatawag na **'tibetone[.]org'**, na inilarawan ang sarili bilang *'naghahatid ng mayaman at mataas na kalidad na mga likha sa mga taong mahilig sa kultura ng Tibet at ginagawang bagong paraan ng pamumuhay ang pagbabasa'.*



Larawan 3: Homepage ng 'tibetone[.]org'.

Ang larawang ito ay na-edit upang gawing mas malinaw ang mga nauugnay na seksyon.

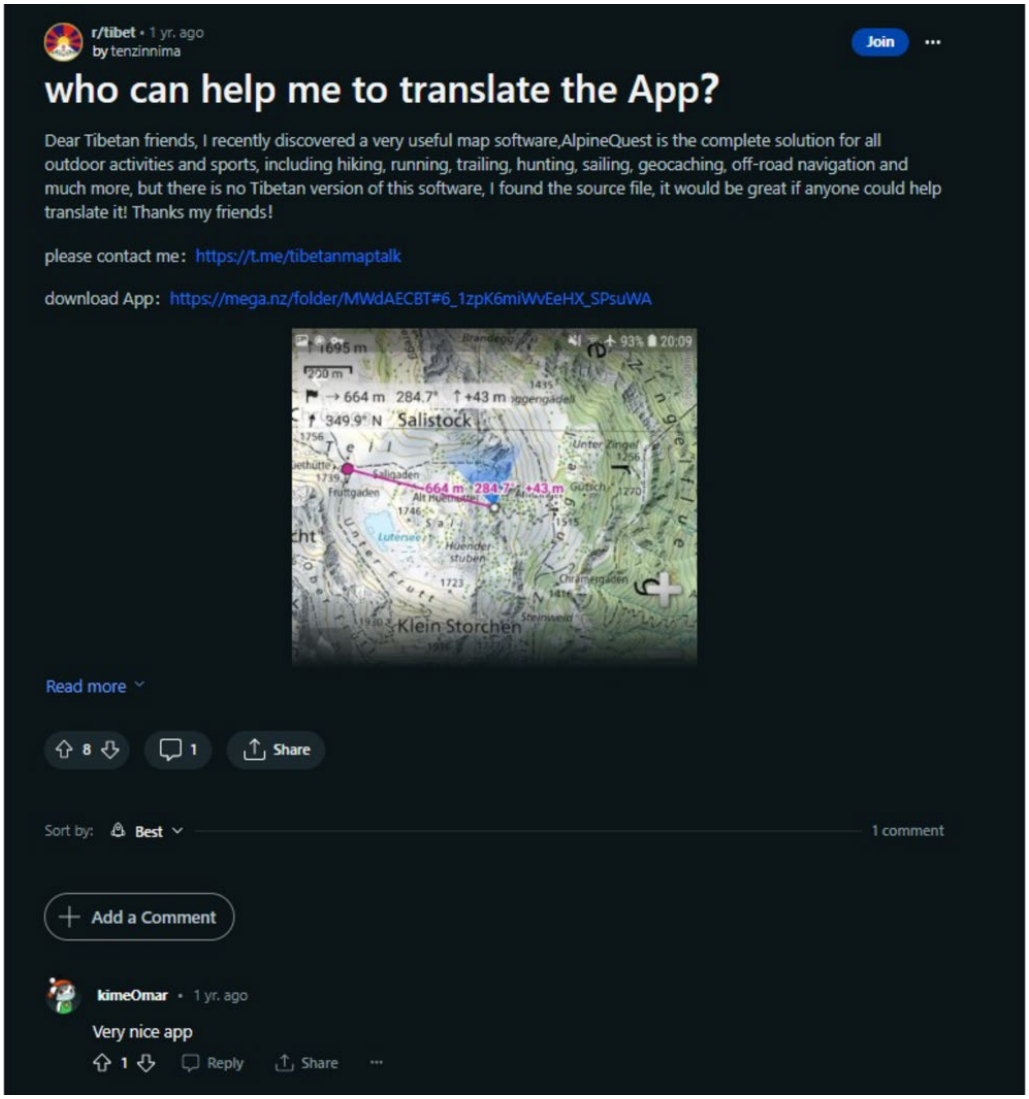
Ang website na ito ay may page para sa mga artikulo na nagpapahintulot sa mga user na mag-iwan ng mga komento. Ang komentong iniwan ng email address na **'choekyi.wangmo@ignitetibet.net',** ay pinaniniwalaang kinokontrol ng malicious actor at malamang na nagpapanggap bilang **'Choekyi Wangmo'** na ang Tibetan Centre of Human Rights and Democracy ay nakalistabilang isang pro-Tibet protestor. Ito ay malamang na isa pang pagtatangka na magbigay ng impresyon na ang app ay tunay na nagtataguyod ng kalayaan ng Tibet.



Larawan 4: 'tibetone[.]org' na page na nagpapakita ng mga komento mula sa mga user na pinaniniwalaang kinokontrol ng malicious actor.

Ang larawang ito ay na-edit upang gawing mas malinaw ang mga nauugnay na seksyon.

Ang '**TenzinNima**' ay isa pang username na nagdagdag ng mga komento sa site na ito. Iniulat ng Volexity na ang username na ito ay ginagamit din sa Reddit upang i-advertise ang Telegram channel na **'Tibetanmaptalk'.** May kasama itong link para mag-download ng malicious sample ng **'AlpineQuest'**, isang navigation app na available sa mga Android device. Ang ibinigay na link sa pag-download ay para sa isang third-party file-sharing service na tinatawag na Mega.



Larawan 5: Reddit post na nag-a-advertise ng malicious application sa pamamagitan ng isang account na pinaniniwalaang kontrolado ng malicious actor.

Napansin din ng Volexity na ang isang user na kilala bilang **'KimeOmar'** na nagkomento sa post ay naobserbahan din na nagbabahagi ng mga malicious app sa isa pang sub-Reddit forum. Ito ay maaaring magpahiwatig na ang mga malicious actor ay gumagamit ng maraming mga profile sa social media upang gawing lehitimo ang kanilang mga post.

Pagtatasa

Gumagamit ang BADBAZAAR at MOONSHINE ng ilang pamamaraan ng social engineering para partikular na i-target ang mga komunidad ng Uyghur, Tibetan at Taiwanese, katulad ng:

- pag-trojanise ng mga app na mahalaga sa mga komunidad na ito, tulad halimbawa ang Uyghur language Quran app ay halos tiyak na iniangkop sa target na biktima
- pagdaragdag ng mga na-trojanise na app na ito sa mga to official app store ay malamang na nagbibigay ng anyo ng pagiging lehitimo, at ang pagbabahagi sa mga group chat ay malamang na nilayon upang samantalahin ang mga pinagkakatiwalaang relasyon sa loob ng mga komunidad na ito

Ang BADBAZAAR at MOONSHINE ay nangongolekta ng datos na tiyak na may halaga sa estado ng China. Bagama't ang BADBAZAAR at MOONSHINE ay naobserbahan na nagta-target ng mga Uyghur, Tibetan at Taiwanese na mga indibidwal, mayroong iba pang malware na nagta-target ng iba pang mga grupo ng minorya sa China. Ang mga mamamayan mula sa mga co-sealing na bansa, sa China at sa ibang bansa, na itinuturing na sumusuporta sa mga paglaban sa mga nagbabanta sa katatagan ng rehimen, ay tiyak na binabantaan ng mobile malware gaya ng BADBAZAAR at MOONSHINE. Ang kakayahan (capability) na mag-capture ng datos ng lokasyon, audio at larawan ay tiyak na nagbibigay ng pagkakataong ipaalam sa hinaharap na pagsubaybay (surveillance) at mga operasyon ng panliligalig sa pamamagitan ng pagbibigay ng real-time na impormasyon sa aktibidad ng target.

Mga hakbang sa mitigasyon para sa mga user ng mobile app

Hinihikayat ng mga ahensyang may akda ang mga sumusunod na kagawian sa seguridad upang maprotektahan laban sa mga banta na inilarawan sa mga case study. Ang mga rekomendasyong ito ay pinagtibay ng gabay sa pinakamahusay na kagawian ng NCSC. Tingnan ang seksyong 'karagdagang mababasa' para sa mga link sa gabay sa pinakamahusay na kagawian para sa mga mambabasa sa Australya at US.

Panatilihing secure ang iyong device

- Mag-download lamang ng mga app mula sa mga **official app store, gaya ng Google's Play Store o Apple's App Store.** Ang Google's Play Store at App Store ng Apple ay nag-i-scan ng software para sa mga virus bago ito gawing available, na nagbibigay sa iyo ng higit na katiyakan na ligtas ang iyong dina-download. Ang mga app mula sa mga pinagkakatiwalaang store ay maaari pa ring magkaroon ng panganib, ngunit ang mga pag-download mula sa iba pang mga mapagkukunan ay maaaring walang anumang mga proteksyon. Ang NCSC ay may ulat ng threat sa mga app store: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Panatilihing up-to-date ang iyong device at app.** Mag-install ng mga update sa iyong app at software ng device sa sandaling maging available ang mga ito. I-on ang 'awtomatikong pag-update' sa mga setting ng iyong device kung available para hindi mo na kailangang tandaan na gawin ito. Tingnan ang gabay ng NCSC tungkol sa pananatiling secure sa online, upang maprotektahan laban sa mga kilalang virus at iba pang uri ng malware. Kadalasang kasama sa mga update ang mga pagpapahusay at bagong feature: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Huwag i-'jailbreak' o 'i-root' ang iyong device** dahil ito ay gumagamit ng unpatched na mga kahinaan upang i-bypass ang mga security control na inilagay. Dahil dito, mas mahina ang device sa mga pag-atake. Tingnan ang gabay ng NCSC: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Pamahalaan ang iyong mga app

- **Suriin ang iyong mga app at ang kanilang mga permiso.** Kung hindi mo na kailangan ng app, tanggalin ito. Kung saan maaari, paghigpitan ang mga permiso ng app upang mabawasan ang pagkakalantad ng datos, dahil ang malware ay kadalasang idinisenyo upang ma-access ang mga protektadong file o peripheral, gaya ng mga camera at mikropono.
  - Paano dapat i-check ang mga permiso ng app para sa mga user ng Apple: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Paano dapat i-check ang mga permiso ng app para sa mga user ng Android: https://support.google.com/android/answer/9431959?hl=en-GB

- **Awtomatikong magpadala ng mga hindi kilalang app sa Google.** Kung isa kang user ng Android at nag-download ng app na hindi mula sa Google's Play Store, maaari mo itong ipadala sa Google sa pamamagitan ng pag-enable sa 'Pagbutihin ang pagtuklas sa nakakapinsalang app' sa mga setting ng app sa Google's Play Store sa ilalim ng 'Play Protect'. Ii-scan nito ang app para sa malware detection na tutulong sa pagprotekta sa mga user. Impormasyon kung paano ito i-set up: https://support.google.com/android/answer/2812853?hl=fil

Gumamit ng mga serbisyo sa cyber

- **Gumamit ng mga serbisyong may reputasyon ng URL bago mag-click sa isang link.** Maaari mong tingnan kung ligtas ang isang link mula sa isang email, text message o saanman sa pamamagitan ng pag-scan muna nito gamit ang mga serbisyo gaya ng Google Transparency Report o Virus Total. Maaari ka ring mag-upload ng mga kahina-hinalang file at app sa isang malware analyzer, gaya ng Virus Total na makakatulong sa pagtukoy kung malicious ang isang file. Tandaan na ang mga serbisyo sa pag-scan (scanning services) ay maaaring gumawa ng mga false negatives.

- **Mag-enrol sa programa ng Google Advanced na Proteksyon.** Ito ay isang libreng serbisyo na idinisenyo upang pangalagaan ang mga indibidwal na gumagamit ng mga serbisyo ng Google (Gmail, Play Store, atbp) na nasa panganib na ma-target. Nagbibigay ang serbisyong ito ng mas mataas na seguridad kapag gumagamit ng mga serbisyo ng Google: https://landing.google.com/advancedprotection/

- **Mag-enrol sa mga karagdagang resilience srvice, kung saan available ang mga ito.** Halimbawa, ang mga indibidwal na may mataas na panganib sa UK ay maaaring maging karapat-dapat para sa mga karagdagang defensive service upang tumulong sa kanilang cyber security. Tingnan ang pagiging kwalipikado at alamin ang higit pa: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Mag-ulat ng mga banta

- **Pagkilala at pag-uulat ng mga pekeng account.** Ang mga malicious na cyber actor ay gumagawa ng mga pekeng account o nagha-hack ng mga totoong account upang isulong ang kanilang mga layunin. Kung pinaghihinalaan mong peke o nakompromiso ang isang account, iulat ito sa platform at i-block ito. Maraming serbisyo ang may proseso para i-verify ang mga account, gaya ng 'mga na-verify na badge' para sa Instagram at Facebook. Makakatulong ito na matukoy kung ang isang account ay tunay. May gabay ang NCSC sa ligtas na paggamit ng social

media na kinabibilangan ng mga detalye kung paano i-verify at iulat ang mga nakompromisong account: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Phishing gamit ang mga scam email, SMS at mga link.** Maaaring siyasatin ng NCSC ang mga kahina-hinalang email address at website. Kung sa tingin mo ay kahina-hinala ang isang site, email o message, maaari mo itong iulat: https://www.ncsc.gov.uk/collection/phishing-scams

Glossary ng NCSC

- **Android**

Ang mobile operating system ng Google, na ginagamit ng ilang tagagawa ng smartphone at tablet.

- **App**

Ang application, o app, ay isang software package na maaaring i-install o paunang i-install ng mga user sa isang device upang magbigay ng karagdagang functionality o content sa kanilang device.

- **Cyber Security**

Ang proteksyon ng mga device, serbisyo at network - at ang impormasyon sa mga ito - mula sa hindi awtorisadong pag-access, pagnanakaw o pinsala.

- **Device**

Computer-based na hardware na pisikal na umiiral, gaya ng desktop computer, smartphone o tablet.

- **iOS**

Ang mobile operating system ng Apple na ginagamit sa suite ng mga mobile device nito.

- **Malware**

Nagmula sa 'malicious software', ang malware ay anumang uri ng software na maaaring makapinsala sa mga computer system, network o device. May kasamang mga virus, ransomware at trojan.

- **Operating system**

Ang pangunahing software na tumatakbo sa mga computer, tablet at smartphone, na kinakailangan upang magpatakbo ng mga karagdagang application at hardware.

- **Phishing**

Mga scam na email o text message na naglalaman ng mga link sa mga website na maaaring naglalaman ng malware, o maaaring linlangin ang mga user na magbunyag ng sensitibong impormasyon (gaya ng mga password) o maglipat ng pera.

- **Spyware**

Isang uri ng malware na nag-i-install sa isang device nang walang pahintulot ng user, nangongolekta ng datos at pagkatapos ay ipinapadala ito sa isang third party.

- **Social media**

Mga website at app, gaya ng Facebook, X at Instagram, na nagbibigay-daan sa mga tao na magbahagi at tumugon sa user-generated content (mga text post, larawan at video).

- **Smartphone**

Mga modernong mobile phone na gumagampan ng kumplikadong functionality kabilang ang mga may Android at iOS operating system.

- **Trojan**

Isang uri ng malware, na itinago bilang lehitimong software, na ginagamit upang makakuha ng hindi awtorisadong pag-access sa device ng biktima.

- **URL**

Uniform Resource Locator. Isang address sa world wide web gaya ng domain name (halimbawa www.bbc.co.uk).

- **Virus**

Isang uri ng malware na idinisenyo upang makahawa sa mga lehitimong software program at gumagaya sa mga network kapag na-activate ang mga program na iyon.

Karagdagang pagbabasa

Patnubay mula sa Australian Cyber Security Center

- Mag-ulat ng cybercrime, insidente o kahinaan
- Paano i-secure ang iyong mga device
- I-secure ang iyong mobile phone
- Phishing
- Mga Scam
- I-secure ang iyong social media
- Mga tip sa seguridad para sa social media at mga messaging app

Patnubay mula sa UK NCSC at NPSA

- Pagtatanggol sa Demokrasya
- Social Media: paano ito gamitin nang ligtas
- Gabay sa Seguridad ng Device para sa mga organisasyon kabilang ang mobile
- Ulat ng threat sa mga application store.
- Personal na kaligtasan at seguridad para sa mga indibidwal na may mataas na peligro

Patnubay mula sa US NSA

- Mga Pinakamahuhusay na Kagawian sa Mobile Device

Pagtatatwa

Pakitandaan na ang pabatid na ito ay nagbibigay ng impormasyon na napatunayan sa panahon ng paglalathala.

Ang ulat na ito ay kumukuha ng impormasyong nagmula sa ahensya ng pag-akda at mga pinagkukunan ng industriya. Ang anumang mga natuklasan at rekomendasyong ginawa ay hindi ibinigay na may layuning iwasan ang lahat ng panganib at ang pagsunod sa mga rekomendasyon ay hindi mag-aalis ng lahat ng naturang panganib. Ang pagmamay-ari ng mga panganib sa impormasyon ay nananatili sa may-kinalamang may-ari ng system sa lahat ng oras.

Sa UK, ang impormasyong ito ay hindi exempt sa ilalim ng Freedom of Information Act 2000 (FOIA) at maaaring maging exempt sa ilalim ng iba pang batas sa impormasyon sa UK.

Sumangguni sa anumang mga pagtatanong sa FOIA sa ncscinfoleg@ncsc.gov.uk.

Annex: Naobserbahan ang mga sample ng MOONSHINE at BADBAZAAR

Inililista ng talahanayang ito ang mga app na ginamit sa MOONSHINE at BADBAZAAR campaign sa nakalipas na dalawang taon.

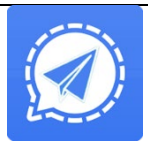
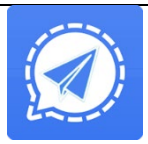
Marami sa mga app na ito ay nagpapakita ng malinaw na pagkakatulad sa mga naitatag na app. Ito ay malamang na isang sinadyang pamamaraan ng actor upang 'gayahin' ang mga kilalang brand.

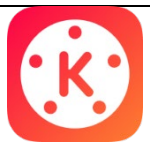
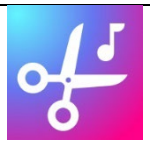
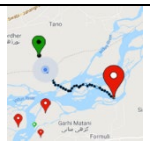
Mahalagang tandaan, ang pangalan ng app, pangalan ng package, at icon ay maaaring lahat gayahin o tumugma sa tunay na application at samakatuwid ay hindi dapat gamitin nang eksklusibo upang matukoy kung ang isang device ay nahawaan.

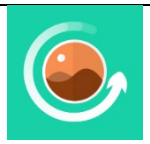
Tulad ng kasama sa seksyon ng mga pagpapagaan o mitigasyon, maaari kang magpadala ng mga app sa iyong Android device sa Google sa pamamagitan ng pag-enable sa 'Improve harmful app detection' (Pagbutihin ang pagtukoy sa nakakapinsalang ng app), na mag-i-scan ng mga app sa iyong device na na-install mula sa labas ng Play Store.

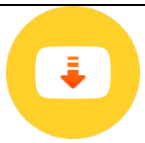
App title	Pangalan ng package	App icon
99 na mga Pangalan ni ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	

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	

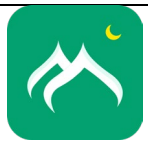
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	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	

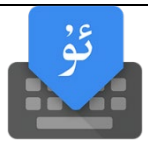
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
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