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

Saran

BADBAZAAR dan MOONSHINE: Spyware menargetkan kelompok Uighur, Taiwan, dan Tibet serta aktor masyarakat sipil

9 April 2025

BADBAZAAR dan MOONSHINE: Spyware menargetkan kelompok Uighur, Taiwan, dan Tibet serta aktor masyarakat sipil

NCSC dan para mitra menerbitkan informasi baru dan langkah-langkah mitigasi bagi mereka yang berisiko tinggi terhadap dua varian spyware.

Ringkasan

Dengan dukungan dari Cyber League Inggris Raya, penasihat ini telah diproduksi bersama oleh Pusat Keamanan Siber Nasional (NCSC UK) dan mitra internasional:

- **Pusat Keamanan Siber Australia, bagian dari Direktorat Sinyal Australia**
- **Pusat Keamanan Siber Kanada, bagian dari Badan Keamanan Komunikasi**
- **Badan Intelijen Federal Jerman**
- **Kantor Federal Jerman untuk Perlindungan Konstitusi**
- **Pusat Keamanan Siber Nasional Selandia Baru, bagian dari Biro Keamanan Komunikasi Pemerintah**
- **Biro Investigasi Federal Amerika Serikat**
- **Badan Keamanan Nasional Amerika Serikat**

Tujuannya adalah untuk meningkatkan kesadaran tentang meningkatnya ancaman yang ditimbulkan oleh pelaku kejahatan siber terhadap individu yang terkait dengan berbagai topik termasuk Taiwan, Tibet, Daerah Otonomi Uighur Xinjiang, gerakan demokrasi, dan Falun Gong.

Penasihat ini mencakup dua studi kasus yang merinci berbagai teknik yang digunakan oleh pelaku kejahatan siber dengan menggunakan perangkat mata-mata yang dikenal sebagai BADBAZAAR dan MOONSHINE untuk menargetkan data pada perangkat seluler termasuk telepon pintar yang dapat menarik minat negara Tiongkok. Hal ini juga memberikan petunjuk untuk membantu individu melindungi diri mereka sendiri, perangkat mereka, dan data mereka.

Bersamaan dengan nasihat ini, NCSC telah menerbitkan detail teknis lengkap dengan panduan terpisah.

Siapa yang berisiko?

Badan penyusun dan mitra industri telah mengamati bahwa BADBAZAAR dan MOONSHINE secara khusus menargetkan individu yang terkait dengan topik yang dianggap oleh negara Tiongkok sebagai ancaman terhadap otoritas domestik, ambisi, dan reputasi global mereka. Mereka yang paling berisiko termasuk, tetapi tidak terbatas pada, siapa pun yang terkait dengan:

- **Kemerdekaan Taiwan**
- **Tibetan Prayer**
- **Muslim Uighur dan etnis minoritas lainnya di atau dari Daerah Otonomi Uighur Xinjiang di Tiongkok**
- **advokasi demokrasi (termasuk Hong Kong)**
- **gerakan spiritual Falun Gong**

Ini termasuk organisasi non-pemerintah (LSM), jurnalis, bisnis, dan individu yang mengadvokasi, mengidentifikasi diri dengan, atau mewakili kelompok-kelompok ini. Cara penyebaran spyware ini secara daring yang tidak pandang bulu juga berarti ada risiko bahwa infeksi dapat menyebar ke luar korban yang dituju.

Nasihat ini bertujuan untuk membantu mereka yang berisiko menanggapi secara efektif ancaman khusus dari spyware BADBAZAAR dan MOONSHINE. Mitigasi yang disarankan melengkapi saran keamanan siber yang lebih luas dan tidak boleh dianggap terpisah.

Dengan mengikuti panduan yang dirujuk dalam nasihat ini, pengguna dapat mengurangi risiko infeksi pada perangkat seluler dan data mereka.

Ancaman

MOONSHINE dan BADBAZAAR adalah contoh trojan; keduanya memiliki fungsi jahat yang tersembunyi di dalam aplikasi yang berfungsi dengan baik yang dapat diunduh dari toko aplikasi atau layanan berbagi berkas daring.

Aplikasi ini dirancang untuk mengelabui pengguna agar mengunduh dan memasangnya di perangkat. Setelah aplikasi dipasang, aplikasi tersebut menggunakan kerentanan pada perangkat untuk menjalankan fungsi yang tidak sah, atau mungkin mengandalkan pengguna untuk memberikan izin aplikasi guna mengakses dan mengunduh informasi dari perangkat, termasuk:

- **data lokasi termasuk pelacakan waktu nyata**
- **akses ke mikrofon dan kamera**
- **pesan, foto, dan berkas lain yang tersimpan di perangkat**
- **informasi perangkat dan lainnya**

Para pelaku kemudian mengeksploitasi kepentingan sah kelompok berisiko, untuk mengidentifikasi dan menginfeksi sebanyak mungkin korban, dan mendapatkan akses ke data mereka. Salah satu cara mereka melakukannya adalah dengan merancang aplikasi yang mereka tahu akan menarik bagi korbannya, seperti aplikasi yang mendukung bahasa asli mereka, atau berisi konten khusus untuk lokasi seperti wilayah Tibet di Tiongkok atau Xinjiang.

Studi kasus dalam nasihat ini memberikan beberapa contohnya, termasuk aplikasi TibetOne dan Uyghur Quran.

Para pelaku aktif di forum daring tempat terdapat basis pengguna korban yang mereka tuju, yang memaksimalkan peluang mereka untuk menginfeksi korban. Mereka telah diamati dengan sengaja membagikan spyware di saluran Telegram terkait Tibet dan forum Reddit. Studi kasus dalam nasihat ini juga memberikan contoh metode ini.

Aplikasi berbahaya sering dibagikan sebagai file mandiri, seperti file APK di Android, yang harus diunduh dan diinstal oleh pengguna. Para pelaku mencoba membuat spyware mereka tampak lebih sah dengan mengunggahnya ke toko aplikasi resmi seperti Google Play Store dan Apple App Store atau dengan menambahkan kode berbahaya ke aplikasi yang sebelumnya tidak berbahaya, meskipun toko resmi memiliki fitur keamanan dan proses pemeriksaan yang membuat taktik ini kurang berhasil. Hal ini membuat aplikasi dari toko resmi lebih aman, tetapi seperti yang ditunjukkan dalam studi kasus dan Laporan Ancaman App Store NCSC, proses ini tidak sempurna.

Mengikuti 4 kiat ini dapat membantu melindungi Anda dari ancaman yang diuraikan dalam nasihat ini.

Untuk saran yang lebih terperinci, lihat bagian mitigasi.

Studi kasus

Kedua studi kasus ini menggambarkan cara kerja MOONSHINE dan BADBAZAAR, dan bagaimana pelaku kejahatan siber menargetkan mereka yang paling berisiko.

Studi kasus satu: MOONSHINE

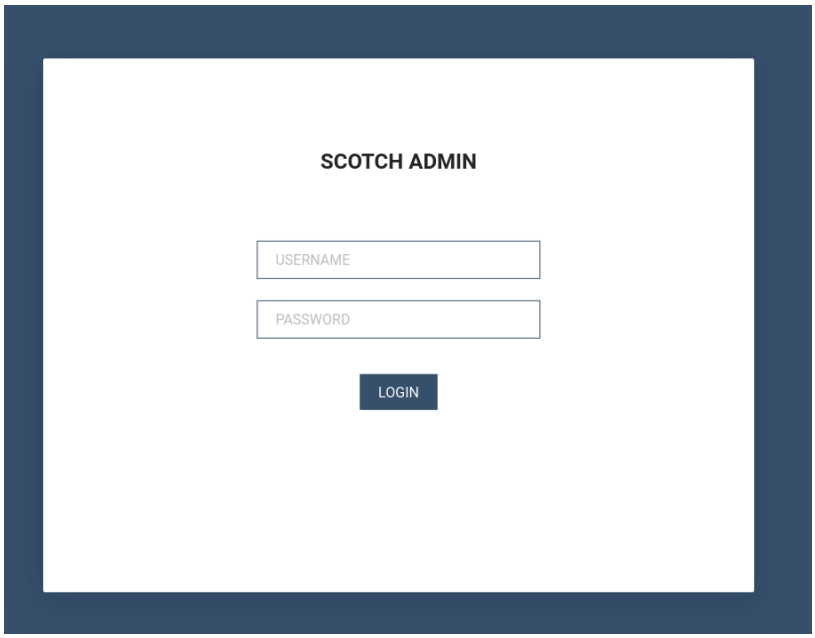
MOONSHINE adalah spyware Android yang dilaporkan pada tahun 2019 oleh Citizen Lab yang menargetkan kelompok Tibet. MOONSHINE menyamar sebagai aplikasi sah untuk memikat korban agar menginstalnya. Aplikasi ini telah dibagikan melalui saluran Telegram dan tautan yang dikirim melalui WhatsApp.

MOONSHINE memiliki kemampuan pengawasan yang luas, seperti:

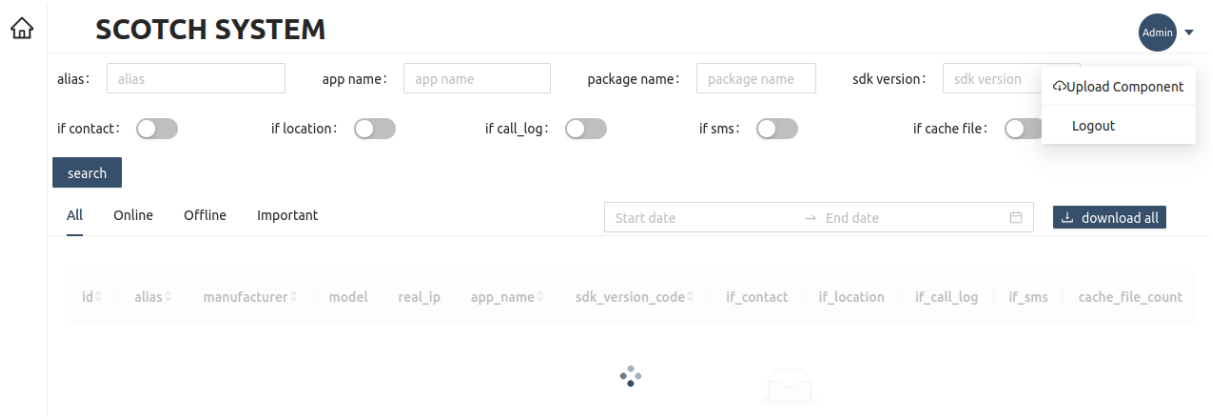
- **data lokasi termasuk pelacakan waktu nyata**
- **pengambilan audio dan foto secara langsung**
- **pengunduhan file dari perangkat**
- **pengambilan informasi perangkat**
- **pemutaran audio pada perangkat**

Aplikasi '**ئاۋازلىق قۇرئان.apk**', yang diterjemahkan menjadi '**Audio Quran.apk**', adalah contoh bagaimana MOONSHINE digunakan untuk menargetkan warga Uyghur. Penggunaan bahasa Uighur dalam nama berkas, yang menunjukkan aplikasi Al-Quran, kemungkinan dirancang untuk menarik perhatian Muslim Uighur.

Setelah terinstal, pelaku kejahatan siber dapat mengumpulkan informasi dari perangkat korban. Informasi ini diakses melalui panel 'SCOTCH ADMIN'.



Setelah masuk, pelaku dapat mengakses halaman yang ditunjukkan pada gambar di bawah. Halaman ini menampilkan detail perangkat yang terinfeksi dan tingkat akses yang dimiliki pelaku terhadap perangkat yang terinfeksi:



Panel manajemen malware menunjukkan data yang dikumpulkan, termasuk:

- **tingkat akses ke perangkat**
- **pesan SMS**
- **log panggilan**
- **data lokasi**
- **informasi perangkat**

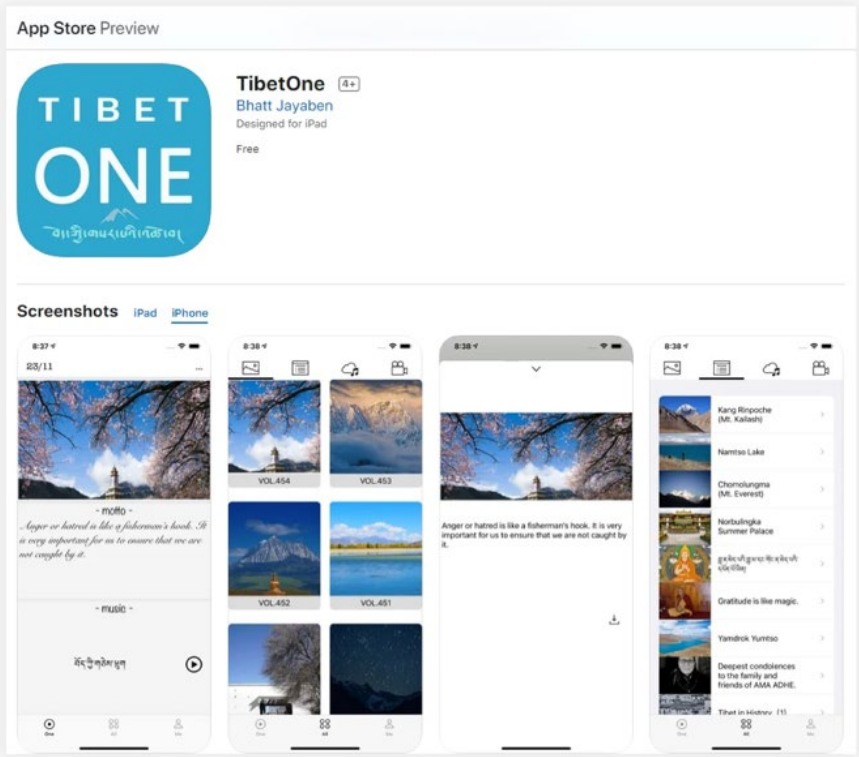
Dalam kerja samanya dengan Cyber League, NCSC telah mengembangkan pelaporan dari Trend Micro industri untuk menemukan tumpang tindih antara perangkat eksploitasi MOONSHINE dan panel login yang memuat 'UPSEC' dalam judul HTML. Detail selengkapnya ada pada nasihat teknis yang disertakan.

Menurut Intelligence Online, UPSEC adalah referensi ke 'Sichuan Dianke Network Security Technology Co. Ltd'. Badan penyusun pernyataan ini belum memverifikasinya.

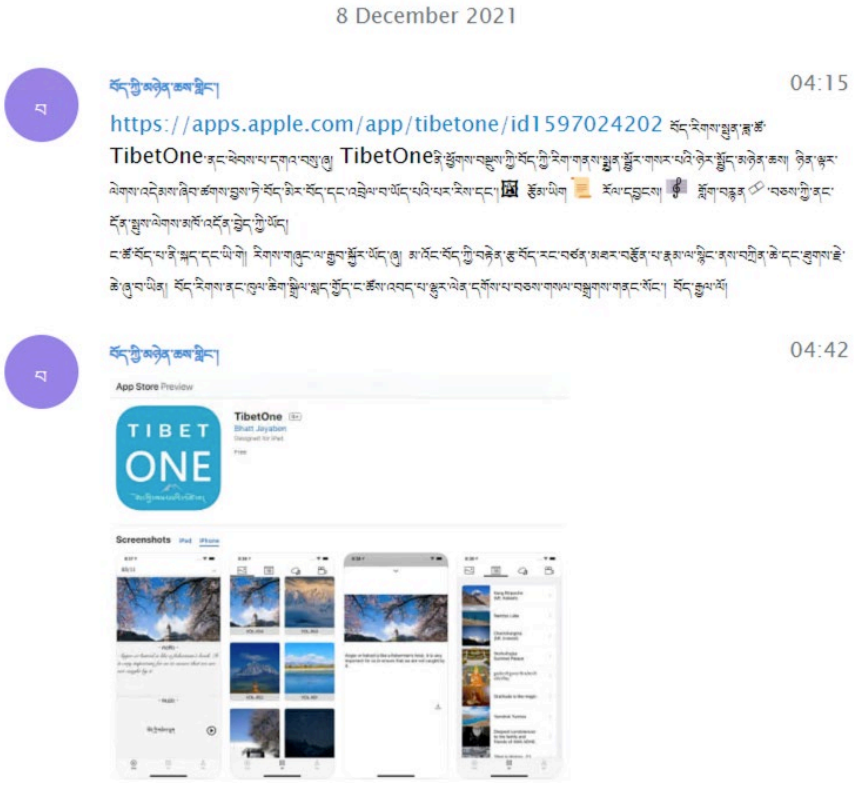
Studi kasus kedua: BADBAZAAR

BADBAZAAR adalah malware seluler dengan varian iOS dan Android yang telah menargetkan warga Uighur, Tibet, dan Taiwan. Malware ini telah menyebar melalui platform media sosial dan toko aplikasi resmi.

BADBAZAAR telah digunakan untuk menargetkan warga Tibet melalui aplikasi '**TibetOne**', sebagaimana dilaporkan oleh Lookout dan Volexity. **TibetOne** adalah aplikasi iOS yang dibuat oleh pelaku kejahatan, dengan kemampuan untuk mengakses informasi perangkat dan data lokasi. Aplikasi ini diunggah ke Apple App Store pada bulan Desember 2021 tetapi tidak lagi tersedia. Untuk menyebarkan malware lebih jauh, para pelaku juga mengiklankan aplikasi tersebut di saluran Telegram yang disebut '**tibetanphone**'.

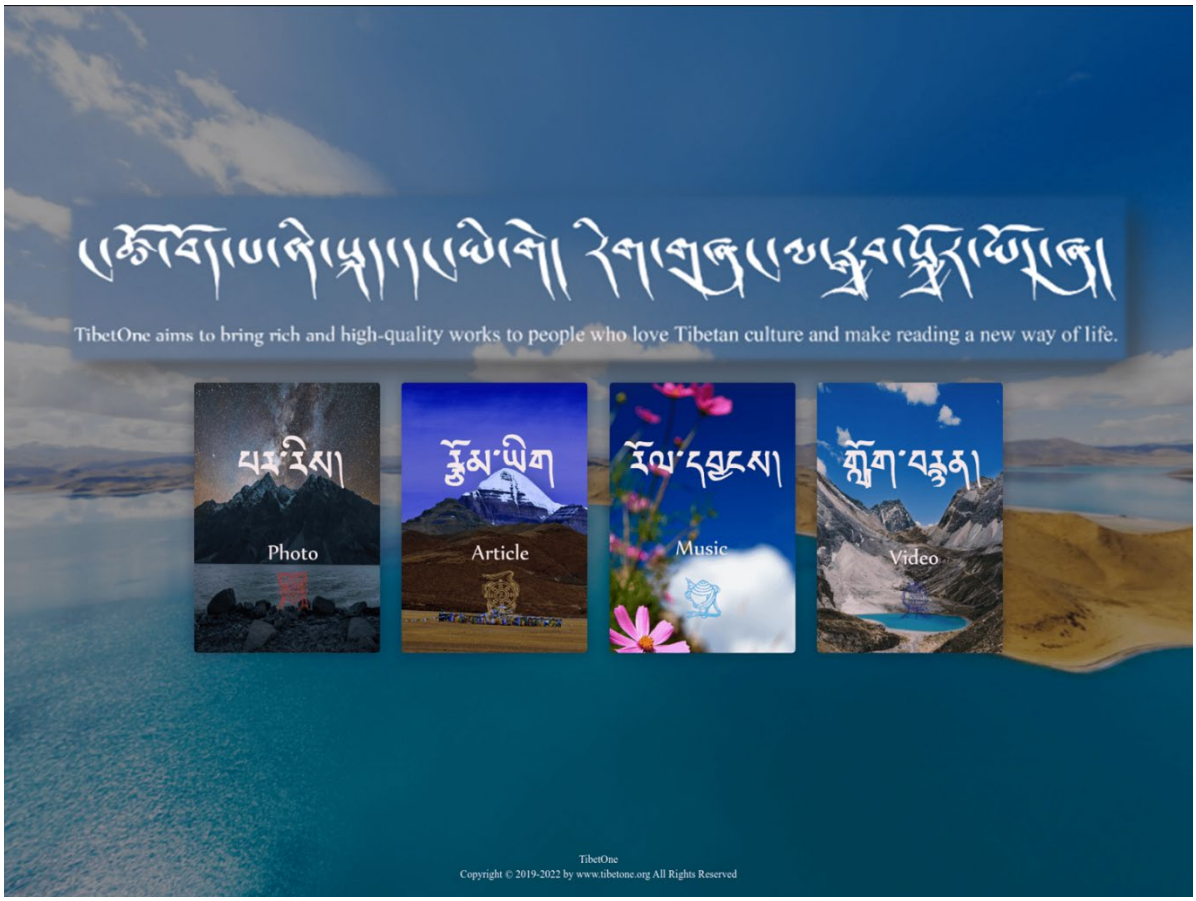


Gambar 1: Halaman aplikasi TibetOne di Apple App Store. Aplikasi tersebut kini telah dihapus.



Gambar 2: TibetOne sebagaimana dibagikan di saluran Telegram.

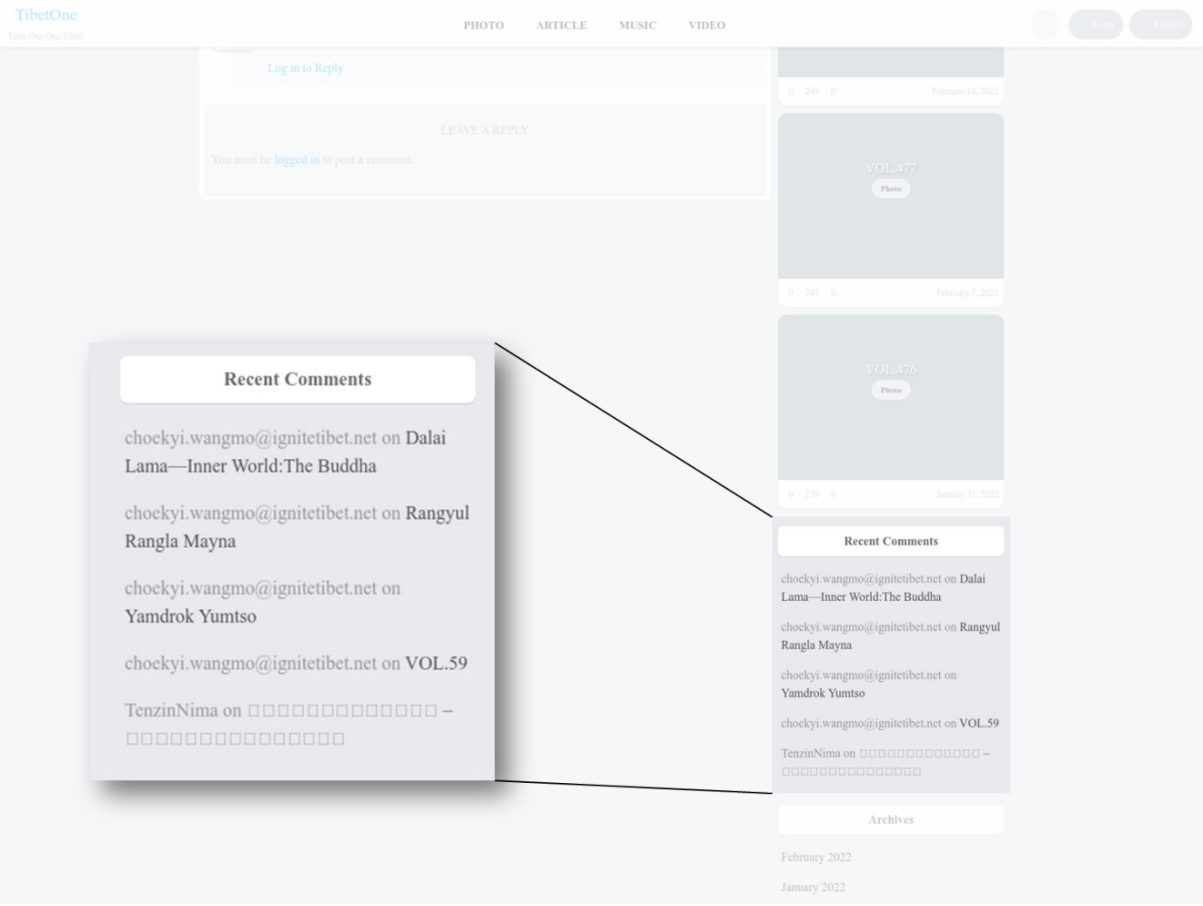
Agar aplikasi tampak sah, para pelaku juga mengembangkan satu situs web yang disebut '**tibetone[.]org**', yang menggambarkan diri sebagai *'memberikan karya luas dan berkualitas tinggi kepada orang-orang yang mencintai budaya Tibet dan menjadikan membaca cara hidup baru*'.



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

Gambar ini telah diedit untuk memperjelas bagian-bagian yang relevan.

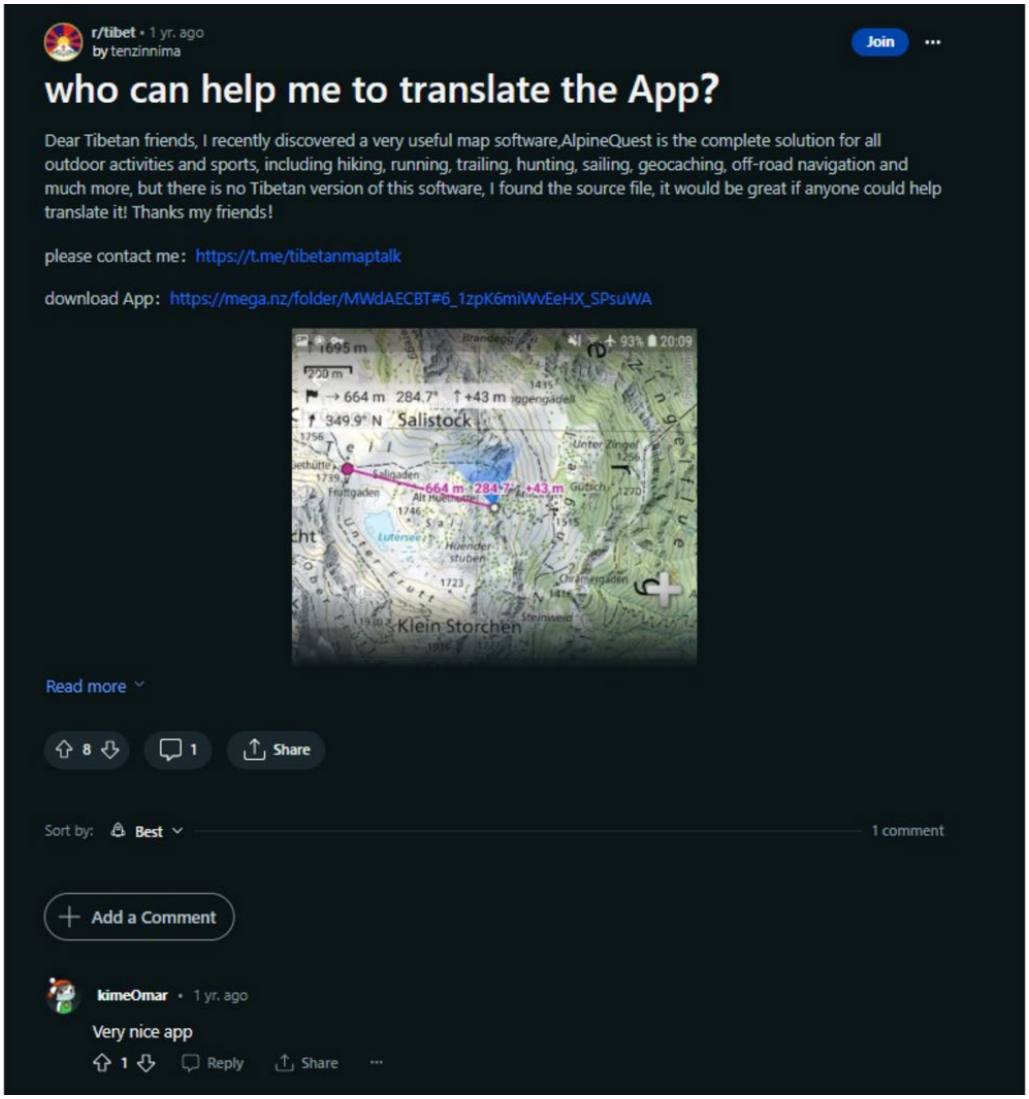
Situs web ini memiliki halaman untuk artikel yang memungkinkan pengguna untuk meninggalkan komentar. Komentar yang ditinggalkan oleh alamat email **'choekyi.wangmo@ignitetibet.net'**, diyakini dikendalikan oleh pelaku kejahatan dan kemungkinan menyamar sebagai **'Choekyi Wangmo'** yang oleh Pusat Hak Asasi Manusia dan Demokrasi Tibet disebut sebagai pengunjuk rasa pro-Tibet. Ini mungkin merupakan upaya lain untuk memberikan kesan bahwa aplikasi tersebut benar-benar menganjurkan kemerdekaan Tibet.



Gambar 4: Halaman 'tibetone[.]org' menampilkan komentar dari pengguna yang diyakini dikendalikan oleh pelaku kejahatan.

Gambar ini telah diedit untuk memperjelas bagian-bagian yang relevan.

'**TenzinNima**' adalah nama pengguna lain yang telah menambahkan komentar di situs ini. Volexity telah melaporkan bahwa nama pengguna ini juga digunakan di Reddit untuk mengiklankan saluran Telegram '**Tibetanmaptalk**'. Termasuk tautan untuk mengunduh sampel berbahaya dari '**AlpineQuest**', sebuah aplikasi navigasi yang tersedia di perangkat Android. Tautan unduhan yang disediakan adalah untuk layanan berbagi berkas pihak ketiga yang disebut Mega.



Gambar 5: Postingan Reddit yang mengiklankan aplikasi berbahaya berdasarkan akun yang diyakini dikendalikan oleh pelaku kejahatan.

Volexity juga mencatat bahwa seorang pengguna yang dikenal sebagai '**KimeOmar**' yang mengomentari unggahan tersebut juga terlihat membagikan aplikasi berbahaya di forum sub-Reddit lainnya. Hal ini dapat menunjukkan bahwa pelaku kejahatan menggunakan beberapa profil media sosial untuk membuat postingan mereka tampak sah.

Penilaian

BADBAZAAR dan MOONSHINE menggunakan beberapa metode rekayasa sosial untuk secara khusus menargetkan komunitas Uighur, Tibet, dan Taiwan, yaitu:

- trojanisasi aplikasi yang menarik bagi komunitas ini, seperti aplikasi Al-Qur'an berbahasa Uighur, hampir pasti disesuaikan dengan basis korban yang menjadi target
- penambahan aplikasi Trojan ini ke toko aplikasi resmi kemungkinan besar memberikan kesan legitimasi, dan berbagi dalam obrolan grup kemungkinan besar dimaksudkan untuk mengeksploitasi hubungan tepercaya dalam komunitas ini

BADBAZAAR dan MOONSHINE mengumpulkan data yang hampir pasti akan berharga bagi negara Tiongkok. Meskipun BADBAZAAR dan MOONSHINE telah diamati menargetkan orang Uighur, Tibet, dan Taiwan, ada malware lain yang menargetkan kelompok minoritas lain di Tiongkok. Warga negara dari negara-negara yang ikut menyegel, di Tiongkok dan luar negeri, yang dianggap mendukung gerakan yang mengancam stabilitas rezim, hampir pasti berada di bawah ancaman malware seluler seperti BADBAZAAR dan MOONSHINE. Kemampuan untuk menangkap data lokasi, audio, dan foto hampir pasti memberikan peluang untuk menginformasikan operasi pengawasan dan pelecehan di masa mendatang dengan memberikan informasi waktu nyata tentang aktivitas target.

Langkah-langkah mitigasi bagi pengguna aplikasi seluler

Badan penyusun menganjurkan praktik keamanan berikut untuk melindungi dari ancaman yang dijelaskan dalam studi kasus. Rekomendasi ini didukung oleh panduan praktik terbaik NCSC. Lihat bagian 'bacaan lebih lanjut' untuk tautan ke panduan praktik terbaik bagi pembaca di Australia dan AS.

Jaga keamanan perangkat Anda

- **Unduh aplikasi hanya dari toko aplikasi resmi, seperti Google Play Store atau Apple App Store.** Play Store milik Google dan App Store milik Apple memindai perangkat lunak untuk mencari virus sebelum menyediakannya, sehingga Anda lebih yakin bahwa apa yang Anda unduh aman. Aplikasi dari toko tepercaya mungkin masih mengandung risiko, tetapi unduhan dari sumber lain mungkin tidak memiliki perlindungan sama sekali. NCSC memiliki laporan ancaman pada toko aplikasi: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Selalu perbarui perangkat dan aplikasi Anda.** Instal pembaruan untuk aplikasi dan perangkat lunak perangkat Anda segera setelah tersedia. Aktifkan 'pembaruan otomatis' di pengaturan perangkat Anda jika tersedia sehingga Anda tidak perlu mengingat untuk melakukannya. Lihat panduan NCSC tentang cara tetap aman saat daring, untuk melindungi diri dari virus yang dikenal dan berbagai jenis malware lainnya. Pembaruan sering kali mencakup penyempurnaan dan fitur baru: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Jangan melakukan 'jailbreak' atau 'root' pada perangkat Anda** karena hal ini menggunakan kerentanan yang belum di-patch untuk melewati kontrol keamanan yang diterapkan. Hal ini membuat perangkat lebih rentan terhadap serangan. Lihat panduan NCSC: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Kelola aplikasi Anda

- **Tinjau aplikasi Anda dan izinnya.** Jika Anda tidak lagi membutuhkan aplikasi tersebut, hapus saja. Jika memungkinkan, batasi izin aplikasi untuk meminimalkan paparan data, karena malware sering kali dirancang untuk mengakses file atau periferal yang dilindungi, seperti kamera dan mikrofon.
  - Cara memeriksa izin aplikasi untuk pengguna Apple: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Cara memeriksa izin aplikasi untuk pengguna Android: https://support.google.com/android/answer/9431959?hl=en-GB

- **Kirim aplikasi yang tidak dikenal ke Google secara otomatis.** Jika Anda adalah pengguna Android dan telah mengunduh aplikasi yang bukan dari Google Play Store, Anda dapat mengirimkannya ke Google dengan mengaktifkan 'Tingkatkan deteksi aplikasi berbahaya' di setelan aplikasi Google Play Store di bawah 'Play Protect'. Ini akan memindai aplikasi untuk mendeteksi malware yang membantu melindungi pengguna. Informasi tentang cara mengaturnya: https://support.google.com/android/answer/2812853?hl=en-GB

Memanfaatkan layanan siber

- **Gunakan layanan reputasi URL sebelum mengklik tautan.** Anda dapat memeriksa apakah tautan dari email, pesan teks, atau tempat lain aman dengan memindainya terlebih dahulu menggunakan layanan seperti Google Transparency Report atau Virus Total. Anda juga dapat mengunggah file dan aplikasi yang mencurigakan ke penganalisis malware, seperti Virus Total yang dapat membantu mendeteksi apakah suatu file berbahaya. Ketahuilah bahwa layanan pemindaian dapat menghasilkan hasil negatif palsu.

- **Daftar dalam program Perlindungan Lanjutan Google.** Ini adalah layanan gratis yang dirancang untuk melindungi individu yang menggunakan layanan Google (Gmail, Play Store, dll) yang berisiko menjadi sasaran. Layanan ini memberikan keamanan yang lebih tinggi saat menggunakan layanan Google: https://landing.google.com/advancedprotection/

- **Daftar di layanan ketahanan tambahan, jika tersedia.** Misalnya, individu berisiko tinggi di Inggris Raya mungkin memenuhi syarat untuk layanan pertahanan ekstra guna membantu keamanan siber mereka. Periksa kelayakan dan cari tahu selengkapnya: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Laporkan ancaman

- **Mengidentifikasi dan melaporkan akun palsu.** Pelaku kejahatan siber membuat akun palsu atau meretas akun asli untuk mencapai tujuan mereka. Jika Anda mencurigai suatu akun palsu atau telah disusupi, laporkan ke platform tersebut dan blokir. Banyak layanan memiliki proses untuk memverifikasi akun, seperti 'lencana terverifikasi' untuk Instagram dan Facebook. Ini dapat membantu mengidentifikasi bahwa suatu akun asli. NCSC memiliki panduan tentang penggunaan media sosial yang aman yang mencakup perincian tentang cara memverifikasi dan melaporkan akun yang telah disusupi: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Phishing menggunakan email, SMS, dan tautan penipuan.** NCSC dapat menyelidiki alamat email dan situs web yang mencurigakan. Jika menurut Anda suatu situs, email, atau pesan mencurigakan, Anda dapat melaporkannya: https://www.ncsc.gov.uk/collection/phishing-scams

Glosarium NCSC

- **Android**

Sistem operasi seluler Google, yang digunakan oleh beberapa produsen ponsel pintar dan tablet.

- **Aplikasi**

Aplikasi, atau app, adalah paket perangkat lunak yang dapat diinstal atau telah diinstal sebelumnya oleh pengguna pada perangkat untuk menyediakan fungsionalitas atau konten tambahan pada perangkat mereka.

- **Keamanan Siber**

Perlindungan perangkat, layanan, dan jaringan - serta informasi di dalamnya - dari akses, pencurian, atau kerusakan yang tidak sah.

- **Perangkat**

Perangkat keras berbasis komputer yang ada secara fisik, seperti komputer desktop, ponsel pintar, atau tablet.

- **iOS**

Sistem operasi seluler Apple yang digunakan pada perangkat selulernya.

- **Malware**

Berasal dari 'malicious software', malware adalah jenis perangkat lunak apa pun yang dapat merusak sistem, jaringan, atau perangkat komputer. Termasuk virus, ransomware, dan trojan.

- **Sistem operasi**

Perangkat lunak dasar yang berjalan pada komputer, tablet, dan telepon pintar, yang diperlukan untuk menjalankan aplikasi dan perangkat keras tambahan.

- **Phishing**

Email atau pesan teks penipuan yang berisi tautan ke situs web yang mungkin berisi malware, atau dapat menipu pengguna agar mengungkapkan informasi sensitif (seperti kata sandi) atau mentransfer uang.

- **Spyware**

Sejenis malware yang dipasang pada perangkat tanpa persetujuan pengguna, mengumpulkan data, lalu mengirimkannya ke pihak ketiga.

- **Media Sosial**

Situs web dan aplikasi, seperti Facebook, X, dan Instagram, yang memungkinkan orang untuk berbagi dan menanggapi konten yang dibuat pengguna (postingan teks, foto, dan video).

- **Ponsel pintar**

Ponsel modern yang menjalankan fungsi kompleks, termasuk yang menggunakan sistem operasi Android dan iOS.

- **Trojan**

Sejenis malware yang menyamar sebagai perangkat lunak sah yang digunakan untuk memperoleh akses tidak sah ke perangkat korban.

- **URL**

Uniform Resource Locator. Alamat di web di seluruh dunia seperti nama domain (misalnya www.bbc.co.uk).

- **Virus**

Jenis malware yang dirancang untuk menginfeksi program perangkat lunak yang sah dan mereplikasi di seluruh jaringan saat program tersebut diaktifkan.

Bacaan lebih lanjut

Panduan dari Pusat Keamanan Siber Australia

- Laporkan kejahatan siber, insiden, atau kerentanan
- Cara mengamankan perangkat Anda
- Amankan ponsel Anda
- Phishing
- Penipuan
- Amankan media sosial Anda
- Tips keamanan untuk media sosial dan aplikasi perpesanan

Panduan dari NCSC UK dan NPSA

- Mempertahankan Demokrasi
- Media Sosial: cara menggunakannya dengan aman
- Panduan Keamanan Perangkat untuk organisasi termasuk perangkat seluler
- Laporan ancaman pada toko aplikasi.
- Keamanan dan keselamatan pribadi untuk individu berisiko tinggi

Panduan dari NSA AS

- Praktik Terbaik Perangkat Seluler

Penafian

Harap perhatikan bahwa saran ini memberikan informasi yang divalidasi pada saat publikasi.

Laporan ini mengacu pada informasi yang diperoleh dari badan penyusun dan sumber industri. Semua temuan dan rekomendasi yang dibuat tidak diberikan dengan maksud untuk menghindari semua risiko dan mengikuti rekomendasi tidak akan menghilangkan semua risiko tersebut. Kepemilikan risiko informasi tetap berada di tangan pemilik sistem yang relevan setiap saat.

Di Inggris Raya, informasi ini dikecualikan berdasarkan Undang-Undang Kebebasan Informasi 2000 (FOIA) dan mungkin dikecualikan berdasarkan undang-undang informasi Inggris Raya lainnya.

Ajukan pertanyaan FOIA apa pun ke ncscinfoleg@ncsc.gov.uk.

Lampiran: Contoh MOONSHINE & BADBAZAAR yang diamati

Tabel ini mencantumkan aplikasi yang digunakan dalam kampanye MOONSHINE dan BADBAZAAR dalam dua tahun terakhir.

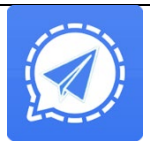
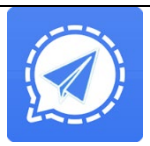
Banyak dari aplikasi ini menunjukkan kemiripan yang jelas dengan aplikasi yang sudah ada. Ini kemungkinan merupakan teknik yang disengaja oleh pelaku untuk 'meniru' merek terkenal.

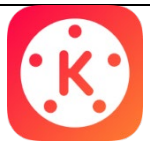
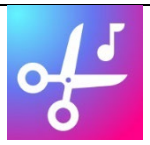
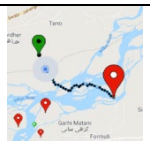
Penting untuk dicatat, nama aplikasi, nama paket, dan ikon semuanya dapat meniru atau menyamai aplikasi asli dan karenanya tidak boleh digunakan secara eksklusif untuk mengidentifikasi apakah suatu perangkat terinfeksi.

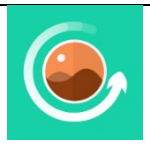
Sebagaimana disertakan dalam bagian mitigasi, Anda dapat mengirim aplikasi di perangkat Android Anda ke Google dengan mengaktifkan 'Tingkatkan deteksi aplikasi berbahaya', yang akan memindai aplikasi di perangkat Anda yang diinstal dari luar Play Store.

Judul aplikasi	Nama paket	Ikon aplikasi
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	
Keyboard Bahasa Arab	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.buddhistssongs1	
Kalkulator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	

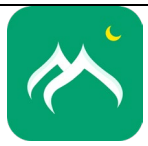
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar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

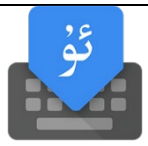
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
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	
Papan Ketik SwiftKey	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	
Papan Ketik Uighur	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	
ئەسەرلەر ئاۋازلىق	com.ewlat.eserler	
قۇرئان ئاۋازلىق	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
قۇرئان ئۇيغۇرچە	com.c9.uyghurquran	
الكريم القرآن	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
كەرىم قۇرئان	ru.omdevelopment.ref.quranuyghur.free	
لۇغىتى كۇھىقاپ	com.kuhiqap.lughitim	
كىرگۈزگۈچ نۇر	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.astrnomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate