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

Panduan Nasihat

BADBAZAAR dan MOONSHINE: Spyware yang menyasarkan kumpulan-kumpulan Uyghur, Taiwan dan Tibet serta para pelaku masyarakat sivil.

9 April 2025

BADBAZAAR dan MOONSHINE: Spyware yang menyasarkan kumpulan-kumpulan Uyghur, Taiwan dan Tibet serta para pelaku masyarakat sivil.

Pihak NCSC dan rakan-rakan kongsinya menerbitkan maklumat dan langkah-langkah pemitigasian baharu bagi mereka yang berisiko tinggi daripada dua varian spyware.

Ringkasan

Dengan sokongan Cyber League UK, panduan nasihat ini telah dihasilkan bersama The National Cyber Security Centre (NCSC UK) dan rakan-rakan kongsi antarabangsa mereka.

- **The Australian Cyber Security Centre (Pusat Keselamatan Siber Australia) sebahagian daripada The Australian Signals Directorate (Direktorat Semboyan Australia)**
- **The Canadian Centre for Cyber Security (Pusat bagi Keselamatan Siber Kanada), sebahagian daripada The Communications Security Establishment (Pertubuhan Keselamatan Komunikasi)**
- **The German Federal Intelligence Service (Perkhidmatan Perisikan Persekutuan Jerman)**
- **The German Federal Office for the Protection of the Constitution (Pejabat Persekutuan Jerman bagi Perlindungan Perlembagaan)**
- **The New Zealand National Cyber Security Centre (Pusat Keselamatan Siber Kebangsaan New Zealand), sebahagian daripada The Government Communications Security Bureau (Biro Keselamatan Komunikasi Kerajaan)**
- **The United States Federal Bureau of Investigation (Biro Penyiasatan Persekutuan Amerika Syarikat)**
- **The United States National Security Agency (Agensi Keselamatan Kebangsaan Amerika Syarikat)**

Tujuannya ialah untuk meningkatkan kesedaran mengenai ancaman yang semakin berkembang daripada para pelaku berniat jahat terhadap individu-individu yang ada kaitan dengan topik-topik berkenaan Taiwan, Tibet, Xinjiang Uyghur Autonomous Region, gerakan demokrasi dan Falun Gong.

Panduan nasihat ini mengandungi dua kajian kes yang memperincikan teknik-teknik yang diguna para pelaku berniat jahat yang menggunakan spyware yang dikenali sebagai BADBAZAAR dan MOONSHINE untuk menyasarkan data pada alat-alat peranti mudah-alih termasuk telefon pintar yang mungkin akan menarik perhatian negara China. Ia juga menyampaikan tanda arah bagi nasihat panduan yang boleh membantu para individu untuk melindungi diri mereka sendiri, alat-alat peranti mereka serta data mereka.

Sejajar dengan panduan nasihat ini, pihak NCSC telah menerbitkan butiran teknikal penuh beserta sebuah garis panduan berasingan.

Siapa yang berisiko?

Pihak agensi pengarang dan rakan-rakan kongsi industri telah memerhatikan bahawa BADBAZAAR dan MOONSHINE sedang menyasarkan secara khusus para individu yang ada kaitan dengan topik-topik yang dianggap negara China sebagai satu ancaman kepada autoriti domestik, cita-cita dan reputasi global mereka. Mereka yang paling berisiko termasuk, tetapi tidak terhad kepada, sesiapa yang ada kaitan dengan:

- **Kemerdekaan Taiwan**
- **Hak-Hak Tibet**
- **Muslim Uyghur dan minoriti etnik dalam atau dari Xinjiang Uyghur Autonomous Region China lain.**
- **advokasi demokrasi (termasuk Hong Kong)**
- **gerakan spiritual Falun Gong**

Ini termasuk badan-badan bukan kerajaan (NGO), wartawan, bisnes dan individu yang beradvokasi bagi, mengidentifikasikan diri dengan, atau sebaliknya mewakili kumpulan-kumpulan ini. Cara tiada berbelah bahagi bagaimana spyware ini disebarkan dalam talian juga bererti terdapat risiko jangkitannya akan menular melangkaui mangsa-mangsa yang disasarkan.

Panduan nasihat ini bermatlamat untuk menolong mereka yang berisiko untuk merespons secara berkesan terhadap ancaman khusus daripada spyware BADBAZAAR dan MOONSHINE. Pemitigasian yang dicadangkan mengiringi nasihat keselamatan siber yang lebih meluas dan tidak sepatutnya dipertimbangkan dengan sendirinya.

Dengan mengikuti panduan yang dirujuk dalam panduan nasihat ini, para pengguna boleh mengurangkan risiko jangkitan pada alat-alat peranti mudah-alih dan data mereka.

Ancaman

MOONSHINE dan BADBAZAAR ialah contoh trojan-trojan; mereka mempunyai fungsi-fungsi berniat jahat yang disembunyikan di dalam app-app yang sebaliknya berfungsi dengan baik, yang boleh dimuat turun daripada stor-stor app atau perkhidmatan-perkhidmatan perkongsian-fail dalam talian.

App-app ini direka untuk menipu pengguna untuk memuat turun dan memasangkannya ke dalam alat peranti. Apabila ia sudah dipasang, ia menggunakan kerentanan dalam alat peranti tersebut untuk melakukan fungsi-fungsi yang tidak dibenarkan, atau ia akan bergantung kepada kebenaran yang diberi pengguna berkenaan kepada app itu untuk mengakses dan memuat turunkan maklumat daripada alat peranti itu, termasuk:

- **data lokasi termasuk penjejakan masa nyata**
- **akses kepada mikrofon dan kamera**
- **pesanan, gambar dan fail-fail lain yang disimpan dalam alat peranti itu**
- **maklumat alat peranti berkenaan dan lebih lagi**

Para pelaku kemudian mengeksploitasikan kepentingan sahih kumpulan-kumpulan berisiko berkennaan, untuk mengenal pasti dan menjangkiti seramai mangsa yang boleh, dan mendapatkan akses kepada data mereka. Salah satu cara mereka berbuat demikian ialah dengan merekacipta app yang mereka tahu akan menarik perhatian mangsa mereka, misalnya app-app yang menyokong bahasa kaum mereka, atau mengandungi konten yang khusus kepada lokasi-lokasi seperti wilayah-wilayah Tibet China atau Xinjiang.

Kajian-kajian kes di dalam panduan nasihat ini menyampaikan beberapa contoh perkara ini, termasuk app-app TibetOne dan Quran Uyghur.

Para pelaku aktif dalam forum-forum di mana terdapat kelompok pengguna dasar mangsa-mangsa sasaran mereka, yang memaksimumkan peluang mereka untuk menjangkiti mangsa mereka. Mereka telah diperhati sengaja mengongsi spyware dalam saluran-saluran Telegram berkaitan-Tibet dan forum-forum Reddit. Kajian-kajian kes dalam panduan nasihat ini juga memberi contoh kaedah-kaedah ini.

App-app berniat jahat sering dikongsi sebagai fail-fail tunggal atau berdiri sendiri, misalnya fail-fail APK pada Android, yang perlu dimuat turun dan dipasang oleh pengguna. Para pelaku ini akan cuba untuk menjadikan spyware

mereka kelihatan lebih sahih dengan memuatnaikkannya ke dalam stor-stor app rasmi seperti Stor Google Play dan Stor App Apple atau dengan menambahkan kod berniat jahat ke dalam app-app yang dahulunya tidak berniat jahat walaupun stor-stor rasmi memiliki ciri-ciri keselamatan dan proses penapisan yang menjadikan taktik ini kurang berjaya. Hal ini menjadikan app-app daripada stor-stor rasmi lebih selamat, tetapi sebagaimana yang ditunjukkan dalam kajian-kajian kes, dan App Store Threat Report NCSC, proses-proses ini tidak sempurna.

Menurut 4 petua ini boleh menolong melindungi anda daripada ancaman-ancaman yang digariskan dalam panduan nasihat ini.

Untuk nasihat lebih terperinci, sila lihat seksyen pemitigasian.

Kajian Kes

Kedua-dua kajian kes ini menunjukkan bagaimana MOONSHINE dan BADBAZAAR bekerja, dan bagaimana pelaku siber berniat jahat sedang menyasarkan mereka yang paling berisiko.

Kajian kes satu: MOONSHINE

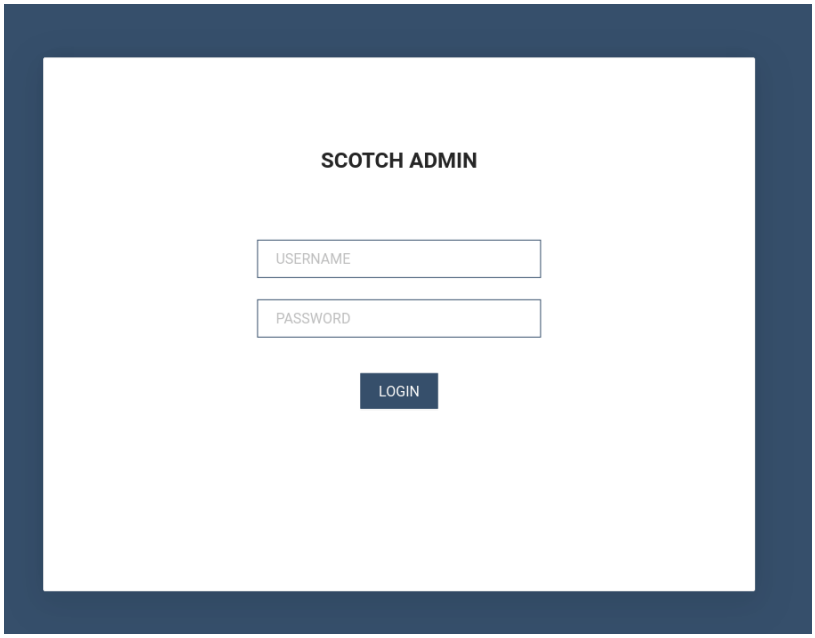
MOONSHINE ialah sebuah spyware Android yang dilaporkan pada 2019 oleh Citizen Lab sebagai menyasarkan kumpulan-kumpulan Tibet. MOONSHINE menyamar sebagai sebuah app sahih untuk mengumpan mangsa untuk memasangnya. Ia telah dikongsi menerusi saluran-saluran Telegram dan pautan-pautan yang dikirim menerusi WhatsApp.

MOONSHINE memiliki keupayaan pengintipan meluas, antaranya:

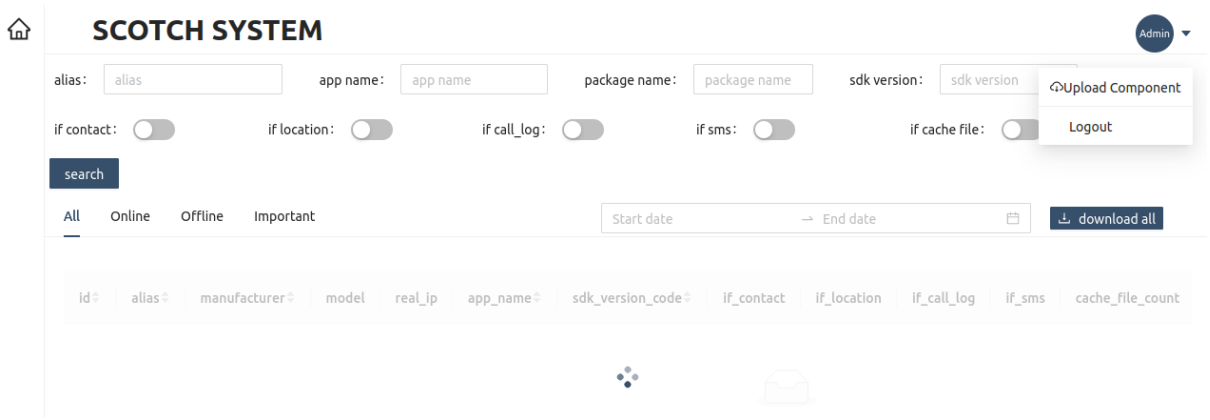
- **data lokasi termasuk penjejakan masa nyata**
- **tangkapan audio dan foto siaran langsung**
- **memuat turun fail-fail dari alat peranti**
- **mengeluarkan maklumat alat peranti**
- **memainkan audio pada alat peranti**

Aplikasi '**ئاۋازلىق قۇرئان.apk**', yang diterjemahkan sebagai '**Audio Quran.apk**', ialah satu contoh bagaimana MOONSHINE diguna untuk menyasarkan orang Uyghur. Penggunaan bahasa Uyghur di dalam nama fail, yang menandakan ianya ialah sebuah aplikasi Quran, ternyata direka sebegitu rupa untuk menarik perhatian Muslim Uyghur.

Apabila ia sudah dipasang, pelaku siber berniat jahat boleh memungut maklumat daripada alat peranti mangsa. Maklumat ini diakses menerusi panel 'SCOTCH ADMIN'.



Apabila mereka sudah mendaftar masuk, para pelaku boleh mengakses halaman yang ditunjukkan dalam tangkap layar di bawah. Halaman ini memaparkan butir-butir alat peranti yang dijangkiti dan tahap akses yang dipunyai pelaku kepada alat-alat peranti yang dijangkiti:



Panel pengurusan malware menunjukkan data yang dipungut, termasuk:

- **tahap akses ke alat peranti**
- **mesej sms**
- **log panggilan**
- **data lokasi**
- **maklumat alat peranti**

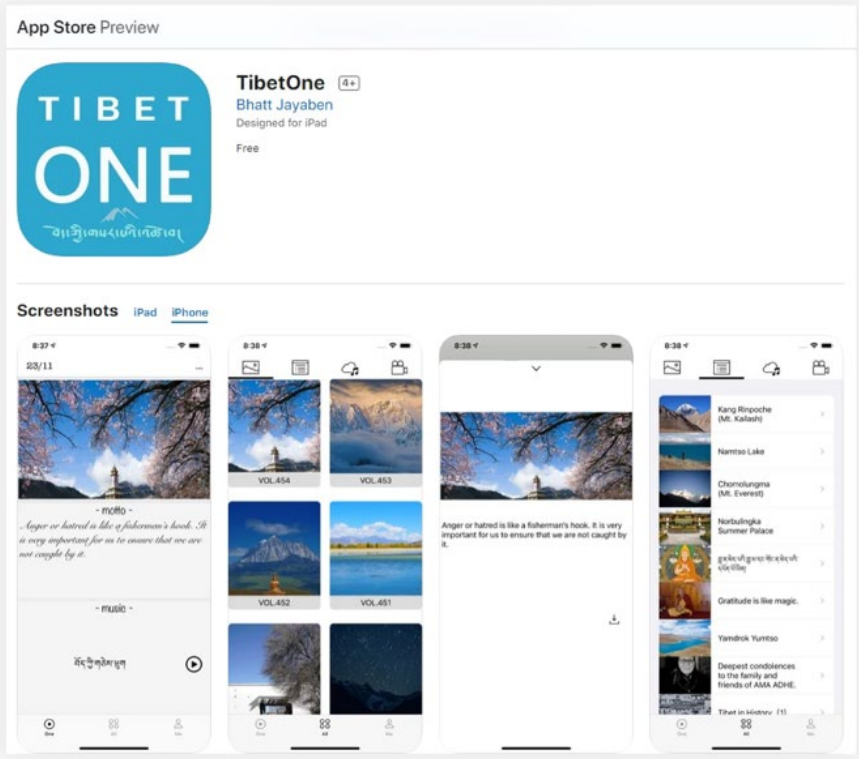
Dengan kolaborasi Cyber League, pihak NCSC telah membina atas laporan industri daripada Trend Micro untuk mencari penindihan antara kit eksploitasi MOONSHINE dan panel-panel daftar masuk yang mengandungi 'UPSEC' di dalam tajuk HTML. Butir-butir penuh terkandung di dalam panduan nasihat teknikal yang disampaikan bersama di bawah ini:

Menurut Intelligence Online, UPSEC merujuk kepada 'Sichuan Dianke Network Security Technology Co. Ltd'. Pihak agensi pengarang belum menentusahkan kenyataan ini.

Kajian kes dua: BADBAZAAR

BADBAZAAR ialah sebuah malware mudah alih dengan varian iOS dan Android yang menyasarkan individu-individu Uyghur, Tibet dan Taiwan. Malware ini telah disebarkan menerusi platform-platform media sosial dan stor-stor app rasmi.

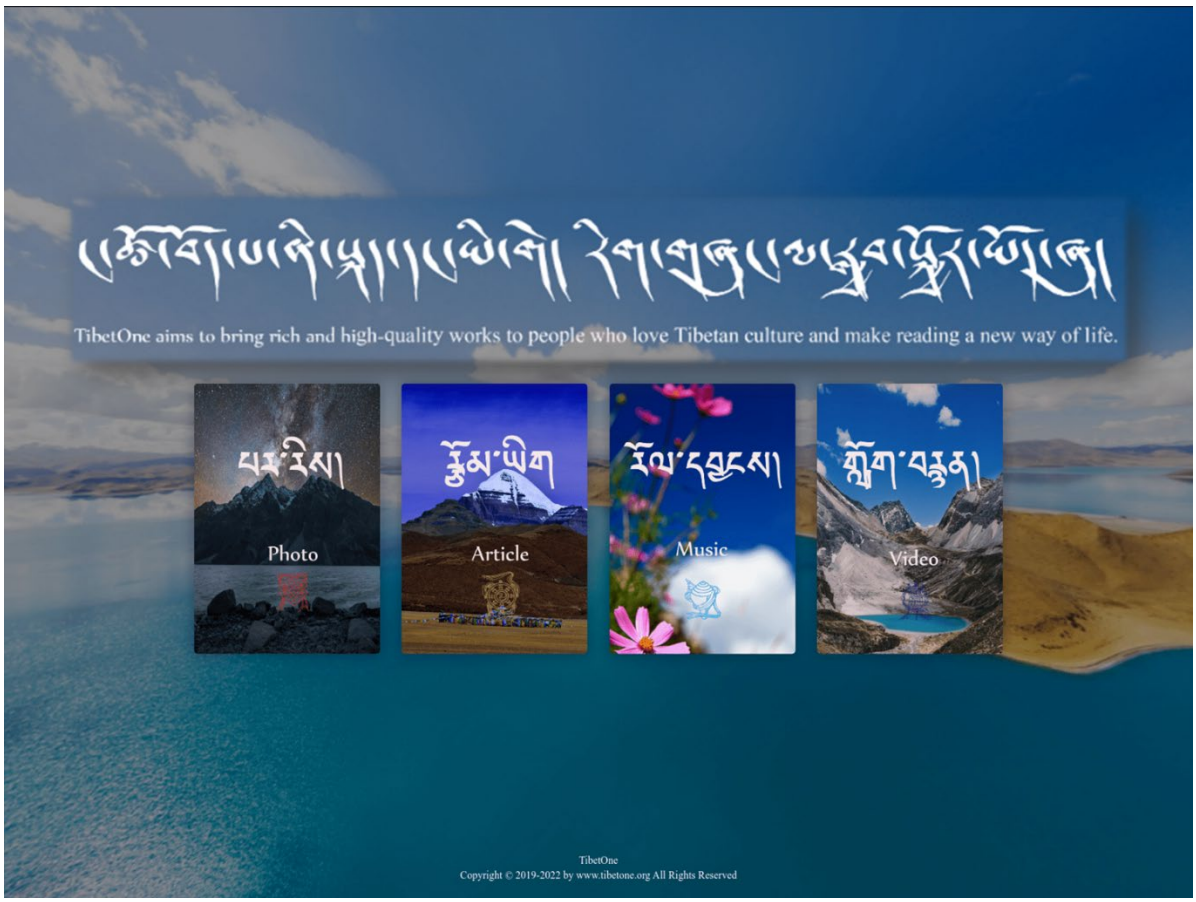
BADBAZAAR telah diguna untuk menyasarkan orang Tibet menerusi app '**TibetOne**', seperti yang dilaporkan oleh Lookout dan Volexity. **TibetOne** ialah sebuah app iOS yang dicipta oleh pelaku berniat jahat, dengan keupayaan untuk mengakses maklumat alat peranti dan data lokasi. Ia telah dimuat naik ke dalam Apple App Store pada Disember 2021 tetapi tidak disediakan lagi. Untuk menyebarkan malware ini dengan lebih meluas, para pelaku juga telah mengiklankan app ini dalam sebuah saluran Telegram yang dipanggil '**tibetanphone**'.



Rajah 1: Halaman app TibetOne pada Apple App Store. App ini kini sudah dikeluarkan.

Rajah 2: TibetOne sebagaimana dikongsi dalam saluran-saluran Telegram.

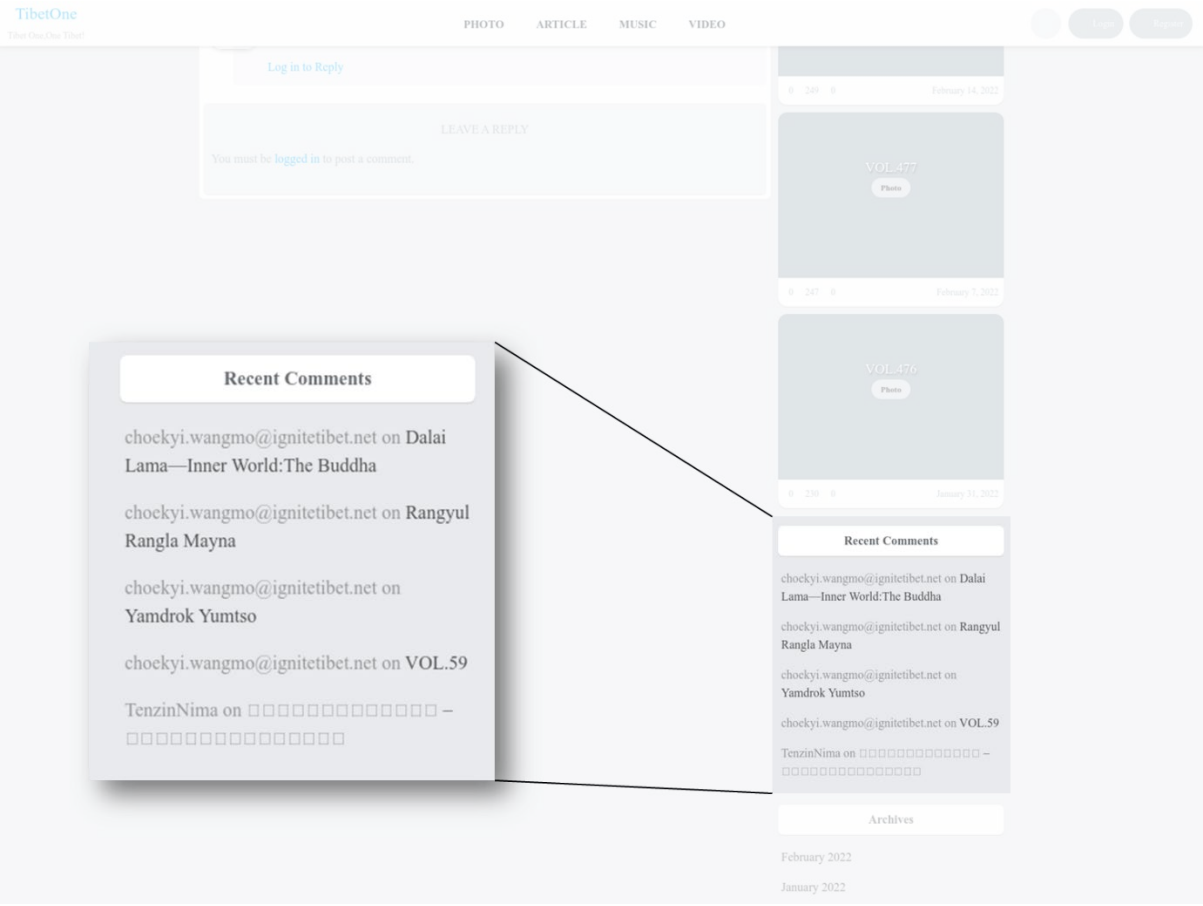
Untuk menambahkan kesahihan kepada app itu, para pelaku berkenaan juga telah membangunkan sebuah laman web yang dipanggil '**tibetone[.]org**', yang menerangkan bahawa ia adalah bertujuan untuk *'membawa karya-karya kaya dan berkualiti-tinggi kepada mereka yang mencintai budaya Tibet dan menjadikan membaca satu gaya kehidupan baharu'.*



Rajah 3: Laman utama 'tibetone[.]org'.

Imej ini telah disunting untuk menjadikan seksyen-seksyen berkenaan lebih jelas.

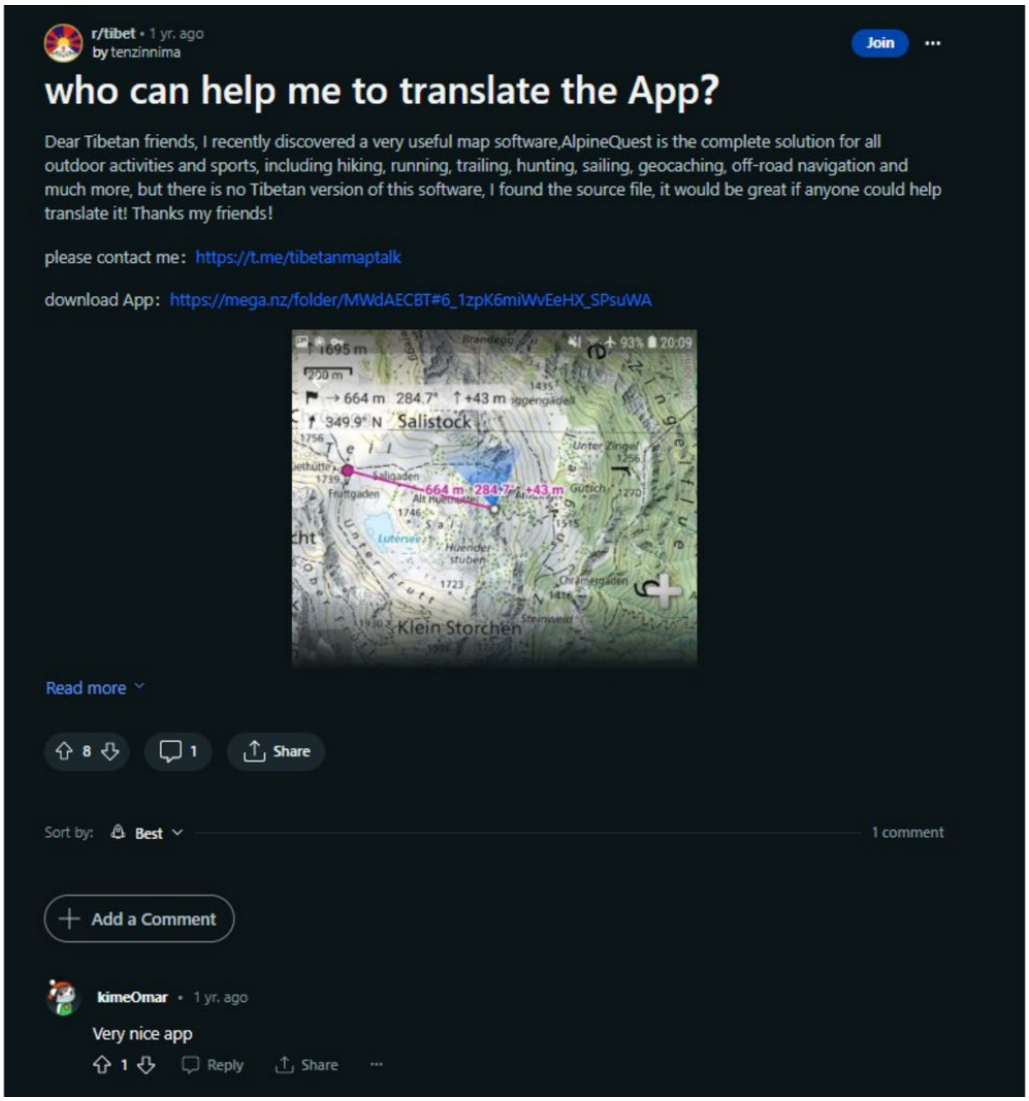
Laman web ini dahulunya mengandungi satu halaman untuk artikel-artikel yang membenarkan pengguna untuk meninggalkan komen. Satu komen yang ditinggalkan oleh alamat e-mel '**choekyi.wangmo@ignitetibet.net**', dipercayai dikawal oleh pelaku berniat jahat dan barangkali menyamar sebagai '**Choekyi Wangmo**' yang disenaraikan oleh Tibetan Centre of Human Rights and Democracy sebagai seorang penunjuk-perasaan pro-Tibet. Ini barangkali merupakan satu lagi percubaan untuk memberikan tanggapan bahawa app ini benar-benar memperjuangkan kemerdekaan Tibet.



Rajah 4: halaman 'tibetone[.]org' menunjukkan ulasan daripada pengguna yang dipercayai dikawal oleh pelaku berniat jahat tersebut.

Imej ini telah disunting untuk menjadikan seksyen-seksyen berkenaan lebih jelas.

'**TenzinNima**' ialah satu lagi nama pengguna yang telah menambahkan komen pada laman ini. Volexity telah melaporkan bahawa nama pengguna ini juga telah diguna pada Reddit untuk mengiklankan saluran Telegram '**Tibetanmaptalk**'. Ia mengandungi pautan untuk memuat turun sebuah sampel berniat jahat '**AlpineQuest**', satu app navigasi yang disediakan pada alat-alat peranti Android. Pautan muat turun yang disediakan ialah untuk satu perkhidmatan perkongsian-fail pihak-ketiga yang dipanggil Mega.



Rajah 5: Hantaran Reddit yang mengiklankan aplikasi berniat jahat oleh akaun yang dipercayai dikawal oleh pelaku berniat jahat.

Volexity juga merakamkan bahawa seorang pengguna yang dikenali sebagai '**KimeOmar**' yang telah meninggalkan komen pada hantaran itu juga telah diperhati mengongsi app-app berniat jahat pada satu lagi forum sub-Reddit. Ini mungkin menunjukkan bahawa pelaku berniat jahat menggunakan pelbagai profil media sosial untuk menjadikan hantaran mereka berupa sahih.

Penilaian

BADBAZAAR dan MOONSHINE menggunakan beberapa kaedah penjanaan sosial untuk menyasarkan komuniti-komuniti Uyghur, Tibet dan Taiwan secara khusus, terutamanya:

- pentrojanan app berkaitan komuniti-komuniti ini, misalnya sebuah app Quran bahasa Uyghur, yang hampir pastinya telah digubah untuk kumpulan dasar mangsa yang disasarkan.
- penambahan app-app yang ditrojankan ini ke dalam stor-stor app rasmi barangkali memberikan rasa kesahihan, dan pengongsiannya dalam chat-chat kumpulan barangkali dibuat dengan niat untuk mengeksploitasikan hubungan yang sudah dipercayai dalam kalangan komuniti-komuniti ini.

BADBAZAAR dan MOONSHINE memungut data yang hampir pasti akan bernilai bagi negara China. Walaupun BADBAZAAR dan MOONSHINE telah diperhati menyasar individu Uyghur, Tibet dan Taiwan, terdapat malware-malware lain yang menyasarkan kumpulan-kumpulan minoriti lain di China. Warganegara daripada negara-negara pemeterai bersama, di China dan di luar negara, yang dianggap menyokong perjuangan yang mengancam kestabilan rejim, hampir sudah pastinya terancam daripada malware mudah alih seperti BADBAZAAR dan MOONSHINE. Keupayaan untuk menangkap data lokasi, audio dan foto hampir pastinya menyampaikan peluang untuk memanfaatkan pengintipan lanjut dan operasi kekacauan dengan menyampaikan maklumat masa-nyata mengenai aktiviti sasaran tersebut.

Langkah-langkah pemitigasian bagi pengguna app mudah alih

Agensi pengarang menggalakkan amalan-amalan keselamatan berikut untuk mendapatkan perlindungan daripada ancaman yang diterangkan dalam kajian-kajian kes. Rekomendasi ini adalah berterapkan amalan-terbaik panduan nasihat NCSC. Sila lihat seksyen 'Further Reading' into pautan kepada panduan nasihat amalan-terbaik bagi pembaca di Australia dan AS.

Pastikan alat peranti anda senantiasa kukuh

- **Hanya muat turunkan app daripada stor-stor app rasmi, seperti Play Store Google atau App Store Apple.** Play Store Google dan App Store Apple mengimbas perisian untuk virus sebelum ia disediakan, dan ini memberi keyakinan tambahan bahawa apa yang anda muat turunkan dalah selamat. App-app daripada stor yang diyakini mungkin masih membawa risiko, tetapi muat turunan daripada sumber-sumber lain mungkin tidak mempunyai sebarang perlindungan langsung. Pihak NCSC mempunyai sebuah laporan ancaman pada stor-stor app: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Pastikan alat peranti dan app anda dikemaskini** Pasangkan pengemaskinian (updates)ke app dan perisian alat peranti anda sebaik sahaja ia disediakan. Pasangkan 'pengemaskinian automatik' (automatic updates) dalam pengesetan alat peranti anda jika ia disediakan supaya anda tidak perlu beringat untuk melakukannya. Sila lihat panduan NCSC mengenai cara bagaimana untuk mengekalkan kekukuhan dalam talian, untuk mendapatkan perlindungan daripada virus-virus yang dikenali dan jenis-jenis malware lain. Pengemaskinian sering mengandungi penambahbaikan dan ciri-ciri baharu: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Jangan 'jailbreak' atau 'root' alat peranti anda** kerana ini menggunakan kerentanan untuk memintas kawalan keselamatan yang ditetapkan. Ini mendedahkan lagi alat peranti berkenaan kepada serangan. Sila lihat panduan NCSC: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Uruskan app-app anda

- **Nilai kembali app-app anda dan izin-izinnya.** Jika anda tidak lagi memerlukan sesuatu app, buangkannya. Di mana anda boleh, hadkan izin app untuk meminimumkan pendedahan data, kerana malware sering direka untuk mengakses fail-fail yang dilindungi atau bersifat pinggiran (peripheral), misalnya kamera dan mikrofon .
    - Bagaimana untuk memeriksa izin app bagi pengguna Apple: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
    - Bagaimana untuk memeriksa izin app bagi pengguna Android: https://support.google.com/android/answer/9431959?hl=en-GB

- **Hantarkan app-app yang tidak dikenali secara automatik kepada Google.** Jika anda seorang pengguna Android dan telah memuat turun sebuah app yang bukan daripada Play Store Google, anda boleh menghantarkannya kepada Goodle dengan membolehkan 'Improve harmful app detection' dalam setting app Play Store Google di bawah 'Play Protect'. Ini akan mengimbas app itu untuk mengesan malware yang membantu melindungi pengguna. Maklumat tentang cara bagaimana untuk memasangnya: https://support.google.com/android/answer/2812853?hl=en-GB

Gunapakai Perkhidmatan Siber

- **Gunakan perkhidmatan reputasi URL sebelum mengeklik pada sesuatu pautan.** Anda boleh memeriksa jika sesuatu pautan daripada sebuah e-mel, pesanan ringkas atau dari tempat lain adalah selamat dengan mengimbasnya terlebih dahulu dengan menggunakan perkhidmatan-perkhidmatan seperti Google Transparency Report atau Virus Total. Anda juga boleh memuat naik fail-fail dan app-app yang dicurigai kepada sebuah penganalisis malware, seperti Virus Total yang boleh menolong mengesan sama ada sesuatu fail berniat jahat. Harap maklum bahawa perkhidmatan mengimbas boleh menghasilkan negatif palsu.

- **Sertai program Google Advanced Protection.** Ini ialah sebuah perkhidmatan percuma yang direka untuk mengukuhkan perlindungan individu yang menggunakan perkhidmatan Google (Gmail, Play Store, dsb) yang berisiko dijadikan sasaran. Perkhidmatan ini menyediakan keselamatan yang dipertingkatkan semasa menggunakan perkhidmatan-perkhidmatan Google: https://landing.google.com/advancedprotection/

- **Sertai perkhidmatan-perkhidmatan ketahanan tambahan, bila ia disediakan.** Contohnya, individu berisiko tinggi di UK mungkin layak untuk perkhidmatan kepertahanan tambahan untuk menolong mereka dengan keselamatan siber mereka. Semak kelayakan anda dan dapatkan maklumat lanjut: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Laporkan ancaman

- **Mengenal pasti dan melaporkan akaun-akaun palsu**. Para pelaku siber berniat jahat mewujudkan akaun-akaun palsu atau menggodam akaun benar untuk melanjutkan matlamat mereka. Jika anda berasa sebuah akaun itu ialah palsu atau telah dikompromi, laporkan kepada platform berkaitan dan sekatkannya. Kebanyakan perkhidmatan mempunyai proses untuk menentusahkan akaun-akaun, misalnya lencana penentusahan ('verified badges') untuk Instagram dan Facebook. Ini boleh menolong mengenal pasti akaun tersebut adalah tulen. NCSC mempunyai panduan nasihat berkenaan penggunaan media sosial secara selamat yang mengandungi butir-butir tentang cara bagaimana untuk menentusah dan melaporkan akaun-akaun yang telah dikompromi : https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Phishing menggunakan e-mel scam, SMS dan pautan**. Pihak NCSC boleh menyiasat alamat-alamat e-mel dan laman web yang mencurigai. Jika anda fikir sesebuah laman web, e-mel atau mesej mencurigakan, anda boleh melaporkannya di: https://www.ncsc.gov.uk/collection/phishing-scams

Kosa Kata NCSC

- **Android**

Sistem pengoperasian mudah alih Google, yang diguna beberapa telefon pintar dan pembuat tablet.

- **App**

Sebuah aplikasi, atau app, ialah sebuah pakej perisian yang boleh dipasang pengguna atau sudah siap dipasang pada sesebuah alat peranti untuk menyediakan pengefungsian tambahan atau konten kepada alat peranti mereka.

- **Keselamatan Siber**

Perlindungan alat peranti, perkhidmatan dan jaringan – dan maklumat yang terkandung di dalamnya – daripada akses yang tidak dibenarkan, kecurian atau kerosakan.

- **Alat Peranti**

Peranti keras berdasarkan-komputer yang wujud secara fizikal, misalnya komputer atas meja, telefon pintar atau tablet.

- **iOS**

Sistem pengeoperasian mudah alih Apple yang diguna pada rangkaian alat-alat peranti mudah alihnya.

- **Malware**

Diringkaskan daripada 'malicious software' (perisian berniat jahat), malware ialah sebarang jenis perisian yang boleh merosakkan sistem komputer, jaringan atau alat-alat peranti. Ia termasuk virus, ransomware dan trojan.

- **Sistem Pengoperasian**

Perisian dasar yang berjalan di dalam komputer, tablet dan telefon pintar yang dikehendaki untuk menjalankan aplikasi dan peranti keras tambahan.

- **Pancingan (Phishing)**

e-Mel atau mesej teks scam yang mengandungi pautan ke laman-laman web yang mungkin mengandungi malware, atau mungkin akan menipu pengguna untuk mendedahkan maklumat sensitif (misalnya kata laluan) atau menghantar wang.

- **Spyware**

Sejenis malware yang memasangkan dirinya pada sesuatu alat peranti tanpa keizinan pengguna, memungut data dan kemudian menghantarkannya kepada pihak ketiga.

- **Media sosial**

Laman-laman wen dan app, misalnya Facebook, X dan Instagram, yang membenarkan orang untuk mengongsi dan merespons kepada konten yang dijana-pengguna (hantaran teks, foto dan video).

- **Telefon Pintar**

Telefon mudah alih moden yang menjalankan pengefungsian kompleks termasuk yang mengandungi sistem-sistem Android dan iOS.

- **Trojan**

Sejenis malware, yang menyamar sebagai perisian sahih, yang diguna untuk mendapatkan akses yang tidak dibenarkan ke dalam alat peranti mangsa.

- **URL**

Pelokasi Sumber Seragam (Uniform Resource Locator) Satu alamat pada web seluruh dunia (world wide web) misalnya sebuah nama domain (contohnya www.bbc.co.uk).

- **Virus**

Sejenis malware yang direka untuk menjangkiti program perisian sahih dan menyalinnya kembali ke seluruh jaringan bila program-program itu sudah diaktifkan.

Bacaan Lanjut

Panduan daripada Australian Cyber Security Centre (Pusat Keselamatan Siber Australia)

- 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

Panduan daripada NCSC UK dan 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

Panduan daripada US NSA

- Mobile Device Best Practices

Penafian

Harap maklum bahawa panduan nasihat ini menyampaikan maklumat yang telah ditentusahkan pada waktu ia diterbitkan.

Laporan ini meraih maklumat yang diperolehi daripada agensi pengarang dan sumber-sumber industri. Sebarang hasil carian dan cadangan yang dibuat tidak disampaikan dengan niat untuk mengelakkan semua risiko dan mengikut cadangan ini tidak akan menghapuskan semua risiko sedemikian. Pemilikan risiko maklumat berkenaan tetap ditanggung oleh pemilik sistem berkaitan pada setiap masa.

Di UK, maklumat ini dikecualikan di bawah Akta Kebebasan Maklumat 2000 (Freedom of Information Act 2000) (FOIA) dan mungkin dikecualikan di bawah peraturan perundangan maklumat UK lain.

Sila rujukkan sebarang pertanyaan FOIA kepada ncscinfoleg@ncsc.gov.uk.

Annex: Sampel-sampel MOONSHINE & BADBAZAAR yang diperhati

Rajah di bawah menyenaraikan app-app yang diguna dalam kempen-kempen MOONSHINE dan BADBAZAAR dalam tempoh masa dua tahun kebelakangan ini.

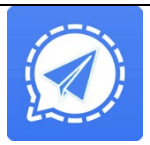
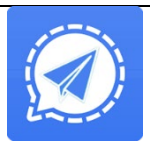
Sebahagian besar app ini menunjukkan persamaan dengan app-app yang sedia ada yang sudah lama ditubuhkan. Ia barangkali merupakan teknik sengaja pelaku untuk menipu-samar atau 'spoof' jenama-jenama yang dikenali ramai.

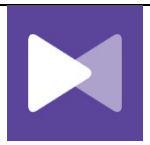
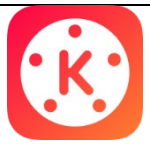
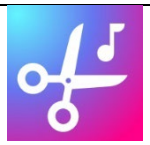
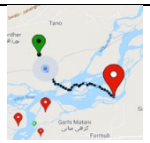
Ia penting untuk mengambil tahu bahawa, tajuk app, nama pakej, dan ikon app semua boleh meniru atau kelihatan serupa dengan aplikasi sebenar dan oleh yang demikian tidak sepatutnya diguna secara eksklusif untuk mengenal pasti sama ada sesuatu alat peranti telah dijangkiti.

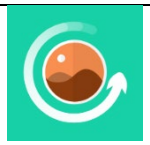
Seperti yang terkandung di dalam seksyen pemitigasian, anda boleh menghantar app-app pada alat peranti Android anda kepada Google dengan membolehkan 'Improve harmful app detection', yang akan mengimbas app-app dalam alat peranti anda yang telah dipasang dari luar Play Store.

Tajuk app	Nama pakej	Ikon app
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	

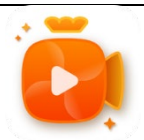
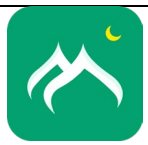
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar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

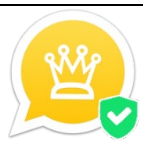
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader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

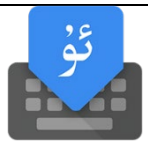
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn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