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

Avis

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

9 avril 2025

BADBAZAAR et MOONSHINE : Logiciels espions ciblant des groupes ouïghours, taïwanais et tibétains ainsi que des acteurs de la société civile

Le NCSC et ses partenaires publient de nouvelles informations et mesures d'atténuation pour les personnes à haut risque face à deux variantes de logiciels espions.

Résumé

Avec le soutien de la Cyber League britannique, cet avis a été rédigé conjointement par le Centre national de cybersécurité (NCSC UK) et des partenaires internationaux :

- **Le Centre australien de cybersécurité, qui fait partie de la Direction australienne des signaux**
- **Le Centre canadien pour la cybersécurité, qui fait partie du Centre de la sécurité des télécommunications**
- **Le Service fédéral allemand du renseignement**
- **L'Office fédéral allemand pour la protection de la Constitution**
- **Le Centre national de cybersécurité de Nouvelle-Zélande, qui fait partie du Bureau de la sécurité des télécommunications du gouvernement**
- **Le Bureau fédéral d'enquête des États-Unis**
- **L'Agence nationale de sécurité des États-Unis**

Son objectif est de sensibiliser à la menace croissante que représentent les cybercriminels pour les individus liés à des sujets tels que Taïwan, le Tibet, la région autonome ouïghoure du Xinjiang, les mouvements démocratiques et le Falun Gong.

Cet avis comprend deux études de cas détaillant les techniques utilisées par les cybercriminels utilisant les logiciels espions BADBAZAAR et MOONSHINE pour cibler les données des appareils mobiles, y compris les téléphones portables, susceptibles d'intéresser l'État chinois. Il indique également des conseils pour aider les individus à se protéger, à protéger leurs appareils et leurs données.

Parallèlement à cet avis, le NCSC a publié des informations techniques complètes accompagnées de conseils distincts.

Qui est à risque ?

Les agences de rédaction et les partenaires industriels ont observé que BADBAZAAR et MOONSHINE ciblaient spécifiquement des personnes liées à des sujets considérés par l'État chinois comme une menace pour son autorité nationale, ses ambitions et sa réputation internationale. Les personnes les plus exposées incluent, sans s'y limiter, toute personne liée à :

- **l'indépendance de Taïwan ;**
- **les droits des Tibétains ;**
- **les musulmans ouïghours et autres minorités ethniques originaires ou résidant dans la région autonome ouïghoure du Xinjiang en Chine ;**
- **la défense de la démocratie (y compris à Hong Kong) ;**
- **le mouvement spirituel Falun Gong.**

Cela inclut les organisations non gouvernementales (ONG), les journalistes, les entreprises et les particuliers qui défendent, s'identifient ou représentent ces groupes. La diffusion indiscriminée de ces logiciels espions en ligne implique également un risque de propagation des infections au-delà des victimes visées.

Cet avis vise à aider les personnes à risque à réagir efficacement à la menace spécifique des logiciels espions BADBAZAAR et MOONSHINE. Les mesures d'atténuation suggérées complètent les conseils plus généraux en matière de cybersécurité et ne doivent pas être considérées isolément.

En suivant les conseils mentionnés dans cet avis, les utilisateurs peuvent réduire le risque d'infection de leurs appareils mobiles et de leurs données.

La menace

MOONSHINE et BADBAZAAR sont des exemples de chevaux de Troie ; ils dissimulent des fonctions malveillantes dans une application fonctionnelle, téléchargeable depuis les boutiques d'applications ou les services de partage de fichiers en ligne.

Ces applications sont conçues pour inciter l'utilisateur à les télécharger et à les installer sur un appareil. Une fois installée, une application exploite les vulnérabilités de l'appareil pour exécuter des fonctions non autorisées, ou peut s'appuyer sur l'autorisation de l'utilisateur pour accéder à des informations et les télécharger, notamment les(l') :

- **données de localisation, y compris suivi en temps réel**
- **accès au microphone et à l'appareil photo**
- **messages, photos et autres fichiers stockés sur l'appareil**
- **informations sur l'appareil et plus encore**

Les acteurs exploitent ensuite les intérêts légitimes des groupes à risque pour identifier et infecter le plus grand nombre possible de victimes et accéder à leurs données. Ils y parviennent notamment en concevant des applications dont ils savent qu'elles plairont à leurs victimes, par exemple des applications prenant en charge leur langue maternelle ou proposant du contenu spécifique à des régions comme le Tibet ou le Xinjiang.

Les études de cas présentées dans cet avis en fournissent quelques exemples, notamment les applications TibetOne et Uyghur Quran.

Les acteurs sont actifs sur des forums en ligne où se trouvent une base d'utilisateurs de leurs cibles, ce qui maximise leurs chances d'infecter leurs victimes. Ils ont été observés partageant délibérément des logiciels espions sur des chaînes Telegram et des forums Reddit liés au Tibet. Les études de cas présentées dans cet avis illustrent également ces méthodes.

Les applications malveillantes sont souvent partagées sous forme de fichiers autonomes, comme les fichiers APK sur Android, que les utilisateurs doivent télécharger et installer. Les acteurs tentent de donner une apparence plus légitime à leurs logiciels espions en les téléchargeant sur des boutiques d'applications officielles telles que le Google Play Store et l'App Store d'Apple, ou en ajoutant du code malveillant à des applications auparavant inoffensives,

quoique, les boutiques officielles disposent de fonctionnalités de sécurité et de processus de vérification qui rendent cette tactique moins efficace. Les applications des boutiques officielles sont ainsi plus sûres, mais comme le démontrent les études de cas et le Rapport sur les menaces de l'App Store du NCSC, ces processus ne sont pas parfaits.

Suivez ces quatre conseils peut vous aider à vous protéger des menaces décrites dans cet avis.

Pour des conseils plus détaillés, consultez la section sur les mesures d'atténuation

Études de cas

Ces deux études de cas illustrent le fonctionnement de MOONSHINE et de BADBAZAAR, et la manière dont les cybercriminels ciblent les personnes les plus vulnérables.

Étude de cas n° 1 : MOONSHINE

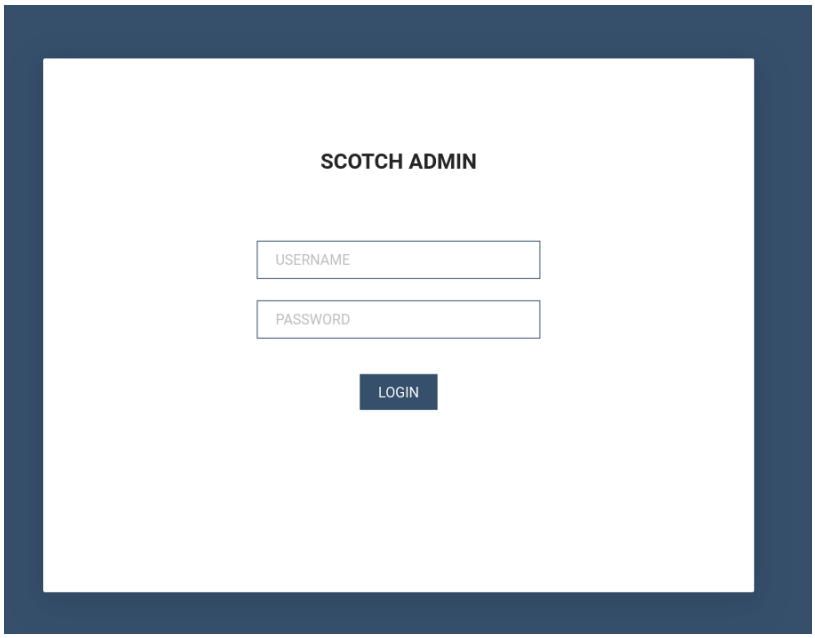
MOONSHINE est un logiciel espion Android signalé en 2019 par Citizen Lab comme ciblant des groupes tibétains. MOONSHINE se fait passer pour une application légitime pour inciter les victimes à l'installer. Elle a été partagée via des chaînes Telegram et des liens envoyés via WhatsApp.

MOONSHINE dispose de capacités de surveillance étendues, telles que :

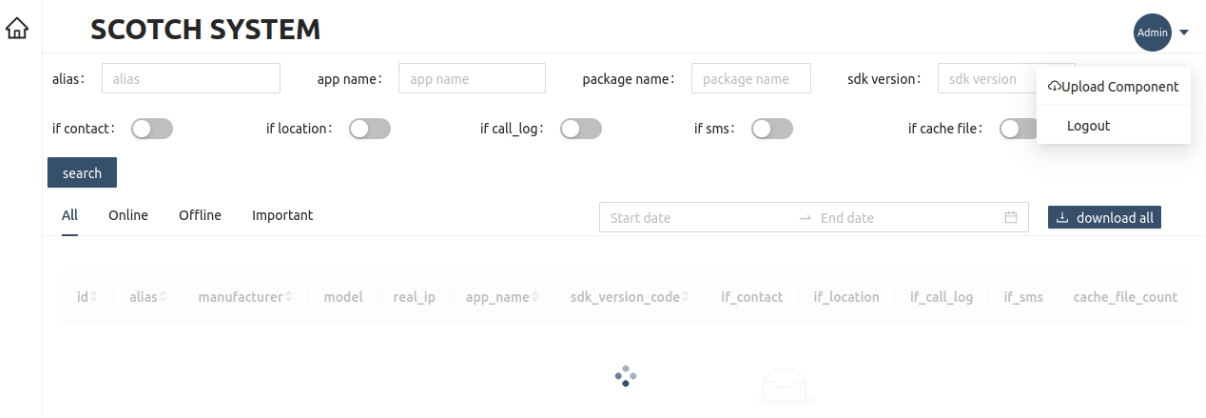
- **données de localisation, y compris suivi en temps réel**
- **capture de l'audio et de la photo en direct**
- **téléchargement de fichiers depuis l'appareil**
- **récupération des informations de l'appareil**
- **lecture de l'audio sur l'appareil**

L'application ‘قۇرئان ئاۋازلىق.**apk**’ qui se traduit par ‘**Coran audio.apk**’, est un exemple de l'utilisation de MOONSHINE pour cibler les Ouïghours. L'utilisation de la langue ouïghoure dans le nom du fichier, indiquant une application coranique, visait probablement à attirer les musulmans ouïghours.

Une fois l'application installée, les cybercriminels peuvent collecter des informations sur les appareils des victimes. Ces informations sont accessibles via le panneau‘ SCOTCH ADMIN ’.



Une fois connectés, les cybercriminels peuvent accéder à la page illustrée dans la capture d'écran ci-dessous. Cette page affiche les détails des appareils infectés et le niveau d'accès de l'acteur.



Le panneau de gestion des logiciels malveillants affiche les données collectées, notamment :

- **niveau d'accès à l'appareil**
- **messages SMS**
- **journaux d'appels**
- **données de localisation**
- **informations sur l'appareil**

En collaboration avec la Cyber League, le NCSC s'est appuyé sur les rapports sectoriels de Trend Micro pour identifier des recoupements entre le kit d'exploitation MOONSHINE et les panneaux de connexion contenant « UPSEC » dans leur titre HTML. Des informations complètes sont disponibles dans l'avis technique joint.

Selon Intelligence Online, UPSEC fait référence à « Sichuan Dianke Network Security Technology Co. Ltd ». Les agences autrices n'ont pas vérifié cette affirmation.

Étude de cas n° 2 : BADBAZAAR

BADBAZAAR est un logiciel malveillant mobile, décliné sur iOS et Android, qui cible les Ouïghours, les Tibétains et les Taïwanais. Ce logiciel malveillant s'est propagé via les réseaux sociaux et les boutiques d'applications officielles.

BADBAZAAR a été utilisé pour cibler les Tibétains via l'application ' **TibetOne '**, comme l'ont rapporté Lookout et Volexity. **TibetOne** est une application iOS créée par des acteurs malveillants, capable d'accéder aux informations de l'appareil et à ses données de localisation. Elle a été mise en ligne sur l'App Store d'Apple en décembre 2021, mais n'est plus disponible. Pour diffuser davantage le logiciel malveillant, les acteurs ont également fait la promotion de l'application sur un canal Telegram appelé ' **tibetanphone '**.

TibetOne

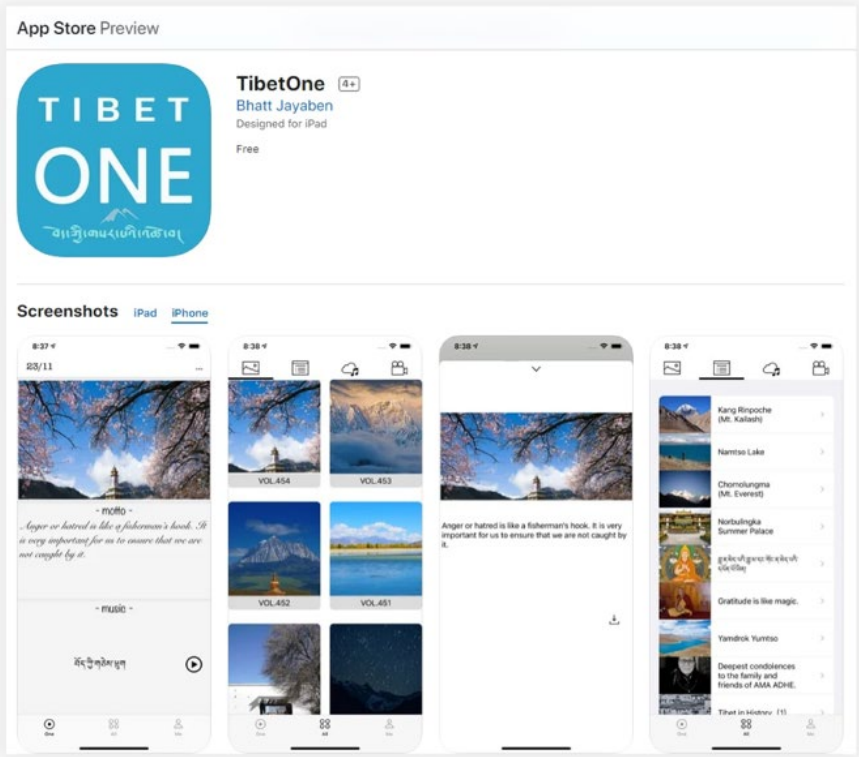


Figure 1 : Page de l'application TibetOne sur l'App Store d'Apple. Elle a depuis été supprimée.

Figure 2 : TibetOne tel que partagé sur les chaînes Telegram.

Pour ajouter de la légitimité à l'application, les acteurs ont également développé un site Web appelé «**tibetone[.]org**», qui se décrit comme *apportant des œuvres riches et de haute qualité aux personnes qui aiment la culture tibétaine et font de la lecture un nouveau mode de vie*.

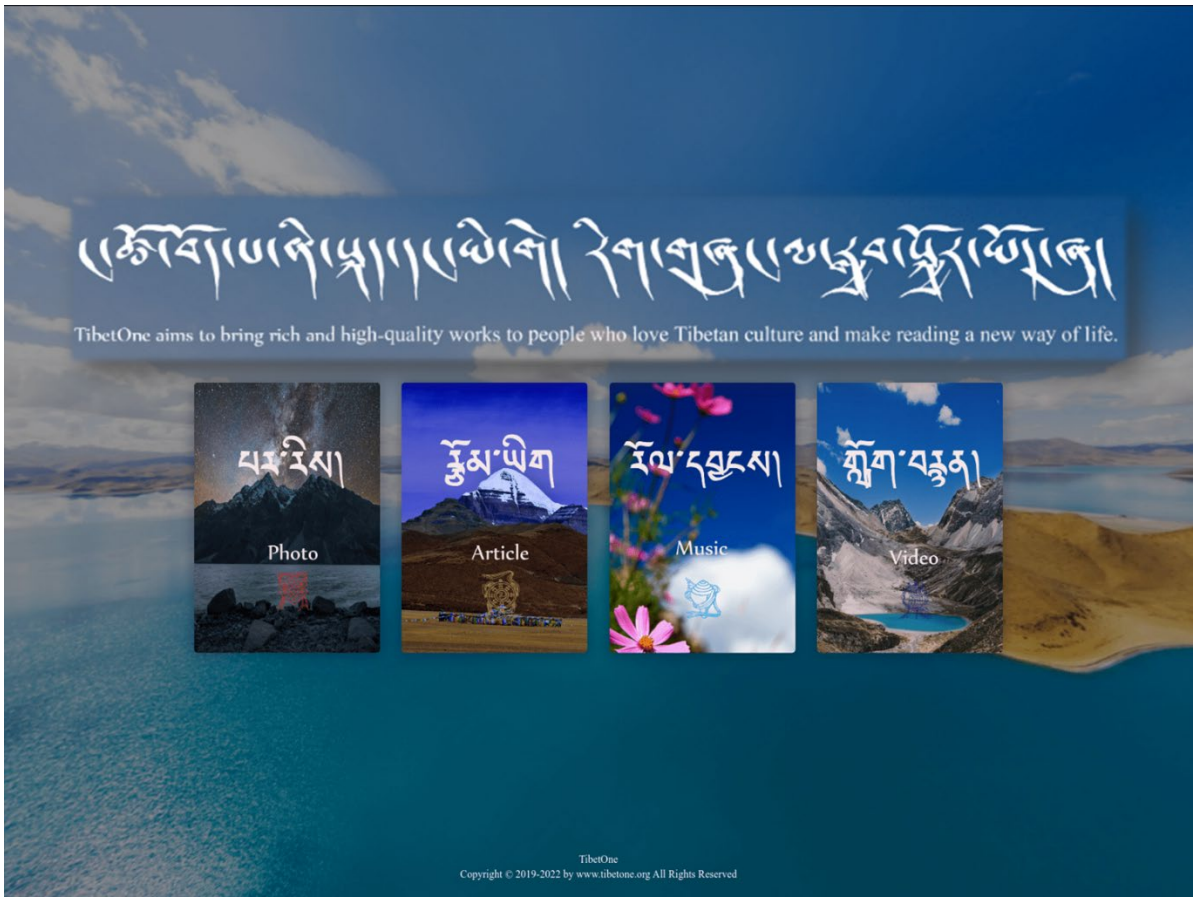


Figure 3 : Page d'accueil de «tibetone[.]org».

Cette image a été modifiée pour clarifier les sections concernées.

Ce site web proposait une page d'articles permettant aux utilisateurs de laisser des commentaires. A comment left by email address '**choekyi.wangmo@ignitetibet.net**', is believed to be controlled by the malicious actor and is likely to impersonate '**Choekyi Wangmo**' who the Tibetan Centre of Human Rights and Democracy litss as a pro-Tibet protestor. Il s'agit probablement d'une nouvelle tentative visant à donner l'impression que l'application défend sincèrement l'indépendance du Tibet.

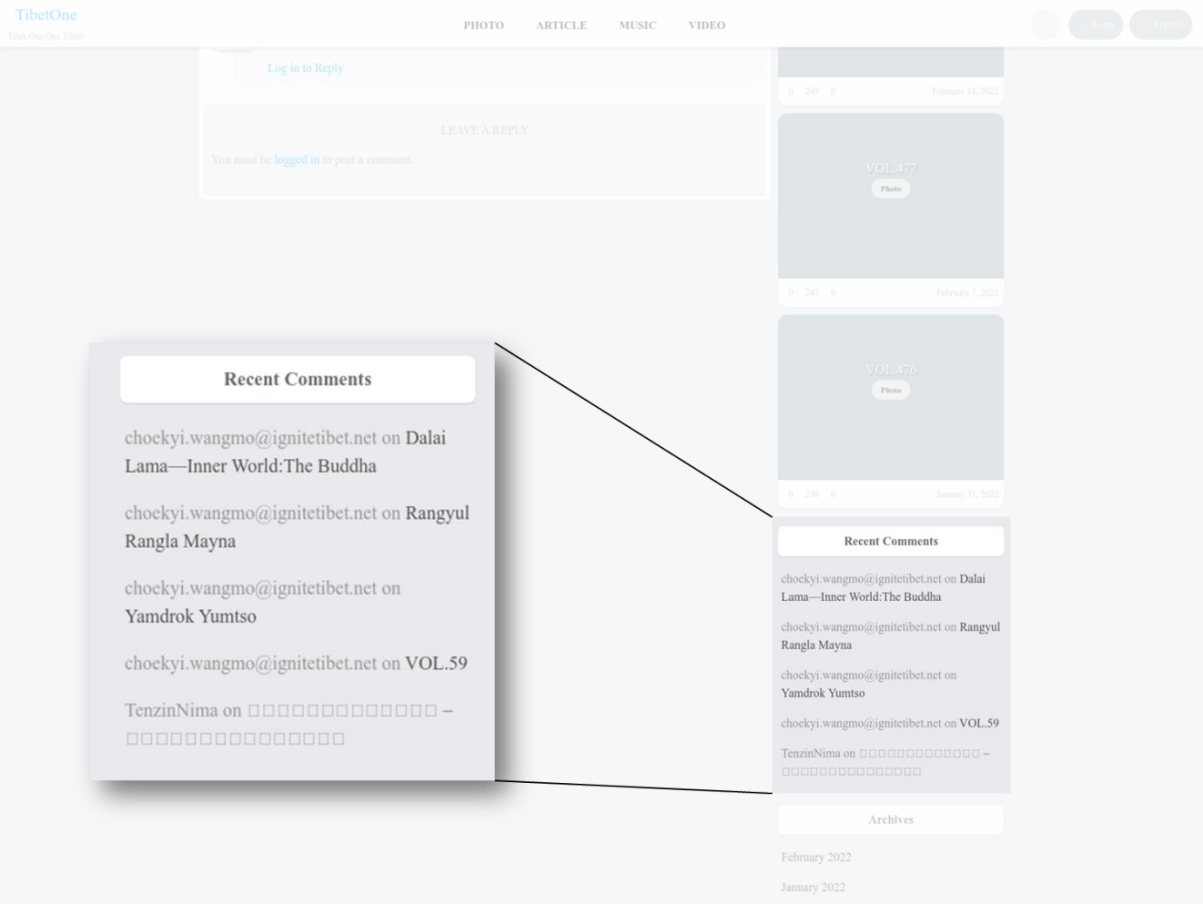


Figure 4 : Page « tibetone[.]org » montrant les commentaires d'utilisateurs soupçonnés d'être contrôlés par l'acteur malveillant.

Cette image a été modifiée pour clarifier les sections concernées.

‘ **TenzinNima ’** est un autre nom d'utilisateur ayant ajouté des commentaires sur ce site. Volexity a signalé que ce nom d'utilisateur est également utilisé sur Reddit pour promouvoir la chaîne Telegram ‘ **Tibetanmaptalk ’**. Il contient un lien permettant de télécharger un échantillon malveillant d'«**AlpineQuest**», une application de navigation disponible sur les appareils Android. Le lien de téléchargement fourni est celui d'un service tiers de partage de fichiers appelé Mega.

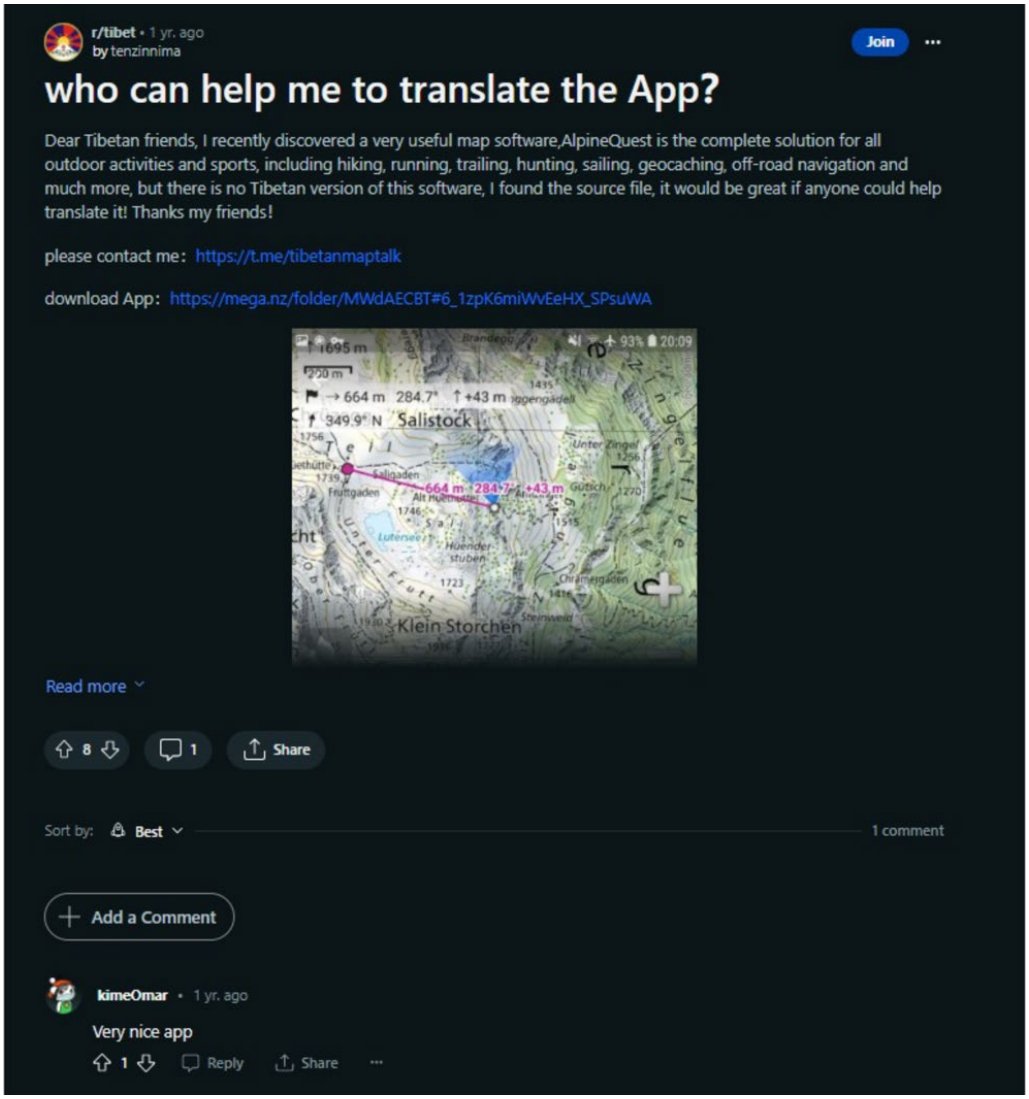


Figure 5 : Publication Reddit faisant la promotion d'une application malveillante par un compte supposément contrôlé par un acteur malveillant.

Volexity note également qu'un utilisateur connu sous le nom de '**KimeOmar'**, qui a commenté la publication, a également été observé partageant des applications malveillantes sur un autre sous-forum Reddit. Cela pourrait indiquer que les acteurs malveillants utilisent plusieurs profils de réseaux sociaux pour donner une apparence légitime à leurs publications.

Évaluation

BADBAZAAR et MOONSHINE utilisent plusieurs méthodes d'ingénierie sociale pour cibler spécifiquement les communautés ouïghoure, tibétaine et taïwanaise.

- La conversion de chevaux de Troie d'applications susceptibles d'intéresser ces communautés, comme une application du Coran en langue ouïghour, est très probablement adaptée à la cible.
- L'ajout de ces applications trojanisées aux boutiques d'applications officielles confère très probablement un sentiment de légitimité, et le partage dans les discussions de groupe vise très probablement à exploiter les relations de confiance au sein de ces communautés.

BADBAZAAR et MOONSHINE collectent des données qui seraient très certainement utiles à l'État chinois. Bien que BADBAZAAR et MOONSHINE aient été observés ciblant des Ouïghours, des Tibétains et des Taïwanais, d'autres logiciel malveillants ciblent d'autres groupes minoritaires en Chine. Les citoyens des pays co-scellés, en Chine et à l'étranger, perçus comme soutenant des causes menaçant la stabilité du régime, sont très probablement menacés par des logiciel malveillants mobiles tels que BADBAZAAR et MOONSHINE. La capacité de capturer des données de localisation, audio et photo offre très certainement la possibilité d'éclairer les futures opérations de surveillance et de harcèlement en fournissant des informations en temps réel sur l'activité de la cible.

Mesures d'atténuation pour les utilisateurs d'applications mobiles

Les organismes auteurs encouragent les pratiques de sécurité suivantes pour se protéger contre les menaces décrites dans les études de cas. Ces recommandations s'appuient sur celles du NCSC en matière de bonnes pratiques. Voir la section « Lectures complémentaires » pour accéder aux recommandations de bonnes pratiques destinées aux lecteurs australiens et américains.

Protégez votre appareil

- **Téléchargez uniquement des applications depuis les boutiques d'applications officielles, telles que le Play Store de Google ou l'App Store d'Apple.** Le Play Store de Google et l'App Store d'Apple analysent les logiciels à la recherche de virus avant de les publier, vous garantissant ainsi la sécurité de vos téléchargements. Les applications provenant de boutiques d'applications de confiance peuvent néanmoins présenter un risque, mais les téléchargements provenant d'autres sources peuvent ne bénéficier d'aucune protection. Le NCSC publie un rapport sur les menaces concernant les boutiques d'applications : https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Maintenez votre appareil et vos applications à jour.** Installez les mises à jour de vos applications et du logiciel de votre appareil dès qu'elles sont disponibles. Activez les « mises à jour automatiques » dans les paramètres de votre appareil si elles sont disponibles pour ne pas avoir à vous en soucier. Consultez les conseils du NCSC sur la sécurité en ligne pour vous protéger contre les virus connus et autres types de logiciels malveillants. Les mises à jour incluent souvent des améliorations et de nouvelles fonctionnalités : https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Ne débloquez pas et ne 'rootez' pas votre appareil**, car cela exploite des vulnérabilités non corrigées pour contourner les contrôles de sécurité mis en place. Cela rend l'appareil plus vulnérable aux attaques. Consultez les directives du NCSC : https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Gérez vos applications

- **Vérifiez vos applications et leurs autorisations.** Si vous n'avez plus besoin d'une application, supprimez-la. Dans la mesure du possible, limitez les autorisations des applications afin de minimiser l'exposition des données, car les logiciels malveillants sont souvent conçus pour accéder à des fichiers ou périphériques protégés, tels que des caméras et des microphones{1}.
  - Comment vérifier les autorisations des applications pour les utilisateurs Apple : https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Comment vérifier les autorisations des applications pour les utilisateurs Android : https://support.google.com/android/answer/9431959?hl=en-GB

- **Envoyer automatiquement les applications inconnues à Google.** Si vous utilisez Android et avez téléchargé une application qui ne provient pas du Play Store de Google, vous pouvez l'envoyer à Google en activant 'Améliorer la détection des applications malveillantes' dans les paramètres de l'application Google Play Store, sous 'Play Protect'. Cette opération analysera l'application à la recherche de logiciels malveillants, contribuant ainsi à la protection des utilisateurs. Pour en savoir plus sur la configuration : https://support.google.com/android/answer/2812853?hl=en-GB

Utiliser les services en ligne

- **Utilisez les services de réputation d'URL avant de cliquer sur un lien.** Vous pouvez vérifier la sécurité d'un lien provenant d'un courriel, d'un SMS ou d'un autre site en l'analysant au préalable à l'aide de services tels que Google Transparency Report ou Virus Total. Vous pouvez également télécharger des fichiers et applications suspects vers un analyseur de logiciels malveillants, tel que Virus Total, qui peut vous aider à détecter si un fichier est malveillant. Sachez que les services d'analyse peuvent générer de faux négatifs.

- **Inscrivez-vous au programme Protection Avancée de Google.** Il s'agit d'un service gratuit conçu pour protéger les utilisateurs des services Google (Gmail, Play Store, etc.) qui risquent d'être ciblés. Ce service offre une sécurité renforcée lors de l'utilisation des services Google : https://landing.google.com/advancedprotection/

- **Inscrivez-vous à des services de résilience supplémentaires, lorsqu'ils sont disponibles.** Par exemple, les personnes à haut risque au Royaume-Uni peuvent bénéficier de services de défense supplémentaires pour renforcer leur cybersécurité. Vérifiez votre éligibilité et apprenez-en plus : https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Signaler les menaces

- **Identifier et signaler les faux comptes.** Les cybercriminels créent de faux comptes ou piratent des comptes réels pour atteindre leurs objectifs. Si vous suspectez qu'un compte est faux ou compromis, signalez-le à la plateforme et bloquez-le. De nombreux services disposent d'un processus de vérification des comptes, comme les « badges vérifiés » pour Instagram et Facebook. Cela peut aider à confirmer l'authenticité d'un compte. Le NCSC propose des conseils pour une utilisation

sécurisée des réseaux sociaux, notamment sur la vérification et le signalement des comptes compromis. : https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Hameçonnage utilisant des courriels, des SMS et des liens frauduleux.** Le NCSC peut enquêter sur les adresses de courriels et les sites web suspects. Si vous pensez qu'un site, un courriel ou un message est suspect, vous pouvez le signaler : https://www.ncsc.gov.uk/collection/phishing-scams

Glossaire NCSC

- **Android**

Système d'exploitation mobile de Google, utilisé par plusieurs fabricants de téléphones portables et de tablettes.

- **Application**

Une application est un logiciel que les utilisateurs peuvent installer ou préinstaller sur un appareil pour lui fournir des fonctionnalités ou du contenu supplémentaires.

- **Cybersécurité**

Protection des appareils, des services et des réseaux, ainsi que des informations qu'ils contiennent, contre tout accès non autorisé, vol ou dommage.

- **Appareil**

Matériel informatique physiquement présent, tel qu'un ordinateur de bureau, un téléphone portable ou une tablette.

- **iOS**

Système d'exploitation mobile d'Apple utilisé sur sa gamme d'appareils mobiles.

- **Logiciel malveillant**

Dérivé de « logiciel malveillant », un logiciel malveillant désigne tout type de logiciel susceptible d'endommager les systèmes informatiques, les réseaux ou les appareils. Comprend les virus, les logiciels de rançon et les chevaux de Troie.

- **Système d'exploitation**

Logiciel de base fonctionnant sur les ordinateurs, les tablettes et les téléphones portables, nécessaire à l'exécution d'applications et de matériel supplémentaires.

- **Hameçonnage**

Courriels ou SMS frauduleux contenant des liens vers des sites web susceptibles de contenir des logiciels malveillants ou d'inciter les utilisateurs à révéler des informations sensibles (comme des mots de passe) ou à transférer de l'argent.

- **Logiciel espion**

Un type de logiciel malveillant qui s'installe sur un appareil sans le consentement de l'utilisateur, collecte des données et les transmet à un tiers.

- **Réseaux sociaux**

Sites web et applications, tels que Facebook, X et Instagram, qui permettent de partager et de répondre au contenu généré par les utilisateurs (publications, photos et vidéos).

- **Smartphone**

Téléphones portables modernes dotés de fonctionnalités complexes, notamment ceux fonctionnant sous Android et iOS.

- **Cheval de Troie**

Un type de logiciel malveillant, déguisé en logiciel légitime, utilisé pour accéder sans autorisation à l'appareil d'une victime.

- **URL**

Uniform Resource Locator Une adresse sur le Web, telle qu'un nom de domaine (par exemple www.bbc.co.uk).

- **Virus**

Un type de logiciel malveillant conçu pour infecter des logiciels légitimes et se répliquer sur les réseaux lorsque ces programmes sont activés.

Lectures complémentaires

Conseils du Centre australien de cybersécurité

- Signaler un cybercrime, un incident ou une vulnérabilité
- Comment sécuriser vos appareils
- Sécuriser votre Téléphone portable
- Hameçonnage
- Escroqueries
- Sécurisez vos réseaux sociaux
- Conseils de sécurité pour les réseaux sociaux et les applications de messagerie

Conseils du NCSC et de la NPSA du Royaume-Uni

- Défendre la démocratie
- Médias sociaux : comment les utiliser en toute sécurité
- Conseils de sécurité des appareils pour les organisations, y compris les appareils mobiles
- Rapport sur les menaces pesant sur les boutiques d'applications.
- Sécurité personnelle des personnes à haut risque

Conseils de la NSA américaine

- Bonnes pratiques pour les appareils mobiles

Clause de non-responsabilité

Veuillez noter que cet avis fournit des informations validées au moment de sa publication.

Ce rapport s'appuie sur des informations provenant d'agences rédactrices et de sources industrielles. Les conclusions et recommandations formulées n'ont pas été formulées dans le but d'éviter tous les risques, et le respect de ces recommandations ne les éliminera pas tous. La propriété des risques liés aux informations reste la propriété du propriétaire du système concerné.

Au Royaume-Uni, ces informations sont exemptées de la loi sur la liberté d'information (Freedom of Information Act - FOIA) de 2000 et peuvent l'être en vertu d'autres lois britanniques sur l'information.

Pour toute question relative à la FOIA, veuillez contacter ncscinfoleg@ncsc.gov.uk.

Annexe : Échantillons MOONSHINE et BADBAZAAR observés

Ce tableau répertorie les applications utilisées dans les campagnes MOONSHINE et BADBAZAAR au cours des deux dernières années.

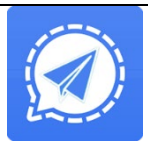
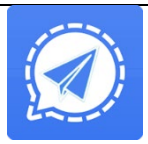
Nombre de ces applications présentent une nette similitude avec des applications établies. Il s'agit probablement d'une technique délibérée visant à usurper l'identité de marques connues.

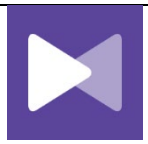
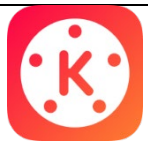
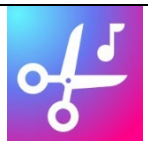
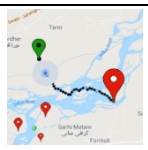
Il est important de noter que le nom de l'application, le nom du progiciel et l'icône peuvent tous imiter ou correspondre à l'application réelle et ne doivent donc pas être utilisés exclusivement pour identifier si un appareil est infecté.

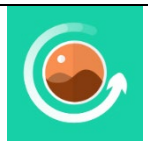
Comme indiqué dans la section sur les mesures d'atténuation, vous pouvez envoyer des applications de votre appareil Android à Google en activant l'option « Améliorer la détection des applications malveillantes », qui analysera les applications installées sur votre appareil depuis un autre appareil que le Play Store.

Titre de l'application	Nom du progiciel	Icône de l'application
99 Noms d'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	
Clavier arabe	com.arabic.keyboard.arabic.language.keyboard.app	
Cutteur audio et vidéo	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Chansons bouddhistes (1)	com.bigkidsapps.buddhistsongs1	
Calculatrice	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	

Dictionnaire EN-UG gratuit	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
RAPIDE	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
Gestionnaire de fichiers +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Pass Wi-Fi gratuit	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Coran Hefz	com.golap.hefzquran	

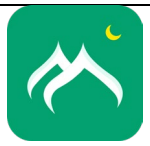
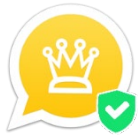
Hégire Calendrier	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
Créateur de sonneries et de MP3	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Calculateur de distance cartographique	com.routemap.mapdownload.gpsroute planner	
Récupération de médias	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	

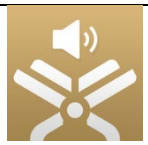
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
Lecteur PDF	pdf.pdfreader.pdfviewer.pdfeditor	
Lecteur PDF	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Éditeur	com.iudesk.android.photo.editor	
Récupération de photos	recover.restore.undelete.photo.video.file	
Studio photo	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Livre de prières	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	

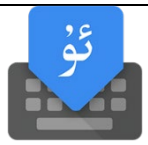
Coran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restaurer les photos supprimées	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Sons de bols chantants HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	

Clavier SwiftKey	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	
Système de divination tibétain MO	net.rhombapp.mo	
Prière tibétaine	com.chorig.tibetanprayer	
Traducteur AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	

Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Clavier ouïghour	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Ouïghour Kirguzguch	com.ziipin.softkeyboard	
Convertisseur vidéo	com.inverseai.video_converter	
Découpeur vidéo	com.naing.cutter	
Téléchargeur vidéo	downloader.video.download.free	
Créateur vidéo	com.bstech.slideshow.videomaker	
Lecteur vidéo pour 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 Enregistreur	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Météo	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	

Whoscall	gogolook.callgogolook2	
Wi-Fi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
Téléchargeur YouTube	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