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

アドバイザリー

BADBAZAAR と MOONSHINE：ウイグル、台湾、チベットのグループや市民社会を標的とするスパイウェア

2025 年 4 月 9 日

BADBAZAAR と MOONSHINE：ウイグル、台湾、チベットの団体や市民社会を標的とするスパイウェア

NCSC とそのパートナー機関は、2 種類のスパイウェアによって高いリスクにさらされている人々に向けて、新たな情報と緩和策を発表しました。

概要

本アドバイザリーは、英サイバーリーグの支援を受けて、英国家サイバーセキュリティセンター（NCSC UK）と以下の国際パートナーが共同で作成したものです。

- **オーストラリア信号局の一部門であるサイバーセキュリティセンター**
- **カナダ通信セキュリティ機関の一部門であるサイバーセキュリティセンター**
- **ドイツ連邦情報局**
- **ドイツ連邦憲法擁護庁**
- **ニュージーランド政府通信保安局の一部門である国家サイバーセキュリティセンター**
- **米連邦捜査局**
- **米国家安全保障局**

本アドバイザリーの目的は、台湾、チベット、新疆ウイグル自治区、民主化運動、法輪功などのトピックに関連する個人に対し、悪意あるサイバーアクターがもたらす脅威の高まりについて認識を高めてもらうことにあります。

本アドバイザリーには、BADBAZAAR および MOONSHINE と呼ばれるスパイウェアを用いて、スマートフォンを含む携帯端末上の中国政府が関心を持つ可能性のあるデータを標的とした、悪意あるサイバーアクターの手口を詳述した 2 件の事例が含まれています。また、本アドバイザリーでは、個人が自分自身や端末、データを保護するためのガイダンスも提示しています。

本アドバイザリーと併せて、NCSC は詳細な技術情報と個別のガイダンスを公開しています。

誰が危険にさらされているのか？

作成機関および業界パートナーは、BADBAZAAR および MOONSHINE と呼ばれるスパイウェアが、中国政府にとって国内の統治、国家的野心、国際的評価に対する脅威と見なされるトピックに関連する個人を標的としていることを確認しています。最もリスクの高い対象には、以下の関係者が含まれます（ただし、これに限定されるものではありません）。

- **台湾の独立**
- **チベットの権利**
- **中国の新疆ウイグル自治区に居住している、または出身であるウイグル人イスラム教徒およびその他の少数民族**
- **民主主義の擁護活動（香港に関連するものを含む）**
- **法輪功の精神運動**

これには、これらの団体を擁護したり、同調したり、何らかの形で関係を持つ非政府組織（NGO）、ジャーナリスト、企業、個人が含まれます。このスパイウェアは無差別にオンライン上で拡散されているため、本来の標的以外にも感染が広がるリスクがあります。

本アドバイザリーは、BADBAZAAR および MOONSHINE と呼ばれるスパイウェアがもたらす特定の脅威に対して、リスクにさらされている人々が効果的に対応できるよう支援することを目的としています。本アドバイザリーで示された対策は、包括的なサイバーセキュリティ上の助言を補完するものであり、単独で講じるべきものではありません。

本アドバイザリーで参照されているガイダンスに従うことで、携帯端末およびデータがスパイウェアに感染するリスクを低減することができます。

脅威

MOONSHINE および BADBAZAAR は、トロイの木馬型マルウェアの一種であり、正常に動作するアプリに悪意のある機能を隠し持っています。これらのアプリは、アプリストアやオンラインのファイル共有サービスを通じて配布される可能性があります。

これらのアプリは、ユーザーに誤ってダウンロードおよびインストールさせるよう巧妙に設計されています。アプリが一度インストールされると、端末の脆弱性を悪用して不正な機能を実行したり、ユーザーにアプリの権限を許可させることで端末内の情報にアクセスし、データを取得したりする可能性があります。対象となる情報には、以下が含まれます。

- **位置情報（リアルタイム追跡を含む）**
- **マイクおよびカメラへのアクセス**
- **端末に保存されているメッセージ、写真、その他のファイル**
- **端末情報など**

アクターはその後、リスクにさらされている人々の正当な関心を巧みに悪用し、できる限り多くの対象者を特定・感染させて、彼らのデータへアクセスします。彼らがこのような手口を使う一例として、被害者の関心を引くことが分かっているアプリを設計することが挙げられます。たとえば、被害者の母国語に対応したアプリや、中国のチベット地域や新疆など、特定の地域に関連するコンテンツを含むアプリなどです。

本アドバイザリーに掲載されているケーススタディでは、TibetOne アプリやウイグル語のコーランアプリなど、その具体例が紹介されています。

アクターは、標的とする被害者層が利用するオンラインフォーラム上で活動することで、マルウェア感染の機会を最大化しています。彼らがチベット関連の Telegram チャンネルや Reddit のフォーラムでスパイウェアを意図的に共有していることが確認されています。本アドバイザリーに掲載されているケーススタディも、こうした手口の例を示しています。

悪意のあるアプリは、Android の APK ファイルのようなスタンドアロン形式のファイルとして共有されることが多く、ユーザー自身がそれをダウンロードしてインストールする必要があります。アクターは、スパイウェアを正規のアプリに見せかけるために、Google Play ストアや Apple の App Store などの公式アプリストアにアップロードしたり、本来は無害なアプリに悪意のあるコードを埋め込んだりすることがあります。ただし、これらの公式ストアにはセキュリティ機能や審査プロセスが備わっているため、こうした手口が成功する可能性は比較的低いとされています。これにより、公式ストアのアプリはより安全になりましたが、本アドバイザリーの事例や NCSC の「アプリストアに関する脅威レポート」で示されているように、これらのプロセスも完全ではありません。

以下の 4 つの対策を実践することで、本アドバイザリーで説明されている脅威から身を守ることができます。

詳細については、緩和策のセクションをご覧ください。

ケーススタディ

これら 2 つの事例は、MOONSHINE および BADBAZAAR がどのように機能するのか、また、悪意あるサイバーアクターが最もリスクの高い人々をどのように標的にしているのかを示しています。

ケーススタディ 1：MOONSHINE

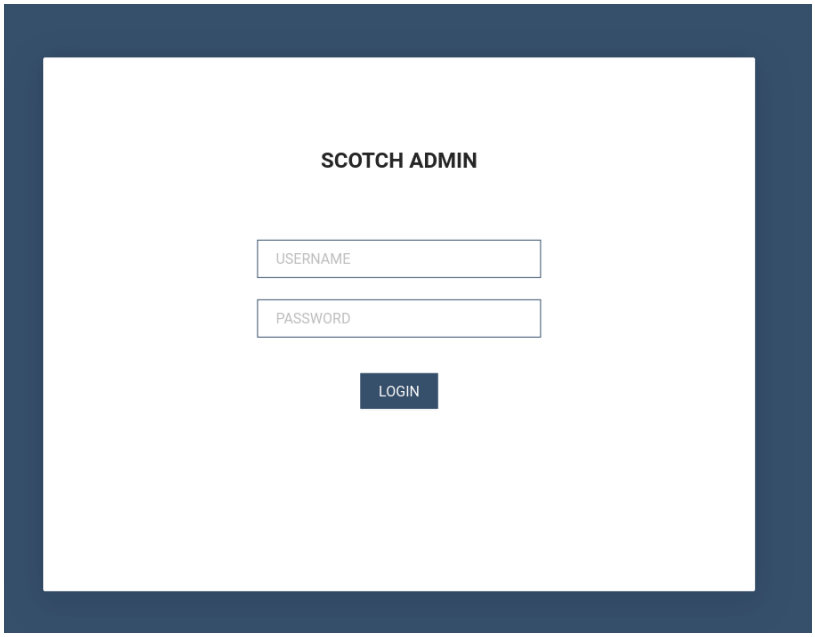
MOONSHINE は、チベット系団体を標的とした Android 向けスパイウェアであり、2019 年にシチズン・ラボによって報告されました。MOONSHINE は正規のアプリを装い、被害者にインストールさせるよう誘導します。このスパイウェアは、Telegram のチャンネルや WhatsApp で送信されたリンクを通じて拡散されています。

MOONSHINE には、以下のような広範な監視機能があります：

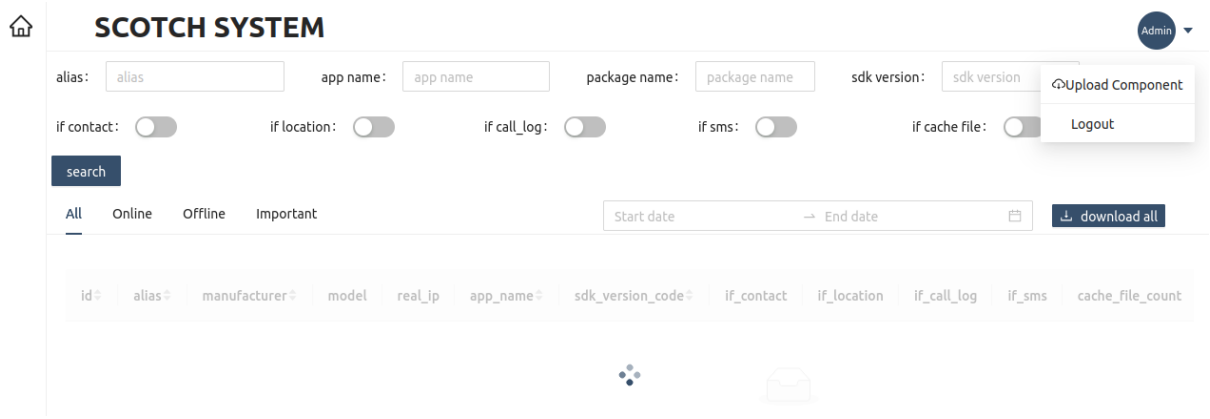
- **位置情報（リアルタイム追跡を含む）**
- **音声および写真のリアルタイム取得**
- **端末からのファイルのダウンロード**
- **端末情報の取得**
- **端末上での音声の再生**

「**ئاۋازلىق قۇرئان.apk**」（訳：**音声コーラン.apk**）というアプリは、MOONSHINE がウイグル人を標的とする手口の一例です。ウイグル語でコーランアプリであることを示すこのファイル名は、ウイグル系イスラム教徒の関心を引くことを意図して付けられた可能性があります。

一度インストールされると、悪意あるサイバーアクターは被害者の端末から情報を収集することができます。この情報は、「SCOTCH ADMIN」パネルを通じてアクセスされます。



ログインすると、アクターは以下のスクリーンショットに示すページにアクセスできます。このページには、感染端末の詳細と、アクターが持つアクセス権限のレベルが表示されます。



マルウェアの管理パネルには、以下を含む収集済みのデータが表示されます。

- **端末へのアクセスレベル**
- **SMS メッセージ**
- **通話履歴**
- **位置情報**
- **端末情報**

NCSC はサイバーリーグと連携し、トレンドマイクロ社による業界レポートをもとに、MOONSHINE のエクスプロイトキットと、HTML タイトルに「UPSEC」を含むログインパネルと

の間に共通点があることを突き止めました。詳細については、添付のテクニカル・アドバイザリーをご参照ください。

Intelligence Online によると、UPSEC とは「四川電科網絡安全技術有限公司（Sichuan Dianke Network Security Technology Co. Ltd）」を指しているとされています。この内容については、作成機関による裏付けは取られていません。

ケーススタディ 2：BADBAZAAR

BADBAZAAR は、iOS および Android 向けの亜種を持つモバイルマルウェアであり、ウイグル人、チベット人、台湾人を標的としています。このマルウェアは、ソーシャルメディアプラットフォームや公式アプリストアを通じて拡散しています。

BADBAZAAR は、Lookout および Volexity の報告によると、「**TibetOne**」というアプリを通じてチベット人を標的とするために使用されています。**TibetOne** は、悪意あるアクターによって作成された iOS アプリであり、端末情報や位置情報にアクセスする機能を備えています。このアプリは 2021 年 12 月に Apple の App Store に公開されましたが、現在は利用できなくなっています。このマルウェアをさらに拡散させるために、アクターは「**tibetanphone**」という Telegram チャンネルでもこのアプリを宣伝していました。

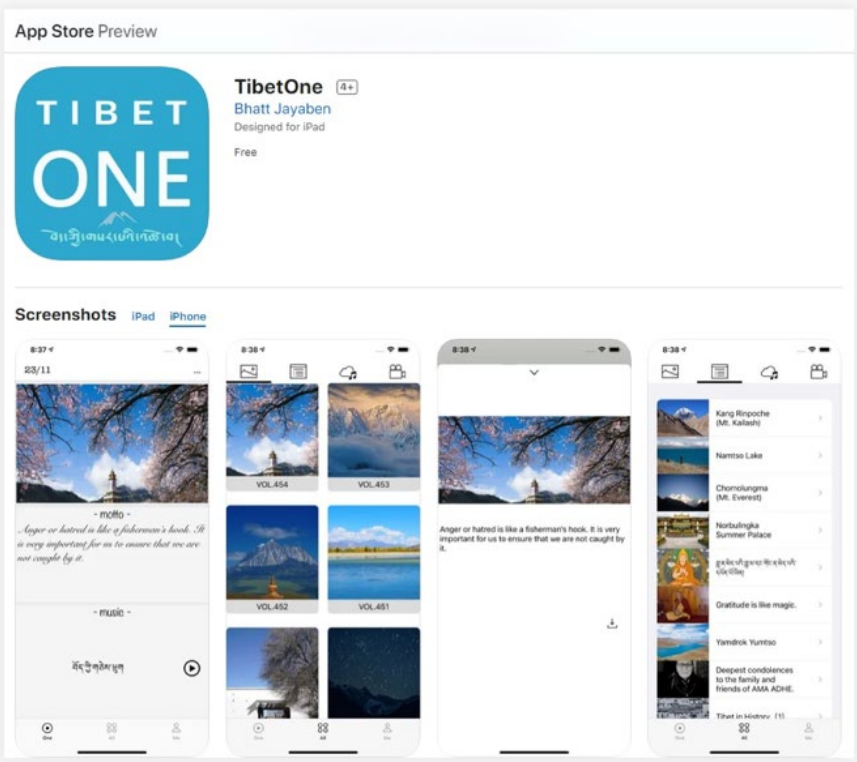


図 1：Apple App Store 上の TibetOne アプリのページ。このアプリはその後削除されました。

図 2：Telegram チャンネルで共有された TibetOne。

アクターはアプリの信頼性を高めるために、「tibetone[.]org」というウェブサイトも開設しました。このサイトでは、自らを「チベット文化を愛する人々に豊かで高品質な作品を届け、読書を新しいライフスタイルとする」ことを目的とするものと紹介していました。

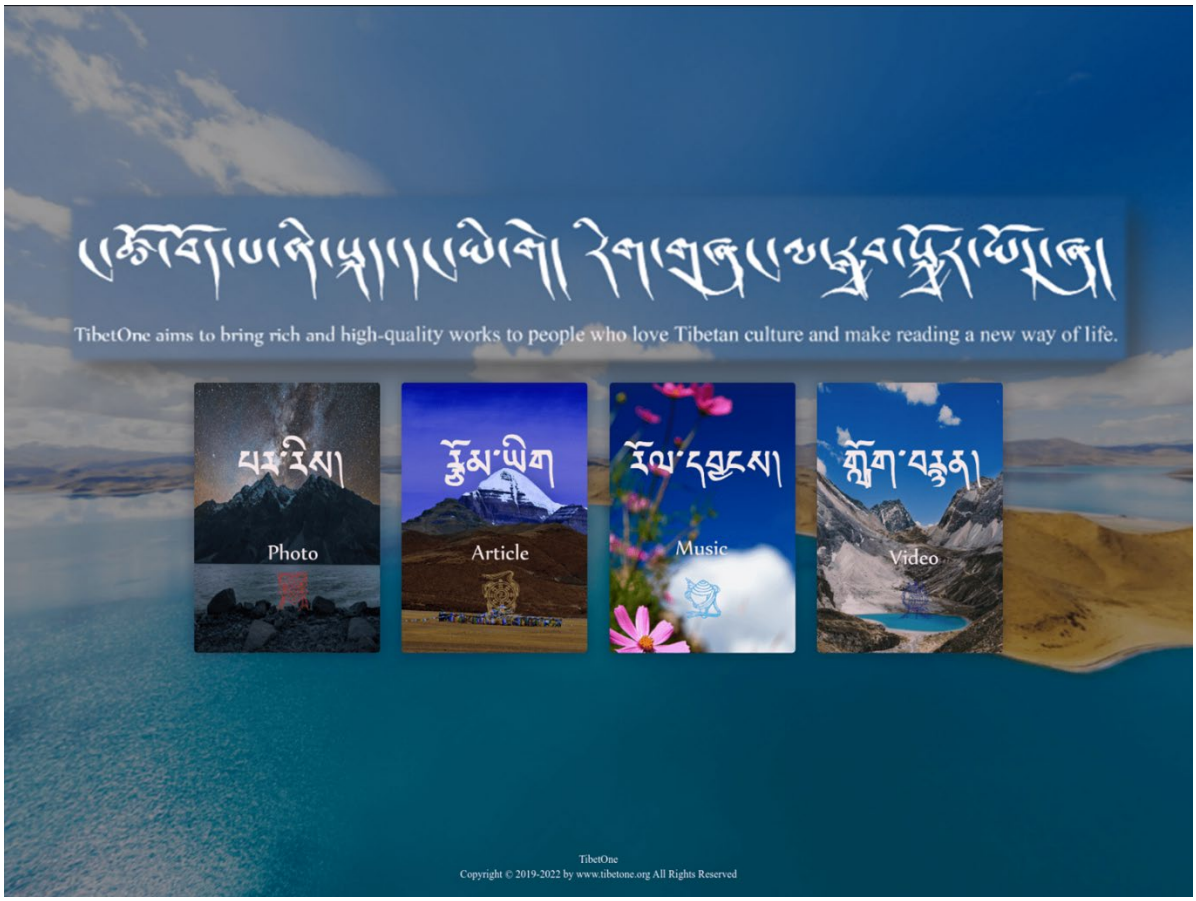


図 3：tibetone[.]org のホームページ。

この画像は、該当箇所をより分かりやすくするために編集されています。

このウェブサイトには記事を掲載したページがあり、ユーザーがコメントを残せるようになっていました。「choekyi.wangmo@ignitetibet.net」という、悪意あるアクターが管理していると考えられるメールアドレスから投稿されたコメントは、チベット人権民主センター（Tibetan Centre for Human Rights and Democracy）が親チベット系の抗議活動家として記載している「Choekyi Wangmo」になりすましている可能性があります。これも、アプリがチベット独立を支持しているかのような印象を与えることを目的とした試みであると考えられます。

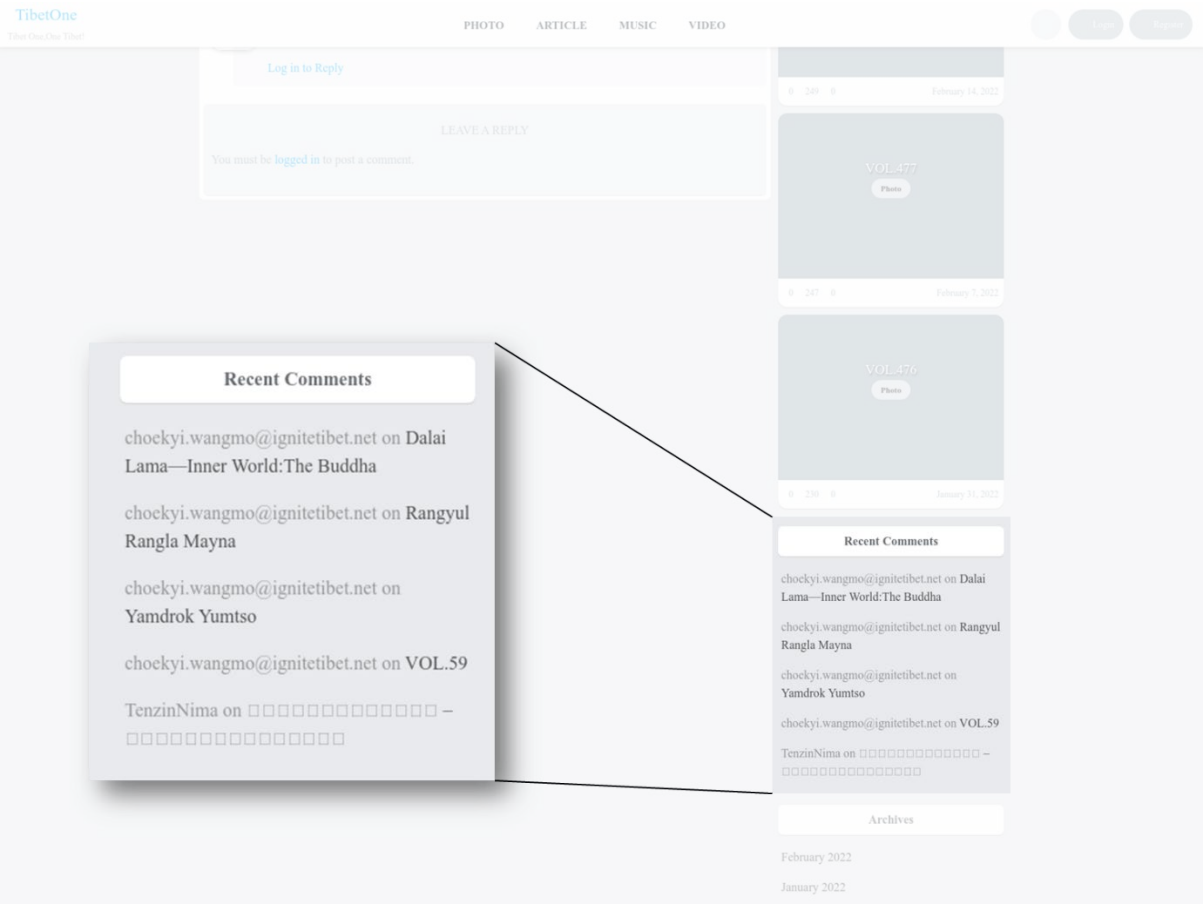


図４：悪意あるアクターが管理しているとされるユーザーアカウントからのコメントが表示されている、tibetone[.]org のページ

この画像は、該当箇所をより分かりやすくするために編集されています。

「**TenzinNima**」も、このサイトにコメントを投稿したユーザー名の一つです。Volexity の報告によると、このユーザー名が Reddit 上でも使用されており、Telegram チャンネル「**Tibetanmaptalk**」の宣伝に使われているということです。これには、Android 端末向けのナビゲーションアプリ「**AlpineQuest**」の悪意あるサンプルをダウンロードするためのリンクが含まれています。このダウンロードリンクは、Mega というサードパーティのファイル共有サービスに接続されています。

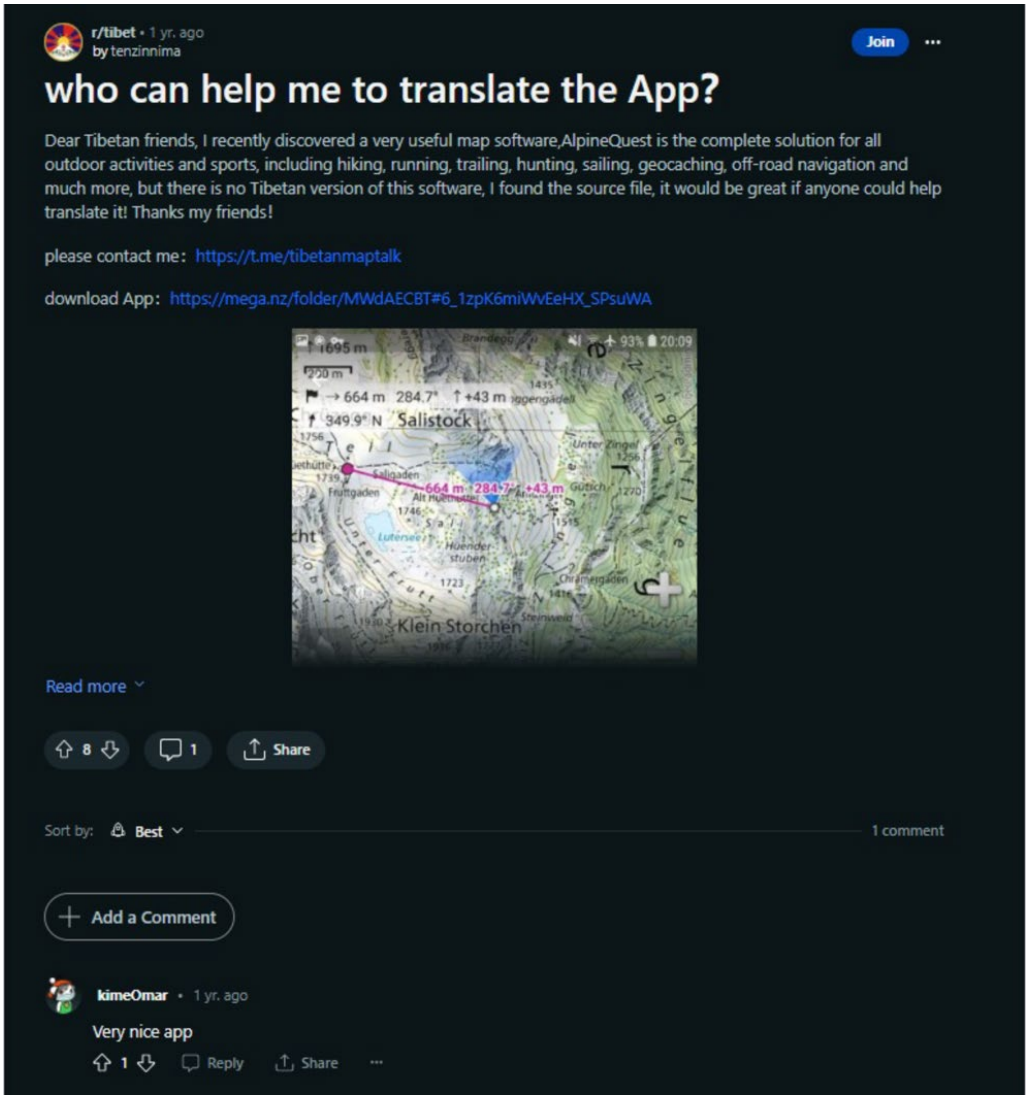


図 5：悪意あるアクターが管理していると考えられるアカウントによる、悪意あるアプリを宣伝する Reddit の投稿

Volexity はまた、この投稿にコメントした「KimeOmar」というユーザーが、別の Reddit フォーラムでも悪意あるアプリを共有していることが確認されていると指摘しています。これは、悪意あるアクターが複数のソーシャルメディアアカウントを使用し、投稿を正当なものに見せかけている可能性を示唆しています。

評価

BADBAZAAR と MOONSHINE は、特にウイグル人、チベット人、台湾人コミュニティを標的とし、複数のソーシャルエンジニアリング手法を用いています。具体的には以下のとおりです。

- ウイグル語のコーランアプリのように、対象コミュニティが関心を持つアプリをトロイの木馬化する手法は、ほぼ確実に標的となる被害者層に合わせて意図的に仕組まれたものと考えられます。
- これらのトロイの木馬化されたアプリを公式アプリストアに掲載する行為は、正当性を装うための手段である可能性が極めて高く、また、グループチャット内での共有は、これらのコミュニティ内における信頼関係を悪用する意図があると考えられます。

BADBAZAAR および MOONSHINE は、中国政府にとってほぼ確実に価値のあると考えられるデータを収集しています。BADBAZAAR および MOONSHINE は、ウイグル人、チベット人、台湾人を標的にしていることが確認されていますが、中国国内の他の少数民族を標的とする別のマルウェアも存在します。中国国内外を問わず、共同署名国（co-sealing nations）の市民で、体制の安定を脅かすと見なされる活動を支持していると認識されている者は、BADBAZAAR や MOONSHINE のようなモバイルマルウェアによる脅威にさらされている可能性が極めて高いといえます。位置情報、音声、写真データを取得する機能は、対象者の行動に関するリアルタイム情報を提供することにより、将来的な監視や嫌がらせ行為に活用される可能性が極めて高いと考えられます。

モバイルアプリ利用者向けの緩和策

ケーススタディで説明された脅威への対策として、作成機関は以下のセキュリティ対策の実施を推奨しています。これらの推奨事項は、NCSC のベストプラクティスに基づいています。オーストラリアおよび米国におけるベストプラクティスに関するガイダンスについては、「参考資料」セクションのリンクをご参照ください。

端末のセキュリティを確保する

- **アプリは、Google Play ストアや Apple App Store など、公式のアプリストアからのみダウンロードしてください。**Google の Play Store や Apple App Store では、ソフトウェアが公開される前にウイルススキャンが行われるため、ダウンロードするアプリが安全であるという一定の安心感が得られます。信頼性のあるストアから提供されるアプリであっても一定のリスクは残りますが、非公式なソースからダウンロードされたアプリには、セキュリティ保護が一切講じられていない可能性があります。NCSC は、アプリストアに関する脅威レポートを公開しています：https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **端末とアプリを常に最新の状態に保つ**アプリや端末ソフトウェアのアップデートが利用可能になったら、速やかにインストールしましょう。設定で「自動アップデート」を有効にしておけば、更新するのを忘れる心配がありません。既知のウイルスやその他のマルウェアへの対策として、NCSC によるオンライン上の安全確保に関するガイダンスの参照を推奨します。アップデートには、改善や新機能が含まれていることがよくあります：https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **端末を「脱獄（ジェイルブレイク）」や「ルート化」しないでください。**これらの行為は、実装されているセキュリティ対策を回避し、未修正の脆弱性が悪用されるリスクを高めます。これにより、端末は攻撃に対してより脆弱な状態になります。NCSC のガイダンスをご参照ください：https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

アプリを管理する

- **アプリとその権限設定を見直しましょう。**不要になったアプリは削除しましょう。可能な限りアプリの権限を制限し、データの漏えいリスクを最小限に抑えてください。マルウェアは、保護されたファイルや、カメラやマイクなどの周辺機器へのアクセスを目的として設計されていることがよくあります。。
  - Apple ユーザーがアプリの権限を確認する方法：https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Android ユーザーがアプリの権限を確認する方法：https://support.google.com/android/answer/9431959?hl=en-GB

- **不明なアプリを Google に自動送信する** Android ユーザーで、Google Play ストア以外からダウンロードしたアプリがある場合は、Google Play ストアアプリの設定内にある「Play プロテクト」で「有害なアプリの検出精度を改善」を有効にすると、そのアプリが Google に送信されます。これにより、アプリがマルウェアかどうかスキャンされ、ユーザーの保護につながります。設定方法：https://support.google.com/android/answer/2812853?hl=en-GB

サイバーサービスを活用する

- **リンクをクリックする前に、URL の評価サービスを利用してください。**メールやテキストメッセージなどに含まれるリンクが安全かどうかを確認するには、Google 透明性レポートや VirusTotal などのサービスを使って、事前にリンクをスキャンするのが有効です。不審なファイルやアプリは、VirusTotal などのマルウェア解析サービスにアップロードすることで、それらが悪意のあるものであるかどうかを検出できます。スキャンサービスによっては、偽陰性が出ることがあるので注意してください。

- **Google の高度な保護機能プログラムに登録しましょう。**これは、Gmail や Play ストアなどの Google サービスを利用しており、標的にされるリスクのある個人を保護するための無料サービスです。このサービスは、Google サービス利用時のセキュリティをより強化します。https://landing.google.com/advancedprotection/

- **利用可能な場合は、追加のレジリエンス強化サービスにも登録しましょう。**たとえば、英国ではハイリスクの個人が、サイバーセキュリティ対策を支援するための追加防御サービスを受けられる場合があります。資格の確認と詳細 https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

脅威を報告する

- **なりすましアカウントの特定と報告**悪意のあるサイバーアクターは、自らの目的を達成するために偽のアカウントを作成したり、本物のアカウントを乗っ取ったりします。アカウントが偽アカウントまたは乗っ取られていると疑われる場合は、プラットフォームに報告のうえ、ブロックしてください。Instagram や Facebook の「認証バッジ」のように、多くのサービスにはアカウントを確認する仕組みが用意されています。これは、アカウントが本物であることを識別する助けになります。NCSC は、アカウントの確認方法や、乗っ取られたアカウントの報告方法などを含む、ソーシャルメディアを安全に利用するためのガイダンスを提供しています：https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **詐欺メールや SMS、リンクを利用したフィッシング** NCSC は、不審なメールアドレスやウェブサイトの調査を行うことができます。ウェブサイトやメール、メッセージに不審な点があると思った場合は、報告することができます：https://www.ncsc.gov.uk/collection/phishing-scams

NCSC 用語集

Android（アンドロイド）

Google のモバイルオペレーティングシステムであり、複数のスマートフォンやタブレットのメーカーに採用されています。

アプリ

アプリケーション（アプリ）とは、ユーザーが端末にインストールするか、あらかじめインストールされているソフトウェアのパッケージであり、端末に追加機能やコンテンツを提供するものです。

サイバーセキュリティ

端末、サービス、ネットワークおよびそれらに含まれる情報を、不正アクセス、盗難、損害から保護すること。

端末（デバイス）

デスクトップコンピュータ、スマートフォン、タブレットなど、物理的に存在するコンピュータベースのハードウェア。

iOS

Apples 社製のモバイル端末に搭載されているモバイルオペレーティングシステム（OS）。

マルウェア

「マルウェア（malware）」は「悪意のあるソフトウェア（malicious software）」に由来し、コンピュータシステムやネットワーク、端末に損害を与える可能性がある、あらゆる種類のソフトウェア。ウイルス、ランサムウェア、トロイの木馬などが含まれます。

オペレーティングシステム

コンピュータ、タブレット、スマートフォンで動作する基本ソフトウェアであり、追加のアプリケーションやハードウェアを動作させるために必要となります。

フィッシング

マルウェアが仕込まれたウェブサイトへのリンクを含むものや、パスワードなどの機密性の高い情報を入力させたり、金銭の送金を促したりする詐欺メールやテキストメッセージ。

スパイウェア

ユーザーの同意なしに端末にインストールされ、データを収集して第三者に送信するタイプのマルウェア。

ソーシャルメディア

Facebook、X、Instagram などのように、ユーザーが投稿した文章・写真・動画などのコンテンツを共有し、それに対して他のユーザーが応答できるウェブサイトやアプリ。

スマートフォン

Android や iOS などのオペレーティングシステムを搭載し、高度な機能を備えた最新の携帯電話。

トロイの木馬

正規のソフトウェアを装い、被害者の端末に不正アクセスするために使用されるタイプのマルウェアの一種。

URL

ユニフォーム・リソース・ロケーター（Uniform Resource Locator）の頭文字をとったもの。ドメイン名のような、ワールドワイドウェブ上のアドレス（例：www.bbc.co.uk）

ウイルス

正規のソフトウェアに感染し、そのソフトウェアが実行されるとネットワークを通じて複製するように設計されたマルウェアの一種

参考資料

オーストラリア・サイバーセキュリティセンターのガイダンス

- サイバー犯罪、インシデント、脆弱性を報告する
- 端末のセキュリティ対策方法
- 携帯電話のセキュリティを確保する
- フィッシング
- 詐欺
- ソーシャルメディア上でセキュリティを確保する
- ソーシャルメディアやメッセージアプリのセキュリティ対策のヒント

英国 NCSC および NPSA のガイダンス

- 民主主義を守る
- ソーシャルメディア：安全な使い方
- 携帯端末を含む、組織向けのデバイスセキュリティガイダンス
- アプリストアに関する脅威レポート
- ハイリスク個人のための安全・セキュリティ対策

米 NSA のガイダンス

- 携帯端末に関するベストプラクティス

免責事項

本アドバイザリーは、公開時点で確認された情報に基づいていますのでご留意ください。

本報告書は、作成機関および業界の情報源に基づいて作成されています。本報告書における所見や推奨事項は、あらゆるリスクを回避することを目的として提供されているものではなく、推奨事項に従ったとしても、すべてのリスクが排除されるわけではありません。情報に関するリスクの責任は、常に関連するシステムの所有者にあります。

英国では、この情報は 2000 年情報公開法（FOIA）の適用除外となっており、他の英国の情報関連法令においても非開示とされる可能性があります。

FOIA（情報公開法）に関するお問い合わせは、ncscinfoleg@ncsc.gov.uk までお願いします。

付録：MOONSHINE& BADBAZAAR の確認例

この表は、過去 2 年間に MOONSHINE および BADBAZAAR による攻撃活動で利用されたアプリを一覧にしたものです。

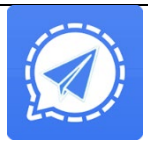
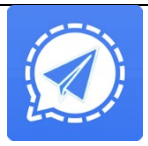
これらのアプリの多くは、既存の正規アプリと極めて類似しています。これは、著名なブランドを偽装するために攻撃者が意図的に用いた手法である可能性が高いです。

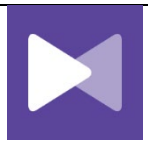
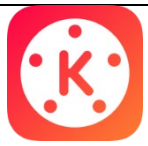
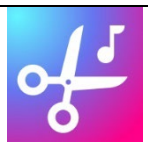
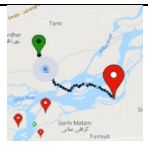
アプリ名やパッケージ名、アイコンは正規アプリと同じに見えることがあるため、それだけで感染の有無を判断するのは適切ではありません。

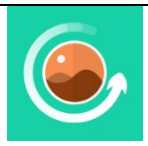
緩和策のセクションでも述べられているとおり、「有害なアプリの検出精度を改善」機能を有効にすることで、Google にアプリを送信し、Play ストア以外からインストールされたアプリをスキャンさせることができます。

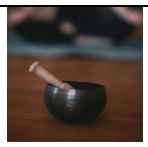
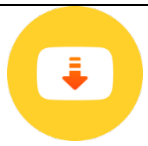
アプリ名	パッケージ名	アプリのアイコン
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

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	

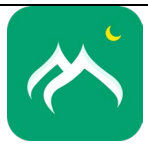
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar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

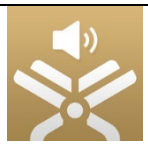
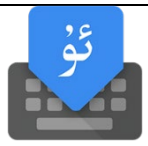
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn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