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

公告

BADBAZAAR 和 MOONSHINE：針對維吾爾族、台灣和藏族團體以及社運人士的間諜軟件

2025 年 4 月 9 日

BADBAZAAR 和 MOONSHINE：針對維吾爾族、台灣和藏族團體以及社運人士的間諜軟件

NCSC 及其合作夥伴公布新的資訊和緩解措施，幫助高風險人士應對兩種間諜軟件變種。

概要

在英國 網路聯盟 的支持下，英國國家網路安全中心 (NCSC UK) 和國際合作夥伴共同發布了此公告：

- **澳洲網路安全中心，隸屬於澳洲信號局**
- **加拿大網路安全中心，隸屬於加拿大通訊安全機構**
- **德國聯邦情報局**
- **德國聯邦憲法保衛局**
- **紐西蘭國家網路安全中心，隸屬於紐西蘭政府通訊安全局**
- **美國聯邦調查局**
- **美國國家安全局**

本公告旨在提高公眾對惡意網路行為者所帶來的日益嚴重威脅的認識，主要與台灣、西藏、新疆維吾爾自治區、民主運動和法輪功等議題相關的人士。

本公告包括兩個個案研究，詳細解釋惡意網路行為者使用名為 BADBAZAAR 和 MOONSHINE 的間諜軟件及其技術，用於從目標的流動裝置（如智慧型手機）獲取中國政府可能感興趣的資訊。同時亦提供指導建議，幫助個人保護自己、設備和資料。

除此公告外，NCSC 還發布了完整的技術細節，另附指南。

哪些人士正面臨風險？

本公告的撰寫機構和業界夥伴發現，BADBAZAAR 和 MOONSHINE 專門針對和個別議題有關的人士，而這些議題是被中國政府視為威脅，如影響其國內權威、宏願和全球聲譽。 面臨風險最高的人士，包括但不限於，與下列議題有關的任何人：

- **台灣獨立**
- **藏人權利**
- **維吾爾族穆斯林及其他正身處或來自中國新疆維吾爾自治區境內的少數民族**
- **民主倡議（包括香港）**
- **法輪功**

當中包括倡導、認同或以其他方式代表這些群體的非政府組織 (NGO)、記者、企業和個人。這種間諜軟件在網路上不分區別地傳播，也代表可能蔓延至目標受害者之外的人士。

此公告旨在幫助面臨風險的人士有效應對來自 BADBAZAAR 和 MOONSHINE 間諜軟件的威脅。所建議的緩解措施應與更廣泛的網路安全建議互相補充，不應被單獨考慮。

透過遵循本公告中引用的指引，使用者可以降低其流動裝置和數據受到感染的風險。

威脅

MOONSHINE 和 BADBAZAAR 是木馬程式，其惡意功能隱藏在可從應用程式商店或網上檔案共用服務下載，且能正常運作的應用程式當中。

這些應用程式旨在誘騙用戶下載並安裝至裝置中。應用程式安裝後，會利用裝置上的漏洞，執行未經授權的功能，或可能依賴使用者授予權限，讓應用程式存取和下載裝置資訊，包括：

- **包括實時追蹤的位置數據**
- **麥克風和攝影機的存取**
- **裝置上儲存的訊息、照片和其他文件**
- **裝置資訊等**

攻擊者及後會利用這些高風險群體的關注事項，識別和盡可能感染更多受害者，並盜取他們的數據。方法包括設計能吸引受害者的應用程式，例如支援其母語，或包含特定地區（如中國西藏地區或新疆）的內容。

本公告的個案研究中提供了使用這方法的例子，包括 TibetOne 和 Uyghur Quran 應用程式。

攻擊者活躍於線上論壇，主要用戶群體就是他們的目標受害群體，務求把感染受害者的機會提升至最高。據觀察，他們會故意在與西藏相關的 Telegram 頻道和 Reddit 論壇上分享間諜軟件。本公告的個案研究也舉出了這些方法的例子。

惡意應用程式通常會以獨立檔案的形式共享，例如 Android 的 APK 檔案，要由用戶下載並安裝。為使間諜軟件看起來更為正當，攻擊者試圖把這些軟件上傳到官方應用程式商店（例如 Google Play Store 和 Apple App Store），或在之前無害的應用程式中加入惡意程式碼，但因為官方商店具有安全功能和審查流程，令這種策略不太成功。即使來自官方商店的應用程式會更為安全，但正如在個案研究和 NCSC 的 App Store 威脅報告 中所表明，這些流程並非完美。

遵循這 4 個建議可助您免受本公告中所概述的威脅。

更多詳細的建議，請參閱緩解措施部分。

個案研究

這兩個案例說明 MOONSHINE 和 BADBAZAAR 是如何運作，以及惡意網路行為者如何針對那些高風險群體。

個案研究（一）：MOONSHINE

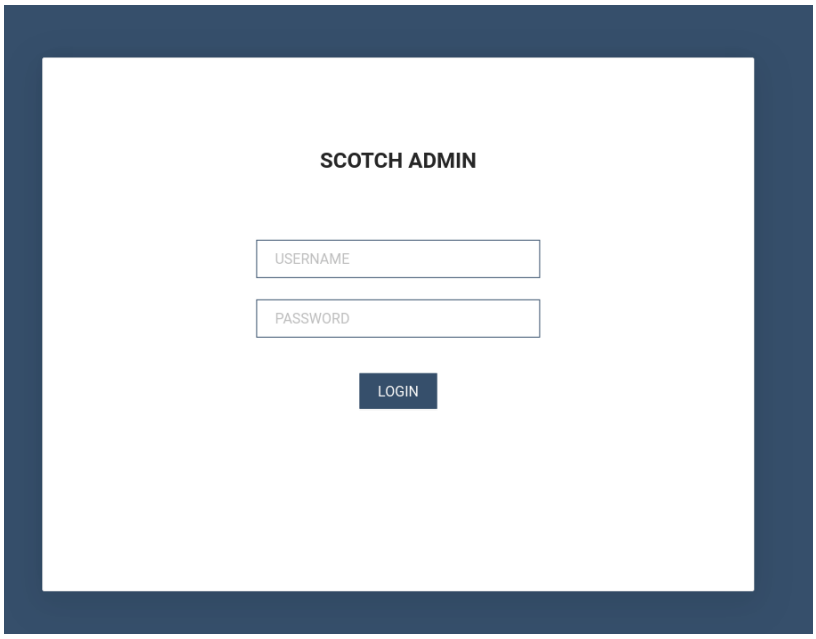
MOONSHINE 是一款 Android 間諜軟件，由公民實驗室 於 2019 年報告，指其針對的是藏族群體。MOONSHINE 偽裝成正當的應用程式以引誘受害者安裝。這應用程式是透過 Telegram 頻道和 WhatsApp 發送的連結分享。

MOONSHINE 具有廣泛的監視能力，例如：

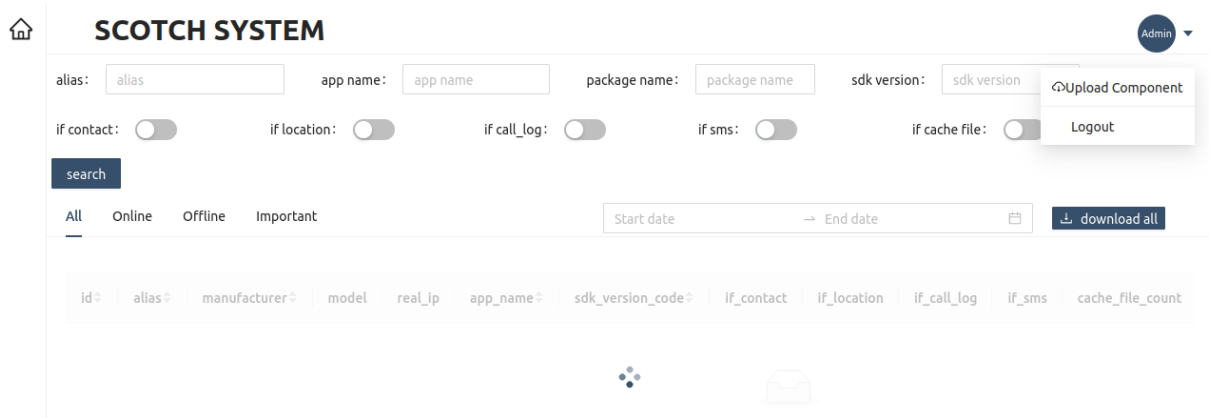
- **包括實時追蹤的位置數據**
- **捕捉即時音訊和照片**
- **從裝備下載文件**
- **取得裝備資訊**
- **於裝置播放音訊**

應用程式 **'قۇرئان ناۋازلىق.apk'**，中譯為「**語音古蘭經.apk**」，是 MOONSHINE 利用來針對維吾爾族人的例子。維吾爾語的檔案名稱表明這是一個《古蘭經》應用程式，很可能是為了吸引維吾爾族穆斯林。

一旦安裝，惡意網路行為者就可以從受害者的裝置收集資訊。資訊可以透過「SCOTCH ADMIN」面板存取。



一旦登錄，攻擊者就可以前往下面螢幕截圖所示的頁面。此頁面顯示受感染裝置的詳細資訊，以及攻擊者對受感染裝置的存取等級：



惡意軟件的管理面板會顯示收集到的數據，包括：

- 裝置存取級別
- **SMS** 短訊
- 通話紀錄
- 位置資訊
- 裝置資訊

NCSC 與 Cyber League 合作，根據業界機構 趨勢科技的報告，發現 MOONSHINE 入侵工具包與 HTML 標題中包含「UPSEC」的登入面板之間，兩者存在相同之處。完整詳細資訊請參閱隨附的技術公告。

根據 情報在線 的資訊，UPSEC 指的是「四川電科網路安全技術有限公司」。撰寫機構尚未證實此說法。

個案研究（二）：BADBAZAAR

BADBAZAAR 是一種有 iOS 和 Android 版本的惡意流動應用軟件 ，以維吾爾族、藏族和台灣人為目標。此惡意軟件是透過社交媒體和官方應用程式商店傳播。

Lookout 和 Volexity 的通報指，BADBAZAAR 透過「**TibetOne**」應用程式以攻擊藏人。**TibetanOne** 是一款由惡意行為者製作的 iOS 應用程式，能夠存取裝置資訊和位置資料。這應用程式在 2021 年 12 月被上傳至 Apple App Store，但現在已被下架。為進一步傳播該惡意軟件，攻擊者還在名為「**tibetanphone**」的 Telegram 頻道中宣傳該應用程式。

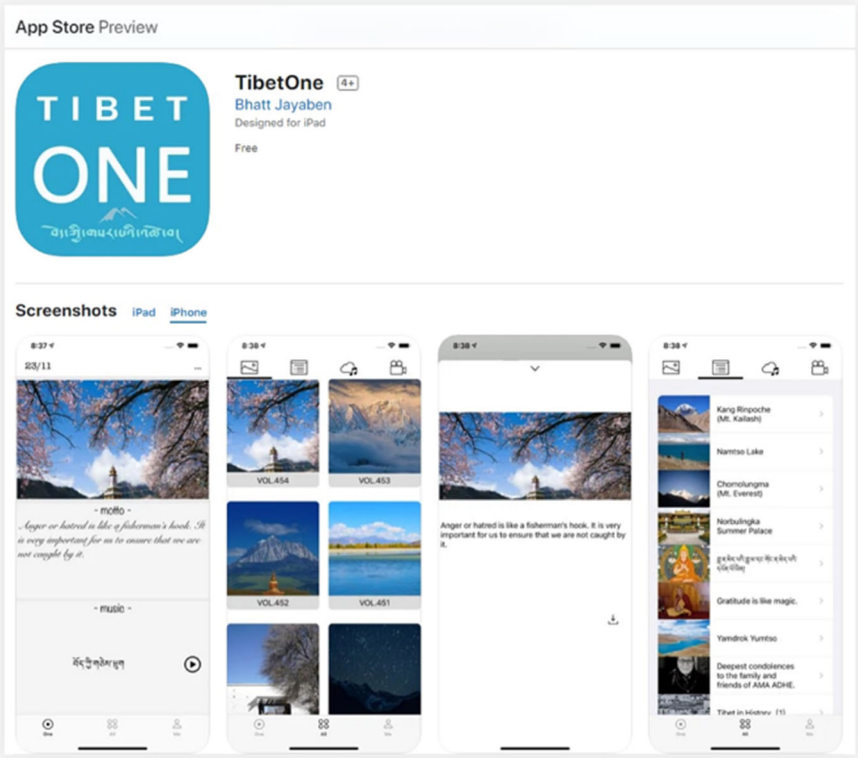


圖 1:TibetOne 應用程式在 Apple App Store 中的頁面。此應用程式已被移除。

Figure 2:TibetOne 在 Telegram 頻道中分享。

為令該應用程式看起來是正當的，攻擊者還開發了一個名為「**tibetone[.]org**」的網站，並自稱「為熱愛西藏文化的人們帶來豐富及優質的作品，並讓閱讀成為一種新的生活方式」。

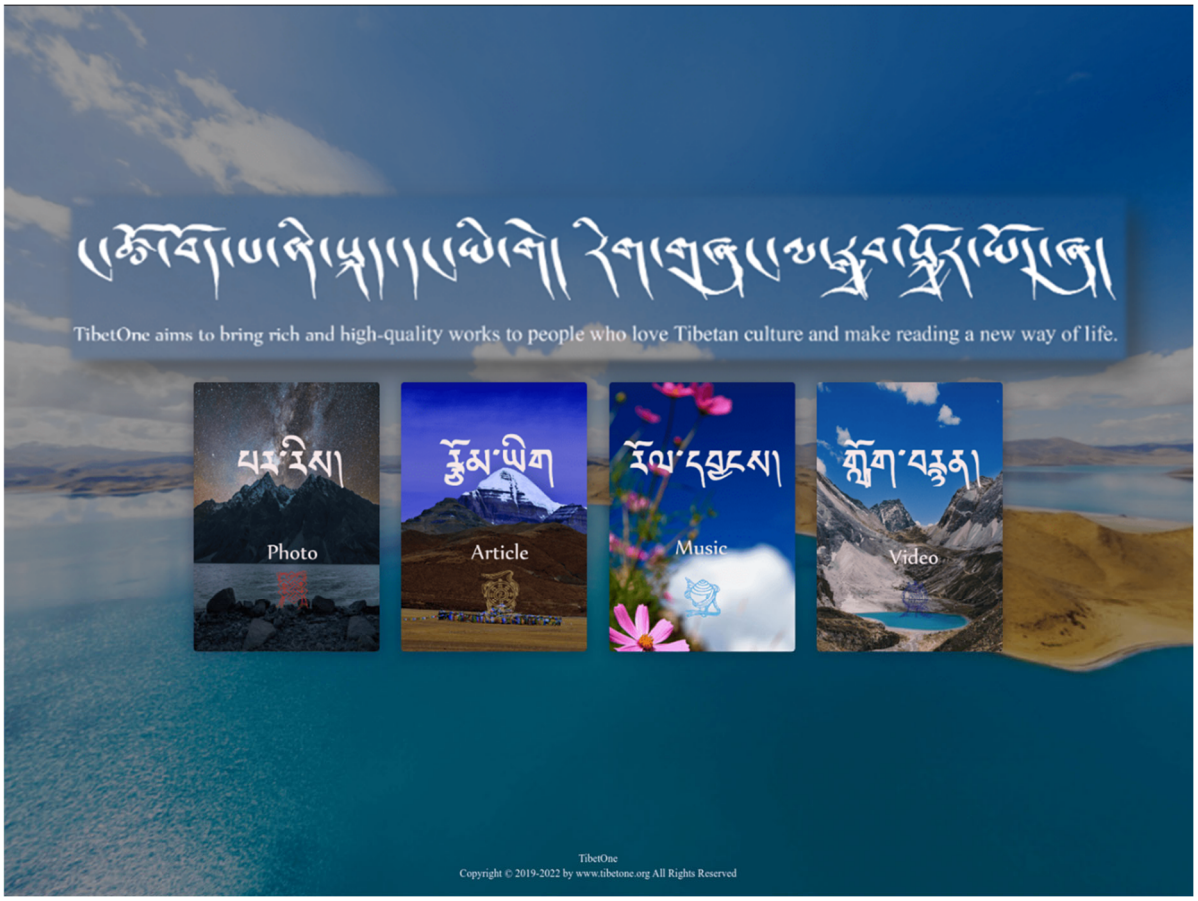


圖 3:「tibetone[.]org」的首頁。

本圖像已被編輯，使相關部分更加清晰。

該網站有一文章頁面，允許使用者發表評論。當中的一個評論，是從 電子郵件 地址「**choekyi.wangmo@ignitetibet.net**」發表，相信是由惡意行為者控制的，可能是冒充「**Choekyi Wangmo**」，而西藏人權與民主中心指他是支持西藏的抗議人士。該應用程式試圖藉此讓人留下他們真心主張西藏獨立的印象。

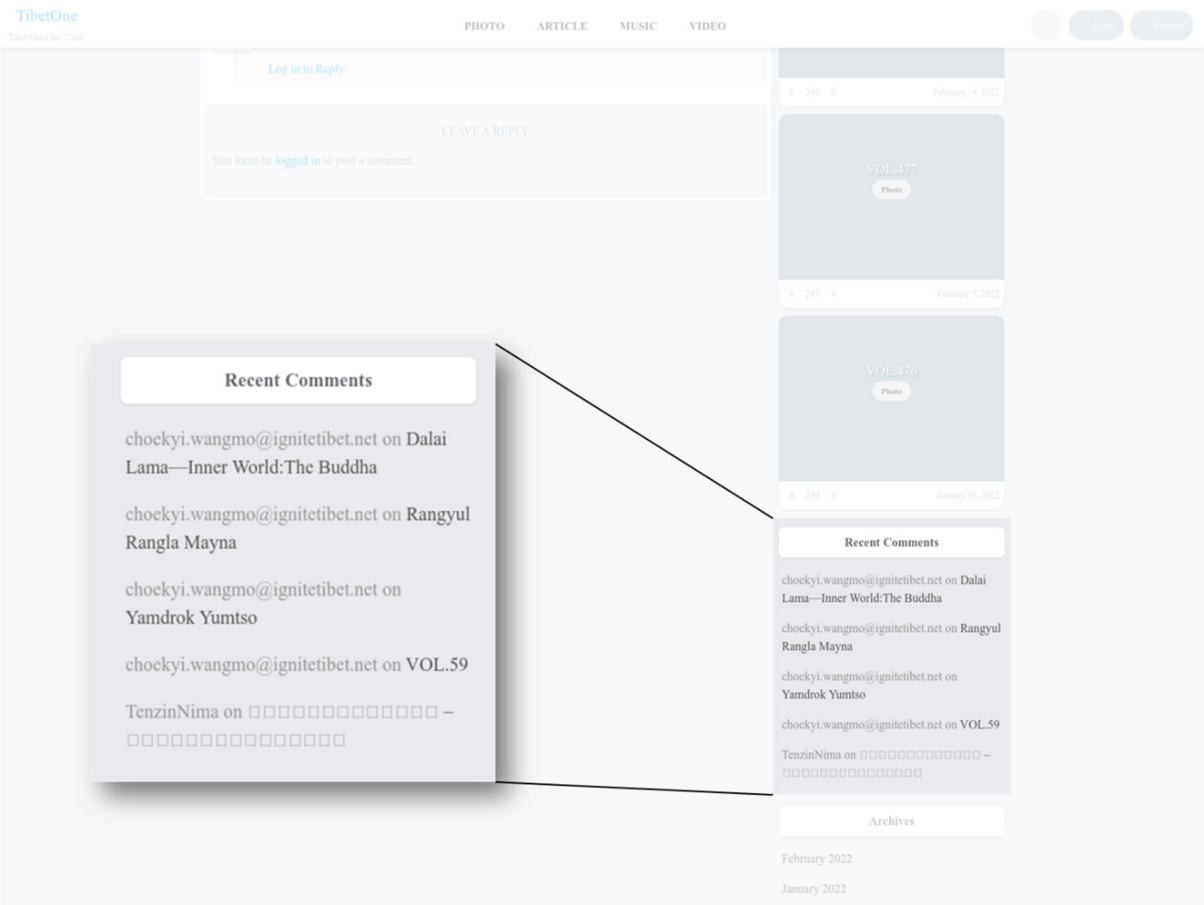


圖 4: 'tibetone[.]org' 的頁面顯示了相信是由惡意行為者操控的使用者評論。

本圖像已被編輯，使相關部分更加清晰。

「**TenzinNima**」 是另一個在該網站加入評論的使用者名稱。Volexity 的通報指出，此使用者名稱也在 Reddit 上宣傳 Telegram 頻道「**Tibetanmaptalk**」。並包含一個下載「**AlpineQuest**」惡意樣本的鏈接，這是一款在 Android 裝置上使用的導航應用程式。所提供的下載連結，是連接一個名為 Mega 的第三方檔案共享服務。

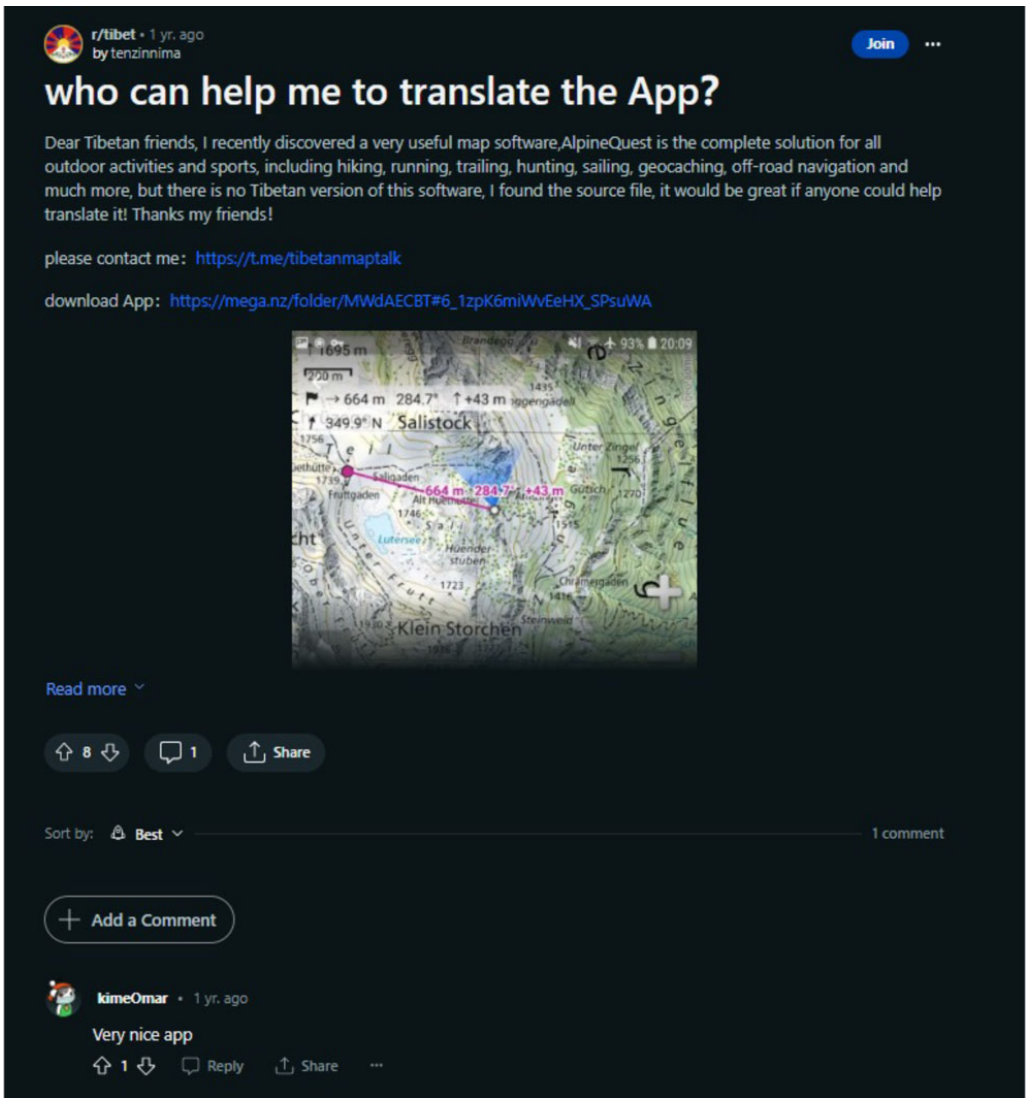


*圖 5:*Reddit 貼文宣傳惡意應用程式，帳戶相信是由惡意行為者所控制。

Volexity 也指出，在該貼文下發表評論，名為「**KimeOmar**」的用戶，也被發現在另一個 Reddit 子論壇上分享惡意應用程式。這可能表明惡意行為者使用多個社交媒體資料，以使他們的貼文看起來正當合法。

評估

BADBAZAAR 和 MOONSHINE 使用多種社會工程方法，專門針對維吾爾族、藏族和台灣群體，如下：

- 針對這些群體的興趣，為目標受害者度身訂製木馬應用程式（例如維吾爾語《古蘭經》應用程式）。
- 將這些木馬應用程式添加到官方應用程式商店，務求帶給人一種合法正當的感覺，而在聊天群組中分享，很可能是為了利用社群內的信任關係。

BADBAZAAR 和 MOONSHINE 所收集的數據，幾乎肯定是對中國政府有所價值。儘管根據觀察，BADBAZAAR 和 MOONSHINE 的目標是維吾爾族、藏族和台灣人，但也有其他惡意軟件的目標是中國境內的其他少數民族群體。來自封閉國家的人民，不論是在中國或國外，如果被認定為支持對政權穩定有威脅的議題，幾乎肯定會受到像 BADBAZAAR 和 MOONSHINE 之類的流動惡意軟件所威脅。而具記錄位置、音訊和照片資料的能力，代表能顯示目標人物的活動和即時資訊，幾乎肯定會提供加強監視和進行騷擾行動的機會。

針對移動應用程式用戶的緩解措施

撰寫機構鼓勵採取下列安全措施，以防範個案研究中提及的威脅。這些建議是以 NCSC 指引中的最佳實踐為基礎。請參閱「更多資訊」部分中的連結，以取得為澳洲和美國讀者提供的最佳實踐指南。

確保您的裝置安全

- **只從官方應用程式商店下載應用程式，例如 Google Play Store 或 Apple App Store。**Google Play Store 和 Apple 的 App Store 會在軟件上線前掃描病毒，讓您對下載內容的安全性更放心。縱然從可信的程式應用商店下載仍有風險，但若從其他來源下載，根本沒有任何保護可言。NCSC 發布了一份關於應用程式商店的威脅報告：https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **確保您的裝置和應用程式為最新版本。**一旦應用程式和裝置的軟件有更新，應立即安裝。在裝置設定中開啟自動更新，以省卻自己手動更新的需要。 請參閱 NCSC 關於如何保持線上安全的指南，以防禦已知病毒和其他類型的惡意軟件。更新通常包括改進和新的功能：https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **不要「越獄」或「root」您的裝置**，因為這會讓未修補的漏洞繞過已實行的安全控制措施，使裝置更容易受到攻擊。請參閱 NCSC 指南：https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

管理您的應用程式

- **檢查您的應用程式及權限。**如果您不再需要某個應用程式，請將其刪除。盡可能限制應用程式權限，最大限度地減少資料洩露，因為惡意軟件的設計通常是為了存取受保護的檔案或週邊設備，例如攝影機和麥克風。
  - 如何在 Apple 檢查應用程式的使用者權限：https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - 如何在 Android 檢查應用程式的使用者權限：https://support.google.com/android/answer/9431959?hl=en-GB

- **自動將未知的應用程式傳送給 Google。**如果您是 Android 用戶，並且下載了非 Google Play 商店的應用程式，您可以在 Google Play 商店應用程式內設定「Play Protect」，以啟用「改進有害應用程式偵測功能」，將該應用程式傳送給 Google。應用程式便會被掃描，以檢測惡意軟件，保護用戶。如何設定：https://support.google.com/android/answer/2812853?hl=en-GB

利用網路服務

- **點擊連結之前，請使用 URL 信譽服務。** 您可以先使用 Google Transparency Report 或 Virus Total 等服務，掃描電子郵件、短訊或其他地方的連結是否安全。您也可以將可疑檔案和應用程式上傳到惡意軟件分析器，例如 Virus Total，這些分析器能幫助偵測檔案是否為惡意檔案。請注意，掃描服務或會出現誤報情況。

- **加入 Google 進階保護計畫。**這項免費服務旨在保護使用 Google 服務（Gmail、Play Store 等）且有被攻擊風險的人士。此服務可在使用 Google 服務時，能提供更高的安全性： https://landing.google.com/advancedprotection/

- **如果有，請加入其他和復原相關的服務。**例如，英國的高風險個別人士，或有資格獲得額外的防禦服務，以幫助他們保障網路安全。檢查申請資格並了解更多：https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

通報威脅

- **識別並舉報虛假帳戶。**惡意的網路行為者會建立虛假帳戶或入侵真實帳戶，以實現其目的。如果您懷疑某帳戶是假的或已被盜用，請向平台舉報並將其封鎖。許多服務都有驗證帳號的流程，例如 Instagram 和 Facebook 的「驗證徽章」，有助識別帳戶是否真確。NCSC 提供了有關安全使用社交媒體的指南，當中包括如何驗證和舉報被盜帳戶的詳細資訊：https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **使用詐騙電郵、短訊和連結進行網路釣魚。**NCSC 能調查可疑的電子郵件地址和網站。如您認為某網站、電子郵件或訊息有可疑，您可以在此通報：https://www.ncsc.gov.uk/collection/phishing-scams

Android

Google 的移動操作系統，獲多間智能手機和平板電腦製造商所採用。

應用程式

應用程式或 App 是使用者可以安裝，或已預先被安裝於裝置內，使裝置能提供額外的功能或內容。

網路安全

網路安全指保護設備、服務和網路，以及其中的資訊，免遭未經授權的存取、竊盜或損壞。

裝置

實體電腦硬件，例如桌上電腦、智能手機或平板電腦。

iOS

蘋果在其移動裝置系列上使用的移動操作系統。

惡意軟件

其英文簡 malware 是「惡意軟件」，指任何可能損害電腦系統、網路或裝置的軟件，包括病毒、勒索軟件和木馬。

操作系統

在電腦、平板電腦和智能手機上運行的基本軟件，用於執行其他應用程式和硬件。

網路釣魚

透過傳送詐騙電子郵件或短訊，誘導連接至含有惡意軟件的網站，或誘騙用戶洩露敏感資訊（例如密碼）或轉帳。

間諜軟件

一種未經用戶同意就安裝在裝置上，並收集資料然後傳送給第三方的惡意軟件。

社交媒體

可讓人們分享和回應用戶自創內容（文字貼文、照片和影片）的網站和應用程式，如 Facebook、X 和 Instagram。

智能手機

具複雜功能的現代手機，包括搭載 Android 和 iOS 操作系統的手機。

木馬

一種偽裝成合法正當的惡意軟件，用於在未經授權的情況下存取受害者裝置。

網址

統一資源定位符。互聯網上的地址，如網域名稱（例子： www.bbc.co.uk）。

病毒

一種惡意軟件，旨在感染合法軟件程式，並在這些程式啟動時，透過網絡複製。

更多參考資料

澳洲網路安全中心的指引

- 報告網路罪案、事件或漏洞
- 如何保護您的裝置
- 保護您的手機安全
- 網路釣魚
- 詐騙
- 保護您的社交媒體
- 社交媒體與通訊應用程式的安全建議

英國 NCSC 和 NPSA 的指引

- 捍衛民主
- 社交媒體：如何安全使用
- 適用於機構的裝置安全指引，包括手機
- 應用程式商店威脅報告。
- 高風險人士的人身安全與保障

美國國家安全局的指引

- 移動裝置最佳實務守則

免責聲明

請注意，本公告內容是在發布當時獲驗證的資訊。

報告借鑒了來自撰寫機構和業界提供的資訊。任何調查結果和建議均不是為了避免所有風險，遵循這些建議也不代表能消除所有此類風險。資訊風險的責任始終在於相關系統的所有者。

在英國，本資訊根據 2000 年《資訊自由法》（FOIA）獲得豁免，並可能根據其他英國的資訊法例獲得豁免。

如有任何 FOIA 查詢，請電郵至 ncscinfoleg@ncsc.gov.uk。

附件：**MOONSHINE** 和 **BADBAZAAR** 的觀察樣本

本表格列出了過去兩年 MOONSHINE 和 BADBAZAAR 活動時利用到的應用程式。

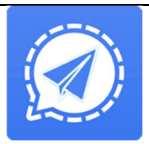
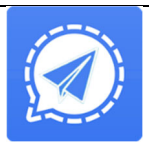
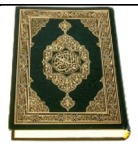
許多都與現有應用程式有明顯的相似，這很可能是攻擊者故意「模仿」知名品牌的伎倆。

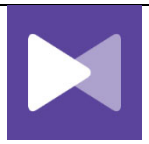
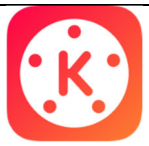
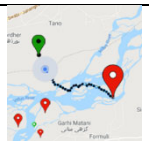
請注意，應用程式的名稱、套件名稱和圖標都可以被模仿或設計成與真實的應用程式相同，因此不應只利於這些資訊以識別裝置有否被感染。

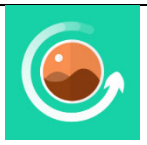
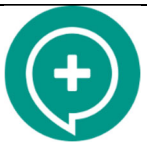
正如緩解措施部分所述，您可以將 Android 裝置上的應用程式傳送給 Google，方法是透過啟用「改進有害應用程式偵測」，這將掃描您裝置上從 Play 商店以外安裝的應用程式。

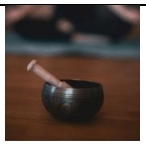
應用程式標題	套件名稱	應用程式圖標
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

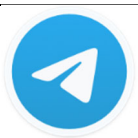
AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam 维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
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	

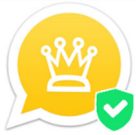
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
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	

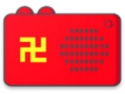
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	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	
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 ىقاپ^كۇ	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.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate