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

Khuyến cáo

BADBAZAAR và MOONSHINE: Phần mềm gián điệp nhắm vào các nhóm người Duy Ngô Nhĩ, Đài Loan và Tây Tạng cùng các tổ chức xã hội dân sự

Ngày 9 tháng 4 năm 2025

BADBAZAAR và MOONSHINE: Phần mềm gián điệp nhắm vào các nhóm người Duy Ngô Nhĩ, Đài Loan và Tây Tạng cùng các tổ chức xã hội dân sự

NCSC (Trung tâm An ninh Mạng Quốc gia) và các đối tác đăng tải thông tin mới và các biện pháp giảm thiểu rủi ro, dành cho những người có nhiều nguy cơ bị ảnh hưởng từ hai biến thể phần mềm gián điệp.

Tóm tắt

Với sự giúp đỡ từ Cyber League(Liên Minh Mạng) của Vương quốc Anh, khuyến cáo này được Trung tâm An ninh Mạng Quốc gia Vương quốc Anh (National Cyber Security Centre - NCSC UK) và các đối tác quốc tế phối hợp soạn thảo:

- **Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc**
- **Trung tâm An ninh Mạng Gia Nã Đại, trực thuộc Cơ quan An ninh Truyền thông Gia Nã Đại**
- **Cơ quan Tình báo Liên bang Đức**
- **Văn phòng Liên bang Đức về Bảo vệ Hiến pháp**
- **Trung tâm An ninh Mạng Quốc gia Tân Tây Lan, trực thuộc Cục An ninh Truyền thông Chính phủ**
- **Cục Điều tra Liên bang Hoa Kỳ**
- **Cơ quan An ninh Quốc gia Hoa Kỳ**

Mục đích của tài liệu này là nhằm nâng cao nhận thức về mối đe dọa ngày càng gia tang, mà các tác nhân mạng độc hại gây ra đối với những cá nhân có liên quan đến các chủ đề bao gồm Đài Loan, Tây Tạng, Khu tự trị Tân Cương của người Duy Ngô Nhĩ, các phong trào dân chủ và Pháp Luân Công.

Khuyến cáo này bao gồm hai tình huống nghiên cứu mô tả chi tiết các kỹ thuật được sử dụng bởi các tác nhân mạng độc hại, sử dụng phần mềm gián điệp mang tên BADBAZAAR và MOONSHINE nhắm mục tiêu vào dữ liệu trên các thiết bị di động, bao gồm điện thoại thông minh, có thể thu hút sự quan tâm của Nhà nước Trung Quốc. Khuyến cáo cũng đưa ra các hướng dẫn giúp các cá nhân tự bảo vệ bản thân, thiết bị và dữ liệu của mình.

Song song với khuyến cáo này, NCSC đã đăng tải thông tin kỹ thuật đầy đủ kèm theo hướng dẫn riêng biệt.

Ai là người có nguy cơ bị ảnh hưởng?

Các cơ quan soạn thảo và đối tác trong ngành đã quan sát thấy BADBAZAAR và MOONSHINE đặc biệt nhắm vào những cá nhân có liên quan đến các chủ đề mà Nhà nước Trung Quốc coi là mối đe dọa đối với quyền lực trong nước, tham vọng và uy tín toàn cầu của họ. Những người có nguy cơ cao nhất bao gồm, nhưng không giới hạn ở, bất kỳ ai có liên quan đến:

- **Độc lập cho Đài Loan**
- **Quyền của người Tây Tạng**
- **Người Hồi giáo Duy Ngô Nhĩ và các dân tộc thiểu số khác ở trong hoặc đến từ Khu tự trị Tân Cương của Trung Quốc**
- **Vận động cho dân chủ (bao gồm cả Hồng Kông)**
- **Phong trào tâm linh Pháp Luân Công**

Những người này bao gồm các tổ chức phi chính phủ (non-governmental organisations - NGO), nhà báo, doanh nghiệp và các cá nhân ủng hộ, đồng cảm, hoặc đại diện cho các nhóm này. Các phần mềm gián điệp này được phát tán tràn lan một cách bừa bãi trên mạng, cũng đồng nghĩa với việc có nguy cơ sự lây nhiễm sẽ lan rộng lớn hơn vượt ra ngoài các nạn nhân mà phần mềm nhắm tới từ ban đầu.

Khuyến cáo này nhằm giúp đỡ cho những người có nguy cơ, để họ có thể phản ứng một cách hiệu quả trước mối đe dọa cụ thể từ phần mềm gián điệp BADBAZAAR và MOONSHINE. Các biện pháp giảm thiểu được đưa ra bổ sung cho các khuyến nghị an ninh mạng tổng thể, và không nên được xem xét một cách riêng lẻ.

Bằng cách làm theo các hướng dẫn được đề cập trong khuyến cáo này, người sử dụng có thể giảm thiểu nguy cơ thiết bị di động và dữ liệu của mình bị lây nhiễm.

Mối đe dọa

MOONSHINE và BADBAZAAR là những ví dụ về Trojan (là một loại phần mềm độc hại nguy trang); chúng chứa các chức năng độc hại nằm ẩn bên trong một ứng dụng có vẻ hoạt động bình thường, có thể được tải xuống từ các cửa hàng ứng dụng, hoặc các dịch vụ chia sẻ tập hồ sơ trực tuyến.

Các ứng dụng này được thiết kế nhằm đánh lừa người sử dụng để họ tải xuống và cài đặt vào thiết bị của họ. Sau khi được cài đặt, ứng dụng sẽ khai thác các lỗ hổng trên thiết bị để thực hiện các chức năng trái phép, hoặc dựa vào việc người sử dụng cấp quyền cho ứng dụng để truy cập và tải thông tin từ thiết bị, bao gồm:

- **vị trí dữ liệu (đề cập đến thông tin về vị trí địa lý cụ thể của một thiết bị, vật thể hoặc cá nhân), bao gồm cả theo dõi thời gian thực**
- **truy cập vào micro và camera**
- **tin nhắn, hình ảnh và các tập hồ sơ khác được lưu trữ trên thiết bị**
- **thông tin về thiết bị và nhiều nội dung khác**

Các tác nhân sau đó lợi dụng mối quan tâm chính đáng của các nhóm có nguy cơ để xác định và lây nhiễm cho càng nhiều nạn nhân càng tốt, đồng thời truy cập vào dữ liệu của họ. Một trong những cách thức chúng thực hiện điều này là, thiết kế các ứng dụng mà chúng biết sẽ thu hút nạn nhân, chẳng hạn như các ứng dụng hỗ trợ ngôn ngữ bản địa của họ, hoặc chứa nội dung liên quan đến các khu vực cụ thể như vùng Tây Tạng của Trung Quốc hoặc Tân Cương.

Các tình huống được nghiên cứu trong khuyến cáo này nêu ra một số ví dụ về điều đó, bao gồm các ứng dụng TibetOne và Uyghur Quran.

Các tác nhân này hoạt động tích cực trên các diễn đàn trực tuyến nơi có nhiều người sử dụng thuộc nhóm nạn nhân được nhắm vào, nhằm tối đa hóa cơ hội lây nhiễm. Chúng đã bị phát hiện khi cố tình chia sẻ phần mềm gián điệp trên các phương tiện Telegram liên quan đến Tây Tạng và các diễn đàn Reddit. Các tình huống được nghiên cứu trong khuyến cáo này cũng đưa ra ví dụ về những phương thức này.

Các ứng dụng độc hại thường được chia sẻ dưới dạng các tập hồ sơ riêng lẻ, chẳng hạn như tập hồ sơ APK trên Android, mà người sử dụng phải tải xuống và cài đặt. Các tác nhân cố gắng làm cho phần mềm gián điệp của họ trông hợp pháp hơn bằng cách tải lên các cửa hàng ứng dụng chính thức như Play Store của Google và App Store của Apple, hoặc bằng cách cho thêm mã độc vào các ứng dụng vốn dĩ vô hại trước đó, mặc dù các cửa hàng ứng dụng chính thức có các tính năng bảo mật và quy trình kiểm duyệt khiến chiến thuật này kém thành công hơn. Điều này khiến các ứng dụng từ các cửa hàng ứng dụng chính thức an toàn hơn, nhưng như được minh họa trong các tình huống được nghiên cứu và Trình báo Mối đe dọa của Cửa hàng Ứng dụng của NCSC, các phương sách này không hoàn hảo.

Áp dụng 4 mẹo sau đây có thể giúp bảo vệ quý vị từ các mối đe dọa được nêu ra trong khuyến cáo này.

Để biết thêm lời khuyên chi tiết, hãy xem phần: các biện pháp giảm thiểu.

Nghiên cứu các trường hợp điển hình

Hai tình huống được nghiên cứu này minh họa cách thức MOONSHINE và BADBAZAAR hoạt động, và các tác nhân nhắm vào những người có nguy cơ cao nhất bằng phương sách nào.

Nghiên cứu trường hợp điển hình 1: MOONSHINE

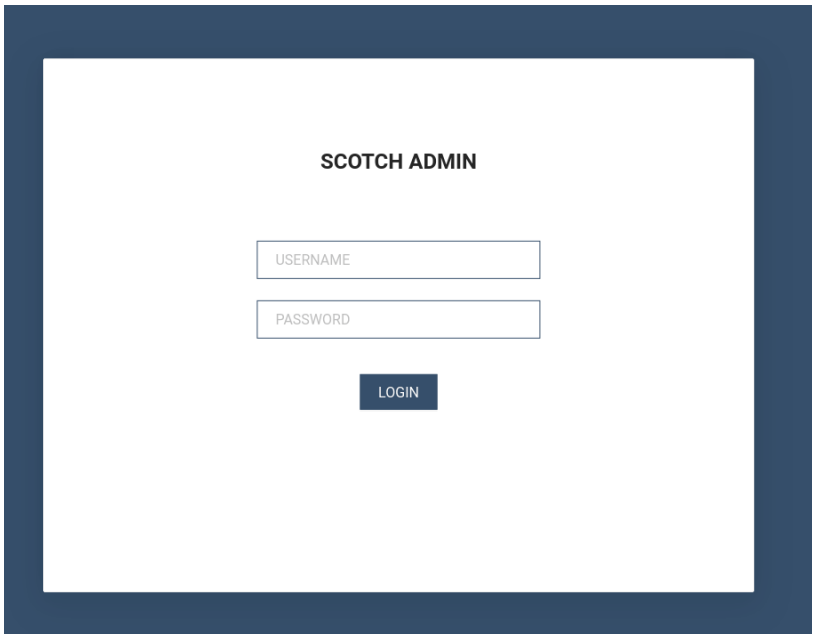
MOONSHINE là một phần mềm gián điệp trên hệ điều hành Android được trình báo vào năm 2019 bởi Citizen Lab, với mục đích là nhắm vào các nhóm người Tây Tạng. MOONSHINE nguỵ trang thành một ứng dụng hợp pháp để dụ dỗ nạn nhân cài đặt nó. MOONSHINE đã được chia sẻ qua các kênh Telegram và các đường dẫn được gởi qua WhatsApp.

MOONSHINE có khả năng giám sát rộng, bao gồm:

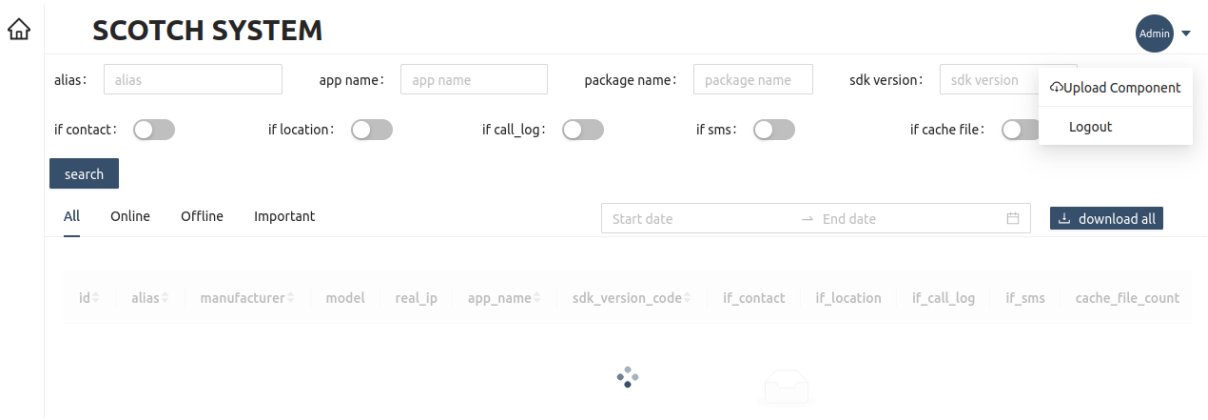
- **dữ liệu vị trí, bao gồm theo dõi theo thời gian thực**
- **ghi âm và chụp hình ảnh trực tiếp**
- **tải các tập hồ sơ từ thiết bị**
- **thu thập thông tin về thiết bị**
- **phát ra âm thanh trên thiết bị**

Ứng dụng ‘ئاۋازلىق قۇرئان.**apk**’, có nghĩa là ‘**Audio Quran.apk**’, là một ví dụ cho thấy MOONSHINE được sử dụng để nhắm vào người Duy Ngô Nhĩ. Việc sử dụng ngôn ngữ Duy Ngô Nhĩ trong tên hồ sơ, cho thấy đây là một ứng dụng Kinh Koran, có thể đã được thiết kế để thu hút người Hồi giáo Duy Ngô Nhĩ.

Khi đã được cài đặt, các tác nhân mạng độc hại có thể thu thập thông tin từ thiết bị của nạn nhân. Thông tin này được truy cập qua bảng điều khiển ‘SCOTCH ADMIN’.



Sau khi đăng nhập, các tác nhân có thể truy cập vào trang được minh họa như trong ảnh chụp màn hình bên dưới. Trang này cho thấy thông tin chi tiết về các thiết bị đã bị lây nhiễm và mức độ truy cập mà tác nhân có đối với các thiết bị đó:



Bảng điều khiển quản lý phần mềm độc hại cho thấy dữ liệu đã thu thập, bao gồm:

- **mức độ truy cập vào thiết bị**
- **tin nhắn SMS**
- **nhật ký cuộc gọi**
- **dữ liệu vị trí**
- **thông tin về thiết bị**

Phối hợp với Cyber League *(Liên Minh Mạng),* NCSC đã dựa trên các trình báo từ Trend Micro để phát hiện điểm tương đồng giữa bộ công cụ khai thác MOONSHINE và các bảng đăng nhập có chứa 'UPSEC' trong tựa đề HTML. Các chi tiết đầy đủ có trong tài liệu kỹ thuật đi kèm.

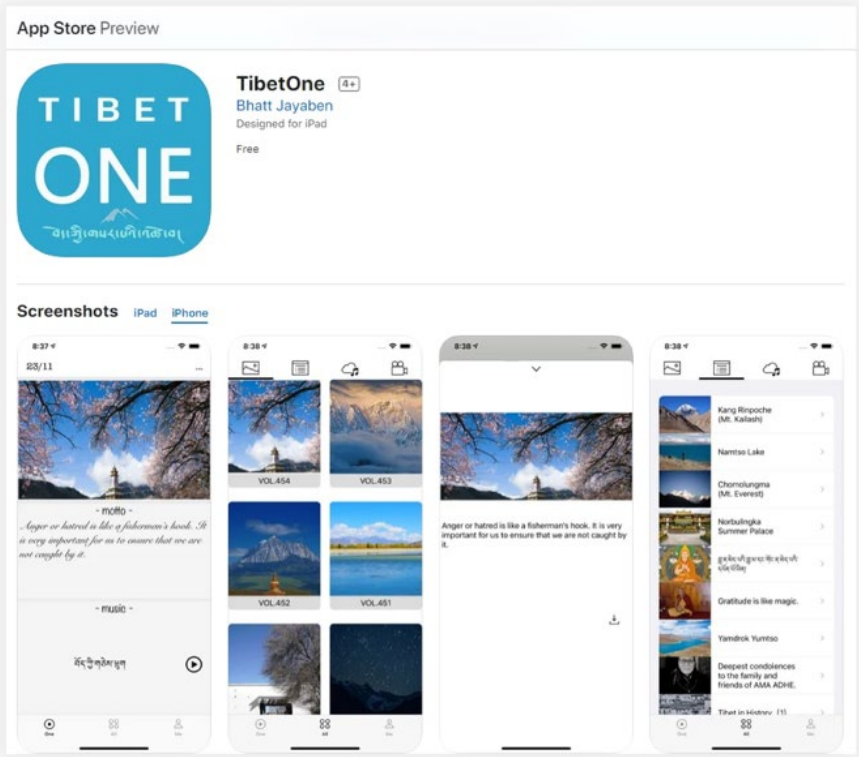
Theo Intelligence Online (Thông tin Tình báo Trên Mạng), UPSEC là tên viết tắt của 'Công ty TNHH Công nghệ An ninh Mạng Tứ Xuyên Dianke'. Các cơ quan soạn thảo chưa xác minh tuyên bố này.

Nghiên cứu trường hợp điển hình 2: BADBAZAAR

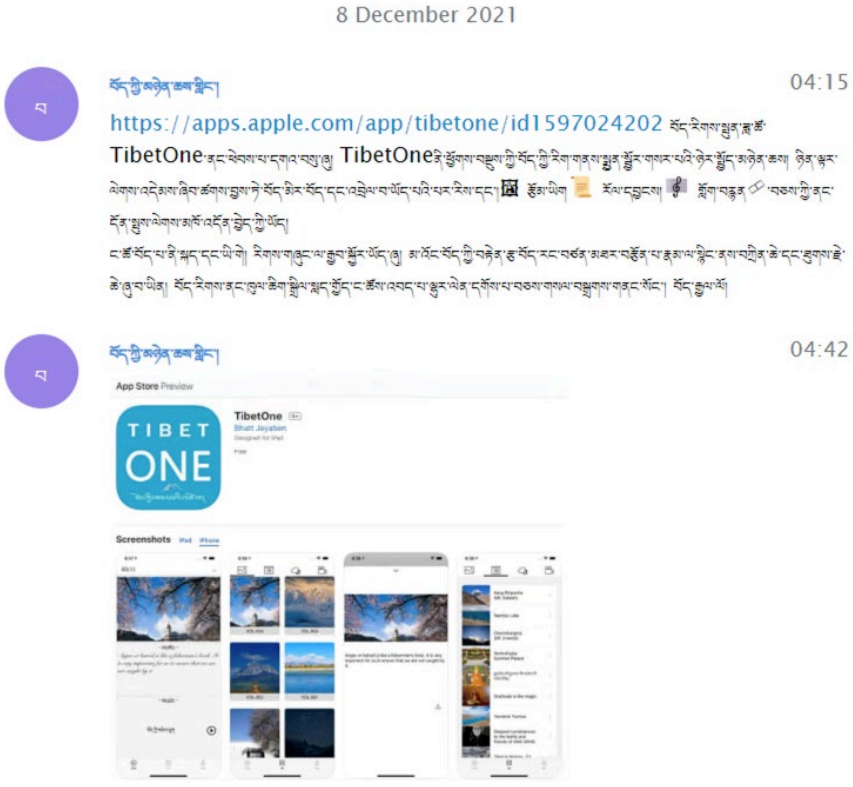
BADBAZAAR là một phần mềm độc hại trên thiết bị di động với các biến thể trên iOS và Android, đã nhắm vào người Duy Ngô Nhĩ, người Tây Tạng và người Đài Loan. Phần mềm độc hại này đã được phát tán qua các nền tảng mạng xã hội và các cửa hàng ứng dụng chính thức.

BADBAZAAR đã được sử dụng để nhắm vào người Tây Tạng qua ứng dụng **'TibetOne'**, theo phúc trình của Lookout và Volexity. **TibetOne** là một ứng dụng iOS do các tác nhân độc hại tạo ra, có khả năng truy cập thông tin thiết bị và dữ liệu vị trí (Dữ liệu vị trí còn được gọi là dữ liệu định vị địa lý, là thông tin xác định chính xác vị trí địa lý của thiết bị, đối tượng hoặc người sử dụng). Ứng dụng này đã được tải lên Apple App Store vào tháng 12 năm 2021 nhưng hiện không còn nữa. Để phát tán phần mềm độc hại rộng hơn, các tác nhân còn quảng bá ứng dụng này trên một phương tiện Telegram có tên là **'tibetanphone'**.

TibetOne

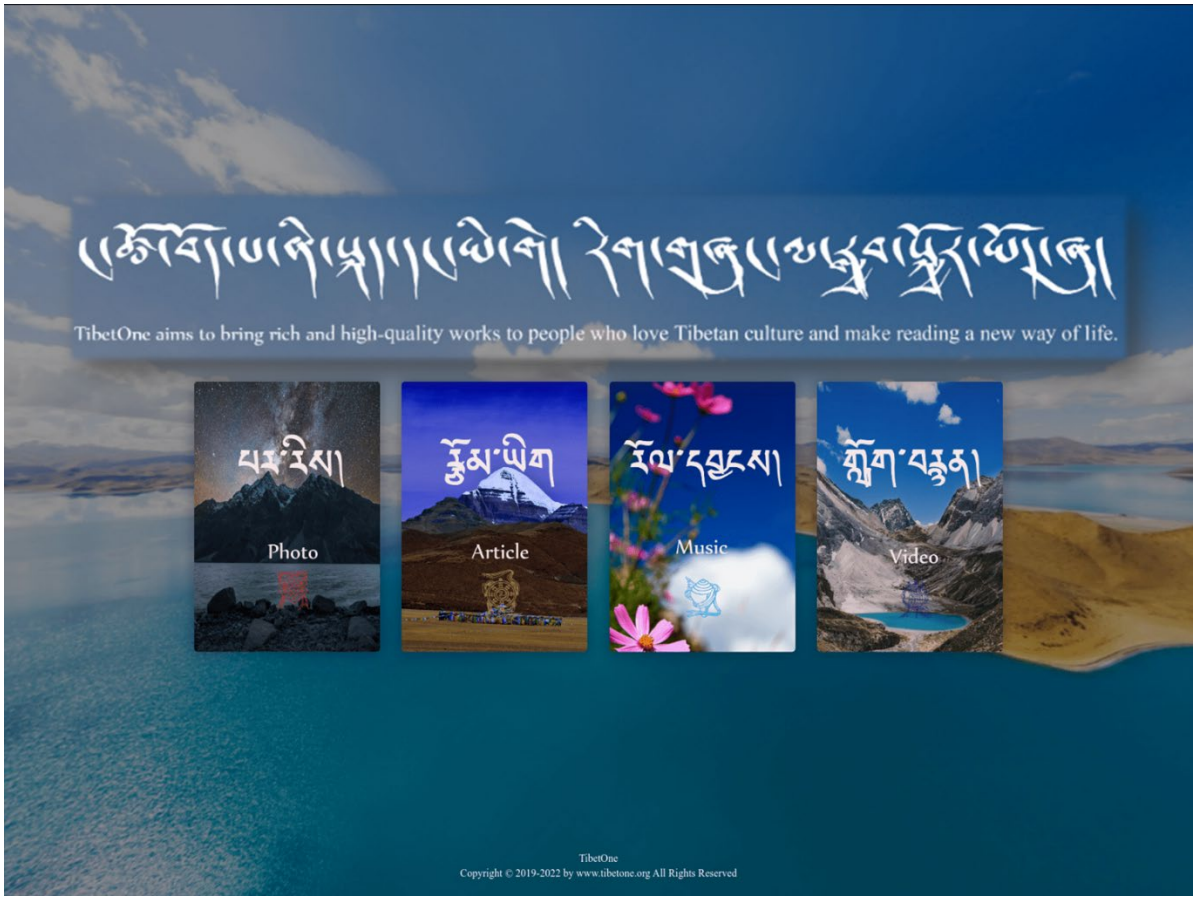


Hình 1: Trang ứng dụng TibetOne trên Apple App Store. Ứng dụng này đã bị gỡ bỏ.



Hình 2: TibetOne được chia sẻ trên các kênh Telegram.

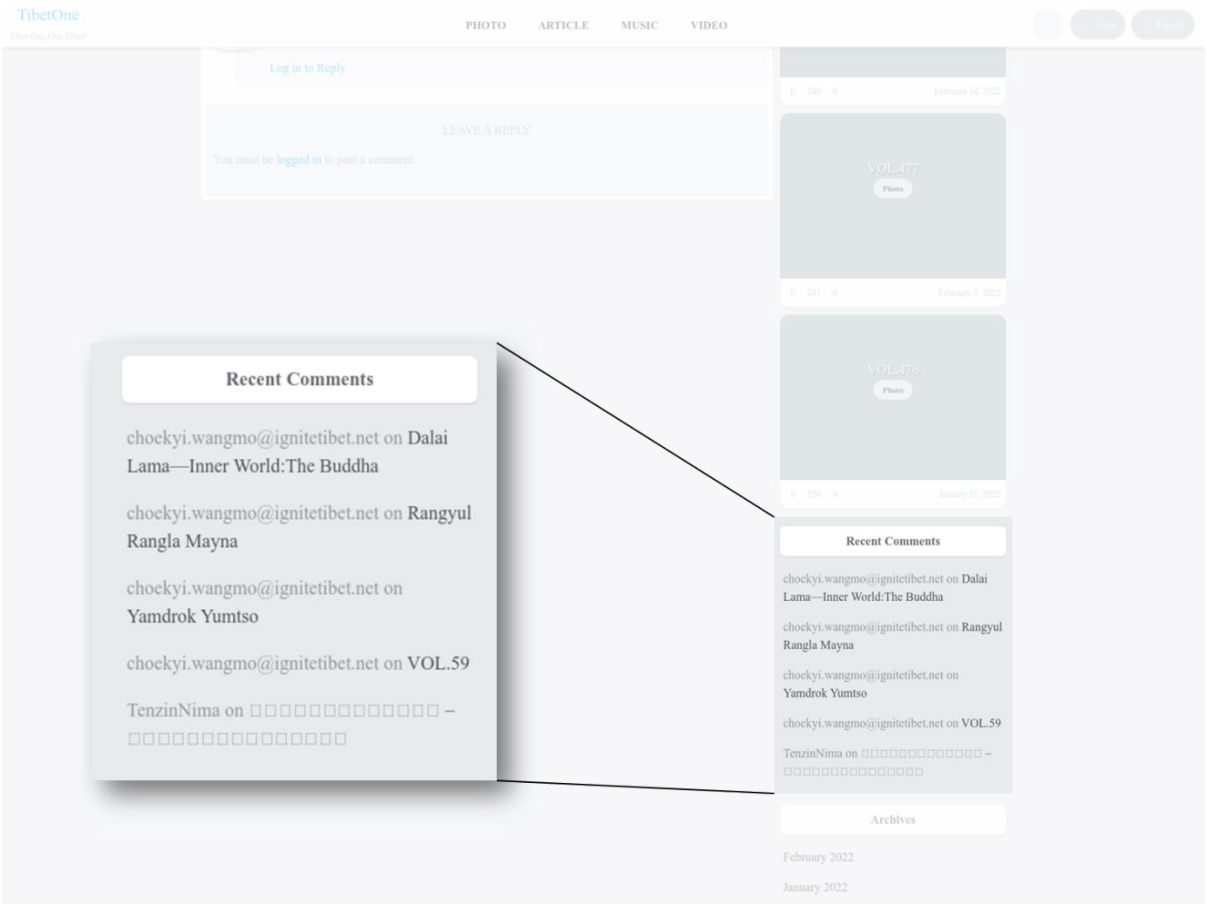
Để làm tăng tính hợp pháp cho ứng dụng, các tác nhân còn thiết kế một trang mạng mang tên '**tibetone[.]org'**, tự mô tả là 'mang đến những tác phẩm phong phú với phẩm chất cao cho những người yêu văn hóa Tây Tạng, và biến việc đọc trở thành một cách sống mới'.



Hình 3: Trang chủ của 'tibetone[.]org'.

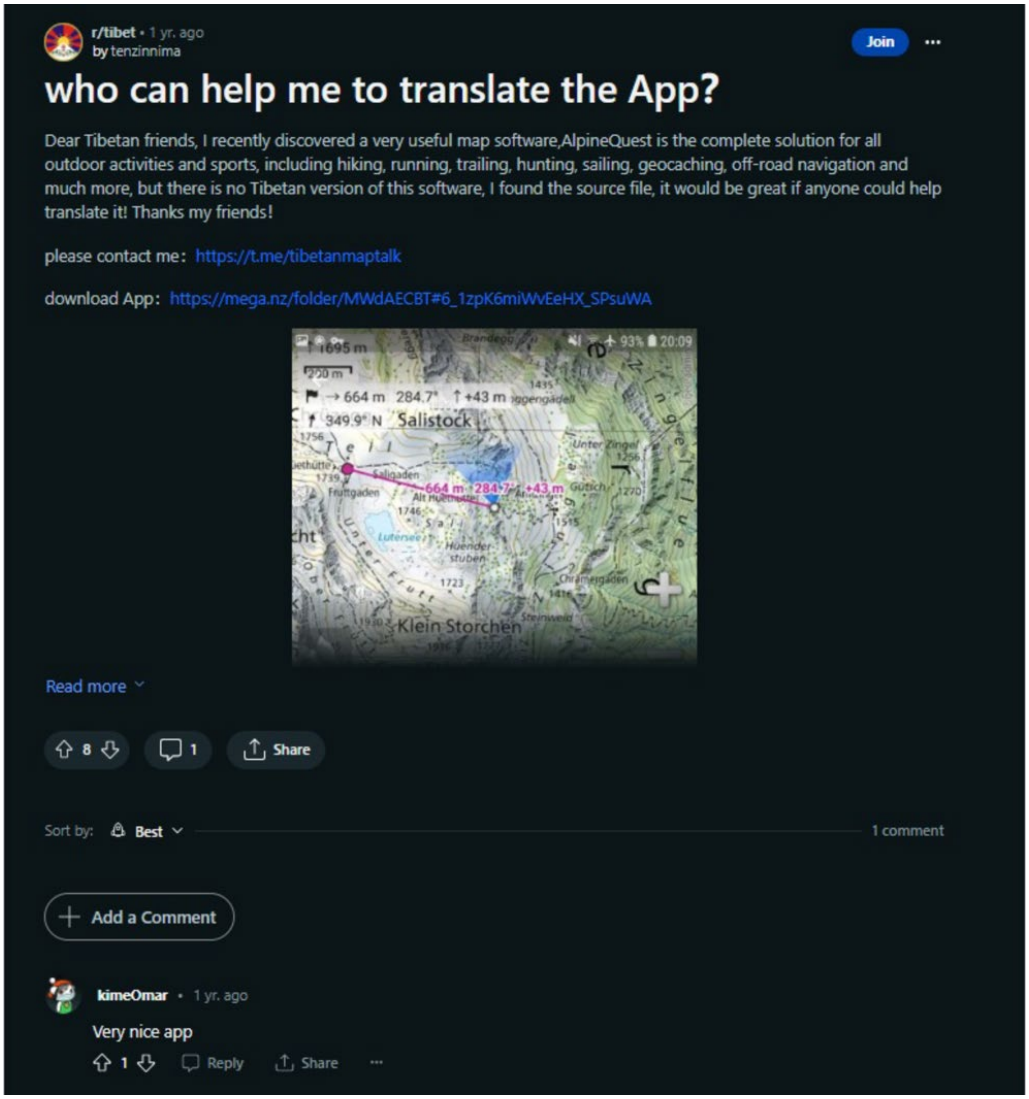
Hình ảnh này đã được chỉnh sửa để làm rõ các phần liên quan.

Trang mạng này có một trang dành cho bài viết cho phép người sử dụng để lại bình luận. Một bình luận được để lại bởi địa chỉ email '**choekyi.wangmo@ignitetibet.net**', được cho là do tác nhân độc hại kiểm soát và có thể được dùng để giả mạo '**Choekyi Wangmo**', người mà Trung tâm Nhân quyền và Dân chủ Tây Tạng liệt kê là một người biểu tình ủng hộ Tây Tạng. Điều này rất có thể là một nỗ lực khác nhằm tạo ấn tượng rằng ứng dụng thực sự ủng hộ độc lập cho Tây Tạng.



Hình 4: Trang 'tibetone[.]org' cho thấy các bình luận từ người sử dụng được cho là do tác nhân độc hại kiểm soát. Hình ảnh này đã được chỉnh sửa để làm rõ các phần liên quan.

'**TenzinNima**' là một tên người sử dụng khác đã để lại bình luận trên trang này. Volexity đã trình báo rằng, tên người sử dụng này cũng đã được sử dụng trên Reddit để quảng bá các kênh Telegram '**Tibetanmaptalk**'. Phương tiện này bao gồm một đường dẫn để tải xuống một mẫu phần mềm độc hại của '**AlpineQuest**', một ứng dụng định vị có trên các thiết bị Android. Đường dẫn tải xuống được cung cấp, là từ một dịch vụ chia sẻ tập hồ sơ bên thứ ba mang tên Mega.



Hình 5: Bài đăng trên Reddit quảng cáo ứng dụng độc hại bởi tài khoản được cho là do tác nhân độc hại kiểm soát.

Volexity cũng ghi nhận rằng, một người sử dụng được biết với cái tên '**KimeOmar**' đã bình luận trong bài đăng này và cũng từng được quan sát thấy chia sẻ các ứng dụng độc hại trên một diễn đàn con khác của Reddit. Điều này có thể cho thấy các tác nhân độc hại sử dụng nhiều danh tánh mạng xã hội khác nhau nhằm làm cho các bài đăng của họ trông có vẻ hợp pháp hơn.

Đánh giá

BADBAZAAR và MOONSHINE sử dụng nhiều phương pháp kỹ thuật xã hội (social engineering) để tấn công nhằm nhắm mục tiêu cụ thể vào cộng đồng người Duy Ngô Nhĩ, Tây Tạng và Đài Loan, bao gồm:

- việc cấy mã độc vào các ứng dụng được các cộng đồng này quan tâm, chẳng hạn như một ứng dụng Kinh Koran bằng tiếng Duy Ngô Nhĩ, gần như chắc chắn được thiết kế riêng để phù hợp với nhóm nạn nhân được nhắm tới
- việc đưa các ứng dụng đã được cài mã độc vào các cửa hàng ứng dụng chính thức rất có thể nhằm tạo cảm giác hợp pháp, và việc chia sẻ chúng trong các nhóm trò chuyện gần cũng rất có thể được dùng để lợi dụng các mối quan hệ tin cậy trong các cộng đồng này.

BADBAZAAR và MOONSHINE thu thập dữ liệu mà gần như chắc chắn sẽ có giá trị đối với nhà nước Trung Quốc. Mặc dù BADBAZAAR và MOONSHINE đã được phát hiện nhắm vào các cá nhân người Duy Ngô Nhĩ, Tây Tạng và Đài Loan, vẫn còn các phần mềm độc hại khác nhắm đến các nhóm thiểu số khác ở Trung Quốc. Công dân từ các quốc gia đồng ký kết, kể cả ở Trung Quốc và nước ngoài, những người được cho là ủng hộ các phong trào gây nguy hại đến sự ổn định của chế độ, gần như chắc chắn đang bị đe dọa bởi các phần mềm độc hại như BADBAZAAR và MOONSHINE trên thiết bị di động. Khả năng thu thập dữ liệu vị trí, âm thanh và hình ảnh gần như chắc chắn tạo cơ hội để hỗ trợ các hoạt động giám sát và quấy rối trong tương lai, bằng cách cung cấp thông tin theo thời gian thực về hoạt động của mục tiêu.

Các biện pháp giảm thiểu dành cho người sử dụng ứng dụng di động

Các cơ quan soạn thảo khuyến khích áp dụng các biện pháp bảo mật sau để bảo vệ trước các mối đe dọa được mô tả trong các trường hợp điển hình được nghiên cứu. Những khuyến nghị này được soạn thảo dựa trên hướng dẫn thực hành tốt nhất của NCSC. Xem phần "tham khảo thêm" để biết các đường dẫn đến các phương pháp thực hành tốt nhất dành cho độc giả tại Úc và Hoa Kỳ.

Giữ cho thiết bị của quý vị được an toàn

- **Chỉ tải ứng dụng từ các cửa hàng ứng dụng chính thức, chẳng hạn như Google Play Store hoặc Apple App Store.** Play Store của Google và App Store của Apple quét phần mềm để phát hiện vi-rút trước khi phân phối, giúp quý vị yên tâm hơn vì biết ứng dụng quý vị tải về là an toàn. Các ứng dụng từ các kho đáng tin cậy vẫn có các rủi ro tiềm ẩn, nhưng các ứng dụng tải xuống từ những nguồn khác có thể hoàn toàn không có bất kỳ biện pháp bảo vệ nào. NCSC có một báo cáo về mối đe dọa liên quan đến các cửa hàng ứng dụng: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Giữ cho thiết bị và ứng dụng của quý vị luôn được cập nhật.** Cài đặt các bản cập nhật cho ứng dụng và phần mềm thiết bị ngay khi có sẵn. Bật tính năng 'tự động cập nhật' trong phần cài đặt thiết bị nếu có, để quý vị không cần phải nhớ và phải tự cập nhật. Xem hướng dẫn của NCSC về cách giữ an toàn trực tuyến , nhằm bảo vệ quý vị khỏi các loại vi-rút đã biết và các hình thức phần mềm độc hại khác. Các bản cập nhật thường bao gồm những cải tiến và tính năng mới: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Không nên "jailbreak"** (đề cập đến quá trình vượt qua các giới hạn phần mềm) **hoặc "root"** (là quá trình giành quyền kiểm soát đặc quyền đối với nhiều hệ thống con khác nhau của thiết bị) **thiết bị** của quý vị vì hành động này khai thác các lỗ hổng chưa được vá để vượt qua các biện pháp kiểm soát bảo mật được áp dụng. Việc này khiến thiết bị dễ bị tấn công hơn. Xem hướng dẫn của NCSC: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Quản lý ứng dụng của quý vị

- **Xem xét lại các ứng dụng và quyền truy cập của chúng.** Nếu quý vị không còn cần đến một ứng dụng nào đó, thì hãy xoá nó đi. Khi có thể, hãy hạn chế quyền truy cập của ứng dụng để giảm thiểu việc lộ dữ liệu, vì phần mềm độc hại thường được thiết kế để truy cập vào các tập hồ sơ được bảo vệ hoặc thiết bị ngoại vi như máy ảnh và micro.
  - Làm sao để kiểm tra quyền truy cập ứng dụng đối với người sử dụng Apple: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Làm sao để kiểm tra quyền truy cập ứng dụng đối với người sử dụng Android: https://support.google.com/android/answer/9431959?hl=en-GB

- **Tự động gởi các ứng dụng không rõ nguồn gốc đến Google**. Nếu quý vị là người sử dụng Android và đã tải xuống một ứng dụng không phải từ Play Store của Google, quý vị có thể gởi ứng dụng đó đến Google bằng cách bật tính năng 'Cải thiện phát hiện ứng dụng độc hại' (Improve harmful app detection) trong phần cài đặt ứng dụng của Play Store, dưới mục 'Play Protect'. Tính năng này sẽ quét ứng dụng để phát hiện phần mềm độc hại, giúp bảo vệ người sử dụng. Thông tin về cách thiết lập : https://support.google.com/android/answer/2812853?hl=en-GB

Sử dụng dịch vụ an ninh mạng

- **Dịch vụ kiểm tra độ uy tín của URL trước khi nhấp vào đường dẫn**. Quý vị có thể kiểm tra xem một đường dẫn từ email, tin nhắn hoặc nguồn khác có an toàn hay không bằng cách quét nó trước qua các dịch vụ như Google Transparency Report or Virus Total. Quý vị cũng có thể tải các tập hồ sơ và ứng dụng nghi ngờ lên công cụ phân tích phần mềm độc hại, chẳng hạn như Virus Total, để giúp phát hiện xem tập hồ sơ đó có độc hại hay không. Lưu ý rằng các dịch vụ quét có thể cho kết quả âm tính giả (kết quả âm tính giả là kết quả của một thử nghiệm một cách khoa học cho thấy một thứ gì đó không tồn tại hoặc không hiện hữu, trong khi thực tế không phải vậy).

- **Ghi danh tham gia chương trình Bảo vệ Hiện đại của Google.** Đây là một dịch vụ miễn phí được thiết kế để bảo vệ những ai sử dụng các dịch vụ của

Google (Gmail, Play Store, v.v.) có nguy cơ bị tấn công. Dịch vụ này cung cấp mức độ bảo mật cao hơn khi sử dụng các dịch vụ của Google: https://landing.google.com/advancedprotection/

- **Ghi danh tham gia thêm với các dịch vụ tăng cường khả năng phòng chống khác nếu có sẵn.** Ví dụ, những ai có nguy cơ cao tại Vương quốc Anh có thể hội đủ điều kiện nhận các dịch vụ phòng thủ bổ sung để hỗ trợ bảo mật mạng. Kiểm tra tiêu chuẩn hội đủ điều kiện và tìm hiểu thêm tại: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Trình báo các mối đe dọa

- **Nhận diện và trình báo các tài khoản giả mạo**. Các tác nhân mạng độc hại tạo tài khoản giả hoặc xâm phạm các tài khoản thật để thực hiện mục đích riêng của họ. Nếu quý vị nghi ngờ một tài khoản là giả mạo hoặc bị xâm phạm, hãy trình báo với nền tảng và chặn tài khoản đó. Nhiều dịch vụ có phương sách xác minh tài khoản, chẳng hạn như "huy hiệu đã được xác minh" trên Instagram và Facebook. Điều này giúp nhận biết tài khoản đó là thật. NCSC có hướng dẫn về việc sử dụng mạng xã hội an toàn, bao gồm chi tiết về cách xác minh và trình báo các tài khoản bị xâm phạm : https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Lừa đảo qua email giả mạo, tin nhắn SMS và các các đường dẫn**. NCSC có thể điều tra các địa chỉ email và trang mạng đáng nghi ngờ. Nếu quý vị nghi ngờ một trang web, email hoặc tin nhắn, quý vị có thể phúc trình tại: https://www.ncsc.gov.uk/collection/phishing-scams

Thuật ngữ của NCSC

- **Android**

Hệ điều hành di động của Google, được nhiều nhà sản xuất điện thoại thông minh và máy tính bảng sử dụng.

- **Ứng dụng**

Ứng dụng, hay app, là một gói phần mềm mà người sử dụng có thể cài đặt hoặc đã được cài sẵn trên thiết bị, nhằm cung cấp các chức năng hoặc nội dung bổ sung cho thiết bị đó.

- **An ninh Mạng**

Là việc bảo vệ các thiết bị, dịch vụ và mạng - cũng như các thông tin trên đó - khỏi việc truy cập trái phép, trộm cắp hoặc hư hại.

- **Thiết bị**

Phần cứng hữu hình trên máy vi tính, chẳng hạn như máy vi tính để bàn, điện thoại thông minh hoặc máy tính bảng.

- **iOS**

Hệ điều hành di động của Apple, được sử dụng trên các thiết bị di động của hãng.

- **Phần mềm Độc hại**

Được viết tắt từ cụm từ “malicious software”, phần mềm độc hại là bất kỳ loại phần mềm nào có thể gây hư hại cho hệ thống máy vi tính, mạng hoặc thiết bị. Bao gồm các loại như vi-rút, ransomware (mã độc tống tiền) và trojan (mã độc ngụy trang).

- **Hệ Điều hành**

Là phần mềm cơ bản chạy trên vi máy tính, máy vi tính bảng và điện thoại thông minh, cần thiết để vận hành các ứng dụng và phần cứng bổ sung.

- **Lừa đảo qua Email**

Là các email hoặc tin nhắn giả mạo có chứa đường dẫn đến các trang mạng có thể chứa phần mềm độc hại, hoặc lừa người sử dụng tiết lộ thông tin nhạy cảm (chẳng hạn như mật mã) hoặc chuyển tiền.

- **Phần mềm Gián điệp**

Là một loại phần mềm độc hại được cài đặt trên thiết bị mà không có sự đồng ý của người sử dụng, thu thập dữ liệu và sau đó gởi đến bên thứ ba.

- **Mạng xã hội**

Các trang mạng và ứng dụng như Facebook, X và Instagram, cho phép người sử dụng chia sẻ và phản hồi nội dung do người sử dụng tạo ra (bài đăng văn bản, hình ảnh và video).

- **Điện thoại thông minh**

Là điện thoại di động hiện đại có thể thực hiện nhiều chức năng phức tạp, bao gồm các thiết bị chạy hệ điều hành Android và iOS.

- **Trojan**

Là một loại phần mềm độc hại được ngụy trang dưới dạng phần mềm hợp pháp, được sử dụng để truy cập trái phép vào thiết bị của nạn nhân.

- **URL**

Lập trình Định vị Nguồn lực trên Mạng. Là địa chỉ trên mạng internet, chẳng hạn như tên miền (ví dụ: www.bbc.co.uk).

- **Vi-rút**

Là một loại phần mềm độc hại được thiết kế để lây nhiễm vào các chương trình phần mềm hợp pháp và tự nhân bản qua các mạng khi các chương trình đó được khởi động.

Tham khảo thêm

Hướng dẫn từ Trung tâm An ninh Mạng Úc

- Report a cybercrime, incident or vulnerability(Trình báo tội phạm mạng, các vấn đề hoặc lỗ hổng bảo mật)
- How to secure your devices (Bảo vệ thiết bị của quý vị)
- Secure your mobile phone (Bảo mật điện thoại di động của quý vị)
- Phishing (Lừa đảo qua mạng, email hoặc tin nhắn)
- Scams (Các hình thức lừa đảo)
- Secure your social media (Bảo mật mạng xã hội của quý vị)
- Security tips for social media and messaging apps (Mẹo bảo mật cho mạng xã hội và ứng dụng nhắn tin)

Hướng dẫn từ Trung tâm An ninh Mạng Quốc gia và Cơ quan Bảo vệ An ninh Quốc gia Vương quốc Anh

- Defending Democracy (Bảo vệ nền dân chủ)
- Social Media: how to use it safely (Mạng xã hội: cách sử dụng an toàn)
- Device Security Guidance for organisations including mobile (Hướng dẫn bảo mật thiết bị cho các tổ chức, bao gồm cả thiết bị di động)
- Threat report on application stores. (Trình báo mối đe dọa liên quan đến các cửa hàng ứng dụng)
- Personal safety and security for high-risk individuals (An toàn và bảo mật cá nhân cho những người có nguy cơ cao)

Hướng dẫn từ Cơ quan An ninh Quốc gia Hoa Kỳ

- Mobile Device Best Practices (Thực hành Tốt Nhất cho Thiết bị Di động)

Tuyên bố Miễn trừ Trách nhiệm

Xin lưu ý: khuyến cáo này cung cấp thông tin đã được xác minh tại thời điểm đăng tải.

Phúc trình này dựa trên thông tin thu được từ cơ quan soạn thảo và các nguồn lực trong ngành. Bất kỳ phát hiện và khuyến nghị nào được đưa ra đều không nhằm mục đích loại bỏ hoàn toàn tất cả các rủi ro, và việc tuân theo các khuyến nghị cũng sẽ không loại bỏ được hoàn toàn những rủi ro đó. Việc chịu trách nhiệm về các rủi ro thông tin, vào mọi lúc, luôn thuộc về chủ sở hữu hệ thống có liên quan.

Tại Vương quốc Anh, thông tin này được miễn chiếu theo Đạo luật Tự do Thông tin Năm 2000 (Freedom of Information Act - FOIA) và có thể được miễn theo các quy định pháp luật thông tin khác của Vương quốc Anh.

Mọi thắc mắc về FOIA xin vui lòng gửi đến địa chỉ ncscinfoleg@ncsc.gov.uk.

Phụ lục: Các mẫu MOONSHINE & BADBAZAAR đã được quan sát

Bảng danh sách dưới đây liệt kê các ứng dụng đã được sử dụng trong các chiến dịch MOONSHINE và BADBAZAAR trong hai năm qua.

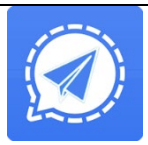
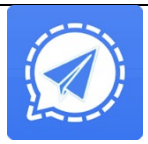
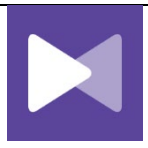
Nhiều ứng dụng trong số này có sự tương đồng rõ rệt với các ứng dụng nổi tiếng hiện có. Đây rất có thể là một kỹ thuật cố ý của các tác nhân tấn công nhằm 'giả mạo' các thương hiệu nổi tiếng.

Điều quan trọng cần lưu ý là tên ứng dụng, tên của gói, và biểu tượng có thể đều được bắt chước hoặc trùng khớp với ứng dụng thật. Vì vậy, không nên chỉ đơn thuần dựa vào những yếu tố này để xác định xem thiết bị có bị nhiễm phần mềm độc hại hay không.

Như đã đề cập trong phần biện pháp giảm thiểu, quý vị có thể gởi các ứng dụng trên thiết bị Android của mình tới Google bằng cách bật tính năng 'Cải thiện phát hiện ứng dụng độc hại'. Tính năng này sẽ quét các ứng dụng trên thiết bị của quý vị đã được cài đặt từ bên ngoài Play Store.

Tên của ứng dụng	Tên của gói ứng dụng	Biểu tượng của ứng dụng
99 Names of ALLAH (99 Danh hiệu của ALLAH)	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer (Khám phá địa hình)	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard (Bàn phím tiếng Ả Rập)	com.arabic.keyboard.arabic.language.keyboard.app	
Chương trình Cắt Video và Âm thanh	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1) Bài Hát Phật Giáo	com.bigkidsapps.buddhistsongs1	
Calculator (Máy tính)	com.android2.calculator3	
Compass (La bàn) 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 + (Chương trình quản lý tập hồ sơ)	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass (Thẻ WiFi Miễn Phí)	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

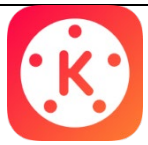
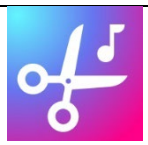
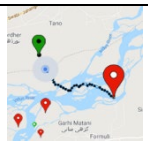
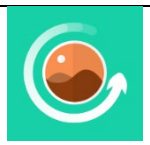
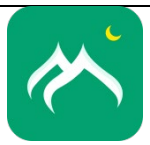
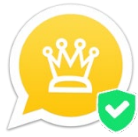
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker (Chương trình Cắt MP3 & Tạo Nhạc chuông)	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator (Máy tính khoảng cách bản đồ)	com.routemap.mapdownload.gpsroute planner	
Media Recovery (Phục hồi phương tiện)	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 (Chương trình đọc PDF)	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader (Chương trình đọc PDF)	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	

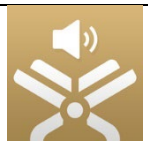
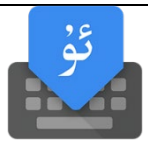
Photo Editor (Chương trình Chỉnh sửa Hình ảnh)	com.iudesk.android.photo.editor	
Photo Recovery (Chương trình Phục hồi Hình ảnh)	recover.restore.undelete.photo.video.file	
Photo Studio (Không gian để Chụp Hình ảnh)	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book (Sách cầu nguyện)	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran (Koran)	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics (Phục hồi Hình ảnh đã bị Xoá)	com.restore.deleted.pictures.video	
Signal (Tín hiệu)	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 (Kinh tiếng Tây Tạng)	com.chorig.tibetanprayer	
Translator (Thông ngôn) AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard (Bàn phím tiếng Duy Ngô Nhĩ)	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Video Converter (Chương trình Chuyển đổi Video)	com.inverseai.video_converter	
Video Cutter (Chương trình Cắt video)	com.naing.cutter	
Video Downloader (Chương trình Tải Xuống Video)	downloader.video.download.free	
Video Maker (Chương trình Tạo ra Video)	com.bstech.slideshow.videomaker	

Video Player for Android (Chương trình Phát Video cho 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 (Chương trình Ghi Âm thanh)	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast (Dự báo Thời tiết)	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 (Chương trình tải 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