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

# 지침

# BADBAZAAR 및 MOONSHINE:

## 위구르, 대만 및 티베트 단체 및 시민사회 운동가들을 대상으로 한 스파이웨어

2025 4 9

# BADBAZAAR 및 MOONSHINE: 위구르, 대만 및 티베트 단체 및 시민사회 운동가들을 대상으로 한 스파이웨어

**NCSC 및 파트너 기관들은 두 가지 스파이웨어 변종 관련 고위험 대상의 개인들을 위해 새로운 정보와 완화 조치를 게시합니다.**

## 요약


본 지침은 영국 Cyber League 이니셔티브의 지지를 받아 영국 사이버 보안 센터(NCSC UK)와 다음 국제 파트너들과의 협업으로 제작되었습니다:

- **The Australian Cyber Security Centre(Australian Signals Directorate 산하)**
- **The Canadian Centre for Cyber Security(Communications Security Establishment 산하)**
- **The German Federal Intelligence Service**
- **The German Federal Office for the Protection of the Constitution**
- **The New Zealand National Cyber Security Centre (Government Communications Security Bureau 산하)**
- **The United States Federal Bureau of Investigation**
- **The United States National Security Agency**

이 지침은 대만, 티베트, 신장 위구르 자치구, 민주화 운동, 파룬궁 등과 관련된 개인에게 악의적인 사이버 공격자들이 가하는 위협이 증가하고 있다는 사실에 대한 인식을 제고하기 위해 제작되었습니다.

이 지침에는 BADBAZAAR 및 MOONSHINE 이라는 스파이웨어를 사용하는 악의적인 사이버 범죄자들이 중국 정부의 관심사가 될 수 있는 스마트폰을 포함한 모바일 기기의 데이터를 표적으로 삼는 수법을 자세히 설명하는 두 가지 사례 연구가 포함됩니다. 또한 개인이 자기 자신과 자신의 기기, 그리고 데이터를 보호하는 데 도움이 되는 지침을 제공합니다.

본 지침은 NCSC 의 출간물과 함께 열람하시기 바랍니다 full technical detail with separate guidance(별도의 지침과 함께 제공되는 테크니컬 내용 전문)

## 위험 대상은 누구인가요?

저작 기관과 업계 파트너들은 BADBAZAAR 및 MOONSHINE 이 중국 정부가 자국의 권위, 야망, 그리고 국제적 명성에 위협이 된다고 여겨지는 것과 관련된 특정 개인들을 표적으로 삼는 것을 관찰했습니다. 가장 위험에 처한 사람들은 다음과 같은 사안과 관련된 사람들을 포함하지만 이에 국한되지는 않습니다:

- **대만의 독립성**
- **티베트인의 권리**
- **위구르 무슬림 및 기타 중국 신장 위구르 자치구 내 또는 출신 소수 민족**
- **민주주의 지지(홍콩 포함)**
- **파룬궁 영성 운동**

이에는 이러한 단체를 지지하거나, 단체와 동일시하거나, 기타 방식으로 단체를 대표하는 비정부기구(NGO), 언론인, 기업 및 개인이 포함됩니다. 이 스파이웨어가 온라인에서 무차별적으로 유포된다는 것은 감염이 원래 의도된 피해자 이상으로 확산될 위험이 있음을 의미합니다.

이 지침의 목적은 위험 대상 개인들이 BADBAZAAR 및 MOONSHINE 스파이웨어의 특정 위협에 효과적으로 대응할 수 있도록 돕기 위함입니다. 제안된 완화 조치는 광범위한 사이버 보안 지침을 보완하는 것이므로, 단독으로 고려되어서는 안 됩니다.

본 지침을 따르면 사용자는 자신의 휴대 기기 및 데이터의 감염 위험을 줄일 수 있습니다.

# 위협 요소

MOONSHINE 및 BADBAZAAR 는 트로이 목마의 예입니다. 앱 스토어나 온라인 파일 공유 서비스에서 다운로드할 수 있으며, 악성 기능이 안에 숨겨져 있는 것 빼고는 정상적인 앱처럼 기능합니다.

이러한 앱은 사용자를 속여 기기에 다운로드하고 설치하도록 설계되었습니다. 앱 설치가 완료되면 이는 기기의 취약점을 이용해 무단으로 기능을 수행하거나, 사용자가 앱 권한을 허용하도록 유도하여 다음과 같은 기기 정보에 접근하고 이를 다운로드할 수 있습니다:

- **실시간 추적을 포함한 위치 정보**
- **마이크 및 카메라 액세스**
- **기기에 저장된 메시지, 사진 및 기타 파일**
- **기기 정보 및 그 외**

이들 공격자는 위험군의 정당한 관심사를 악용하여 최대한 많은 피해자를 식별하고 감염시키며, 그들의 데이터에 접근하려고 합니다. 그러기 위해 사용하는 방법 중 하나는 피해자의 관심을 끌 수 있는 앱을 설계하는 것입니다. 예를 들어, 모국어를 지원하거나, 중국의 티베트 지역이나 신장 등 특정 지역과 관련된 콘텐츠를 포함하는 등의 전략이 있습니다.

지침에 포함된 사례 연구(TibetOne 앱, 위구르어 코란 앱 등)는 이러한 전략을 보여줍니다.

이들 공격자는 표적 대상자들이 활동하는 온라인 포럼에서 활발히 활동하고 있으며, 이는 피해자를 감염시킬 가능성을 최대치로 증가시킵니다. 실제로 티베트 관련 텔레그램 채널이나 Reddit 포럼에서 스파이웨어를 의도적으로 공유한 정황도 확인되었습니다. 이러한 방식 또한 이 지침의 사례 연구에 포함되어 있습니다.

악성 앱은 종종 안드로이드에서의 APK 파일과 같은 독립 실행 파일 형태로 공유되며, 이는 사용자가 직접 다운로드하고 설치해야 합니다. 악의적 공격자들은 자신들의 스파이웨어가 합법적인 앱처럼 보이도록 하기 위해, Google Play Store 나 Apple App Store 와 같은 공식 앱 스토어에 업로드하거나, 기존에 문제없이 정상 작동한 앱에 악성 코드를 삽입하기도 합니다.하지만 공식 앱 스토어에는 보안 기능과 검증 절차가 존재하기 때문에 이러한 방식은 상대적으로 성공률이 낮습니다. 그렇기 때문에 공식 앱 스토어에서 제공되는 앱이 비교적 더 안전하지만, 본 지침에 소개된 사례와 NCSC 의 App Store Threat Report 가 보여주듯, 이러한 보안 절차 또한 완벽하지는 않습니다.

다음 4 가지 팁을 따르면 지침에 설명된 위협으로부터 스스로를 보호하는 데 도움이 될 수 있습니다.

자세한 내용은 완화 조치 섹션을 참조하세요.

# 사례 연구

이 두 가지 사례는 MOONSHINE 과 BADBAZAAR 의 작동 방식과 악의적인 공격자들이 가장 위험이 높은 대상자들을 어떻게 표적으로 삼는지 보여줍니다.

## 사례 연구 1: MOONSHINE

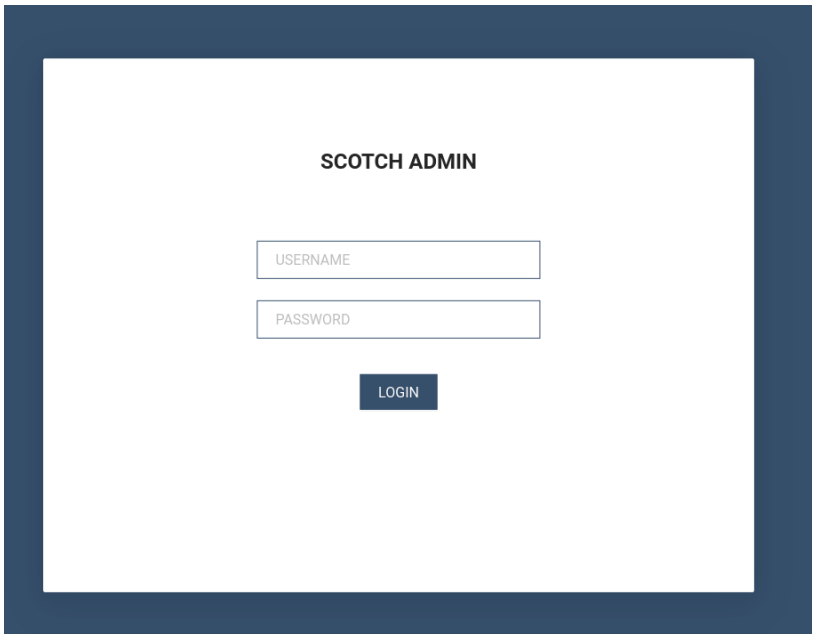
MOONSHINE 은 Citizen Lab 이 2019 년에 티베트 단체를 표적으로 삼는 안드로이드 스파이웨어라고 보고했습니다. MOONSHINE 은 적법한 앱으로 가장해 피해자들이 이를 다운로드 받도록 유도합니다. 텔레그램 채널에서 공유되었으며 WhatsApp 을 통해서 링크가 전송됩니다.

MOONSHINE 은 다음과 같은 광범위한 감시 기능을 갖추고 있습니다:

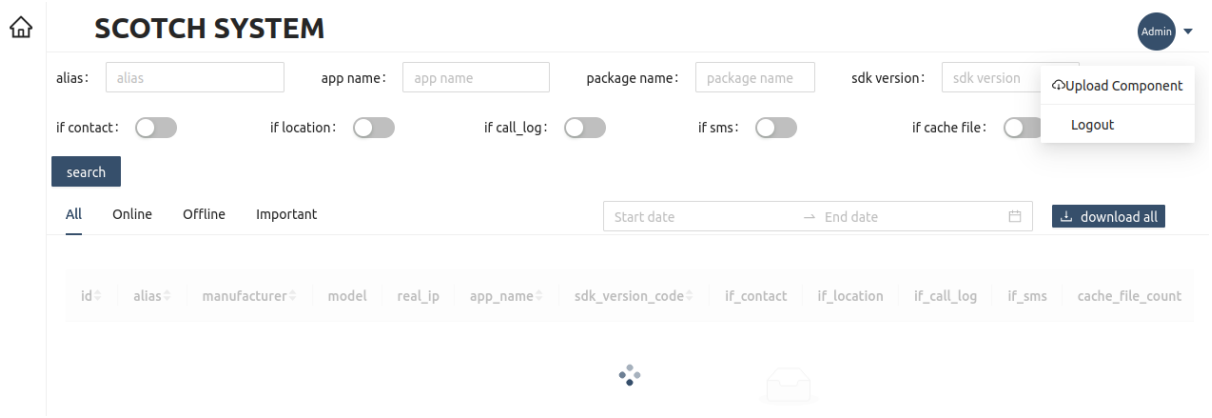
- **실시간 추적을 포함한 위치 정보**
- **실시간 오디오 및 사진 캡처**
- **기기를 통한 파일 다운로드**
- **기기 정보 조회**
- **기기에서 오디오 재생**

**'Audio Quran.apk'**로 번역되는 **'ئاۋازلىق قۇرئان.apk'** 앱은 위구르족을 표적으로 삼기 위해 MOONSHINE 이 사용되는 방법의 한 예입니다. 파일 이름에 위구르어가 사용된 것은 쿠란 앱임을 시사하며, 위구르 무슬림을 유인하기 위해 고안되었을 가능성이 높습니다.

악의적 사이버 공격자는 설치 후 피해자의 기기에서 정보를 수집할 수 있습니다. 이 정보는 'SCOTCH ADMIN' 패널을 통해 확인할 수 있습니다.




로그인 후 공격자는 아래 스크린샷에 표시된 페이지에 접근할 수 있습니다. 이 페이지는 감염된 기기의 세부 정보와 공격자가 감염된 기기에 대해 가진 접근 권한 정도를 표시합니다.




맬웨어 관리 패널은 다음을 비롯한 수집된 정보를 보여줍니다:

- **기기에 대한 액세스 정도**
- **SMS 문자**
- **통화 기록**
- **위치 정보**
- **기기 정보**

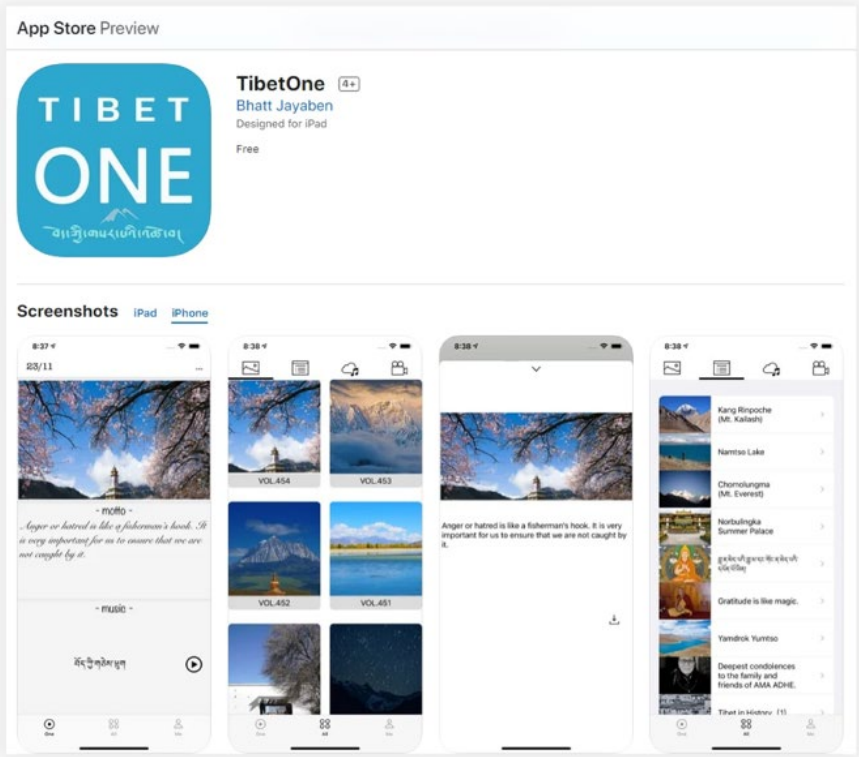
NCSC 는 Cyber League 와 협력해 업계 Trend Micro 의 보고를 바탕으로 HTML 제목에 'UPSEC'이 포함된 로그인 패널과 MOONSHINE 악용 키트 간의 공통점을 발견했습니다. 전체 정보는 함께 제공된 기술 자문에서 찾아볼 수 있습니다.

Intelligence Online 에 따르면 'UPSEC'는 'Sichuan Dianke Network Security Technology Co. Ltd'와 관련이 있습니다. 저작 기관들은 해당 주장의 사실 여부를 확인하지 않았습니다.

## 사례 2: BADBAZAAR

BADBAZAAR 는 위구르족, 티베트인, 대만인을 표적으로 삼은 iOS 및 Android 변종을 보유한 모바일 악성코드입니다. 이 악성코드는 소셜 미디어 플랫폼과 공식 앱 스토어를 통해 유포되었습니다.

Lookout 과 Volexity 에 따르면, BADBAZAAR 는 '**TibetOne**' 앱을 통해 티베트인을 표적으로 삼는 데 사용되었습니다. **TibetOne** 은 악의적 공격자가 만든 iOS 앱으로, 기기 정보 및 위치 데이터에 접근할 수 있는 기능을 갖추고 있습니다. 2021 년 12 월에 Apple 앱 스토어에 업로드되었으나 현재는 삭제된 상태입니다. 악성코드를 더욱 널리 유포하기 위해, 악의적 공격자들은 **'tibetanphone**'이라는 텔레그램 채널에서도 해당 앱을 광고했습니다.



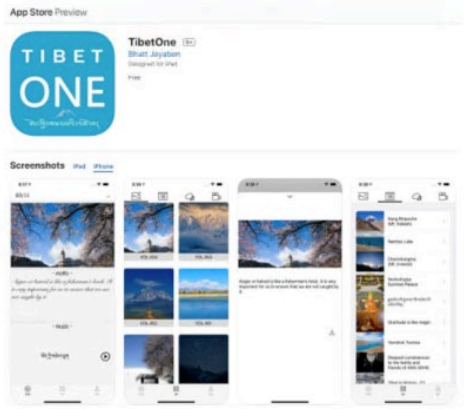

*이미지 1: 애플 앱스토어 상 TibetOne 앱 페이지 해당 앱은 현재 삭제되었습니다.*

8 December 2021

04:15

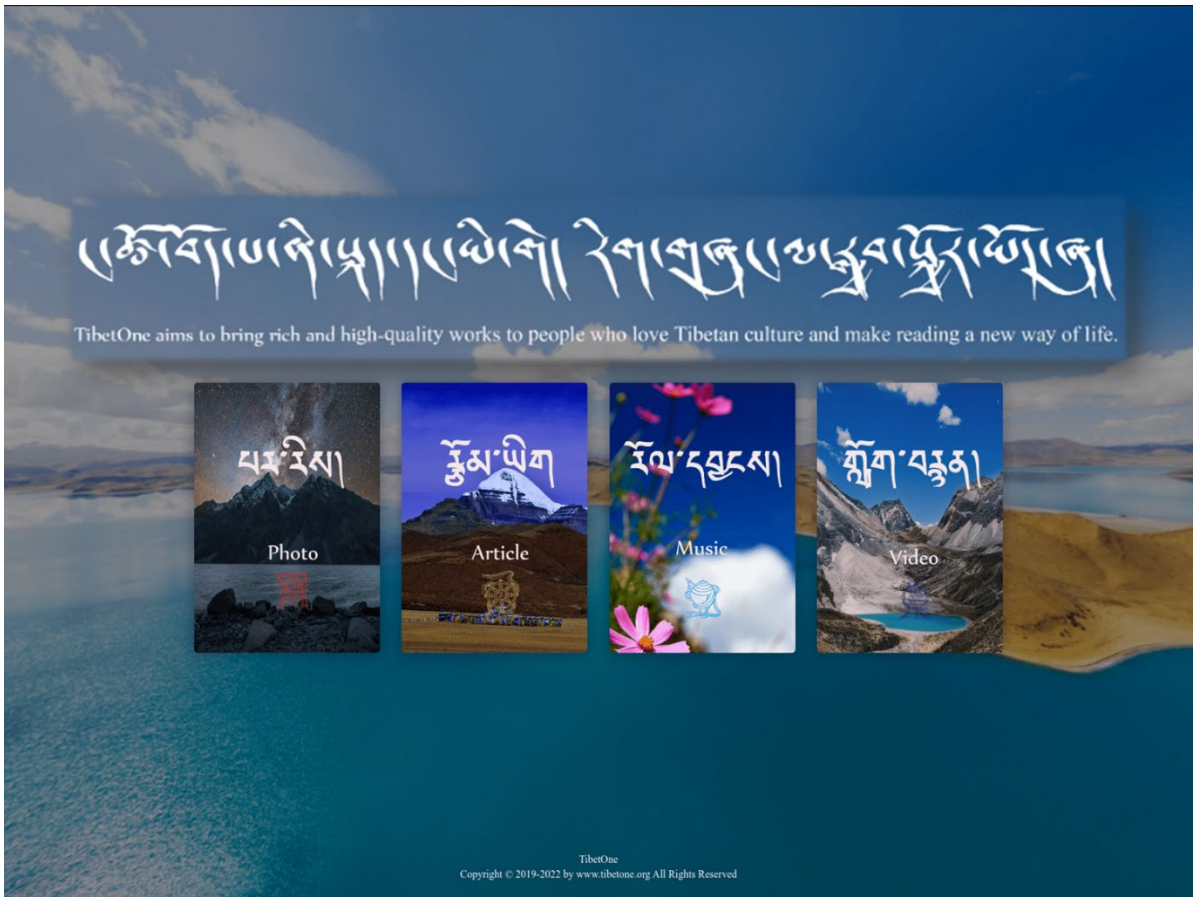
https://apps.apple.com/app/tibetone/id1597024202 TibetOne

04:42




*2: TibetOne*

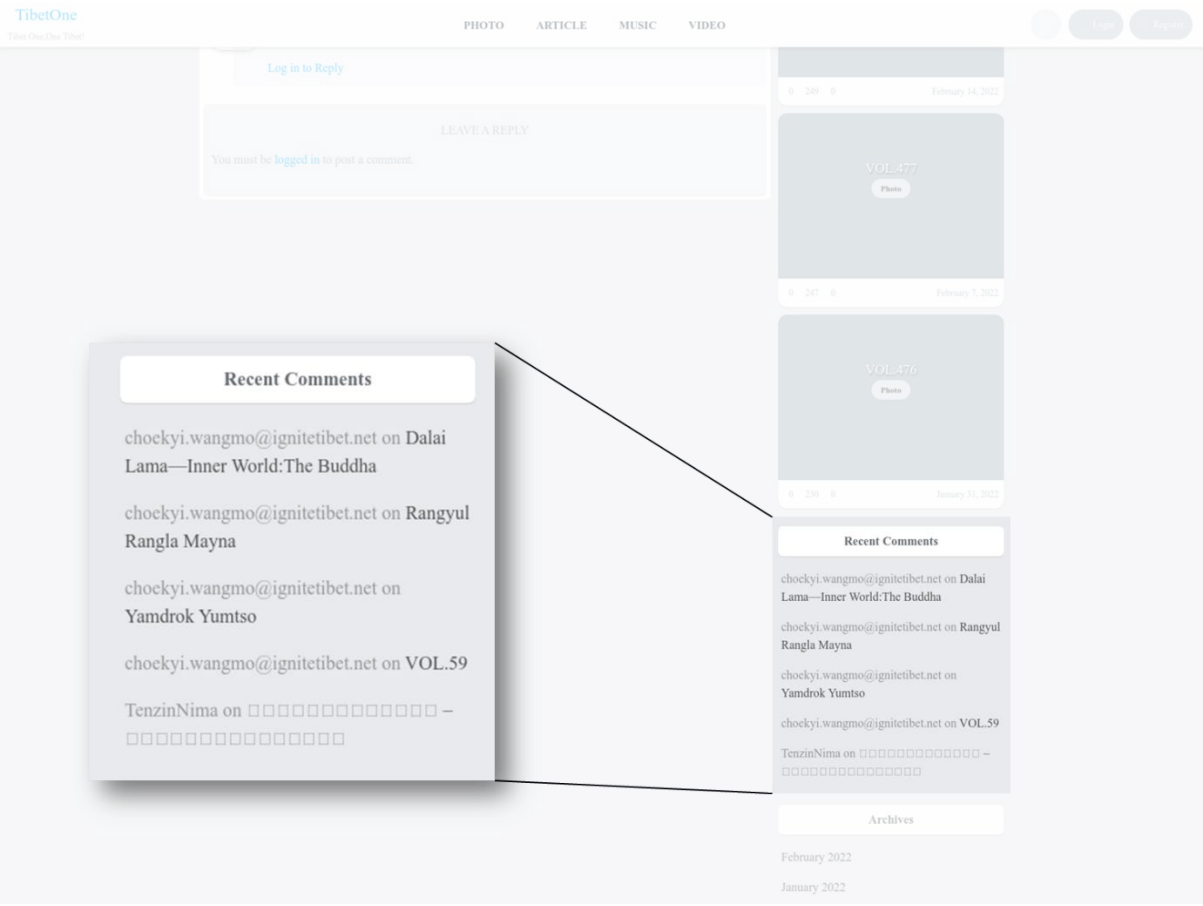
앱에 대한 적법성을 더하기 위해 악의적 공격자들은 '**tibetone[.]org**' 주소의 웹사이트를 개발했습니다. 웹사이트에 적힌 설명은 다음과 같습니다. *'티베트 문화를 사랑하는 사람들에게 풍부하고 고품질의 작품을 제공하고 독서를 새로운 삶의 방식으로 만들어 드립니다.'*




*이미지 3: 'tibetone[.]org' 홈페이지*

*본 이미지는 관련 부분이 더 선명하도록 편집되었습니다.*

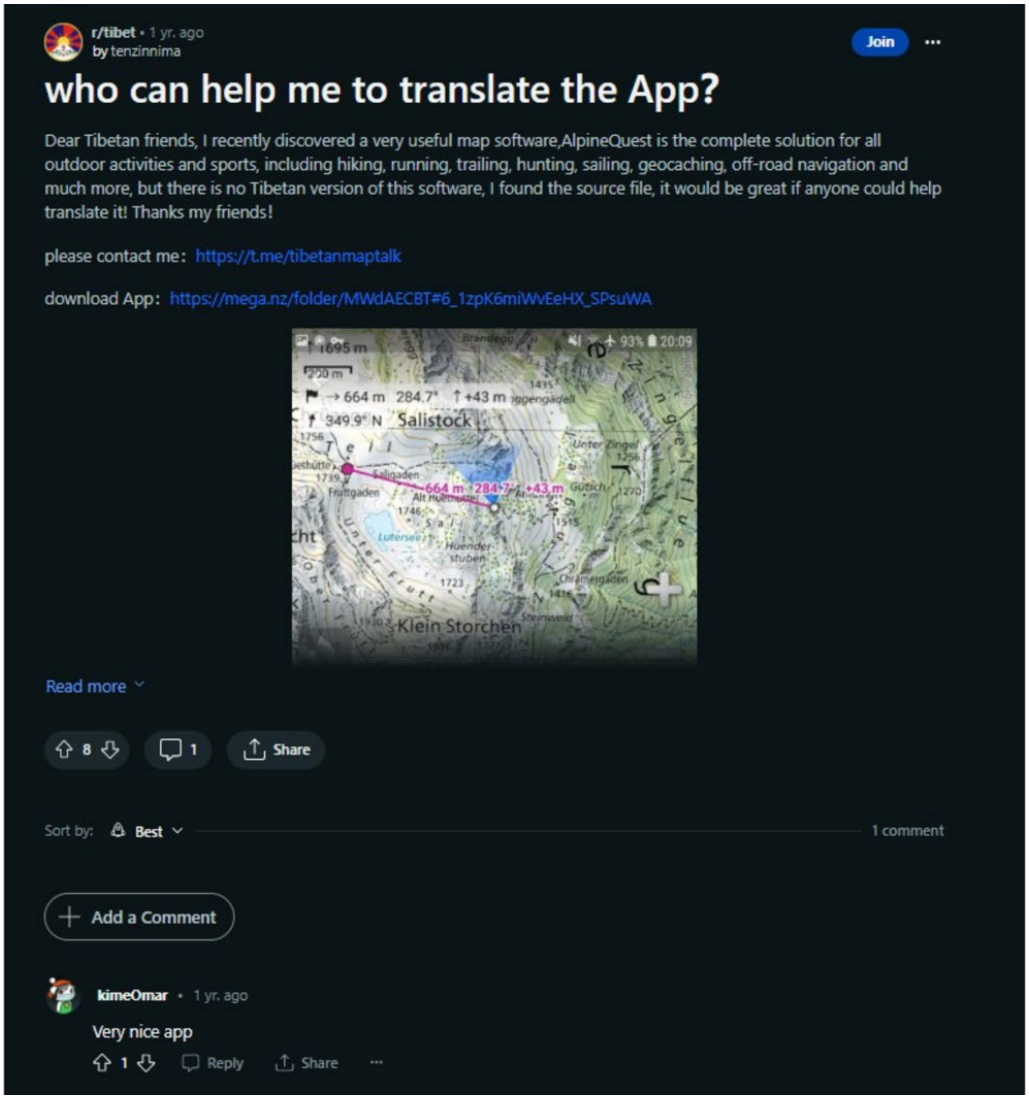
이 웹사이트에는 사용자가 댓글을 남길 수 있는 기사 페이지가 있었습니다. 이메일 주소 **'choekyi.wangmo@ignitetibet.net'**이 남긴 댓글은 악의적인 공격자가 조종하는 것으로 추정되며, 해당 유저는 티베트 인권 민주주의 센터(Tibetan Centre of Human Rights and Democracy) 가 티베트 지지자로 지정한 **'Choekyi Wangmo'** 를 사칭하는 것으로 보입니다. 이는 해당 앱이 티베트 독립을 진심으로 옹호하는 것처럼 보이려는 시도일 가능성이 높습니다.




*이미지 4: 'tibetone[.]org' 페이지 상에서 악의적인 공격자가 조종하는 것으로 추정되는 사용자의 댓글*

*본 이미지는 관련 부분이 더 선명하도록 편집되었습니다.*

'**TenzinNima**'는 이 사이트에 댓글을 남긴 또 다른 사용자의 이름입니다. Volexity 는 해당 사용자 이름이 Reddit 에서 텔레그램 채널 '**Tibetanmaptalk**'를 광고하는 데에도 사용된다고 보고했습니다. 이에는 안드로이드 기기에서 사용 가능한 내비게이션 앱 '**AlpineQuest**'의 악성 샘플을 다운로드하는 링크가 포함되어 있습니다. 제공된 다운로드 링크는 Mega 라는 타사 파일 공유 서비스로 연결됩니다.




*이미지 5: 악의적 공격자가 조종하는 것으로 추정되는 계정에서 악성 애플리케이션을 광고하는 Reddit 게시물*

또한 Volexity 는 해당 게시물에 댓글을 단 '**KimeOmar**'라는 사용자가 다른 Reddit 하위 포럼에서도 악성 앱을 공유하는 모습을 관찰했습니다. 이는 악의적인 공격자들이 여러 소셜 미디어 프로필을 사용하여 게시물을 합법적으로 보이게 한다는 것을 시사할 수 있습니다.

# 평가

BADBAZAAR 및 MOONSHINE 은 위구르, 티베트 및 대만 커뮤니티를 특정적 표적으로 삼아 이들을 대상으로 여러 사회공학적 기법을 사용하고 있습니다.

- 예를 들어, 위구르어 코란 앱과 같이 해당 커뮤니티 내에서 관심도가 높을 수 있는 앱에 트로이 목마를 삽입하는 것을 보아 특정 대상에 맞춰 조정된 것이라고 확신할 수 있습니다.
- 트로이 목마가 설치된 이러한 앱을 공식 앱 스토어에 등록함으로써 신뢰도를 높이는 것으로 보이며, 공동체의 그룹 채팅 공유를 통해 그들의 신뢰 관계를 악용하려는 목적이 있는 것으로 강하게 추정됩니다.

BADBAZAAR 및 MOONSHINE 은 중국 정부에 분명 가치가 있을 만한 데이터를 수집합니다. BADBAZAAR 와 MOONSHINE 의 경우에는 위구르인, 티베트인, 대만인을 겨냥한 것으로 관찰되었지만, 중국 내 다른 소수민족 집단을 표적으로 삼는 악성코드도 존재합니다. 중국과 해외에 소재한 공동서명 국가 시민들은 정권 안정을 위협하는 취지를 지지하는 것으로 여겨지면서 BADBAZAAR 및 MOONSHINE 과 같은 모바일 맬웨어의 위협을 받고 있을 가능성이 매우 높습니다. 이러한 악성코드는 위치 정보, 오디오, 사진 데이터 등을 수집할 수 있는 기능을 갖추고 있으며, 이는 표적의 활동에 대한 실시간 정보를 제공함으로써 향후 감시 및 괴롭힘 작전을 계획하는 데 활용될 가능성이 매우 높습니다

### 모바일 앱 사용자를 위한 완화 전략

저작 기관에서는 사례 연구에 설명된 위협으로부터 보호하기 위해 다음과 같은 보안 관행을 권장합니다. 이들 권장사항은 NCSC 지침에 따른 가장 이상적인 관행에 기반했습니다. 호주와 미국 독자를 위한 모범 관행 지침에 대한 링크는 '추가 자료' 부분을 참조하세요.

# 기기 보안을 유지하기

- **Google 플레이 스토어 또는 Apple 앱 스토어와 같은 공식적인 앱 스토어에서만 앱을 다운 받습니다.** Google Play 스토어 와 Apple 앱 스토어는 소프트웨어를 공개하기 전에 바이러스 검사를 실시하여 다운로드하는 콘텐츠가 안전하다는 더 많은 확신을 사용자에게 줍니다. 신뢰할 수 있는 스토어에서 다운로드한 앱도 완벽히 안전할 순 없지만, 다른 출처에서 다운로드한 앱은 아무런 보호 기능이 없을 수 있습니다. NCSC 는 앱 스토어에 대한 위험 보고서를 제공하고 있습니다: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **기기 및 앱을 최신 상태로 유지합니다.** 앱 및 기기 소프트웨어 업데이트가 제공될 때마다 바로 설치하세요. 기기 설정에서 '자동 업데이트'가 가능한 경우 활성화시킴으로써 수동으로 수행해야 하는 번거로움을 피하세요. 알려진 바이러스 및 기타 악성코드로부터 기기를 보호하려면 NCSC 의 온라인 보안 유지 지침을 참조하세요. 업데이트는 대개 개선 사항과 새로운 기능을 포함합니다: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **기기를 '탈옥(jailbreak)'하거나 '루팅(root)'하지 마세요.** 이는 패치되지 않은 취약점을 이용하여 보안 제어 장치를 우회합니다. 이로 인해 기기가 공격에 더 취약해집니다.. NCSC 지침 열람: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

# 앱 관리하기

- **앱 및 해당 앱의 권한을 검토합니다.** 앱이 더이상 필요없는 경우, 기기에서 삭제하세요. 맬웨어는 보호된 파일이나 카메라, 마이크 등의 주변 장치에 접근하도록 설계되는 경우가 많기 때문에 가능하다면 앱 권한을 제한하여 데이터 노출을 최소화하세요.
  - 애플 사용자를 위한 앱 권한 확인 방법: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - 안드로이드 사용자를 위한 앱 권한 확인 방법: https://support.google.com/android/answer/9431959?hl=en-GB

- **모르는 앱은 자동으로 Google 에 전송되도록 설정합니다.** Android 사용자이고 Google Play 스토어가 아닌 다른 곳에서 앱을 다운로드한 경우, Google Play 스토어 앱 설정의 'Play Protect'에서 'Improve harmful app detection(유해한 앱 탐지 개선)'을 활성화하여 해당 앱 정보를 Google 에 전송할 수 있습니다. 이렇게 하면 앱에서 맬웨어를 감지하여 사용자를 보호하는 데 도움이 됩니다. 설치 방법에 대한 정보: https://support.google.com/android/answer/2812853?hl=en-GB

# 사이버 서비스 활용하기

- **링크에 접속하기 전 URL 검증 서비스를 사용합니다.** 이메일, 문자 메시지 또는 기타 소스에서 온 링크가 안전한지 여부를 Google Transparency Report 또는 Virus Total 과 같은 서비스를 사용해 스캔해 보세요. Virus Total 과 같은 맬웨어 감지 시스템에 의심되는 파일과 앱을 업로드하면 파일의 악성 여부를 판단하는 데 도움이 될 수 있습니다. 스캔 서비스에서는 거짓 음성 결과가 나올 수 있음을 유의하세요.

- **Google 의 Advanced Protection 프로그램에 등록합니다.** 이는 Google 서비스(Gmail, Play Store 등)를 사용하고 표적이 될 위험이 있는 개인을 보호하기

위해 고안된 무료 서비스입니다. 이 서비스는 Google 서비스 사용 시 더 강화된 보안을 제공합니다: https://landing.google.com/advancedprotection/

- **사용 가능한 경우 추가 보안 서비스에 등록합니다.** 예를 들어, 영국의 고위험군 개인은 사이버 보안에 도움이 되는 추가적인 방어 서비스를 받을 수 있습니다. 자격 조건 및 더 자세한 정보는 다음 링크에서 찾아볼 수 있습니다: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

# 위험 요소 신고하기

- **거짓 계정 식별 및 신고** 악의적인 사이버 범죄자는 거짓 계정을 만들거나 실제 계정을 해킹하여 목적을 달성합니다. 어떠한 계정이 가짜거나 침해되었다고 생각되는 경우, 관련 플랫폼에 신고한 후 차단하세요. 많은 서비스에는 계정의 진위여부를 판단하는 절차가 있습니다. 예를 들어 Instagram 과 Facebook 에서는 '인증 배지'가 사용됩니다. 이 장치는 해당 계정이 진짜인지를 파악하는 데 도움이 됩니다. NCSC 는 소셜 미디어를 안전하게 사용하기 위한 지침을 제공하며 이에는 침해된 계정을 확인하고 보고하는 방법에 대한 세부 정보가 포함됩니다: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **사기 이메일 주소, SMS 문자 및 링크를 이용한 피싱** NCSC 는 의심되는 이메일 주소 및 웹사이트를 조사할 수 있습니다. 만약 어떠한 사이트, 이메일 또는 메시지가 의심스럽다면, 신고할 수 있습니다: https://www.ncsc.gov.uk/collection/phishing-scams

# NCSC 용어 정의

- **안드로이드**

Google 의 모바일 운영체제로 여러 스마트폰 및 태블릿 제조업체에서 사용됩니다.

- **앱**

애플리케이션, 즉 앱은 이미 기기에 설정되어 있거나 사용자가 따로 설정할 수 있는 소프트웨어 패기지로 기기에 기능 또는 콘텐츠를 추가합니다.

- **사이버 보안**

기기, 서비스 및 네트워크 자체와 이들 시스템에 저장된 정보를 승인되지 않은 사람으로부터의 접근, 도난 또는 손상을 방지합니다.

- **기기**

컴퓨터 기반 하드웨어로 데스크탑 컴퓨터, 스마트폰, 또는 태블릿과 같은 실재하는 물건

- **iOS**

Apple 의 모바일 운영체제로 자사 휴대 기기 전체에 사용됩니다.

- **맬웨어**

'악성 소프트웨어'에서 파생된 맬웨어는 컴퓨터 시스템, 네트워크 또는 장치를 손상시킬 수 있는 모든 종류의 소프트웨어입니다. 이는 바이러스, 랜섬웨어 및 트로이 목마를 포함합니다.

- **운영체제**

컴퓨터, 태블릿, 스마트폰의 추가 앱 및 하드웨어를 작동시키기 위해 기본적으로 탑재된 소프트웨어

- **피싱**

악성 소프트웨어가 포함되어 있거나 사용자를 속여 중요 정보(예: 비밀번호)를 공개하거나 돈을 이체하도록 하는 웹사이트 링크가 포함된 사기성 이메일이나 문자 메시지입니다.

- **스파이웨어**

사용자의 동의 없이 설치되어 데이터를 수집한 다음 이를 제 3 자에게 전송하는 하나의 맬웨어 유형

- **소셜 미디어**

사람들이 사용자 생성 콘텐츠(글 게시물, 사진, 비디오)를 공유하고 응답할 수 있도록 해주는 웹사이트 및 앱(Facebook, X, Instagram 등)

- **스마트폰**

안드로이드 및 iOS 운영체제가 탑재된 기기를 포함하여 복잡한 기능을 수행할 수 있는 현대식 휴대폰

- **트로이 목마**

피해자의 기기에 승인되지 않은 접근권을 획득하기 위해 사용되는 적법한 소프트웨어를 가장한 하나의 맬웨어 유형

- **URL**

Uniform Resource Locator 의 약자 도메인 이름(예: www.bbc.co.uk)과 같은 월드 와이드 웹의 주소

- **바이러스**

적법한 소프트웨어 프로그램을 감염시키고 해당 프로그램이 활성화되면 네트워크 전체에 복제되도록 설계된 하나의 맬웨어 유형

# 추가 자료

## 호주 Australian Cyber Security Centre 제공 지침

- 사이버 범죄, 사건 또는 취약점 신고하기 (Report a cybercrime, incident or vulnerability)
- 여러분의 기기를 보호하는 방법 (How to secure your devices)
- 여러분의 휴대 기기 보호하기 (Secure your mobile phone)
- 피싱 (Phishing)
- 사기 (Scams)
- 여러분의 소셜 미디어 계정 보호하기 (Secure your social media)
- 소셜 미디어 및 문자 앱 보안 팁 (Security tips for social media and messaging apps)

## UK NCSC 및 NPSA 제공

- 민주주의 지키기 (Defending Democracy)
- 소셜 미디어: 안전하게 사용하는 방법 (Social Media: how to use it safely)
- 기관을 위한 휴대폰을 포함한 기기 보안 지침 (Device Security Guidance for organisations including mobile)
- 엡 스토어에 대한 위협 신고 (Threat report on application stores)
- 고위험군 개인을 위한 개인 안전 및 보안 (Personal safety and security for high-risk individuals)

## US NSA 제공 지침

- 가장 이상적인 휴대기기 사용 방법 (Mobile Device Best Practices)

# 면책 조항

본 지침은 발행 당시 검증된 정보를 제공한다는 점을 참고하시기 바랍니다.

이 보고서는 작성 기관과 업계 소스에서 얻은 정보를 바탕으로 작성되었습니다. 모든 조사 결과나 권장사항 또한 모든 위험을 방지하기 위한 의도로 제공된 것은 아니며, 마찬가지로 권장사항을 따른다고 해서 모든 위험이 제거되는 것은 아닙니다. 정보 위험에 대한 책임 소재는 언제나 해당 시스템 소유자에게 있습니다.

영국에서 이 정보는 2000 년 정보공개법(FOIA)에 따라 면제되며, 다른 영국 정보법에 따라서도 면제될 수 있습니다.

모든 FOIA 문의는 다음 주소로 전송해주시기 바랍니다. ncscinfoleg@ncsc.gov.uk

## 별첨: 관찰된 MOONSHINE 및 BADBAZAAR 샘플

아래 표는 지난 2 년 동안 MOONSHINE 과 BADBAZAAR 캠페인에 사용된 앱을 나열한 것입니다.

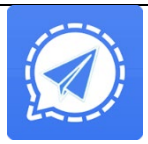
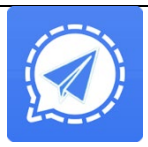
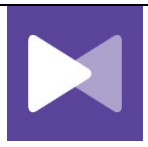
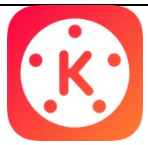
이들 앱 중 대부분은 이미 출시된 앱과 높은 유사성을 나타냅니다. 이는 유명 브랜드를 '스푸핑(도용)'하기 위한 의도적인 기술일 가능성이 높습니다.

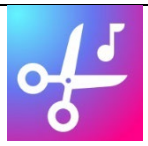
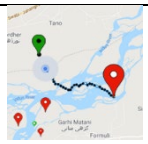
**앱 및 패키지 명, 그리고 아이콘은 실제 앱과 똑같거나 유사할 수 있으므로 아래 정보만으로 기기가 감염되었는지 여부를 판단해서는 안 됩니다.**

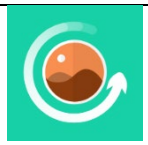
완화 조치 부분에 포함된 대로, '유해한 앱 감지 개선(Improve harmful app detection)'을 활성화하여 Android 기기의 앱 정보를 Google 에 자동 전송할 수 있습니다. 이 기능은 Play 스토어 외부에서 설치된 앱을 기기에서 검사합니다.

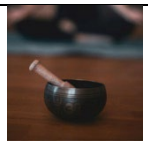
| 앱 명 | 패키지 명 | 앱 아이콘 |
|---|---|---|
| 99 Names of ALLAH | com.Apptriple.Namesofallah.Asmaulhusna |  |
| APKPure | com.apkpure.aegon |  |
| Adobe Acrobat | com.adobe.reader |  |
| Alpine(پښتو) | psyberia.pa.full |  |
| AlpineQuest Off-Road Explorer | psyberia.alpinequest.full |  |
| AlpineQuest Off-Road Explorer | psyberia.alpinequest.full |  |

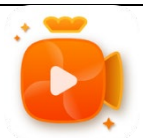
| | | |
|---|---|---|
| AlpineQuest Off-Road Explorer (Lite) | psyberia.alpinequest.free |  |
| AppLock | com.alpha.applock |  |
| Arabic Keyboard | com.arabic.keyboard.arabic.language.keyboard.app |  |
| Audio Video Cutter | bsoft.com.mp3.cutter.ringtone.video.maker.trimmer |  |
| Badam 维语输入法 | com.ziipin.softkeyboard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

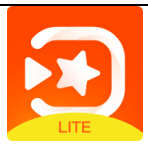
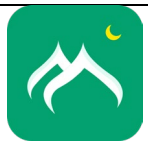
| | | |
|---|---|---|
| FMWhatsApp | com.fmwhatsapp |  |
| File Manager + | com.alphainventor.filemanager |  |
| FlyGram | org.telegram.FlyGram |  |
| Flygram | org.telegram.FlyGram |  |
| Free WiFi Pass | com.cl.wifipassword.share |  |
| GBWhatsApp | com.gbwhatsapp |  |
| Hefz Quran | com.golap.hefzquran |  |
| Hijri Calendar | com.ibrahim.hijricalendar |  |
| InShot | com.camerasideas.instashot |  |
| KMPlayer | com.kmplayer |  |
| KineMaster | com.nexstreaming.app.kinemasterfree |  |

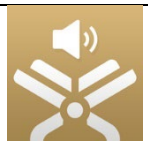
| | | |
|---|---|---|
| MP3 Cutter & Ringtone Maker | ringtone.maker.mp3.cutter.audio |  |
| Malloc | com.mallocprivacy.antistalkerfree |  |
| Maps Distance Calculator | com.routemap.mapdownload.gpsroutplanner |  |
| Media Recovery | com.aaa.media.recovery.androidapp |  |
| Nur.cn | com.nur.reader |  |
| 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 |  |

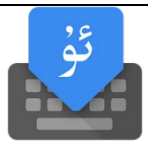
| | | |
|---|---|---|
| Photo Recovery | recover.restore.undelete.photo.video.file |  |
| Photo Studio | com.kvadgroup.photostudio |  |
| Plus | org.telegram.pluspro |  |
| Prayer Book | com.arashpayan.prayerbook |  |
| QuarkVPN | com.speedy.vpn |  |
| Quran | com.tos.quranuighore |  |
| QuranKerim | 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 |  |
| زىكرلەر | com.my.newproject5 |  |
| كەرىم قۇرئان | ru.omdevelopment.ref.quranuyghur.free |  |
| لۇغىتى ىقاپqكۇ | 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 |  |