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

Aviso

BADBAZAAR e MOONSHINE: Spyware direcionado a grupos uigures, taiwaneses e tibetanos e atores da sociedade civil

9 de abril de 2025

BADBAZAAR e MOONSHINE: Spyware direcionado a grupos uigures, taiwaneses e tibetanos e atores da sociedade civil

O NCSC e os seus parceiros publicam novas informações e medidas de mitigação para aqueles que correm alto risco de duas variantes de spyware.

Resumo

Com o apoio do Reino Unido Cyber League, este aviso foi elaborado em conjunto pelo Centro Nacional de Segurança Cibernética (NCSC UK) e parceiros internacionais:

- **O Centro Australiano de Segurança Cibernética, que faz parte da Direção Australiana de Sinais**
- **O Centro Canadiano para a Cibersegurança que faz parte do Estabelecimento de Segurança das Comunicações**
- **O Serviço Federal de Inteligência da Alemanha**
- **O Departamento Federal Alemão para a Proteção da Constituição**
- **O Centro Nacional de Segurança Cibernética da Nova Zelândia, que faz parte do Gabinete de Segurança das Comunicações do Governo**
- **A Agência Federal de Investigação dos Estados Unidos**
- **A Agência de Segurança Nacional dos Estados Unidos**

O seu objetivo é criar consciencialização sobre a crescente ameaça que os cibercriminosos representam para indivíduos ligados a temas que incluem Taiwan, Tibete, Região Autónoma Uigur de Xinjiang, movimentos democráticos e Falun Gong.

Este aviso inclui dois estudos de caso que detalham as técnicas utilizadas por cibercriminosos maliciosos que utilizam spywares conhecidos como BADBAZAAR e MOONSHINE para obter dados em dispositivos móveis, incluindo smartphones, que possam ser do interesse do Estado chinês. Além disso, fornece orientações para ajudar as pessoas a protegerem-se a si próprias, os seus dispositivos e os seus dados.

Juntamente com este aviso, o NCSC publicou detalhes técnicos completos com orientações separadas.

Quem corre risco?

As agências autoras e os parceiros da indústria observaram que o BADBAZAAR e o MOONSHINE visam especificamente indivíduos ligados a temas considerados pelo Estado chinês como uma ameaça à sua autoridade interna, ambições e reputação global. Aqueles que estão em maior risco incluem, mas não se limitam a, qualquer pessoa ligada a:

- **Independência de Taiwan**
- **Direitos tibetanos**
- **Muçulmanos uigures e outras minorias étnicas na ou provenientes da Região Autónoma Uigur de Xinjiang na China**
- **defesa da democracia (incluindo Hong Kong)**
- **o movimento espiritual Falun Gong**

Isto inclui organizações não governamentais (ONGs), jornalistas, empresas e indivíduos que defendem, se identificam com ou representam esses grupos. A forma indiscriminada como este spyware se espalha online também significa que existe o risco de as infeções se espalharem para além das vítimas pretendidas.

Este aviso tem como objetivo ajudar as pessoas em risco a responder eficazmente à ameaça específica dos spywares BADBAZAAR e MOONSHINE. As medidas de mitigação sugeridas complementam as recomendações mais amplas sobre segurança cibernética e não devem ser consideradas isoladamente.

Seguindo as orientações referenciadas neste aviso, os utilizadores podem reduzir o risco de infeção dos seus dispositivos móveis e dados.

A ameaça

MOONSHINE e BADBAZAAR são exemplos de trojans; eles têm funções maliciosas ocultas dentro de uma aplicação que funciona normalmente que pode ser baixada em lojas de aplicações ou serviços de partilha de ficheiros online.

Essas aplicações são concebidas para induzir o utilizador a descarregá-las e instalá-las num dispositivo. Depois de instalada, a aplicação utiliza vulnerabilidades no dispositivo para executar funções não autorizadas ou pode depender da concessão de permissões pelo utilizador para aceder e descarregar informações do dispositivo, incluindo:

- **dados de localização, incluindo rastreamento em tempo real**
- **acesso ao microfone e à câmara**
- **mensagens, fotos e outros ficheiros armazenados no dispositivo**
- **informações do dispositivo e muito mais**

Em seguida, os autores exploram os interesses legítimos dos grupos em risco, para identificar e infetar o maior número possível de vítimas e obter acesso aos seus dados. Uma maneira de fazer isso é através de criação de aplicações que eles sabem que vão atrair as suas vítimas, como aplicações que suportam as suas línguas nativas ou que contêm conteúdo específico de locais como as regiões tibetanas da China ou Xinjiang.

Os estudos de caso neste aviso fornecem alguns exemplos disso, incluindo as aplicações TibetOne e Uyghur Quran.

Os autores atuam em fóruns online onde existe uma base de utilizadores das suas vítimas pretendidas, o que maximiza as suas hipóteses de infetar as vítimas. Foi observado que eles partilham deliberadamente spyware em canais do Telegram e fóruns do Reddit relacionados com o Tibete. Os estudos de caso neste aviso também dão exemplos desses métodos.

As aplicações maliciosas são muitas vezes partilhadas como ficheiros independentes, tais como ficheiros APK no Android, que os utilizadores têm de descarregar e instalar. Os autores tentam fazer com que o seu spyware pareça mais legítimo, carregando-o em lojas de aplicações oficiais, como a Google Play Store e a Apple App Store, ou adicionando código malicioso a aplicações anteriormente benignas, embora as lojas oficiais tenham funcionalidades de segurança e processos de verificação que tornam esta tática menos bem-sucedida. Isso torna as aplicações das lojas oficiais mais seguras, mas, conforme demonstrado nos estudos de caso e no Relatório sobre Ameaças à App Store, do NCSC, esses processos não são perfeitos.

Seguir estas 4 dicas pode ajudar a protegê-lo das ameaças descritas neste aviso.

Para conselhos mais detalhados, consulte a secção sobre medidas de mitigação.

Estudos de caso

Estes dois estudos de caso ilustram como o MOONSHINE e o BADBAZAAR funcionam e como os cibercriminosos estão a almejar as pessoas mais vulneráveis.

Estudo de caso um: MOONSHINE

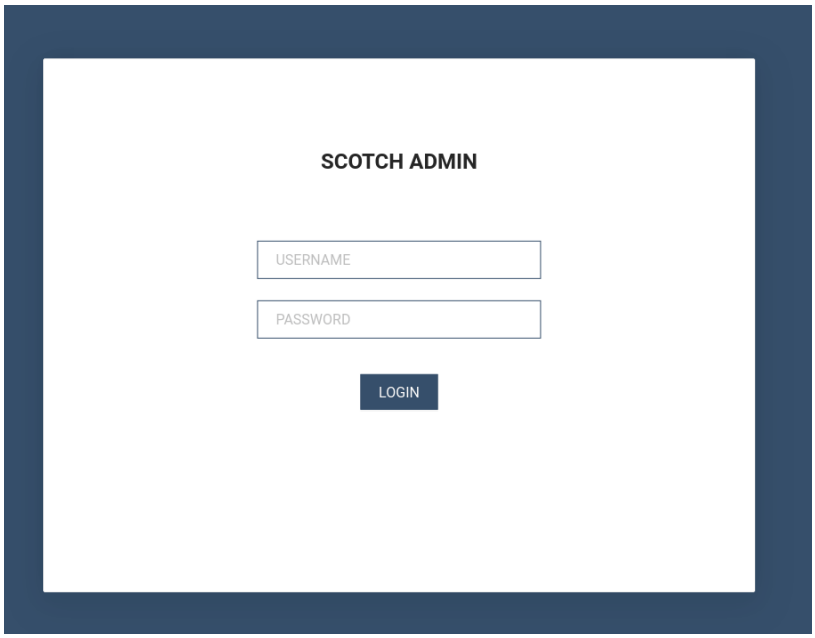
O MOONSHINE é um spyware para Android relatado em 2019 pelo Citizen Lab como almejando grupos tibetanos. O MOONSHINE disfarça-se como uma aplicação legítima para induzir as vítimas a instalá-lo. Foi partilhado através de canais do Telegram e de links enviados pelo WhatsApp.

O MOONSHINE possui amplas capacidades de vigilância, tais como:

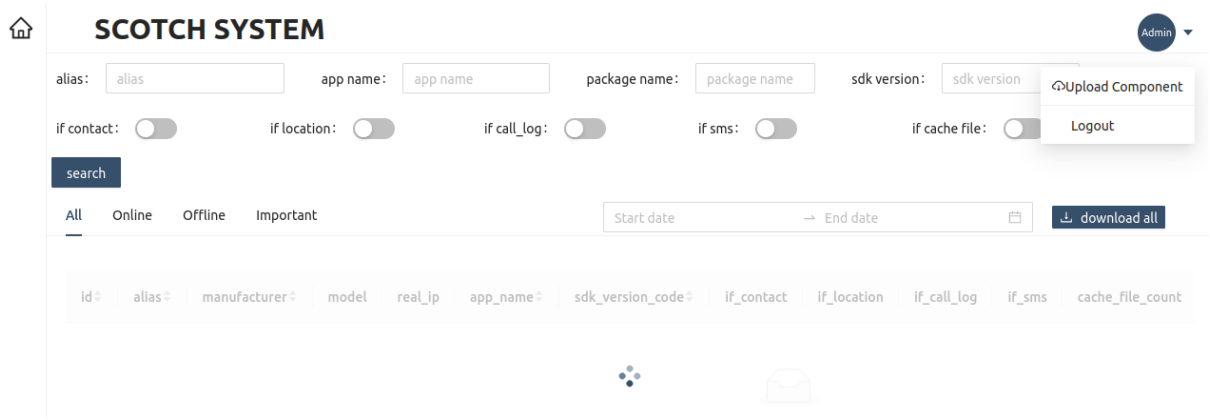
- **dados de localização, incluindo rastreamento em tempo real**
- **captura de áudio e fotos ao vivo**
- **baixar ficheiros do dispositivo**
- **recuperar informações do dispositivo**
- **reproduzir áudio no dispositivo**

A aplicação '**.apk**'قۇرئان ئاۋازلىق, cuja tradução é '**Audio Quran.apk**', é um exemplo de como o MOONSHINE é utilizado para atingir os uigures. O uso da língua uigur no nome do ficheiro, indicando uma aplicação do Alcorão, foi provavelmente concebido para atrair os muçulmanos uigures.

Uma vez instalada, os cibercriminosos podem recolher informação dos dispositivos das vítimas. Essa informação pode ser acedida através do painel 'SCOTCH ADMIN'.



Depois de fazerem login, os autores podem aceder a página mostrada na captura de tela abaixo. Esta página mostra detalhes dos dispositivos infetados e o nível de acesso que o agente tem aos dispositivos infetados:



O painel de gestão de malware mostra os dados recolhidos, incluindo:

- **nível de acesso ao dispositivo**
- **mensagens SMS**
- **registos de chamadas**
- **dados de localização**
- **informação do dispositivo**

Em colaboração com a Cyber League, o NCSC baseou-se em relatórios da indústria da Trend Micro para encontrar sobreposições entre o kit de exploração MOONSHINE e painéis de login que contêm 'UPSEC' no título HTML. Detalhes completos estão no aviso técnico que acompanha este documento.

De acordo com Intelligence Online, UPSEC é uma referência à 'Sichuan Dianke Network Security Technology Co. Ltd'. As agências autoras não verificaram esta declaração.

Estudo de caso dois: BADBAZAAR

O BADBAZAAR é um malware móvel com variantes para iOS e Android que almeja indivíduos uigures, tibetanos e taiwaneses. Este malware foi disseminado através de plataformas de redes sociais e lojas oficiais de aplicações.

O BADBAZAAR tem sido usado para atingir tibetanos através da aplicação **'TibetOne'**, conforme relatado por Lookout e Volexity. O **TibetOne** é uma aplicação iOS criada por agentes maliciosos, com a capacidade de aceder a informações e dados de localização do dispositivo. Foi carregada na Apple App Store em dezembro de 2021, mas já não está disponível. Para espalhar ainda mais o malware, os autores também anunciaram a aplicação num canal do Telegram chamado '**tibetanphone**'.

TibetOne

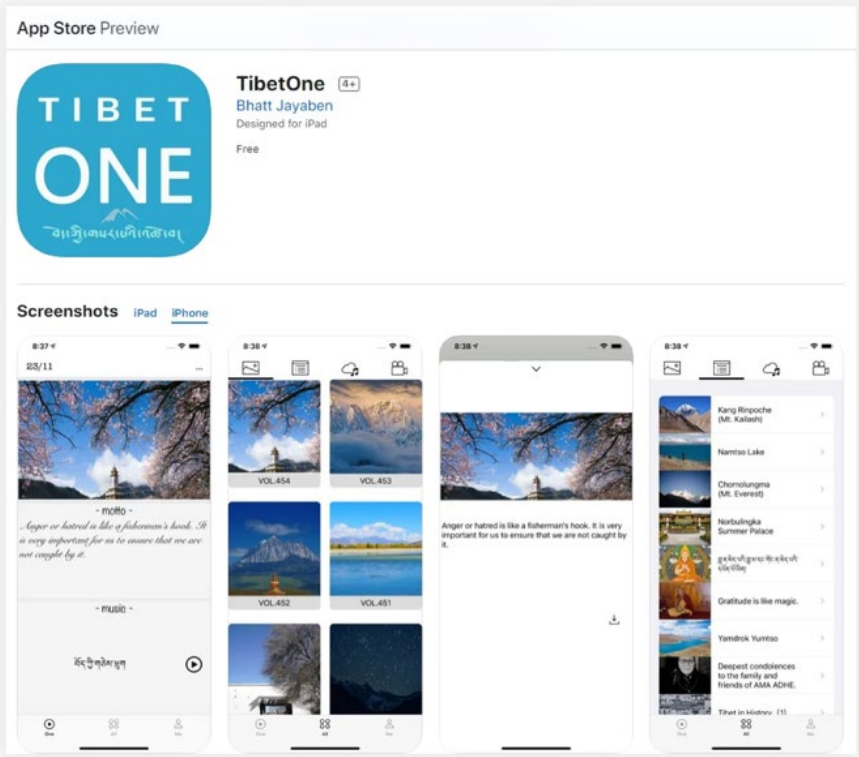


Figura 1: Página da aplicação TibetOne na App Store da Apple. A aplicação foi posteriormente removida.

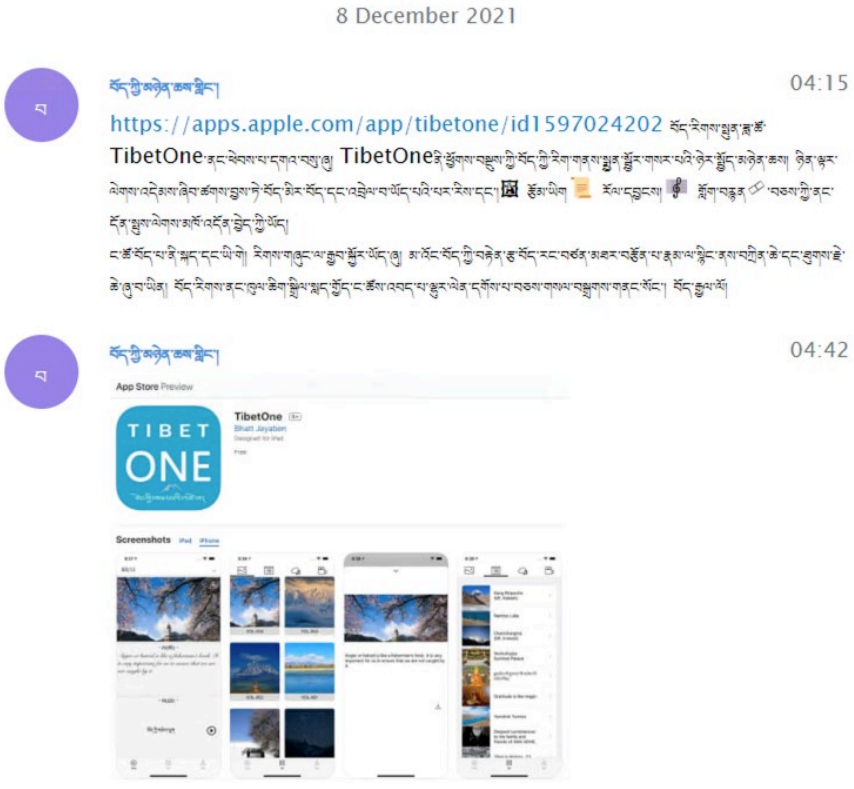


Figura 2: TibetOne conforme partilhada nos canais de Telegram.

Para dar mais legitimidade à aplicação, os autores também criaram um site chamado '**tibetone[.]org**', que se descrevia como *'levando obras ricas e de alta qualidade para pessoas que amam a cultura tibetana e tornando a leitura um novo estilo de vida'.*

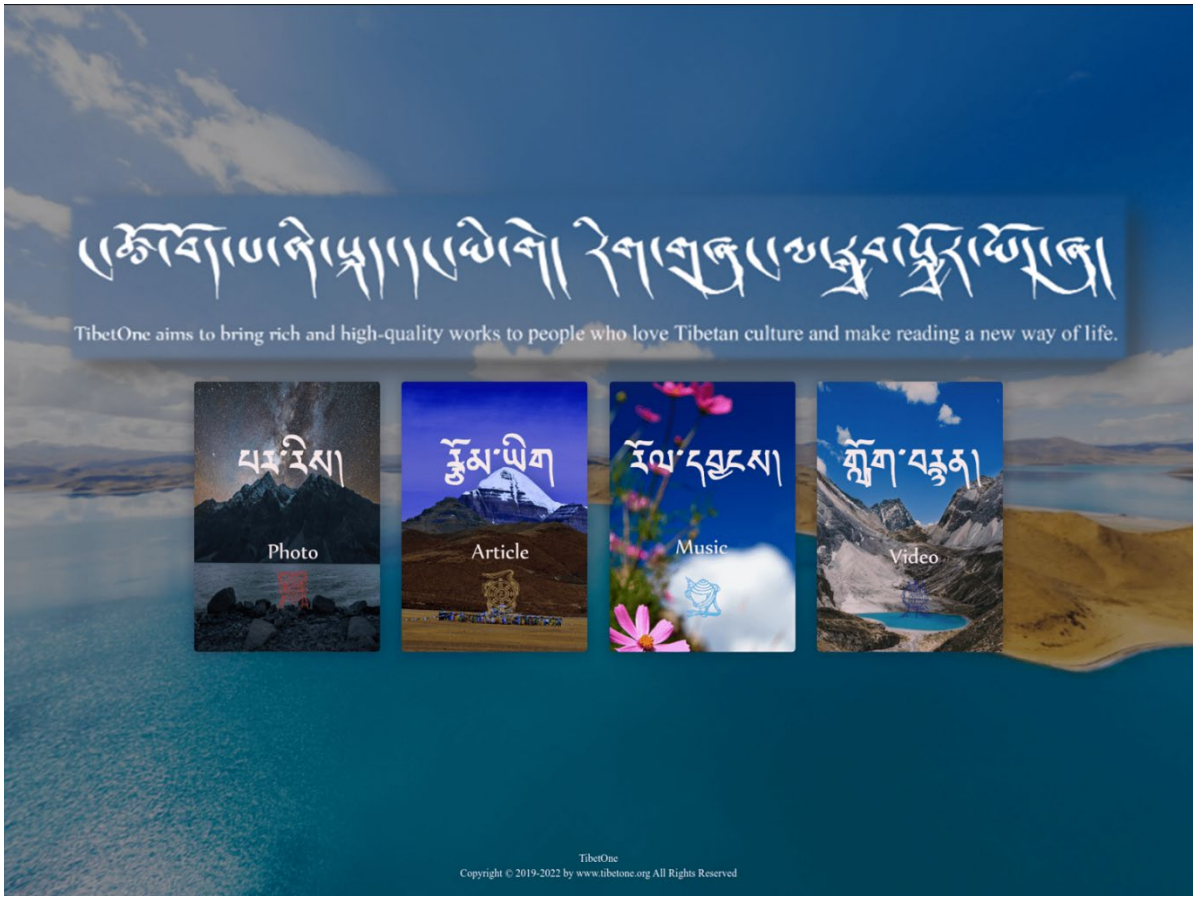


Figura 3: Página inicial de 'tibetone[.]org'.

Esta imagem foi editada para tornar as secções relevantes mais claras.

Este site tinha uma página para artigos que permitia que os utilizadores deixassem comentários. Um comentário deixado por endereço eletrónico '**choekyi.wangmo@ignitetibet.net**', é considerado como sendo controlado pelo autor malicioso e provavelmente que se faz passar por '**Choekyi Wangmo**' que o Centro Tibetano de Direitos Humanos e Democracia lista como um manifestante pró-Tibete. Provavelmente, esta é mais uma tentativa de dar a impressão de que a aplicação defende genuinamente a independência do Tibete.

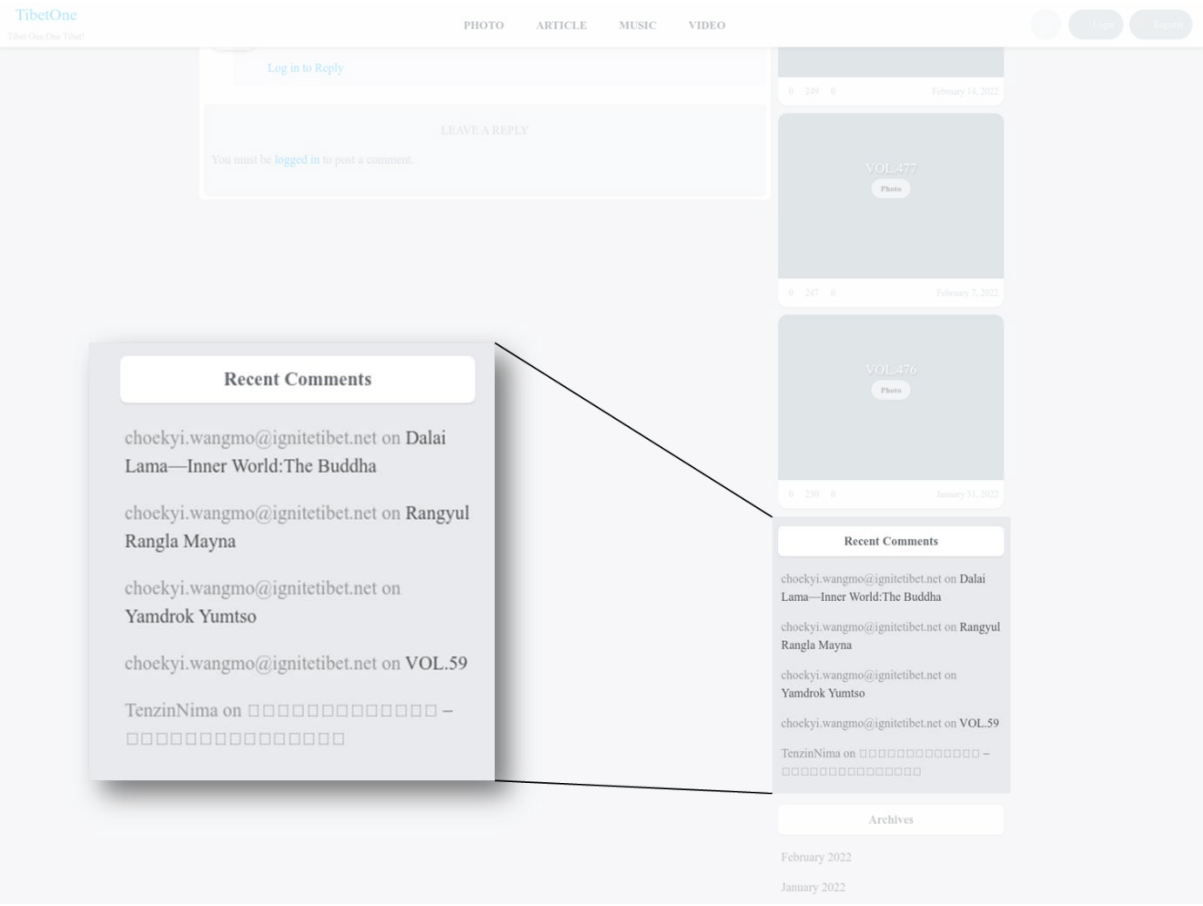


Figura 4: página de 'tibetone[.]org' mostrando comentários de utilizadores que se acredita serem controlados pelo agente malicioso.

Esta imagem foi editada para tornar as secções relevantes mais claras.

'**TenzinNima**' é mais um nome de utilizador que adicionou comentários neste site. Volexity informou que esse nome de utilizador também é usado no Reddit para divulgar o canal do Telegram '**Tibetanmaptalk**'. Inclui um link para baixar uma amostra maliciosa do '**AlpineQuest**', uma aplicação de navegação disponível em dispositivos Android. O link para baixar fornecido é para um serviço de partilha de ficheiros de terceiros chamado Mega.

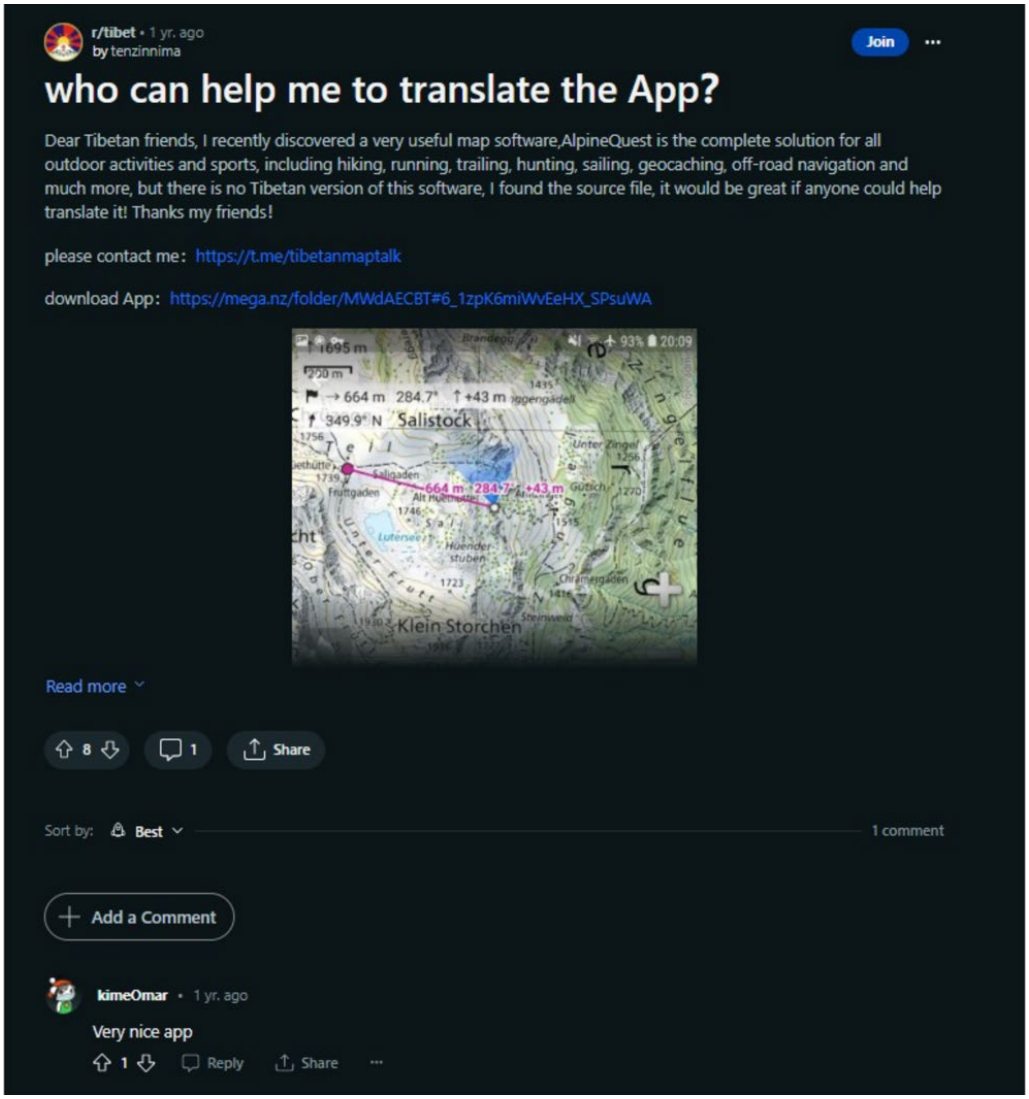


Figura 5: Publicação no Reddit a anunciar uma aplicação maliciosa por uma conta que se acredita ser controlada por um agente malicioso

A Volexity também observa que um utilizador conhecido como '**KimeOmar**', que fez um comentário sobre a publicação, também foi observado a partilhar aplicações maliciosas noutro fórum sub-Reddit. Isto pode indicar que os agentes maliciosos utilizam múltiplos perfis nas redes sociais para fazer com que as suas publicações pareçam legítimas.

Avaliação

O BADBAZAAR e o MOONSHINE utilizam vários métodos de engenharia social para almejar especificamente as comunidades uigur, tibetana e taiwanesa, nomeadamente:

- a trojanização de aplicações de interesse para estas comunidades, como uma aplicação do Alcorão em língua uigur, é quase certamente adaptada à base de vítimas-alvo.
- a adição destas aplicações com trojans às lojas oficiais de aplicações muito provavelmente confere uma sensação de legitimidade, e a partilha em conversas em grupo tem provavelmente como objetivo explorar as relações de confiança dentro dessas comunidades.

O BADBAZAAR e o MOONSHINE recolhem dados que certamente seriam valiosos para o Estado chinês. Embora o BADBAZAAR e o MOONSHINE tenham sido observados a atacar indivíduos uigures, tibetanos e taiwaneses, existem outros malwares que atacam outros grupos minoritários na China. Os cidadãos das nações co-guardiãs, na China e no exterior, que são considerados apoiantes de causas que ameaçam a estabilidade do regime, estão quase certamente sob ameaça de malware móvel, como o BADBAZAAR e o MOONSHINE. A capacidade de capturar dados de localização, áudio e fotos certamente oferece a oportunidade de informar futuras operações de vigilância e assédio, fornecendo informações em tempo real sobre a atividade do alvo.

Medidas de mitigação para utilizadores de aplicações móveis

As agências autoras incentivam as seguintes práticas de segurança para proteção contra as ameaças descritas nos estudos de caso. Estas recomendações são baseadas nas orientações das melhores práticas do NCSC. Ver a secção 'leitura adicional' para links para orientações sobre as melhores práticas para leitores na Austrália e nos EUA.

Mantenha o seu dispositivo seguro

- **Baixe aplicativos apenas de lojas oficiais, como a Play Store do Google ou a App Store do Apple.** a Play Store do Google e App Store do Apple verificam se os softwares têm vírus antes de disponibilizá-los, dando-lhe mais garantia de que o que está a baixar é seguro. As aplicações de lojas confiáveis ainda podem apresentar riscos, mas os downloads de outras fontes podem não ter nenhuma proteção. O NCSC tem um relatório sobre ameaças nas lojas de aplicações: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Mantenha o seu dispositivo e as suas aplicações atualizados.** Instale as atualizações nas suas aplicações e no software do dispositivo assim que estiverem disponíveis. Ative as 'atualizações automáticas' nas definições do seu dispositivo, se disponível, para que não precise de se lembrar de o fazer. Veja as orientações do NCSC sobre como manter a segurança online, para se proteger contra vírus conhecidos e outros tipos de malware. As atualizações geralmente incluem melhorias e novos recursos: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Não faça 'jailbreak' ou 'root' d seu dispositivo** porque isso usa vulnerabilidades não corrigidas para contornar os controlos de segurança implementados. Isto deixa o dispositivo mais vulnerável a ataques. Veja a orientação do NCSC: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Gerencie as suas aplicações

- **Reveja as suas aplicações e as suas autorizações.** Se já não precisa de uma aplicação, elimine-a. Sempre que possível, limite as autorizações das aplicações para minimizar a exposição de dados, porque o malware é frequentemente concebido para aceder a ficheiros ou periféricos protegidos, como câmaras e microfones.
  - Como verificar as autorizações das aplicações para utilizadores do Apple: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Como verificar as autorizações das aplicações para utilizadores de Android: https://support.google.com/android/answer/9431959?hl=en-GB

- **Envie automaticamente aplicações desconhecidas para o Google.** Se você é um utilizador de Android e baixou uma aplicação que não é do Google Play Store, pode enviá-la para o Google ativando a opção 'Melhorar a detecção de aplicações prejudiciais' nas definições da aplicação Google Play Store, em «Play Protect». Isso irá analisar a aplicação para detetar malware, ajudando a proteger os utilizadores. Informações sobre como configurar isto: https://support.google.com/android/answer/2812853?hl=en-GB

Utilize serviços cibernéticos

- **Use serviços de reputação de URL antes de clicar num link.** Pode verificar se um link de um e-mail, mensagem de texto ou outro local é seguro, verificando-o primeiro com serviços como Google Transparency Report or Virus Total. Também pode enviar ficheiros e aplicações suspeitos para um analisador de malware, como o Virus Total, que pode ajudar a detetar se um ficheiro é malicioso. Esteja ciente de que os serviços de verificação podem produzir falsos negativos.

- **Inscreva-se no programa Proteção Avançada do Google.** Este é um serviço gratuito criado para proteger os utilizadores dos serviços do

Google (Gmail, Play Store, etc.) que correm o risco de serem alvo de ataques. Este serviço oferece maior segurança ao utilizar os serviços do Google: https://landing.google.com/advancedprotection/

- **Inscreva-se em serviços adicionais de resiliência, se disponíveis.** Por exemplo, indivíduos de alto risco no Reino Unido podem ter direito a serviços defensivos adicionais para ajudar na sua segurança cibernética. Verifique a elegibilidade e saiba mais: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Denuncie ameaças

- **Identificar e denunciar contas falsas.** Os cibercriminosos criam contas falsas ou invadem contas reais para alcançar os seus objetivos. Se você suspeita que uma conta é falsa ou está comprometida, denuncie-a à plataforma e bloqueie-a. Muitos serviços têm um processo para verificar contas, como os 'selos de verificação' do Instagram e do Facebook. Isso pode ajudar a identificar se uma conta é genuína. O NCSC disponibiliza orientações sobre como utilizar as redes sociais de forma segura, que inclui detalhes sobre como verificar e denunciar contas comprometidas: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Phishing utilizando e-mails, SMS e links fraudulentos.** O NCSC pode investigar endereços de e-mail e sites suspeitos. Se achar que um site, e-mail ou mensagem é suspeito, pode denunciá-lo: https://www.ncsc.gov.uk/collection/phishing-scams

Glossário do NCSC

- **Android**

Sistema operativo móvel do Google, utilizado por vários fabricantes de smartphones e tablets.

- **App**

Uma aplicação, ou app, é um pacote de software que os utilizadores podem instalar ou são pré-instalados num dispositivo para fornecer funcionalidades ou conteúdos adicionais ao seu dispositivo.

- **Segurança cibernética**

A proteção de dispositivos, serviços e redes — e das informações neles contidas — contra acesso não autorizado, roubo ou danos.

- **Dispositivo**

Hardware informático que existe fisicamente, como um computador de secretária, smartphone ou tablet.

- **iOS**

Sistema operativo móvel do Apple utilizado no seu conjunto de dispositivos móveis.

- **Malware**

Derivado de 'software malicioso', malware é qualquer tipo de software que pode danificar sistemas informáticos, redes ou dispositivos. Inclui vírus, ransomware e trojans.

- **Sistema operacional**

O software básico que funciona em computadores, tablets e smartphones, necessário para executar aplicações e hardware adicionais.

- **Phishing**

E-mails ou mensagens de texto fraudulentos que contêm links para sites que podem conter malware ou induzir os utilizadores a revelar informações confidenciais (como palavras-passe) ou a transferir dinheiro.

- **Spyware**

Um tipo de malware que se instala num dispositivo sem o consentimento do utilizador, recolhendo dados e enviando-os para terceiros.

- **Redes Sociais**

Sites e aplicações, como o Facebook, X e Instagram, que permitem às pessoas partilharem e responderem a conteúdos gerados pelos utilizadores (publicações de texto, fotos e vídeos).

- **Smartphone**

Telemóveis modernos que executam funcionalidades complexas, incluindo aqueles com sistemas operativos Android e iOS.

- **Trojan**

Um tipo de malware, disfarçado como software legítimo, que é usado para obter acesso não autorizado ao dispositivo da vítima.

- **URL**

Localizador Uniforme de Recursos. Um endereço na Internet, como um nome de domínio (por exemplo, www.bbc.co.uk).

- **Vírus**

Um tipo de malware concebido para infetar programas de software legítimos e que se replica nas redes quando esses programas são ativados.

Leitura adicional

Orientação do Centro Australiano de Segurança Cibernética

- Denunciar um crime cibernético, incidente ou vulnerabilidade
- Como proteger os seus dispositivos
- Proteja o seu telemóvel
- Phishing
- Scams
- Proteja as suas redes sociais
- Dicas de segurança para redes sociais e aplicações de mensagens

Orientação do NCSC e da NPSA do Reino Unido

- Defender a Democracia
- Redes Sociais: como usá-las com segurança
- Orientação sobre segurança de dispositivos para organizações, incluindo dispositivos móveis
- Relatório de ameaças nas lojas de aplicações.
- Segurança pessoal e proteção para indivíduos de alto risco

Orientação da NSA dos EUA

- Melhores práticas para dispositivos móveis

Isenção de responsabilidade

Observe que este aviso fornece informação que está validada na altura da publicação.

Este relatório baseia-se em informações obtidas junto de agências autorizadas e fontes do setor. Quaisquer conclusões e recomendações apresentadas não foram fornecidas com a intenção de evitar todos os riscos e seguir as recomendações não eliminará todos esses riscos. A responsabilidade pelos riscos relacionados com a informação permanece sempre com o proprietário do sistema relevante.

No Reino Unido, esta informação está isenta ao abrigo da Lei da Liberdade de Informação de 2000 (FOIA) e pode estar isenta ao abrigo de outra legislação britânica em matéria de informação.

Envie quaisquer consultas relacionadas à FOIA para ncscinfoleg@ncsc.gov.uk.

Anexo: Amostras MOONSHINE & BADBAZAAR observadas

Esta tabela lista as aplicações utilizadas nas campanhas do MOONSHINE e do BADBAZAAR nos últimos dois anos.

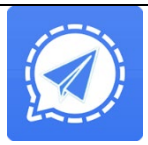
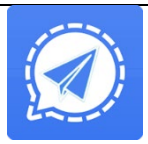
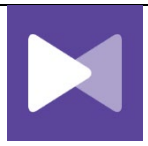
Muitas destas aplicações apresentam uma semelhança evidente com aplicações já estabelecidas. Provavelmente esta é uma técnica deliberada para «falsificar» marcas bem conhecidas.

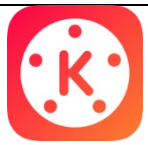
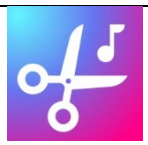
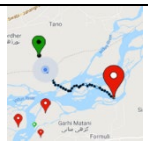
É importante observar que o nome do aplicativo, o nome do pacote e o ícone podem imitar ou corresponder ao aplicativo real e, portanto, não devem ser usados exclusivamente para identificar se um dispositivo está infetado.

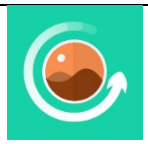
Conforme incluído na secção de mitigação, você pode enviar aplicações no seu dispositivo Android para o Google ativando 'Melhorar a deteção de aplicações prejudiciais', que irá analisar as aplicações no seu dispositivo que foram instaladas fora da Play Store.

Título da aplicação	Nome do pacote	Ícone da aplicação
99 Nomes de 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	
Explorador Off-Road AlpineQuest (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Teclado Árabe	com.arabic.keyboard.arabic.language.keyboard.app	
Cortador de áudio e vídeo	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Canções Budistas (1)	com.bigkidsapps.buddhistsongs1	
Calculadora	com.android2.calculator3	
Bússola 360 Pro	com.pro.app.compass	
Dicionário EN-UG gratuito	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

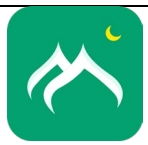
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Passe WiFi gratuito	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Calendário Hijri	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

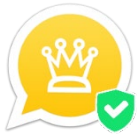
KineMaster	com.nexstreaming.app.kinemasterfree	
Cortador de MP3 e criador de toques	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Calculadora de distâncias em mapas	com.routemap.mapdownload.gpsroute planner	
Recuperação de redes sociais	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
Leitor de PDF	pdf.pdfreader.pdfviewer.pdfeditor	
Leitor de PDF	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	

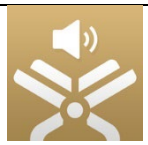
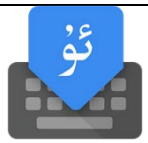
Editor de Fotos	com.iudesk.android.photo.editor	
Recuperação de Fotos	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Livro de Orações	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Alcorão	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restaurar fotos apagadas	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	
Sistema de adivinhação tibetano MO	net.rhombapp.mo	

Oração tibetana	com.chorig.tibetanprayer	
Tradutor AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Teclado uigur	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Conversor de vídeo	com.inverseai.video_converter	
Cortador de vídeo	com.naing.cutter	
Descarregador de vídeos	downloader.video.download.free	
Criador de vídeos	com.bstech.slideshow.videomaker	

Reprodutor de vídeo para Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Gravador de voz	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Previsão do tempo	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	
Downloader do 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