



National Cyber
Security Centre

a part of GCHQ



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre



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

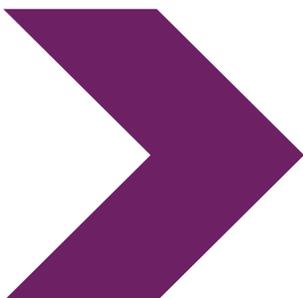


PART OF
THE GCSB



Avizu

**BADBAZAAR no MOONSHINE:
Spyware alvu ba Uigur, ema
Taiwan no grupu Tibetanu no
atór comunidade sosiál sira**



9 Abril 2025

BADBAZAAR no MOONSHINE: Spyware alvu ba Uigur, ema Taiwan no grupu Tibetanu no atór komunidadade sosiál sira

NCSC no parseira sira publika informasaun foun no medidas mitigasaun ba sira ne'ebé iha risku altu husi variante spyware rua.

Rezumu

Ho apoiu husi UK [Cyber League](#), avizu ida ne'e produs hamutuk ho Sentru Seguransa Sibernetika Nasionál (NCSC UK) no parseiru internasionál sira:

- › **Sentru Seguransa Sibernetika Austrália, parte husi Diretóratu Sinal Austrália**
- › **Sentru Kanadá ba Seguransa Sibernetika, parte husi Estabelesementu Seguransa Komunikaun**
- › **Servisu Intelijénsia Federal Alemána**
- › **Konselhu Federal Alemána ba Proteksaun Kona-ba Konstituisaun**
- › **Sentru Nasionál Seguransa Sibernetika Nova Zelandia, parte husi Gabinete Seguransa Komunikaun Governu**
- › **Buréu Federal Investigasaun Estadu Unidos**
- › **Ajénsia Nasionál Seguransa Estadu Unidos**

Nia objetivu ne'e mak atu aumenta konsiente kona-ba kresimentu ameasa katak atór siber malisiozu hatudu ba ema sira mak konekta ba topiku sira inklui Taiwan, Tibete, Rejiaun Autónom Uigur Xinjiang, movimentu demokrátiku Falun Gong.

Avizu ida ne'e inklui estudu kazu rua mak detalle teknika sira uza ho atór siber malisiozu sira ho utiliza spyware ne'ebé konhese nu'udar BADBAZAAR no MOONSHINE atu alvu dadus iha dispositivu movél sira inklui smartphone sira mak bele sai interese ba estadu Xina. Tanba ne'e mos hatudu dalan ba orientasaun atu ajuda individu sira proteje sira-nia an, sira-nia dispositivu no sira-nia dadus.

Hamutuk ho avizu ida ne'e, NCSC publika [detalle tékniku kompletu ho orientasaun separadu](#).

Se mak iha risku?

Ajénsia autoridade ne'ebé no parseiru indústrial sira observa BADBAZAAR no MOONSHINE espesíficamente alvu ba individu sira ne'ebé iha relasaun ho topiku sira mak estadu Xina konsidera ameasa ba sira-nia autoridade doméstiku, ambisaun no reputasaun globál. Sira mak iha risku boot inklui, maibe la limitadu, kualkér ema mak konekta ba:

- › **Independénsia Taiwan**
- › **Direitu Tibetanus**
- › **Musulmanu Uigur no minorias étnika sira seluk iha ka husi Rejiaun Autónoma Uigur Xinjiang**
- › **defesa demokrasia (inklui Hong Kong)**
- › **movimentu espiritual Falun Gong**

Ida ne'e inklui organizasaun naun governu (NGO) sira, jornalista sira, empreza sira no ema sira ne'ebé defende, identifika, ka reprezenta grupu sira ne'e. Dalan indiskrimina spyware ida ne'e ne'e divulga online mós signifika iha risku katak infesaun sira bele divulga passa liu vitima mak intende ona.

Avizu ida ne'e iha objetivu atu ajuda sira ho risku responde efetivamente ba ameasa espesifiku husi spyware BADBAZAAR no MOONSHINE. Mitigasaun mak sujere komplementa aviza seguransa siber luan liutan no la bele konsidera hanesan iha izolasaun.

Ho halo tuir referénsia orientasaun iha avizu ida ne'e, uzadór sira bele redus risku infesaun ba sira-nia dispositivu movél no dados.

Ameasa

MOONSHINE no BADBAZAAR ne'e mak ezemplu husi trojans; sira iha funsaun malisiozu subar iha aplikasaun laran mak funsiona ho di'ak ne'ebé bele deskarga husi loja aplikasaun ka servisu partilla ficheiru online.

Aplikasaun sira ne'e dezenhu atu habosok uzadór ba deskarga no instala sira iha dispozitivu. Kuandu aplikasaun ida instala ona, nia uza vulnerabilidade iha dispozitivu laran atu realiza funsaun naun autorizadu, ka nia depende ba uzadór fó permisaun ba asesu no deskarga informasaun husi dispozitivu, inklui:

- › **dadus lokalizasaun inklui rastreiu tempu real**
- › **asesu ba mikrofon no kamera**
- › **mensajen, foto sira no ficheiru sira seluk mak armajen iha dispozitivu laran**
- › **informasaun dispozitivu no liutan**

Atór ne'e depois explora interese lejitimu husi grupu iha risku, atu identifika no infeta vitima barbarak se posível no hetan asesu ba sira-nia dadus. Dalan ida sira halo ida ne'e ho dezenhu aplikasaun mak sira hatene sei atrai sira-nia vitima, hanesan aplikasaun sira ne'ebé suporta sira-nia lingua orijen, ka konten spesifiku ba lokasaun hanesan rejiaun Tibetanu husi Xina ka Xinjiang.

Estudu kazu iha avizu ida ne'e fornese ezemplu balun ba ida ne'e, inklui aplikasaun TibetOne no Uyghur Quran.

Atór sira ne'e ativu iha forun online sira iha ne'ebé baze uzadór ba sira-nia vitima mak intende ona, ne'ebé maximiza sira-nia oportunidade atu infeta vitima sira. Sira observa ona deliberamente partilla spyware iha kanal Telegrama relasiona ho Tibete no forun Reddit sira. Estudu kazu iha avizu ida ne'e mós fó ezemplu husi metodu sira ne'e.

Aplikasaun melisiozu sira siempre partilla nu'udar ficheiru mesak, hanesan ficheiru APK iha Android, ne'ebé uzadór sira presija deskarga no instala. Atór ne'e tenta atu halo sira-nia spyware parese lejitimu liutan ho deskarga buat ne'e ba loja aplikasaun ofisial hanesan Google Play Store no Apple App Store ka aumenta kódigu malisiozu ba aplikasaun uluk nian mak la perigu, maski loja ofisial sira iha funsaun seguransa no prosesu verifikasaun ne'ebé halo tátika ida ne'e ladun susesu. Ida ne'e halo aplikasaun husi loja ofisial seguru liutan, maibe hanesan demonstra iha estudu kazu no NCSC-nia [Relatóriu Ameasa App Store](#), prosesu sira ne'e la perfektu.

Halo tuir dika 4 sira ne'e bele ajuda Ita husi ameasa sira mak esplika iha avizu ida ne'e.

Ba avizu detalle liutan, haree seksaun mitigasaun.



Four tips to stay safe when using your smartphone

Reduce the risk from malicious apps with good cyber hygiene, then follow these four principles:

Stay Mainstream >

Don't root or jailbreak devices, only use trusted app stores.



Stay Organised >

Review installed apps and permissions regularly.



Stay in Touch >

Report suspicious messages and files to online services.



Stay Alert >

Stay vigilant on social media and check shared files and links.



Estudu kazu

Estudu kazu sira rua ne'e ilustra hanusa MOONSHINE no BADBAZAAR servisu, no hanusa atór siber malisiozu sira alvu ba sira ho risku boot.

Estudu kazu primeiru: MOONSHINE

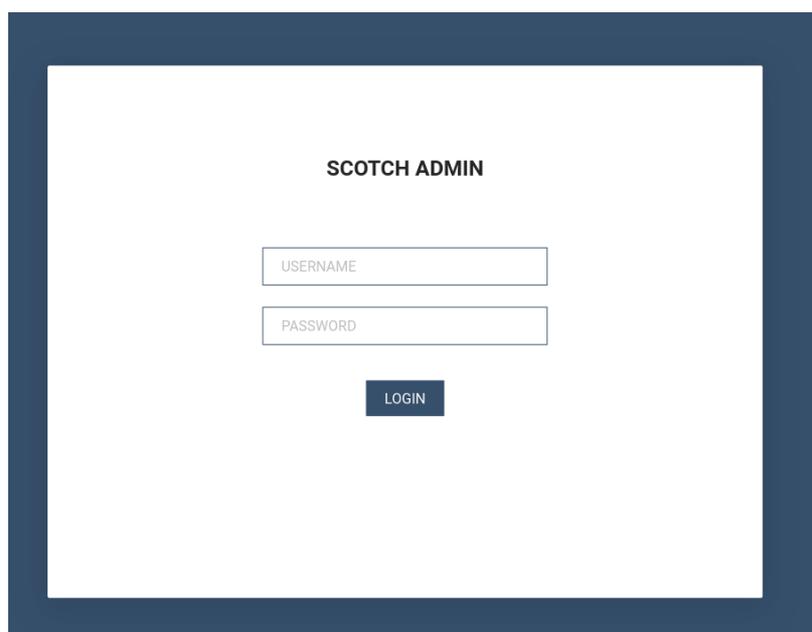
MOONSHINE mak spyware Android ne'ebé relata iha tinan 2019 husi [Citizen Lab](#) no halo alvu ba grupu Tibetanu sira. MOONSHINE imita aplikasaun lejitimu atu hamaus vitima sira ba instala ida ne'e. Ne'e partilla ona liuhusi kanal Telegram sira no link sira manda liuhusi WhatsApp.

MOONSHINE iha kapabilidade vijilánsia estende, hanesan:

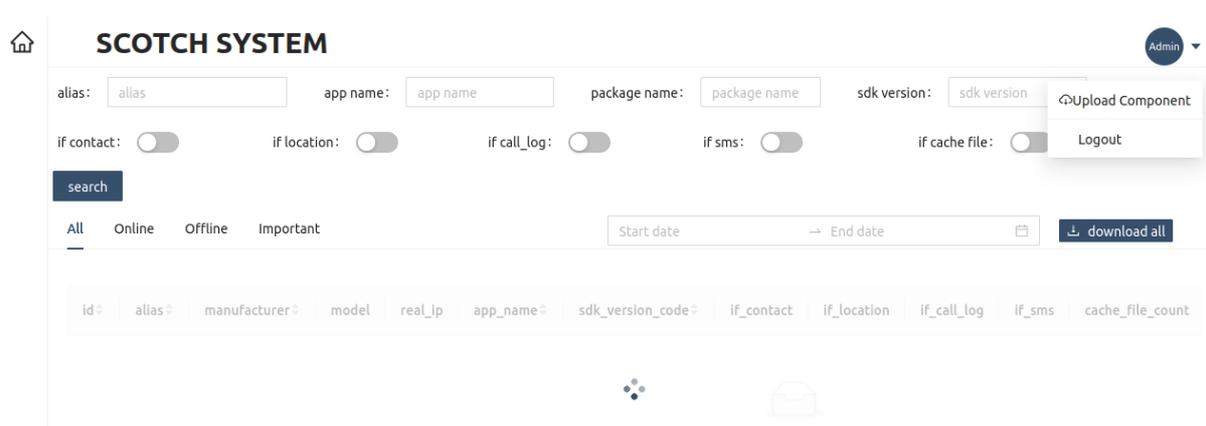
- **dadus lokalizasaun inklui rastreiu tempu real**
- **kaptura áudio no foto vivu**
- **deskarga ficheiru husi dispositivu**
- **rekupera informasaun dispositivu**
- **reprodus áudio iha dispositivu**

Aplikasaun 'ئاۋازلىق قۇرئان.apk', ne'ebé tradus nu'udar '**Audio Quran.apk**', ne'e mak ezemplu husi hanusa MOONSHINE uza atu alvu ema Uigur sira. Uza lingua Uigur iha naran ficheiru, indika aplikasaun Koran posivel dezenha ona atu atrai Musulmamu Uigur sira.

Kuandu instaladu, atór siber malisiozu sira bele kolleta informasaun husi vitima-
nia dispositivu. Informasaun ida ne'e asesu liuhusi painel 'SCOTCH ADMIN'.



Kuandu login, atór bele asesu pájina mak hatudu iha screenshot kraik ne'e. Pájina ida ne'e hatudu detalle husi dispositivu infetadu sira no nivel asesu 'ne'eb ató infeta ona dispositivu sira:



Jerensiamentu painel malware hatudu katak dadus kolletadu, inklui:

- > **nivel asesu ba dispositivu**
- > **mensajen SMS**
- > **lista chamada**
- > **dadus lokasaun**
- > **informasaun dispositivu**

Kolaborasaun ho Cyber League, NCSC konstrui husi industria [relata husi Trend Micro](#) atu ba buka sobrepassa entre feramenta explorasaun MOONSHINE no

painel login ne'ebé konten 'UPSEC' iha titulu HTML. Detalle kompletu iha avizu teknika mak aneksu.

Akordu ba [Intelligence Online](#), UPSEC ne'e mak referénsia ba 'Sichuan Dianke Network Security Technology Co. Ltd'. Ajénsia autoridade ladauk verifika deklarasaun ida ne'e.

Estudu kazu segundu: BADBAZAAR

BADBAZAAR ne mak malware móvel ho varián iOS no Android ne'ebé alvu ona povu Uyghur, Tibetanu no ema Taiwan. Malware ida ne'e distribui liuhosi plataforma média sosiál no loja aplikasaun ofisiál sira.

BADBAZAAR uza ona atu alvu Tibetanu liuhusi app '**TibetOne**', hanesan relata ona ho [Lookout](#) no [Volexity](#). **TibetOne** ne'e app iOS kria ho atór malisiozu sira ho kapabilidade atu asesu informasaun dispozitivu no dados lokasaun. Ida ne'e deskarga ona ba Apple App Store iha Dezembru 2021 maibe agora la iha ona. Atu divulga malware liuta, atór sira mós anuncia app ne'e iha kanal Telegram ho naran '**tibetanphone**'.

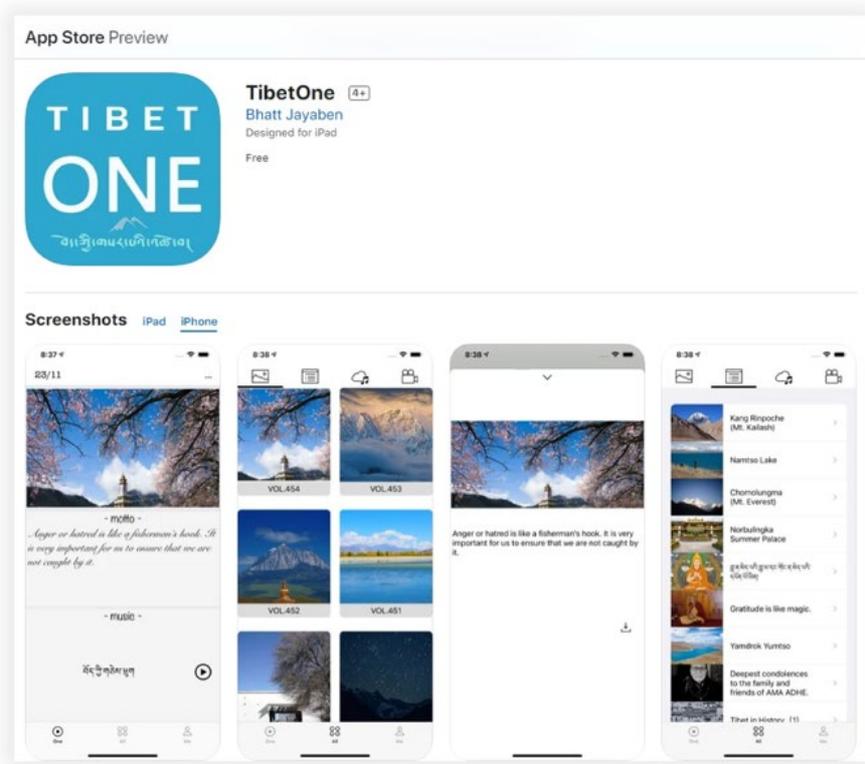


Figura 1: Pájina aplikasaun TibetOne iha Apple App Store. Aplikasaun ne'e elimina ona husi ne'ebá.

8 December 2021

A
04:15

<https://apps.apple.com/app/tibetone/id1597024202>

TibetOne

...

A
04:42

App Store Preview

TibetOne

Screenshots iPad iPhone

Figura 2: TibetOne mak partilla ona iha kanal Telegram sira.

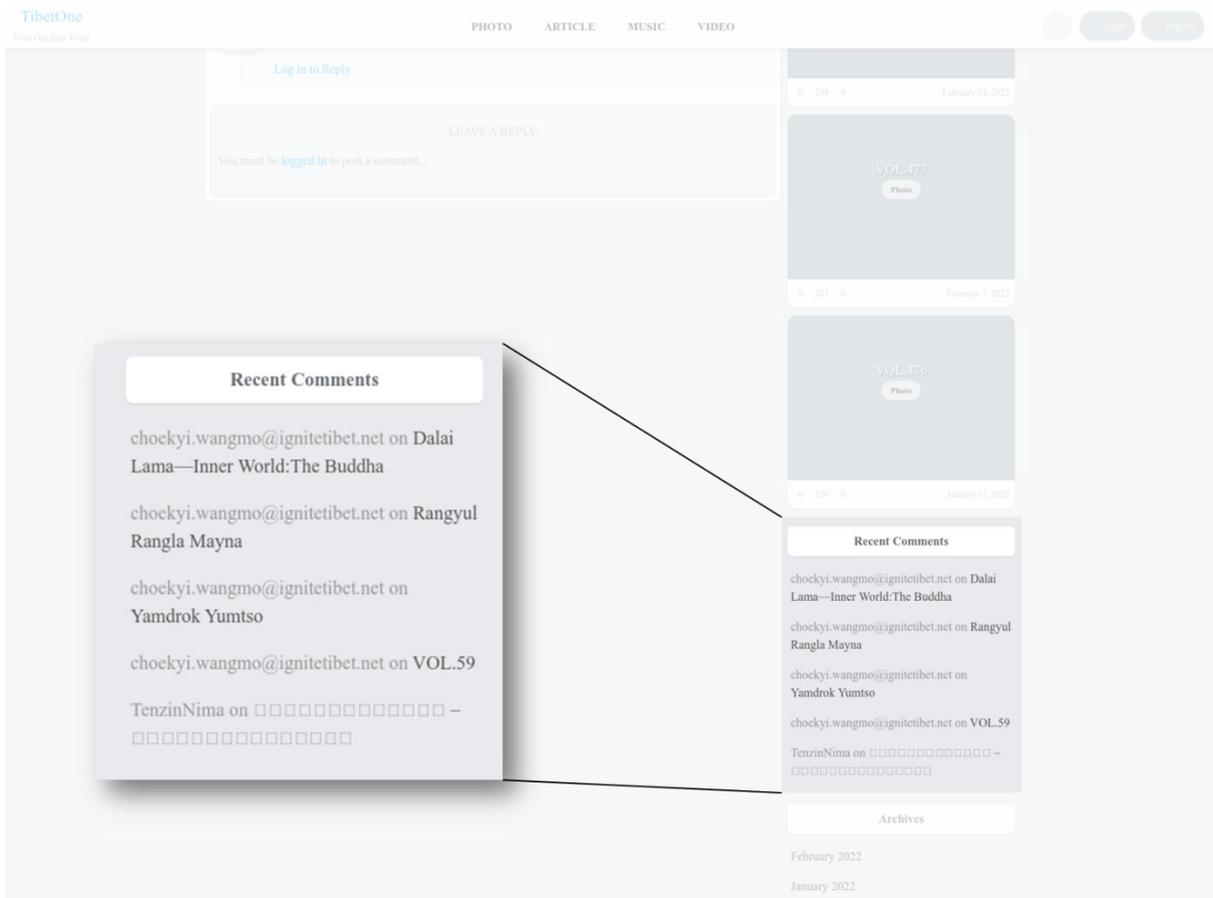


Figure 4: 'tibetone[.]org' nia pájina hatudu komentáriu husi uzadór sira, fiar katak sira kontroladu ho atór maliozосу.

Imajen ida ne'e audita ona atu halo seksaun relevante sai klaru liutan.

'**TenzinNima**' ne'e naran uzadór seluk ne'ebé aumenta komentáriu iha website ida ne'e. [Volexity relata ona katak](#) naran uzadór ida ne'e mós uza iha Reddit ba anunsia kanal Telegram '**Tibetanmaptalk**'. Ne'e inklui link ida atu deskarga amostra malisiozu '**AlpineQuest**', aplikasaun navegadór disponivel iha dispositivu Android. Link deskarga ne'e fornese servisu partilla ficheiru ho parte terseiru hanaran Mega.

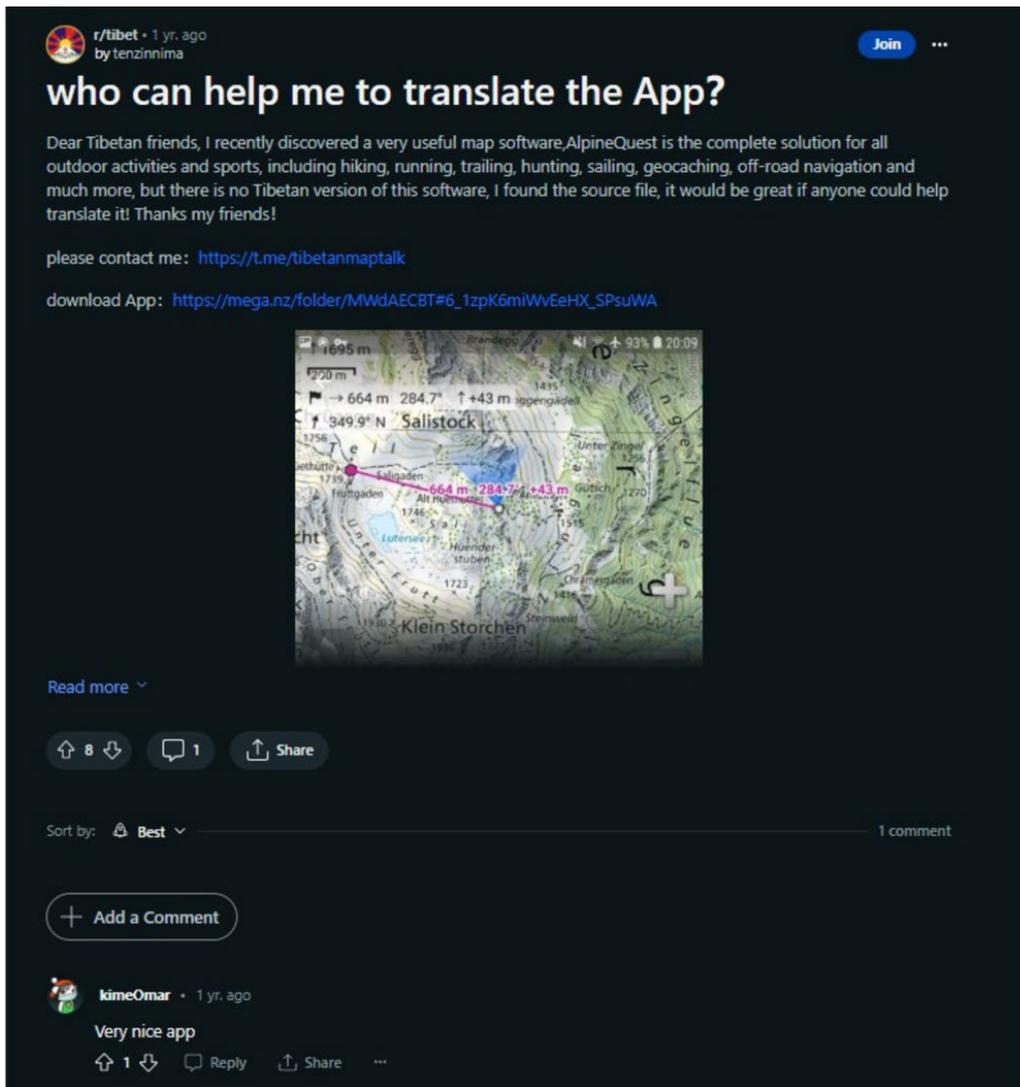


Figura 5: Reddit post anuncia aplikasaun malisiozu ho konta mak fiar katak kontroladu ho atór malisiozu.

Volexity mós nota katak uzadór ida konhese nu'udar '**KimeOmar**' ne'ebé komenta iha post mós hetan observa ona partilla aplikasaun malisiozu iha forun sub Reddit seluk. Ida ne'e bele indika katak atór malisiozu uza pefillu midia sosiál multipla atu halo sira-nia posting parese lejitimu.

Avaliasaun

BADBAZAAR no MOONSHINE uza métodu engenharia sosiál hirak atu fó alvo espésifiku ba comunidade Uighur, Tibetanu no Taiwanés, hanesan:

- trojanizasaun aplikasaun ne'ebé interesa ba comunidade sira ne'e, hanesan aplikasaun Alkoran iha lian Uighur, quase serteza adapta espesiál ba vítima-alvo sira.
- hatama aplikasaun trojan sira ne'e ba loja aplikasaun ofisiál mak quase serteza fó sentidu legitimidade, no partilla iha grupu chat mak quase serteza ho intentu atu explora relasaun konfiável iha comunidade laran sira ne'e.

BADBAZAAR no MOONSHINE koleta dados ne'ebé quase serteza iha valór ba estadu Xina. Mesmu BADBAZAAR no MOONSHINE fó ona atensaun alvo ba ema Uighur, Tibet no Taiwan, iha malware sira seluk ne'ebé fó alvu ba grupu minoritáriu seluk iha Xina. Sidadaun sira husi nasaun sira ne'ebé partisipa iha selamentu, iha Xina no iha rai-liur, ne'ebé konsidera apoia movimentu mak ameasa estabilisadade rejime, kuaze serteza iha ameasa husi malware selulár hanesan BADBAZAAR no MOONSHINE. Kapasidade atu kaptura dados lokál, áudio no foto kuase serteza fó oportunidade atu fornese informasaun ba operasaun vijilánsia no asediu iha futuro, tanba fó dados iha tempu real kona-ba atividade alvu.

Medidas mitigasaun ba uzadór aplikasaun movél sira

Ajénsia autorizadu enkoraja prátika seguransa tuir mai atu proteje kontra ameasa sira mak dekreve ona iha estudu kazu sira. Rekomendasaun sira ne'e sustentadu ho orientasaun prátika melloria husi NSC. Haree ba seksaun 'leitura adisionál' ba link sira kona-ba orientasaun prátika melloria ba letora sira iha Australia no EUA.

Mantein Ita-nia dispositivu seguru

- › **Deskarga deit husi loja aplikasaun ofisial, hanesan Google-nia Play Store ka Apple-nia App Store.** [Google Play Store](#) no Apple [App Store](#) dijitaliza software ba virus sira molok halo ida ne'e disponivel, fó garante liutan ba Ita katak sa'ida mak Ita deskarga ne'e seguru. Aplikasaun sira husi loja konfiável sira bele nafatin lori risku, maibe karga husi rekursu seluk karik la iha protesaun duni. NCSC iha relatóriu ameasa iha app store: <https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf>
- › **Mantein Ita-nia dispositivu no aplikasaun sira atualizadu.** Instala atualizasaun sira ba Ita-nia aplikasaun laran no software dispositivu lalais kedas depois sira disponivel ona. Halakan 'automatic updates' iha Ita-nia konfigurasaun dispositivu karik disponivel entaun Ita lalika ba lembra ba halo ida ne'e. Haree orientasaun NCSC kona-ba mantein seguru ba online, atu proteje virus konhesidu no tipu malware sira seluk. Atualizasaun siempre inklui mellorimentu no fungsionalidade foun sira: <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates>
- › **La bele 'jailbreak' ka 'root' Ita-nia dispositivu** tanba ida ne'e uza vulnerabilidade naun patch atu passa kontrolu seguransa atu realiza ne'e. Ida ne'e halo dispositivu sai vulneravel liutan kona ataque sira. Haree orientasaun NCSC: <https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf>

Jere Ita-nia aplikasaun sira

- **Revizta Ita-nia aplikasaun no sira-nia permisaun.** Karik Ita la presija fali aplikasaun ida, elimina nia. Iha ne'ebé Ita bele, restrita permisaun aplikasaun atu minimiza ekspozu dadus, tanba malware dalaruma dezenha atu asesu ficheiru ho protesaun sira ka perifériku, hanesan kamera no mikrofon sira.
 - Hanusa ba verifika permisaun aplikasaun ba Apple uzadór:
<https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios>
 - Hanusa ba verifika permisaun sira ba uzadór Android sira:
<https://support.google.com/android/answer/9431959?hl=en-GB>
- **Automatikamente manda aplikasaun la konhesidu Google.** Karik Ita ne'e uzadór Android no karga ona aplikasaun ne'ebé laos husi Google Play Store, Ita bele manda app ne'e ba Google ho permite 'Improve harmful app detection' iha konfigurasaun app Google Play Store iha parte 'Play Protect'. Ida ne'e dijitaliza aplikasaun ba detektasaun malware ajuda proteje uzadór. Informasaun kona-ba hanusa configura ida ne'e:
<https://support.google.com/android/answer/2812853?hl=en-GB>

Utiliza servisu siber sira

- **Uza servisu URL ho reputasaun molok kliku ba link ida.** Ita bele verifika karika link ida husi email, mensajen tekstu ka fatin seluk ho dijitaliza ida ne'e uza servisu sira hanesan Relatóriu Transparénsia Google ka [Virus Total](#). Ita mós bele karga ficheiru suspeitu no aplikasaun sira ba analizadór malware, hanesan Virus Total ne'ebé be;e detekta karik ficheiru ida ne'e malisiozu ka lae. Kuidadu katak servisu dijitaliza sira ne'e bele produs negativu falsu.
- **Rejistu ba programa Protesaun Avansadu Google.** Ida ne'e servisu gratuita dezenha atu guarda salva ema sira ne'ebé uza servisu Google sira (Gmail, Play Sotre, nst) ne'ebé sira ne'e iha risku atu sai alvu. Servisu ida ne'e enfaze seguransa kuandu uza servisu Google sira:
<https://landing.google.com/advancedprotection/>

- › **Rejistu ba servisu reziliente adisionál, iha ne'ebé sira disponivel.** Por ezemplu, ema sira ho risku aas iha UK laran bele sai elijivel ba servisu defeza estra atu ajuda ho sira-nia seguransa siber. Verifika elijibilidade no ba buka hatene liutan:
https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Relata ameasa sira

- › **Identifika no relata konta falsu sira.** Atór siber malisiozu kria konta falsu ka hack konta orijinál sira atu atinji sira-nia objetivu. Karik Ita suspeita karik konta ida falsu ka komprente, relata ida ne'e ba plataforma no blokeia nia. Servisu barak mak iha prosesu ba verifika konta sira, hanesan 'verified badges' ba Instagram no Facebook. Ida ne'e bele ajuda atu identifika katak konta ida ne'e orijinál. NCSC iha orientasaun kona-ba uza media sosiál ho seguru inklui detalhe kona-ba oinsa atu verifika no relata konta kompromete sira: <https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- › **Phishing uza emaik, SMS no link fraudulentu sira.** NCSC bele investiga email no enderessu no website sira mak suspeitu. Karik Ita hanoin website ida, email ka mensajen mak suspeitu, Ita bele relata ida ne'e ba: <https://www.ncsc.gov.uk/collection/phishing-scams>

Glossáriu NCSC

> **Android**

Sistema operasaun movél Goggle nian, uza ho smartphone hirak no fabrikante tablet sira.

> **App**

Aplikasaun ida ka app ne'e mak pakote software ne'ebé uzadór sira bele instala ka pré-instala iha dispozitivu ida atu fornese funcionalidade estra ka konten ba sira-nia dispozitivu.

> **Seguransa Sibernetika**

Protesaun ba dispozitivu sira, servisu no rede sira – no informasaun husi sira – husi asesu naun autorizadu, naukten ka hetan estraga.

> **Dispositivu**

Hardware baze komputadór ne'ebé fizikamente eziste, hanesan komputadór desktop ida, smartphone ka tablet.

> **iOS**

Sistema operasaun movél Apple nian mak uza ba ninia dispozitivu movél

> **Malware**

Mai husi "software malisiozu", malware ne'e kualkér tipu software mak bele estraga sistema komputadór sira, rede ka dispozitivu sira. Inklui virus sira, ransomware no trojan sira.

> **Sistema Operasaun**

Software baziku mak hala'o komputadór sira, tablet sira no telefone movél sira, presija hala'o aplikasaun adisionál no hardware.

> **Phishing**

E-mail ka mensajen tekstu fraudulenta ne'ebé liga ba website mak konten ho malware ka habosok uzadór sira ba revela informasaun sensitivu (hanesan senha) ka transfere osan.

> **Spyware**

Tipu malware mak instala ba dispozitivu ida sein konsiente husi uzadór, kolleta dadus no depois manda ba parte terseiru.

> **Midia Sosiál**

Website no aplikasaun sira hanesan Facebook, X no Instagram, ne'ebé permite ema sira partilla no resposta ba konten jeneradu ho uzadór (post tekstu sira, foto no vidio).

> **Smartphone**

Telefone movél modernu ne'ebé opera funcionalidade komplikadu inklui sira ho Android n

> **Trojan**

Tipu malware, imita nu'udar software lejitimu, ne'ebé uza atu hetan asesu naun autorizadu ba dispositivu uzadór nian.

> **URL**

Lokadór Rekursu Uniforma Enderesu ida iha world wide web hanesan naran dominiu (por ezemplu www.bbc.co.uk).

> **Virus**

Tipu malware ne'ebé dezenha atu infetadu programa software lejitimu no replika rede hotu kuandu programa sira ne'e ativadu.

Leitura adisionál

Orientasaun husi Sentru Seguransa Sibernétika Austrália (Australian Cyber Security Centre)

- > [Relata kona-ba krime sibernétika, insidenti ka vulnerabilidade](#)
- > [Oinsá seguru Ita-nia dispozitivu](#)
- > [Seguru Ita-nia telefone movél](#)
- > [Phishing](#)
- > [Golpes](#)
- > [Segura Ita nia midia sosiál](#)
- > [Dika seguransa ba midia sosiál no aplikasaun mensajen sira](#)

Guia husi UK NCSC no NPSA

- > [Defende Demokrasia](#)
- > [Rede Sosiál: oinsá atu uza ho seguransa](#)
- > [Orientasaun Seguransa ba Dispozitivu ba organizasaun inklui móvel](#)
- > [Relatóriu kona-ba ameasa iha loja aplikasaun sira.](#)
- > [Seguransa pesoal no protesaun ba risku aas individual](#)

Guia husi US NSA

- > [Prátika Melloria ba Dispozitivu Movél](#)

Desaprovadór

Favór nota katak avizu ida ne'e fornese informasaun ne'ebé verifikadu iha tempu publikasaun.

Relatóriu ida ne'e bazeia ba informasaun ne'ebé deriva husi fonte ajénsia autór no indústrua. Kualkér deskoberta no rekomendasaun sira ne'ebé fornese laos ho intensaun atu evita risku hotu-hotu no tuir rekomendasaun sira sei la eilimina sira hotu. Propriedade risku informasaun sei hela nafatin ho nain-sistema relevante iha tempu tomak.

Iha UK, informasaun ida ne'e ezenta tuir Freedom of Information Act 2000 (FOIA) no bele mós ezenta tuir legislasaun informasaun UK sira seluk.

Refere kualkér kestaun FOIA ba ncscinfoleg@ncsc.gov.uk.

Aneksu: Amostra MOONSHINE no BADBAZAAR ne'ebé observadu

Tabela ida ne'e lista aplikasaun sira mak uza iha kampaña MOONSHINE no BADBAZAAR iha tinan rua ikus.

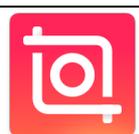
Barak aplikasaun sira ne'e hatudu similaridade klaru ho aplikasaun sira ne'ebé estabelese ona. Nee posível teknika ne'ebé atór halo deit ho intentu atu 'nakfil' marka famozu sira.

Ne'e importante atu nota, naran aplikasaun, naran pakote no ikon bele imita hotu-hotu ka hanesan aplikasaun real nian no tanba ne'e labele uza ezklusivu atu identifika karik dispozitivu ida infetadu ona.

Hanesan inklui ona iha seksaun mitigasaun, Ita bele manda aplikasaun sira iha Ita-nia dispozitivu Android ba Google ho permite 'Improve harmful app detection', ne'ebé sei dijitaliza aplikasaun sira iha Ita-nia dispozitivu laran mak instala ona laos husi Play Store.

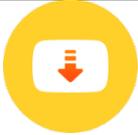
Titulu aplikasaun	Naran pakote	Ikon aplikasaun
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine (بينتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

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 维吾尔输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

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

KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	

Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	

SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.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	
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	قۇرئان
القرآن الكريم	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۆھنەقاپ 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	