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

Avizu

BADBAZAAR no MOONSHINE: Análize tékniku no medidas mitigasaun

9 Abril 2025

BADBAZAAR no MOONSHINE: Análize tékniku no medidas mitigasaun

Rezumu

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

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

Avizu ida ne'e fó dadus foun no kolleta kona-ba ameasa sira husi spyware rua ne'ebé hatene ho naran BADBAZAAR no MOONSHINE, no inklui rekomendasaun ba operadór aplikasaun sira iha loja (app store), dezenvolvedór sira, no kompanhia sira iha mídia sosiál atu ajuda halo uzadór sira seguru.

Avizu ida ne'e sei publika iha tempu hanesan ho Avizu ba vitima sira husi malware sira ne'e.

Dokumentu ida ne'e uza definisaun husi glosáriu NCSC kona-ba spyware: "Tipu malware ida ne'ebé instala iha dispositivu sein konsiente husi uzadór, hodi kolleta dadus no fó ba parte terseru."

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 nu'udar aplikasaun lejítimu atu atrai vitima sira hodi ba instala nia. Spyware ne'e partilla liuhusi kanál Telegram no link sira ne'ebé manda liuhusi WhatsApp.

Peskiza NCSC kona-ba MOONSHINE indika rezultadu sira tuir mai:

- MOONSHINE uza interface jestaun ida ne'ebé hetan alteradu desde relata tempu primeiru nian.
- Interface jestaun ne'e hatudu kapasidade vijilánsia boot, inklui abilidade atu eksfiltrasaun dadus husi dispositivu sira no kaptura audio no grava tela iha tempu real.
- Koleksaun interface jestaun MOONSHINE ne'ebé hetan host virtualmente, mak deskobre tiha ona. Interface sira ne'e iha infrastrutura ne'ebé sobrepasa ho painél login sira ne'ebé konekta ho UPSEC, ne'ebé akordu ho Intelligence Online fó referénsia ba 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Jerensiamentu interface

Relata uluk nian kona-ba interface jestaun MOONSHINE hatudu katak iha ona mudansa, ne'ebé sujere katak dezenvolvimentu ne'e sei kontinua.

Ezemplu primeiru hosi interface jestaun hetan iha relatóriu Citizen Lab iha tinan 2019.

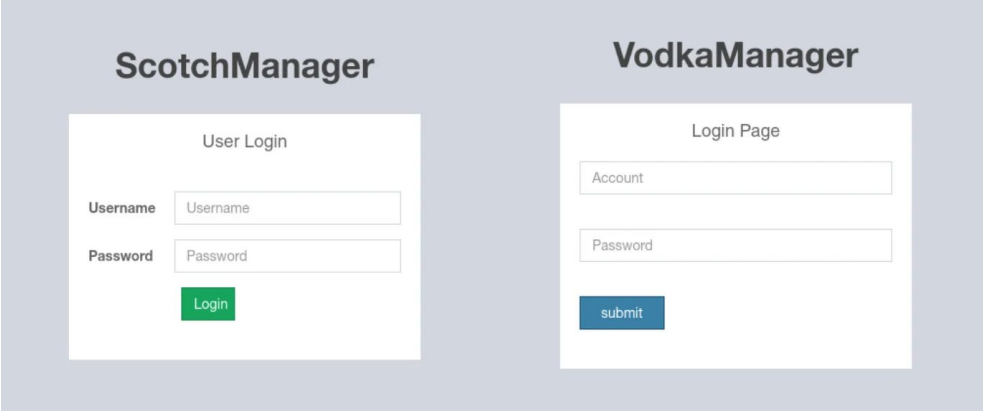


Figura 1: Jestaun interface MOONSHINE ne'ebé observa iha relatóriu Citizen Lab iha 2019, tituladu "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits".

Iha prinsípiu tinan 2022, Lookout relata interface jestaun diferente ida ne'ebé redeseña ona atu sai hanesan iha imajen iha kraik (substitui interface sira uluk iha figura 1):

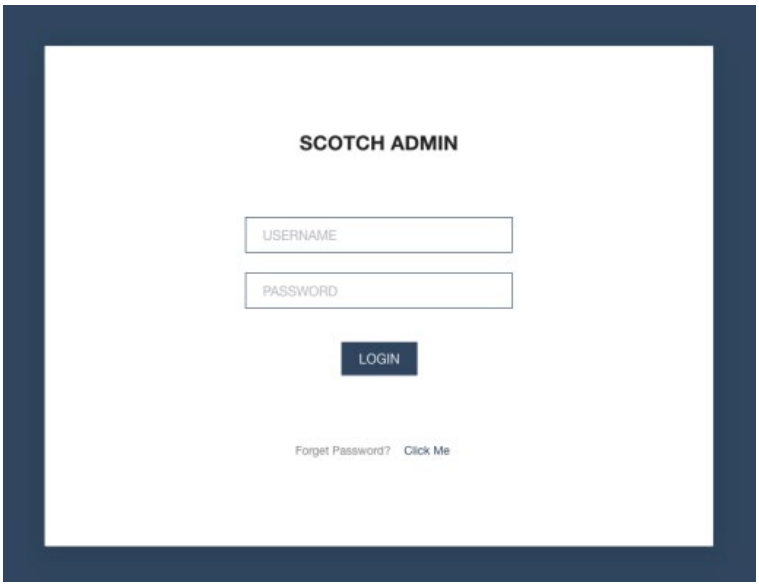


Figura 2: Jestaun interface *MOONSHINE* ne'ebé observa iha Lookout tinan, *2022 relatóriu tituladu 'MOONSHINE: Evolusaun Android Surveillanceware husi Xinés APT POISON CARP hodi alvu ba Tibetanu no Uyghur sira.*

Iha Agostu 2023, varedura ida husi komandu no kontrolu MOONSHINE nian (C2) reveladu interface hanesan ida ho interface 2022 nian ho funsaun '**Forget Password**' la disponivel ona hanesan hatudu iha figura 2:

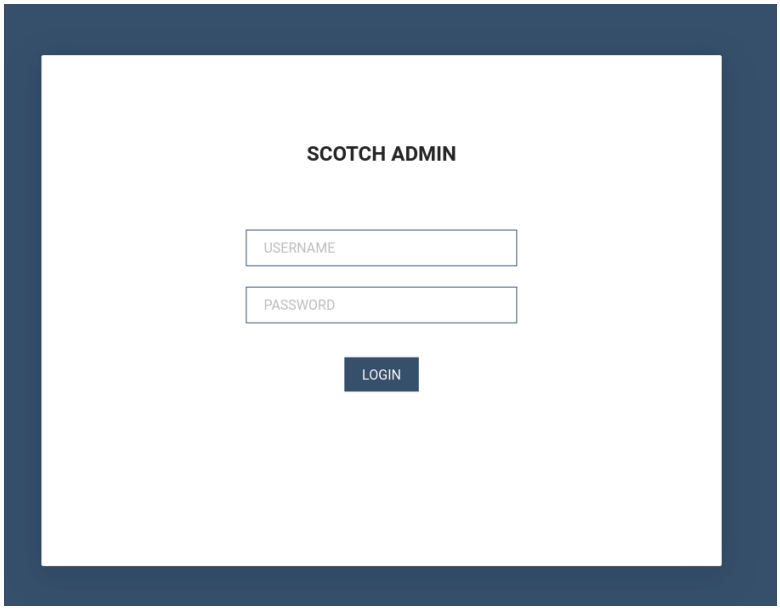


Figura 3: Interface jestaun MOONSHINE ne'ebé observa iha Agostu 2023, ida ne'ebé la iha tan prompt "Forget Password".

Investigasuan liutan ba interface jestaun hatudu kontéudu iha painél laran ne'ebé revela kona-ba oinsa detalle husi dispositivu ne'ebé kompromete sei rekordu.

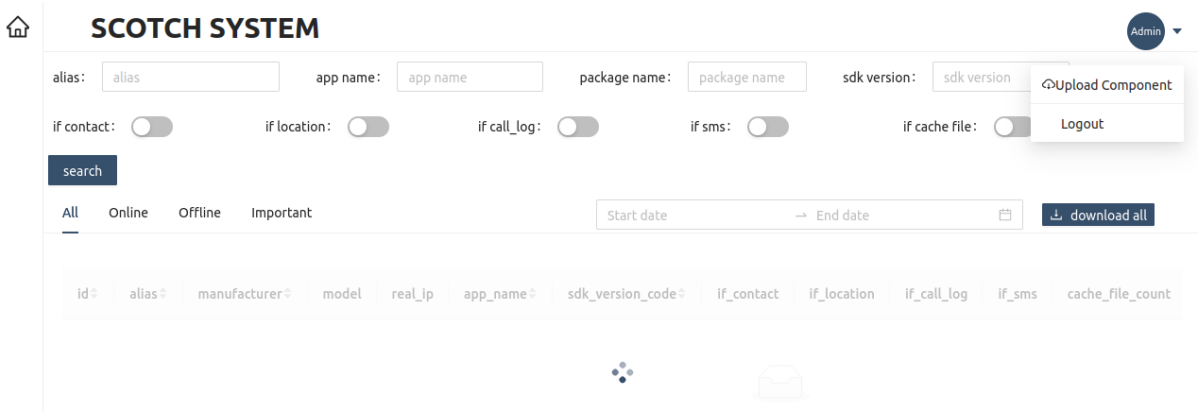


Figura 4: Pájina web iha pájina login nia kotuk husi interface jestaun MOONSHINE.

Peskiza Lookout hatudu katak iha transmisaun "**score**" husi dispositivu vitima ba servidór C2 MOONSHINE nian. Valór husi "score" ne'e bazeia ba permisão sira ne'ebé malware iha dispositivu vitima

Koluna sira hanesan 'if_contact', 'if_location', 'if_call_log' no 'if_sms' iha pájina laran ne'e hatudu katak laos amostra MOONSHINE hotu iha asesu kompletu ba dispositivu sira ne'ebé kompromete. Koñesimentu kona-ba koluna sira ne'e no "score" ne'ebé passa husi dispositivu ba C2 hatudu katak atór ameasadu sira uza "score" atu komunika nivel asesu ne'ebé malware iha ba dispositivu kompromete ba ema sira ne'ebé asesu jestaun interface.

Jeralmente, konsellu pratika di'ak tebes mak atu prevene aplikasaun sira kolekta informasaun husi dispositivu, ne'e mak ba inspesiona permisaun aplikasaun sira no buka buat ne'ebé la komun antes deskarga. Maibé, amostra sira husi MOONSHINE buka permisaun ne'ebé relevante ho funsionamentu aplikasaun nian, tanba ne'e bele parese insuspeitu, maibé sira mós uza permisaun sira ne'e atu kolekta informasaun husi dispositivu.

MOONSHINE mós iha Application Programming Interface (API) ida ne'ebé hatudu estensaun kapasidade ninian. Versaun inisiál sira husi dokumentasaun API konteudu ho naran API sira iha lian Mandarin.

Host virtual sira

Iha peskiza ba painél MOONSHINE sira, deskobre ona instánsia ne'ebé hetan host virtualmente. Hosting virtual mak situasaun ida ne'ebé IP address ida bele host websaít barak iha tempu dala ida deit. IP address sira husi instánsia ne'ebé hetan host virtualmente no domíniu sira ne'ebé hetan host, la observadu iha kualkér amostra malware.

Instánsia sira ne'e husi jestaun interface diferensa, tanba titulu pájina sira ne'e mak '**LOGIN**' duke uluk nian haree ho titulu **SCOTCH ADMIN**'.

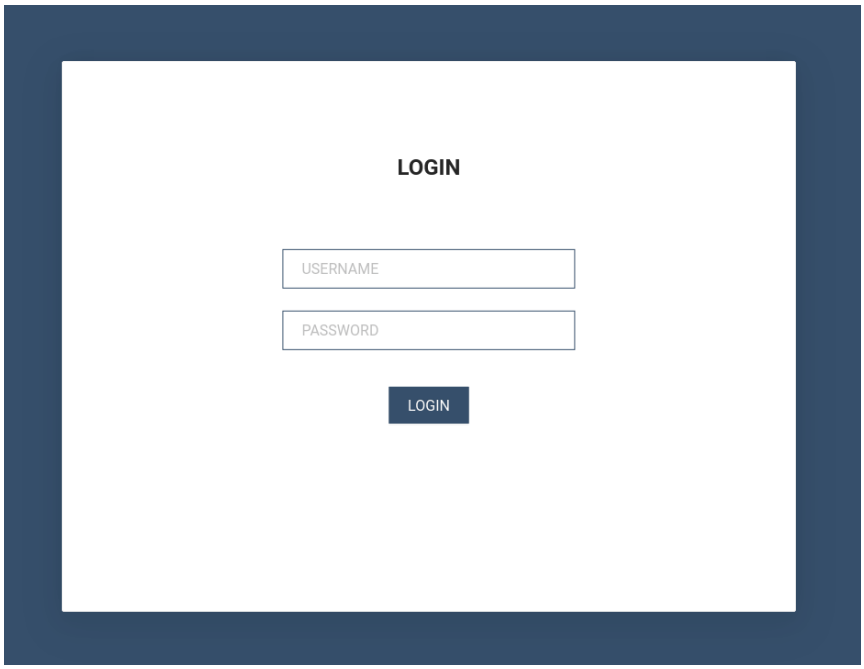


Figura 5: Interface jestaun MOONSHINE uza titulu *LOGIN* laos uza *SCOTCH ADMIN*.

Alénde, kontéudu iha painél laran mós diferente ho figura 4, hanesan observa iha figura 6.

Figura 6: Pájina web iha pájina login nia kotuk husi interface jestaun MOONSHINE ne'ebé hosted virtualmente.

Painél iha figura 6 parese sai versaunn simplifikadu (stripped-down) husi painél iha figura 4. Karakaterístika sira ne'ebé sobrepasa husi painél sira mak naran koluna sira 'id', 'manufacturer' no 'model' iha tabela laran.

Instánsia MOONSHINE ne'ebé hetan host virtualmente no deskobre ona mak hanesan tuir mai:

Domíniu	IP Address
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

Domíniu sira ne'e mak lista husi Trend Micro nu'udar kit esplorasaun MOONSHINE, ne'ebé responsável ba esplora vulnerabilidade iha browser hodi instala malware iha dispositivu móvel. Trend Micro fó naran malware ne'e 'Dark Nimbus'.

Ba klarifikasaun, interface jestaun MOONSHINE ne'e mak plataforma ne'ebé amostra malware MOONSHINE komunika, no iha ne'ebé dadus vitima sira hetan eksfiltrasaun. Kit esplorasaun MOONSHINE relatadu ho Trend Micro, ne'e kapabilidade separadu ne'ebé esplora vulnerabilidade browser sira atu instala malware ida ho naran Dark Nimbus ba dispositivu móvel. Aléinde, Dark Nimbus no MOONSHINE sira ne'e malware ne'ebé diferenta kompletamente.

Tantu, interface jestaun MOONSHINE no kit esplora MOONSHINE iha kode ne'ebé sobrepasa, tanba ne'e prompt login iha figura 3 no 5, no mós kontéudu pájina iha figura 4 no 6. Sira mós iha kontén string 'webpackJsonpreact-scotchui' iha kódigu orijinál (source code).

Atór ameasa sira halo link URL ne'ebé konekta ba feramenta esplorasaun MOONSHINE no depois halo redireksaun ba video sira ne'ebé relevante ba povu Tibetanu no Uyghur, ne'ebé mós sobrepasa ho alvu MOONSHINE.

Iha IP address barak sira ne'ebé hetan host domíniu feramenta esplorasaun MOONSHINE, iha pájina login ho titulu *'VLiteUI'* iha portu 444. Pájina ne'e la observa barak, no nia prezensa iha IP sira ne'e indika posibilidade ligasaun ho operasaun ba atór ameasa sira.

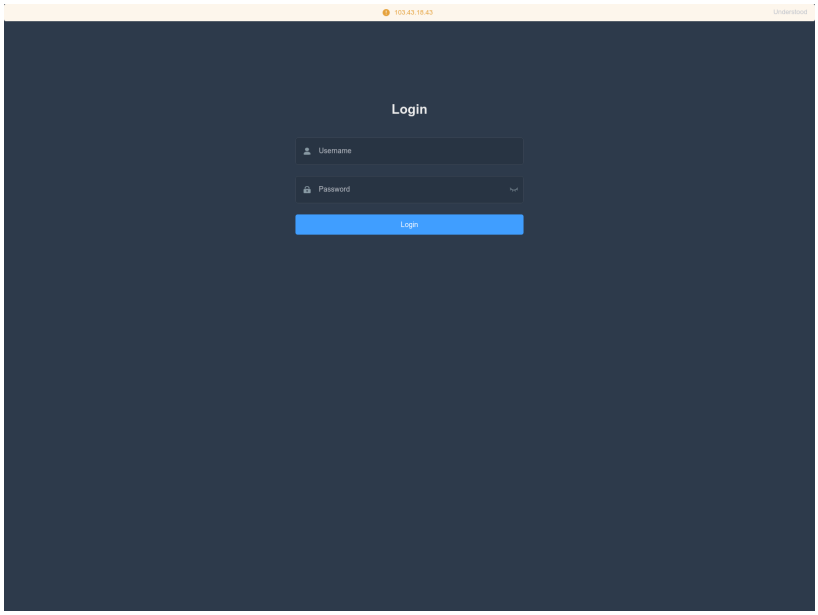


Figura 7: Painél login ho titulun HTML 'VLiteUI' observa iha IP sira ne'ebé mós host feramenta esplorasaun MOONSHINE.

Análize Trend Micro nia kona-ba Dark Nimbus revela katak malware ne'e bele kolleta lista informasaun kompletu husi dispositivu, no nia komunika ho C2 uza protokolu XMPP.

Trend Micro mós esplika katak iha versaun balun husi Dark Nimbus, sira identifika prevalénsia string *'DKNS'*.

'**ansec[.]com**' (lista nu'udar C2 ba Dark Nimbus husi TrendMicro) ne'e mós hetan observa iha servisu XMPP ba IP address seluk sira ne'ebé servi pájina web ho DKNS ho titulu:

- DKNS Android远程取证系统 (Sistema Forénsiku Remotu Android DKNS)
- DKNS云网侦控平台 (Plataforma DKNS Cloud ba Investigasaun no Kontrola Rede)
- DKNS 云网侦控平台 (Plataforma DKNS Cloud ba Investigasaun no Kontrola Rede)
- DKNS远程控制侦查系统 (Sistema Investigasaun Kontrola Remotu DKNS)

Kollesaun IP address sira seluk ho '**ansec[.]com**' iha servisu XMPP iha pájina web ho titulu:

- UPSEC互联网控制指挥系统 (Sistema Komandu Kontrola Internet UPSEC)
- UPSEC无线侦控系统 (Sistema Kontrola no Monitoriza wireless UPSEC)
- UPSEC重点人数据还原系统 (Sistema Restorasaun Dadus Pesoal Prinsipál)

Akordu ba Intelligence Online, 'UPSEC' ne'ebé observa iha titulun pájina HTML refere ba 'Sichuan Dianke Network Security Technology Co., Ltd'.

Estudu kazu segundu: BADBAZAAR

BADBAZAAR ne'e mak malware móvel ho varián iOS no Android ne'ebé alvu ba povu Uyghur, Tibetanu no ema Taiwan. Spyware ida ne'e distribui liuhosi plataforma mídia sosiál no loja aplikasaun ofisiál sira. Relatóriu foun husi Volexity hatudu varián diferente husi BADBAZAAR, ne'ebé separadu nu'udar BadSolar, BADBAZAAR no BadSignal. Varián tolu sira ne'e liga hamutuk ho funsaun sobrepassa ne'ebé uza atu kolleta informasaun husi dispositivu no operadór.

Peskiza NCSC kona-ba BADBAZAAR revela rezultadu sira tuir mai:

- Agrupamentu domíniu C2 revela ligasaun liutan ba domíniu sira ne'ebé relata ona iha intelijénsia ameasa históriku.
- Servidór C2 no amostra malware sira hatudu naran host sira ne'ebé asosiadu ho infraestrutura husi atór ameasa.
- Perfíl sira liutan ne'ebé atór ameasa sira uza ba engeniería sosiál ba distribui malware sira liutan duke loja aplikasaun ofisiál.

Agrupamentu WHOIS / broker domíniu

'UJYJYUJ'

Análize rejistu WHOIS ba domíniu BADBAZAAR '**signalplus[.]org**' (ne'ebé relata husi ESET) hatudu valór '***UJYJYUJ***' iha kampu '**State**'.

Buska ba domíniu sira seluk ho valor hanesan revela domíniu interese tuir mai:

- thetubeplus[.]com
- tubevideoplus[.]org
- pmumail[.]com
- signalplus[.]org

(Haree Aneksu A, imajen 1)

Domíniu **signalplus[.]org**, **tubevideoplus[.]org** no **thetubeplus[.]com** relata ona domíniu C2 BADBAZAAR, kuandu ESET relata sub domíniu **mail.pmumail[.]com** nu'udar servidór proxy FlyGram. FlyGram ne'e mak aplikasaun BADBAZAAR ne'ebé dezenvolve ho atór siber malísiozu (haree ba Apéndise ba lista aplikasaun BADBAZAAR seluk).

Valór keyboard walking

NCSC mós observa padraun keyboard walking iha domíniu C2 BADBAZAAR seluk ne'ebé rejistu ona.

Por ezemplu, domíniu tuir mai sira hotu iha valór **REWR**' ne'ebé observa ona kampu **'State**' (hanesan uza tiha molok ne'e):

- yumoftion[.]com
- fvbyavgyea[.]com
- jkiohreh[.]com
- pmstwocqn[.]com

(Haree Aneksu A, imajen 2)

Domíniu sira ho kampu state valór 'FSDF'

Kollesaun seluk husi domíniu C2 BADBAZAAR iha '**State**' valór '**FSDF**'

- tryhrwserf[.]com
- tibetone[.]org
- comeflxyr[.]com

(Haree Aneksu A, imajen 3)

Relatóriu históriku ho valór keyboard walking

Uza valór keyboard walking sira iha rejistu WHOIS husi domíniu BADBAZAAR mós bele haree iha alvu organizasaun Tibetanu ne'ebé relata istórikamente ho TA413. Recorded Future observa ona domíniu sira ne'ebé kontrola husi atór ameasa, imita organizasaun Tibetanu, no uza valór organizasaun rejistante "**asfasf**".

clublogs[.]com

Amostra BADBAZAAR ne'ebé obtein husi Lookout konten '**xle.clublogs[.]com**' nu'udar domíniu C2. Domíniu root '**clublogs[.]com**' host ona iha IP address '**95.179.210[.]85**' no iha sertifikadu SSL ho valór sujeitu no publikadór husi '**CN=WIN-50QO3EIRQVP**'. Valór sira ne'e kombinadu ho sertifikadu SSL sira ne'ebé hetan iha amostra BADBAZAAR mak uza SSL pinning atu evita interseptasaun komunikasaun

Istória hosting ba IP address **95.179.210[.]85** fó fila fali domíniu interese tuir mai:

- actuallys[.]com
- bre.myloughborough[.]com
- rewrwer[.]com
- www.voiceoftibet[.]net
- clublogs[.]com

(Haree Aneksu A, imajen 4)

www.voiceoftibet[.]net

Domíniu '**www.voiceoftibet[.]net**' parese imita nu'udar estasaun rádio 'Voice of Tibet', hanesan ho TTP mak uza ho TA413.

Domíniu '**rewrwer[.]com**' ne'e hanesan ho uluk nian mak identifikadu '**State**' valóe '**REWR**' hetan iha rejistu WHOIS husi domíniu BADBAZAAR.

Domíniu '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' no '**myloughborough[.]com**' sira hotu rejistu ho email address '**tplutalova@list[.]ru**'.

actuallys[.]com

Rejistu WHOIS ba '**actuallys[.]com**' hatudu instánsia ida ne'ebé email tekniku no administrativu mak '**tplutalova@list[.]ru**' maibe email rejistante ne'e mak '**ivan_s81@mail[.]ru**'.

Informasaun istorikal WHOIS ba domíniu '**actuallys[.]com**' revela email rejistrasaun '**wangminghua6@gmail[.]com**' listadu iha 24 Feveiru 2016. Iha 11 Marsu 2016, email ne'e kontinua troka ba '**ivan_s81@mail.ru**' maski data validade rejistu husi registradór ne'e nafatin la altera.

wangminghua6@gmail[.]com

Email address '**wangminghua6@gmail[.]com**' uza ona atu domíniu hetan iha relatóriu históriku intelijénsia ameasa. Iha 2015, Palo Alto identifika email ne'ebé uza atu rejista domíniu C2 ba malware Cmstar. In 2014, ne'e mós uza atu rejistu domíniu sira ne'ebé identifika ho Mandiant iha kampanha phishing diriji ho APT3. Iha 2013, ne'e mós uza atu rejistu domíniu sira ne'ebé identifika ho CrowdStrike iha

malware dropper ho Program Database (PDB) path ne'ebé konten ho karakter Xinés. Nee hatudu katak kompilasaun halo iha sistema Xinés.

taoyujun@gmail[.]com

Domíniu '**hcjbtt[.]com**' rejistu ho email address '**taoyujun@gmail[.]com**' maibé email administradór rejistu ho '**wangminghua6@gmail[.]com**'.

La iha atividade malísiozu liga ba domíniu '**hcjbtt[.]com**', maibe email address '**taoyujun@gmail[.]com**' hetan ona iha relatóriu históriku intelijénsia ameasa. Iha 2014, ida ne'e uza atu rejistu domíniu mak hetan ho Mandiant iha amostra '**Cueisfry Trojan**' sira atu alvu ba organizasaun Japaun sira.

Email address ne'e mós rejistu domíniu sira hanesan '**iaea-international[.]org**' ne'ebé imita nu'udar **International Atomic Energy Agency** no '**idc-ctbto[.]org**' imita nu'udar **International Data Centre** iha **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

Rejisty Whois uluk nian ba domíniu '**iaea-international[.]org**' hatudu email rejistante ne'e mak '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Domíniu '**udtglobals[.]com**' observa ona uza '**wangminghua6@gmail[.]com**' nu'udar email administradór no '**ocean.nio@rediffmail[.]com**' nu'udar email address rejistante. Rejistu WHOIS sira seluk ba domíniu ida ne'e, hatudu email rejistante hanesan maibe administradór ho email address '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' parese sai imitadór nu'udar '**UDT Global**' ne'ebé ne'e mak ezibisaun internasionál ba kompania sira iha área defeza no seguransa submarina. Naran uzadór '**ocean.nio**' iha email address laran bele sai imita **National Institute of Oceanography (NIO)** ne'ebé eziste iha nasaun barak. Maski uza servisu email '**Rediff**' (ne'ebé bazeia iha India) bele hatudu imitasaun ba **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

Domíniu '**djibdiplomatie[.]com**' parese sai imitasaun ba servisu diplomátiku Djibouti sira, ne'ebé iha rejistu WHOIS hanesan ho '**utdglobals[.]com'.** Iha rejistu hatudu rejistante '**ocean.nio@rediffmail[.]com**' ni administradór '**taoyujun@gmail[.]com**' iha ne'ebé resjitu seluk hatudu

‘**wangminghua6@gmail[.]com**’ nu’udar email address administradór ‘**ocean.nio@rediffmail[.]com**’ nu’udar email rejistante.

Domain sira rua ne’e mós iha valór tipu keyboard walking iha rejistu WHOIS laran. Por ezemplu, ‘**udtglobals[.]com**’ iha valór ‘**ASDF**’ nu’udar ninia sidade rejistante no ‘**djibdiplomatie[.]com**’ iha ‘**DAF DAGF**’ nu’udar ninia valór naran rejistante. Ne’e komparável ho valór sira ne’ebé observa iha domíniu BADBAZAAR sira seluk.

Maski email addresses ‘**wangminghua6@gmail[.]com**’ no ‘**taoyujun@gmail[.]com**’ ne’e mak hetan iha rejistu WHOIS ba domíniu sira mak halo imitasaun nu’udar **eventu globál défesa iha submarina**, **servisu diplomátiku Djibouti** no **Ajénsia Internasionál Energia Atómika**, sira mós rejistu iha WHOIS laran ba domíniu barak seluk naun malísiozu sira.

Mistura entre domíniu ne’ebé halo imitasaun no domíniu naun malísiozu bele hatudu ezistente entidade akuizisaun infraestrutura ida mak uza atu suporta operasaun atór siber malísiozu sira.

Email address ‘**ocean.nio@rediffmail[.]com**’ hetan deit iha domíniu imitasaun hanesan deksreve ona iha leten. ‘**ivan_s81@mail[.]ru**’ no ‘**tplutalova@list[.]ru**’ ida-idak rejistu ona domíniu hirak no balun husi domíniu sira ne’e host ona infraestrutura BADBAZAAR. Email address tolu sira ne’e konfia liga besik ba operasaun atór siber malísiozu sira. Ida ne’e tanba totál domíniu asosiadu ho email mak liga ho atividade malísiozu, kompara ba email sira ‘**wangminghua6@gmail[.]com**’ no ‘**taoyujun@gmail[.]com**’.

(Haree Aneksu A, imajen 5)

Liga ba atór ameasa sira seluk

Karakterístika komun seluk husi domíniu sira ne’ebé relasiona ho BADBAZAAR ‘**actuallys[.]com**’, ‘**clublogs[.]com**’, ‘**myloughborough[.]com**’, ‘**rewrwer[.]com**’, no ‘**voiceoftibet[.]net**’ ne’e mak katak sira hotu rejistu eNom no ‘aloka’ iha ‘**255.255.255[.]254**’.

Tuir investigasaun NCSC uluk nian, domíniu sira seluk ho karaterístika sira ne’e revela atividade mak liga ba **APT5** iha 2019, no **APT14** entre 2009 no 2011.

Domíniu sira ne’ebé relasiona ho APT5-iha rejistu WHOIS istóriku ne’ebé lista ‘**taoyujun@gmail[.]com**’ nu’udar email address rejistante.

Domíniu sira ne'ebé relasiona ho APT14- iha subdomíniu letra tolu ne'ebé parese aprezenta alvu mak intende husi sira-nia operasaun malisiozu. Ezemplu husi ida ne'e mak '**bae.cisconline[.]net**', ne'ebé sujere reuniaun intende husi Sistema BAE hetan ona iha amostra '**Poison Ivy**'.

Karaterístika hanesan ne'e mos observa iha domíniu BADBAZAAR ne'ebé subdomíniu sira relasiona ba naran aplikasaun ne'ebé trojaniza.

Titulu Aplikasaun:	URL C2
Muslim Pro	**mpp**.pmstwocqn[.]com
Video Player for Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Radio Afghanistan	**afg**.collinformations[.]com
EN-UG Dictionary Free	**eud**.titeperformance[.]com
Disk Video Recovery	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

Importante atu nota katak atividade sira ne'ebé konekta ho APT5 no APT14 ne'e mak istóriku, no iha mós domíniu sira seluk ne'ebé rejistu ho eNom no rezolve ba '**255.255.255.254**' ne'ebé la bele liga direta ba atividade malísiozu Portantu, la serteza katak atór sira ne'ebé organiza kampaña sira ne'e mak hanesan ka relasionadu.

Naran Makina

Análize ba BADBAZAAR C2s no amostra sira revela hostname sira mak uza nu'udar valór 'Common Name' iha sertifikadu SSL. Investigasaun NCSC kona-ba hostname sira ne'ebé observadu iha amostra BADBAZAAR no infraestrutura hatudu katak hostname sira nee uza iha IP address barak. IP address sira ne'e mak domíniu hosting sira ne'ebé hetan iha amostra BADBAZAAR laran. Iha detalle liutan iha seksaun laran iha kraik ne'e kona-ba hostname sira no IP address sira ho hosting hostname domíniu C2 BADBAZAAR

Iha kazu kuaze tomak, prezensa sertifikadu sira ho valór hostname ne'e sobrepassa ho resolusaun IP ba naran domíniu malísiozu spesífikadu, no kazu balun iha ne'ebé ida ne'e la akontese esplika ona.

WIN-EU0VLBL7TUJ

Hostname '**WIN-EU0VLBL7TUJ**' observadu ona iha IP addresses tuir mai ne'e ho interese:

- '**116.203.53[.]21**' host domíniu C2 BADBAZAAR sira '**uyapkfinder[.]com**' no '**thewestuniverse[.]com**'.

- '**95.216.169[.]27**' host domíniu C2 BADBAZAAR '**adysfunction[.]com**' no subdomíniu '**download.apkbazar[.]biz**' observadu nu'udar link deskarga ida ba amostra BADBAZAAR.

(Haree Aneksu A, imajen 6)

WIN-70E59JVOB9G

Hostname '**WIN-70E59JVOB9G**' observadu ona iha IP addresses tuir mai ne'e ho interese:

- '**23.88.28[.]220**' host subdomíniu C2 BADBAZAAR, '**aua.rondwsign[.]com**', '**nal.tokenmajorp[.]com**', '**pep.rondwsign[.]com**' '**doa.rondwsign[.]com**', no '**pls.rondwsign[.]com**'**.** Iha tempu loron rua entre tempu sertifikadu ho naran makina haree ba tempu ikus nian no bainhira tempu primeira vez domíniu malísiozu haree ba resolve ba IP.

- '**23.88.28[.]221**' host subdomíniu ligadu BADBAZAAR '**bt.bhvghg[.]com**'.

- '**23.88.28[.]222**' host domíniu C2 BADBAZAAR '**tubevideoplus[.]org**' no '**cde.mpoxcases[.]com**'.

- '**65.21.92[.]67**' host subdomíniu C2 BADBAZAAR '**bat.androidupdated[.]net**'. Ida ne'e mós host subdomíniu '**apps.androidupdated[.]net**' ne'ebé ida ne'e mak malware C2 DoubleAgent.

- '**65.21.92[.]77**' host subdomíniu C2 BADBAZAAR '**wyo.titeperformance[.]com**', '**big.collinformations[.]com**'

‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ no ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ host subdomíniu C2 BADBAZAAR ‘**upd.whoscaller.net**’. no ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ host subdomíniu C2 BADBAZAAR ‘**bvn.lookincategory[.]com**’ no ‘**edr.lookincategory[.]com**’**.** Iha tempu loron sanulu resin ida entre tempu sertifikadu ho naran makina haree ba tempu ikus nian no bainhira tempu primeira vez domíniu malísiozu haree ba resolve ba IP.

- ‘**142.132.131[.]20**’ host subdomíniu ‘**son.onlinegamersgroup[.]com**’ no ‘**system.onlinegamersgroup[.]com**’, fiar sai C2s BADBAZAAR nu’udar sira-nia host embora BADBAZAAR asosiadu ho sertifikadu SSL sira observadu ona iha IP.

- ‘**142.132.131[.]28**’ host domíniu C2 BADBAZAAR ‘**goldplusapp[.]net**’ no subdomíniu ‘**who.goldplusapp[.]net**’ no ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ host subdomíniu C2 BADBAZAAR ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net**’, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, no ‘**aar.alpinemap[.]net**’.

- ‘**162.55.103[.]212**’ host subdomíniu C2 BADBAZAAR ‘**pep.rondwsign[.]com**’, ‘**ckp.jkiohreh[.]com**’, ‘**aar.tokenmajorp[.]com**’, ‘**nal.tokenmajorp[.]com**’, ‘**pls.rondwsign[.]com**’ no ‘**aua.rondwsign[.]com**’**.**

- ‘**195.154.47[.]99**’ host subdomíniu C2 BADBAZAAR ‘**ggl.whoscaller[.]net**’ no ‘**upd.whoscaller.net**’. Iha tempu loron tolu entre tempu sertifikadu ho naran makina haree ba tempu ikus nian no bainhira tempu primeira vez domíniu malísiozu haree ba resolve ba IP.

- ‘**195.154.60[.]3**’ host subdomíniu C2 BADBAZAAR ‘**upd.whoscaller[.]net**’ ‘**ggl.whoscaller[.]net**’.

- '**212.83.189[.]89**' host subdomíniu C2 BADBAZAAR '**wyo.titeperformance[.]com**', '**eud.titeperformance[.]com**', '**vpf.titeperformance[.]com**' no '**afg.collinformations[.]com**'.

- '**212.129.21[.]168**' host domíniu C2 BADBAZAAR, '**fre.lookincategory[.]com**', '**tgr.lookincategory[.]com**', '**fgt.lookincategory[.]com**' '**luj.lookincategory[.]com**' no '**bvn.lookincategory[.]com**'.

(Haree Aneksu A, imajen 7)

WIN-50QO3EIRQVP

Hostname '**WIN-50QO3EIRQVP**' observa iha IP address sira tuir mai ne'ebé interese:

- '**45.76.132[.]91**' host domíniu sira, '**yumoftion[.]com**', '**androidupdated[.]net**'. Domíniu rua sira ne'e liga ba BADBAZAAR nu'udar subdomíniu '**fow.yumoftion[.]com**' no '**bat.androidupdated[.]net**' ne'e mak domíniu C2 BADBAZAAR. Adisionalmente subdomíniu '**apps.androidupdated[.]net**' ne'e mak domíniu C2 DoubleAgent. Ne'e mós host domíniu '**pmstwocqn[.]com**', liga ba BADBAZAAR liuhusi rekordu WHOIS sira.

- '**95.179.210[.]85**' host '**clublogs[.]com**', ne'ebé '**xle.clublogs[.]com**' ne'e mak domíniu C2 BADBAZAAR no mós host ligadu domíniu BADBAZAAR '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**www.voiceoftibet[.]net**' no '**actuallys[.]com**'.

- '**199.247.21[.]34**' host '**titeperformance[.]com**', no '**collinformations[.]com**' ne'ebé subdomíniu sira mak domíniu C2 BADBAZAAR.

- '**217.69.10[.]128**' host domíniu C2 BADBAZAAR '**uyghurdict[.]com**'.

(Haree Aneksu A, imajen 8)

WMSvc-WIN-50QO3EIRQVP

Hostname '**WMSvc-WIN-50QO3EIRQVP**' observa iha IP address sira tuir mai ne'ebé interese:

- '**78.46.185[.]251**' host domíniu C2 BADBAZAAR '**groupgram[.]org**', relata ho Volexity atu uza portu 4432 ba koneksaun malisiozu sira.
- '**65.21.92[.]69**' and '**163.172.205[.]207**' host domíniu '**widelygram[.]org**' ne'ebé fiar sai domíniu C2 BADBAZAAR, embora host hela iha sira rua IP, port 4432 mak loke hela.
- '**163.172.198[.]206**' host domíniu '**maxgram[.]org**' ne'ebé fiar sai domíniu C2 BADBAZAAR, embora host hela ho port 4432 mak loke hela.

(Haree Aneksu A, imajen 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Hostname '**WMSvc-WIN-50QO3EIRQVP**' sira no '**WIN-7LSBB9R0F1L**' observa ona iha IP address tuir mai iha tempu stimultán:

- '**148.251.87[.]245**' host domíniu C2 BADBAZAAR **flygram[.]org**' no '**groupgram[.]org**'.

(Haree Aneksu A, imajen 10)

WIN-N8H8S9BG2P0

Hostname '**WIN-N8H8S9BG2P0**' sira observa ona iha IP address tuir mai:

- '**148.251.87[.]247**' host domíniu C2 BADBAZAAR '**omarwhatsapp[.]org**' no '**flygram[.]org**'.

(Haree Aneksu A, imajen 11)

WIN-I6VBN8MR92A

Hostname '**WIN-I6VBN8MR92A**' sira observa ona iha IP address tuir mai:

- '**148.251.87[.]197**' host domíniu C2 BADBAZAAR '**tryhrwserf[.]com**'.

(Haree Aneksu A, imajen 12)

Bazeia ba dadus komersial disponível, prevalénsia naran mákina sira ne'e iha internét variadu. Balun husi sira ne'e observa iha tempu hanesan iha IP address múltiplu sira, ne'ebé indika katak VM sira ne'e kria husi templatu ida deit. Importante atu nota katak ba hostname sbalun, laos IP sira hotu ne'ebé observa ona bele liga va atividade malisiózu. Ida ne'e bele signifika katak uza hostname sira la ekskluzivu ba atór ameasa sira ne'e deit.

No entantu, prevalénsia naran mákina balun iha IP sira ne'ebé host domíniu C2 BADBAZAAR bele sujere katak entidade ida ne'ebé akuizisaun infraestrutura mak uza atu konfigura mákina sira atu suporta operasaun siber atór malisiózu sira.

Presensa mídia sosiál

Relatóriu anteriór husi Volexity hatudu katak vidio YouTube sira (ne'ebé promove uza aplikasaun malisiózu) kria husi atór siber malisiózu. Vídio sira ne'e inklui tutoriál kona-ba oinsa atu uza aplikasaun sira ne'ebé dezenvolvidu.

NCSC deskobre ona kanal YouTube rua adisionál ne'ebé asosiadu ho operasaun atór ameasa sira. Kanal Youtube ho URL handle '**@josephjoey3499**' parese promove utiliza ba '**Maxgram**' no adisionál kanal ida mak rejistu ho '**@uyghurapks3096**' promove '**Uyghur APK Finder**'.

Adisionálmente, vídio YouTube ne'ebé promove '**Flygram**' no '**Signal Plus**', hatudu atór ameasa sira uza númeru telemóvel ne'ebé visivél. Iha '**Flygram**' vidio, iha minutu 0:36 númeru telemóvel '**+1 (570) 378-7250**' ne'e visivél no durante '**Signal Plus**' vidio, númeru telemóvel '**+1 (267) 298 4259**' ne'e reveladu.

Volexity relata site notísia falsa ho téma '**ignitetibet[.]net**', ne'ebé sira deskobre iha kanal Telegram mak bele konsidera iha operasaun husi atór ameasa sira. Email address '**choekyi.wangmo@ignitetibet[.]net**' ne'e observadu fó komenta ba post sira iha pájina '**tibetone.org**' ne'ebé públikamente relata ho Lookout hanesan pájina C2 uza ba variante iOS BADBAZAAR.

Email address ida ne'e bele konsidera kontrola ho atór, uza pesoal '**Choekyi Wangmo**'

Avaliasaun

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

- trojanizasaun aplikasaun ne'ebé interesa ba komunidade 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 esplora relasaun konfiável iha komunidade laran sira ne'e.

BADBAZAAR no MOONSHINE koleta dadus 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 dadus lokál, áudio no foto kuase serteza fó oportunidade atu fornese informasaun ba operasaun vijilánsia no asediu iha futuru, tanba fó dadus iha tempu real kona-ba atividade alvu.

MITRE ATT&CK®

Relatóriu ida ne'e kompilla ho referénsia ba estrutura MITRE ATT&CK®, baze koñesimentu ne'ebé bele asesu globalmente kona-ba táktika no ténika inimigu, bazeia ba observasaun iha mundu real.

Tátika	ID	Téknika	Prosedimentu
Rekonhesimentu	T1593.001	Buka Peskiza Website/Domíniu: Midia Sosiál	Atór sira enkontra grupu no fórum online ne'ebé kompatível ho vítima-alvo sira atu distribui malware.
Dezenvolvimentu Rekursu	T1583.001	Adkuiri infraestrutura: Domíniu sira	Atór sira rejistu domíniu ba servidór komandu no kontrolu sira.
Dezenvolvimentu Rekursu	T1587.001	Dezenvolve Kapasidade: Malware	Kódigu malisiózu hakerek tiha atu hatama iha aplikasaun trojan.
Dezenvolvimentu Rekursu	T1608.001	Etapa Kapasidade sira Deskarga Malware	Aplikasaun trojaniza upload hela ba plataforma online inklui loja aplikasaun sira
Dezenvolvimentu Rekursu	T1585.001	Estabelese Konta sira: Konta Midia Sosiál	Atór sira kria konta iha website no midia sosiál atu partilla no anunsia malware.
Dezenvolvimentu Rekursu	T1585.002	Estabelese Konta sira: Konta Email sira	Atór sira uza konta email ne'ebe iha host privadu no komersial atu host no partilla malware
Asesu Inisiál	T1189	Kompromisu drive-by	Script ne'ebé malisiózu subar hela iha aplikasaun lejítimu no deskarga ba loja aplikasaun sira
Asesu Inisiál	T1566.003	Phishing: Spearphishing liuhusi Servisu	Atór sira haruka aplikasaun trojan ba grupu-alvu liuhusi mídia sosiál inklui Telegram.
Ezekusaun	T1204.002	Ezekusaun Uzadór: Ficheiru Malisiózu	Vítima tenki instala aplikasaun Trojan atu halo ezekuta payload
Evita Defeza	T1027.009	Ficheiru ka Informasaun ne'ebé disimula Karga ne'ebé hetan implantasaun	Karga perigu disimula iha aplikasaun lejítimu laran.

Evita Defeza	T1036.005	Disimula Kombina ho Naran ka Lokasaun ne'ebé legítimu	Ficheiru trojan kompatível ho naran, aparénsia no funsaun aplikasaun lejítimu.
Evita Defeza	T1656	Imitasaun	Atór sira halo imitasaun ba ema ne'ebé konfiável liuhusi kria website falsu no uza naran-uzuáriu ne'ebé asosia ho grupu-alvo sira.
Kollesaun	T1123	Rejistu Áudio	Aplikasaun trojan bele husu permisaun ne'ebé la presiza inklui asesu ba mikrofon.
Kollesaun	T1125	Rejistu Vídio	Aplikasaun trojan bele husu permisaun ne'ebé la presiza inklui asesu ba kamera.
Kollesaun	T1005	Dadus husi Sistema Lokál	Aplikasaun trojan bele husu permisaun ne'ebé la presiza inklui asesu ba ficheiru lokal.
Komandu no Kontrolu	T1071.001	Protokolu Kapa Aplikasaun: Protokolu Web	Malware konekta ba C2 uza HTTPS no WebSocket.
Komandu no Kontrolu	T1509	Porta Naun Standard	Porta Naun Standard ne'ebé uza hanesan porta 4432 no 2333.
Eksfiltrasaun	T1041	Eksfiltrasaun Liuhusi Kanal C2	Malware halo eksfiltrasaun dadus uza koneksaun HTTPS no WebSocket.
Impaktu	T1565.002	Manipulasaun Dadus: Manipulasaun Dadus Transmitidu	Atór sira obtein dadus husi vítima liuhusi ativa trafiku web aplikasaun ne'ebé la presiza ba funsionamentu aplikasaun.

Indikadór sira

MOONSHINE:

- Iha 1 Abril 2025, peskiza ba painél VLiteUI fó rezultadu tuir mai:

IP Address	Porta	Primeira Vez	Tempu Ikus Nian
103.254.108[.]87	888	2024-10-17	2025-02-14
43.159.192[.]7	444	2024-11-21	2025-02-13
103.27.109[.]109	444	2024-07-11	2025-02-07
45.119.99[.]83	444	2024-12-26	2025-01-24
103.254.108[.]76	444	2024-09-12	2024-12-05
194.71.107[.]160	444	2023-12-10	2024-11-01
103.254.108[.]108	444	2023-11-12	2024-09-25
103.56.17[.]194	444	2024-04-03	2024-08-23
103.254.108[.]87	444	2023-11-14	2024-08-15
62.72.58[.]168	444	2024-01-29	2024-08-07
103.43.18[.]43	444	2024-02-12	2024-07-19
77.91.123[.]208	444	2024-02-04	2024-04-09
46.246.98[.]229	444	2024-03-07	2024-03-26
2.58.15[.]101	444	2024-02-23	2024-02-27
46.246.98[.]209	444	2024-01-08	2024-02-14
103.254.108[.]87	8000	2023-10-17	2023-10-17
103.254.108[.]87	8080	2023-04-15	2023-10-16
103.254.108[.]108	9090	2023-04-13	2023-10-16
103.45.66[.]123	9090	2023-03-02	2023-04-08
103.45.66[.]32	8080	2022-07-29	2023-04-06
27.124.20[.]23	9090	2022-05-28	2023-03-24
27.124.20[.]22	9090	2022-05-28	2023-03-23
27.124.20[.]24	9090	2022-05-27	2023-03-17
69.176.94[.]148	9090	2023-03-04	2023-03-10
69.176.94[.]228	9090	2022-12-24	2023-02-25
103.253.40[.]137	8000	2022-06-24	2022-09-02
27.124.4[.]80	8080	2022-02-25	2022-06-23
27.124.4[.]81	8080	2022-02-25	2022-06-23
47.242.46[.]79	8080	2021-05-03	2022-06-17
27.124.4[.]82	8080	2022-02-24	2022-06-15
27.124.4[.]165	9090	2022-05-14	2022-05-28

27.124.4[.]184	9090	2022-05-14	2022-05-27
27.124.4[.]178	9090	2022-05-13	2022-05-26
103.15.28[.]165	8080	2022-03-05	2022-05-25
69.176.94[.]226	8080	2022-03-05	2022-04-22
27.124.4[.]3	8080	2022-03-11	2022-04-02
103.140.238[.]235	8080	2022-03-04	2022-04-01
27.124.4[.]2	8080	2022-03-12	2022-04-01
165.84.180[.]107	8000	2022-02-25	2022-03-19
69.176.94[.]156	8000	2022-02-25	2022-03-05
141.98.212[.]70	9090	2021-10-05	2022-03-04
5.188.33[.]50	8000	2022-02-15	2022-03-04
5.188.70[.]193	8000	2022-02-15	2022-03-04
69.176.94[.]140	8080	2022-02-24	2022-02-24
27.124.20[.]83	8000	2022-02-14	2022-02-18
208.87.200[.]106	8000	2022-01-02	2022-01-02
121.127.241[.]37	8000	2021-12-08	2021-12-08
156.255.2[.]211	443	2021-10-05	2021-10-05
156.255.2[.]211	8000	2021-10-04	2021-10-04
156.255.2[.]203	8000	2021-10-03	2021-10-03
47.243.43[.]248	8000	2021-07-05	2021-07-05
45.115.236[.]6	8080	2021-05-03	2021-06-01
43.251.118[.]97	8000	2021-01-03	2021-03-01
185.243.43[.]138	8000	2021-01-04	2021-02-02
47.245.59[.]33	8000	2021-01-05	2021-01-05

- Iha 1 Abril 2025, peskiza ba painél SCOTCH ADMIN fó rezultadu tuir mai:

IP Address	Porta	Primeira Vez	Tempu Ikus Nian
104.194.152[.]24	2333	2025-02-06	2025-02-27
172.86.80[.]126	2333	2025-02-07	2025-02-27
154.90.59[.]62	2333	2024-06-20	2024-09-20
154.90.59[.]88	2333	2024-06-21	2024-09-20
154.90.58[.]210	2333	2024-05-16	2024-06-14
154.90.59[.]225	2333	2024-05-17	2024-06-13
38.60.199[.]208	2333	2023-11-26	2024-01-09
38.60.199[.]254	2333	2023-11-28	2024-01-09
38.60.199[.]99	2333	2023-08-26	2023-11-21

38.60.199[.]44	2333	2023-07-20	2023-09-11
194.163.34[.]23	443	2022-09-30	2023-04-14
45.32.125[.]112	10443	2022-10-01	2023-03-17

- Iha 14 Marsu 2024, peskiza ba painél virtual SCOTCH ADMIN fó rezultadu tuir mai:

Domíniu	IP Address
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

BADBAZAAR:

Deskrisaun	Sertifikadu SSL observa iha BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Iha loron 1 Abril 2025, peskiza ba sertifikadu BADBAZAAR iha leten ne'ebá fó rezultadu tuir mai ne'e:

IP Address	Porta	Primeira Vez	Tempu Ikus Nian
65.108.192[.]173	31237	2025-03-14	2025-03-28
65.108.192[.]173	31236	2025-03-14	2025-03-28
65.108.192[.]173	31235	2025-03-14	2025-03-28
157.90.129[.]73	31236	2025-03-27	2025-03-27
142.132.131[.]15	31236	2024-07-24	2025-03-27

142.132.131[.]15	31235	2024-07-26	2025-03-27
142.132.131[.]20	31237	2023-08-11	2025-03-27
142.132.131[.]15	31237	2024-07-24	2025-03-27
142.132.131[.]20	31236	2023-09-27	2025-03-26
142.132.131[.]20	31235	2023-10-18	2025-03-26
65.108.192[.]155	31236	2024-12-05	2025-02-20
65.108.192[.]155	31237	2024-12-05	2025-02-20
65.108.192[.]155	31235	2024-12-05	2025-02-19
23.88.28[.]222	31237	2024-04-25	2024-11-29
23.88.28[.]222	31235	2024-05-02	2024-11-28
23.88.28[.]222	31236	2024-05-01	2024-11-28
212.129.21[.]168	31235	2023-10-16	2024-03-17
212.129.21[.]168	31237	2023-08-24	2024-03-17
212.129.21[.]168	31236	2023-09-26	2024-03-14

Deskrisaun	Sertifikadu SSL observadu iha C2s BADBAZAAR sira
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62d b3db1baa

- Iha loron 1 Abril 2025, peskiza ba sertifikadu BADBAZAAR iha leten ne'ebá fó rezultadu tuir mai ne'e:

IP Address	Porta	Primeira Vez	Tempu Ikus Nian
162.55.103[.]211	20122	2023-01-12	2025-03-28
162.55.103[.]212	20121	2022-06-30	2025-03-28
162.55.103[.]212	20122	2023-07-14	2025-03-28
162.55.103[.]211	20121	2022-06-03	2025-03-28
162.55.103[.]211	20123	2023-07-22	2025-03-27
162.55.103[.]212	20123	2023-07-22	2025-03-27
212.83.162[.]152	9090	2022-10-13	2025-03-27
23.88.28[.]221	20422	2023-07-28	2023-09-30
23.88.28[.]221	20421	2023-05-18	2023-09-28
23.88.28[.]221	20423	2023-07-28	2023-09-28

162.55.103[.]210	20121	2022-09-30	2023-02-23
65.21.92[.]67	20121	2021-11-02	2022-10-13
65.21.92[.]67	20122	2022-08-10	2022-10-13
23.88.28[.]220	20121	2021-12-08	2022-05-13
94.130.92[.]230	20121	2021-01-04	2021-10-05
88.99.150[.]246	20121	2021-04-06	2021-09-08
45.76.132[.]91	20121	2021-02-02	2021-03-01

- Domíniu WHOIS

Iha kraik ne'e tabela domíniu sira ne'ebé agora ka historikamente iha rejistu WHOIS ho valór sira ne'ebé kompatível ho domíniu C2 BADBAZAAR ne'ebé observa ona.

Valór WHOIS	Domíniu sira
Estadu Rejistante: UJYJYUJ **Nasaun Rejistante: Bolivia** **Rejistadór: eNom**	• ntc-mobile[.]com • microtik[.]net • ntc-ftth[.]net • axisupdating[.]com • axisupdate[.]com • telegramrouter[.]org • telegramtor[.]com • fufijxgkg[.]com • jindjjdtc[.]com • tubevideoplus[.]org • thetubeplus[.]com • tbgram[.]org • signalplus[.]org • pmumail[.]com
Estadu Rejistante: REWR **Nasaun Rejistante: CF** **Rejistadór: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

Estadu Rejistante: FSDF **Nasaun Rejistante: AL** **Rejistadór: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

Email Address sira
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

Kanal YouTube sira
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

Link sira iha kraik ne'e mak indikadór kompromisu seluk (IoC) ne'ebé asosiadu ho BADBAZAAR no MOONSHINE. NCSC la bele konfirma vididade informasaun tomak iha link sira nee, no halo rekomenda ba leitór sira atu verifika sira-nia akuradu independente no relevansia:

- ESET
- Trend Micro
- Lookout
- Lookout
- Volexity
- Citizen Lab

Mitigasaun

NCSC enkoraja ba adota rekomendasaun sira iha kraik atu defende kontra ameasa sira ne'ebé deskreve iha estudu kazu sira.

- **Operadór loja aplikasaun, inklui loja aplikasaun parte-terseiru, no dezenvolvedór sira tenke garante katak aplikasaun sira iha plataforma sira nian ne'e seguru no kompri ho Kódigu Prátika governamentál.** Haree Guia: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version

- **Apoiu lian barak:** Dezenvolvedór aplikasaun sira tenke investe iha esforsu atu lokaliza aplikasaun famozu ba uzadór sira ne'ebé ko'alia iha lian minoritáriu iha grupu alvo sira inklui Uighur, Tibetanu, Taiwanés Hokkien no Kantonés. Orientasaun husi Apple kona-ba lokalizasaun iha aplikasaun: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Guia husi Google kona-ba tradús aplikasaun: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Mantén ita-nia plataforma midia sosiál seguru:** Kompañia mídia sosiál bele halo araska liutan ba atór siber malisiózu atu kria konta falsu no partilla ficheiru ka link malisiózu iha plataforma sira iha komunidade online ne'ebé lejítimu. Bainhira possível, kompañia sira tenki partilla indikadór malísiozu ho indústria boot liutan atu aumenta kompreensaun koletivu kona-ba ameasa no ajuda medida protesaun.

- **Planu remedia ba kliente sira:** Organizasaun sira tenki iha prosedimentu atu informa kliente sira ne'ebé instala aplikasaun malísiozu uza servisu sira. Alerta sira nee tenki atrai atensaun no fó informasaun klaru. Bainhira apropriadu, organizasaun sira tenki fó orientasaun kona-ba oinsa atu hasai software no estimula vitima sira hato'o relatóriu ba autoridade sira, hanesan NCSC iha UK.

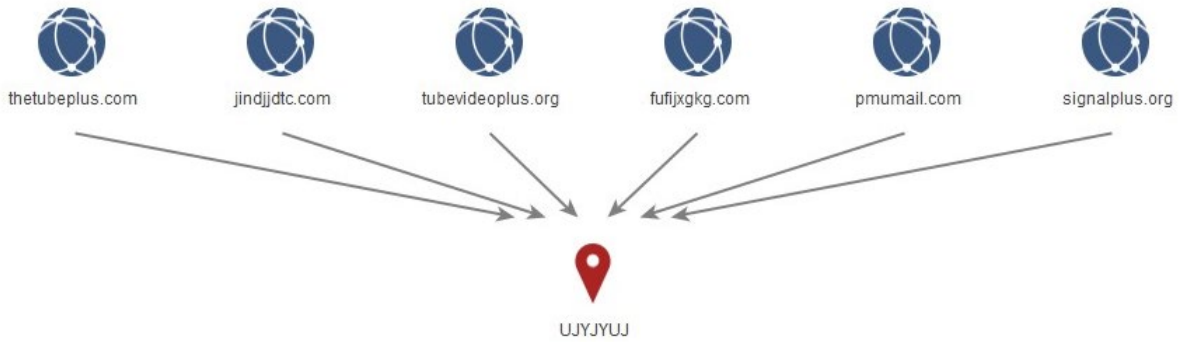
Hare Kódigu Prátika ba App Store ba informasaun liutan: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Grupu traballu ba kolaborasaun:** Kompañia midia sosiál bele forma grupu traballu, hodi fó oportunidade ba ekipamentu seguransa sira nian atu partilla indikadór malísiozu, TTP sira no observasaun, hodi halo araska liu ba atór sira atu uza plataforma sira-ne'e atu suporta kampaña malísiozu.

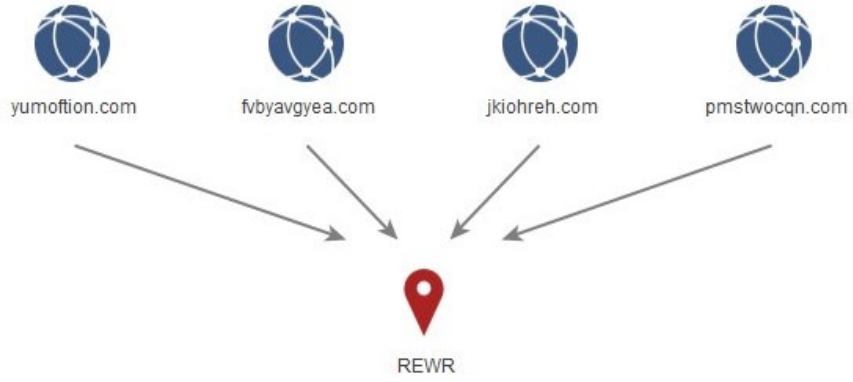
- **Deteta aplikasaun ne'ebé altera ona:** Bainhira possível, dezenvolvedór aplikasaun sira tenki inklui funsionalidade atu informa uzuáriu se sira deskarga versaun 'la-ofisiál' ida husi aplikasaun, hodi ajuda prevene kopiá malísiozu.

Apendise A: Gráfiku husi klasterizasaun WHOIS BADBAZAAR / informasaun broker domíniu

Imajen 1 - 'UKYJYUJ'



Imajen 2 – Valór Keyboard walking



Imajen 3 – Domíniu adisionál sira ho valór kampu estadu 'FSDF'

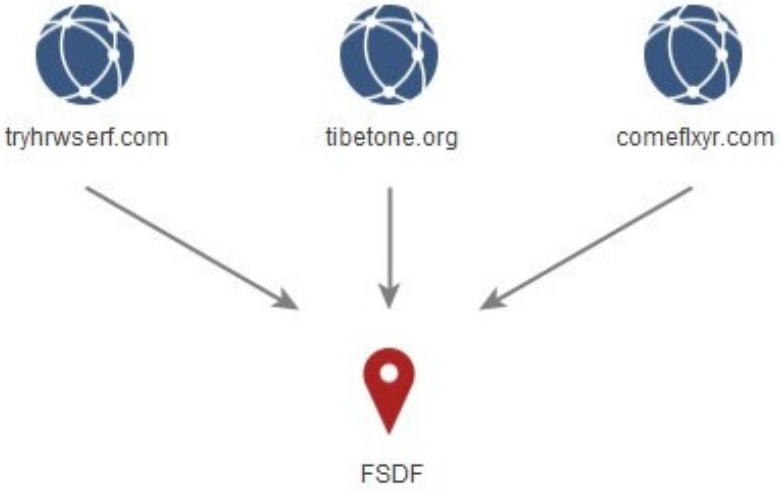


Image 4 – **95.179.210[.]85**

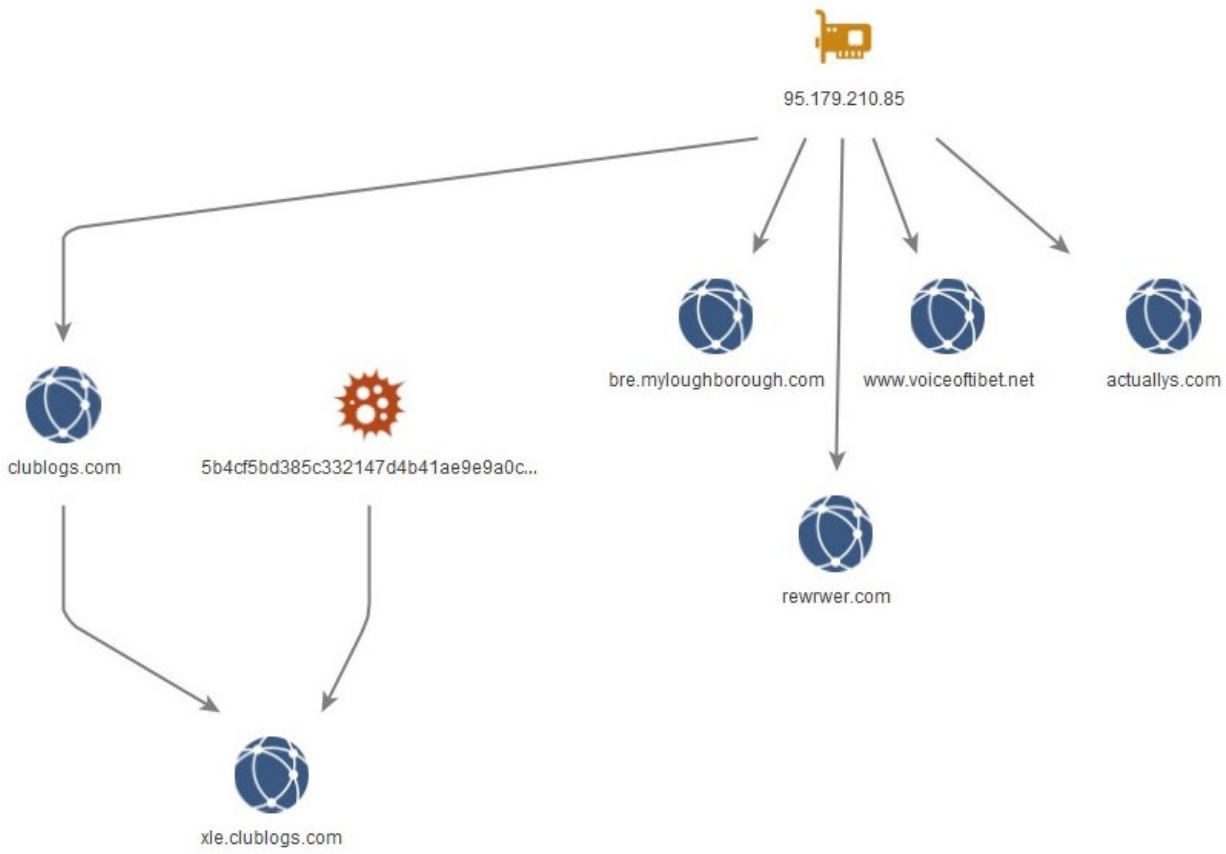
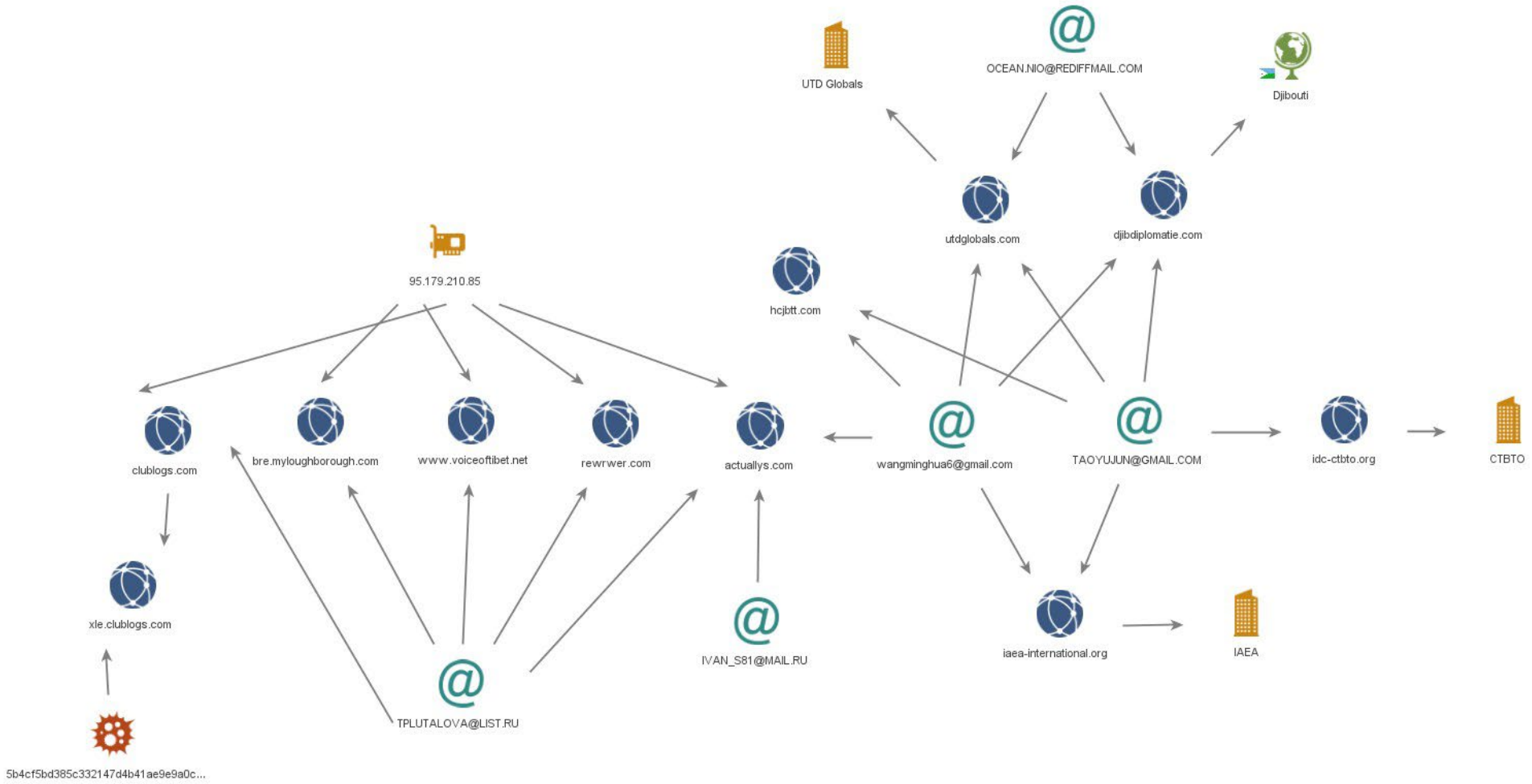
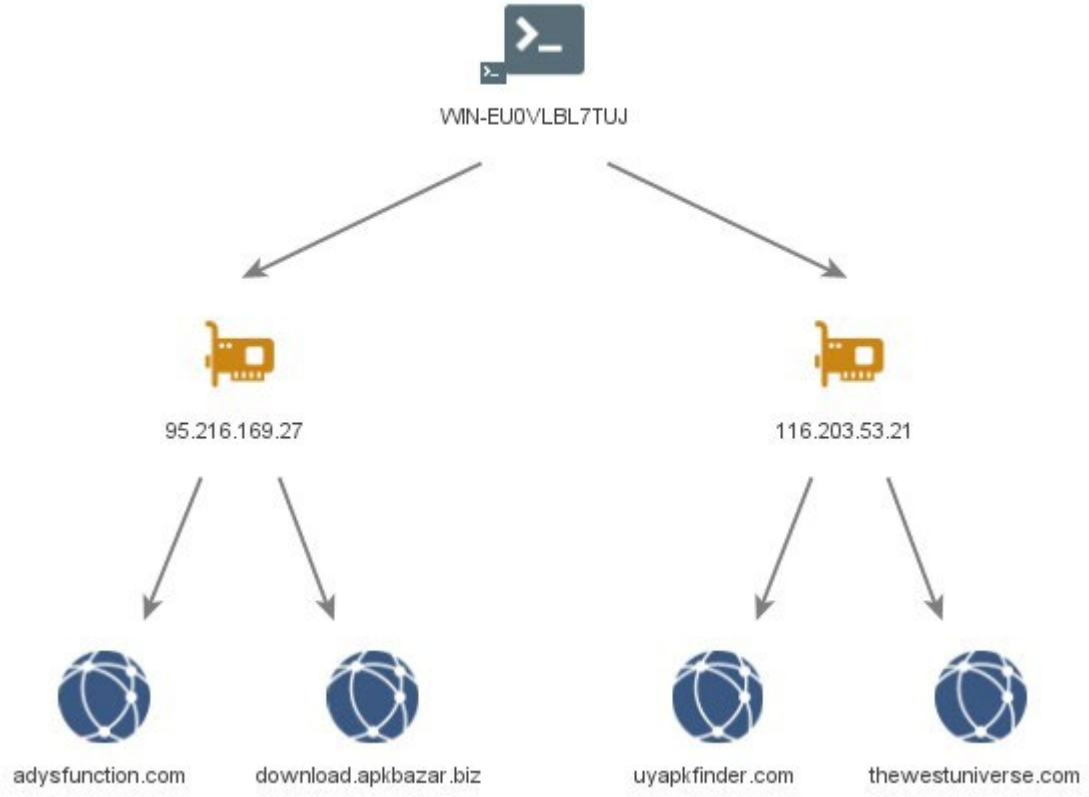


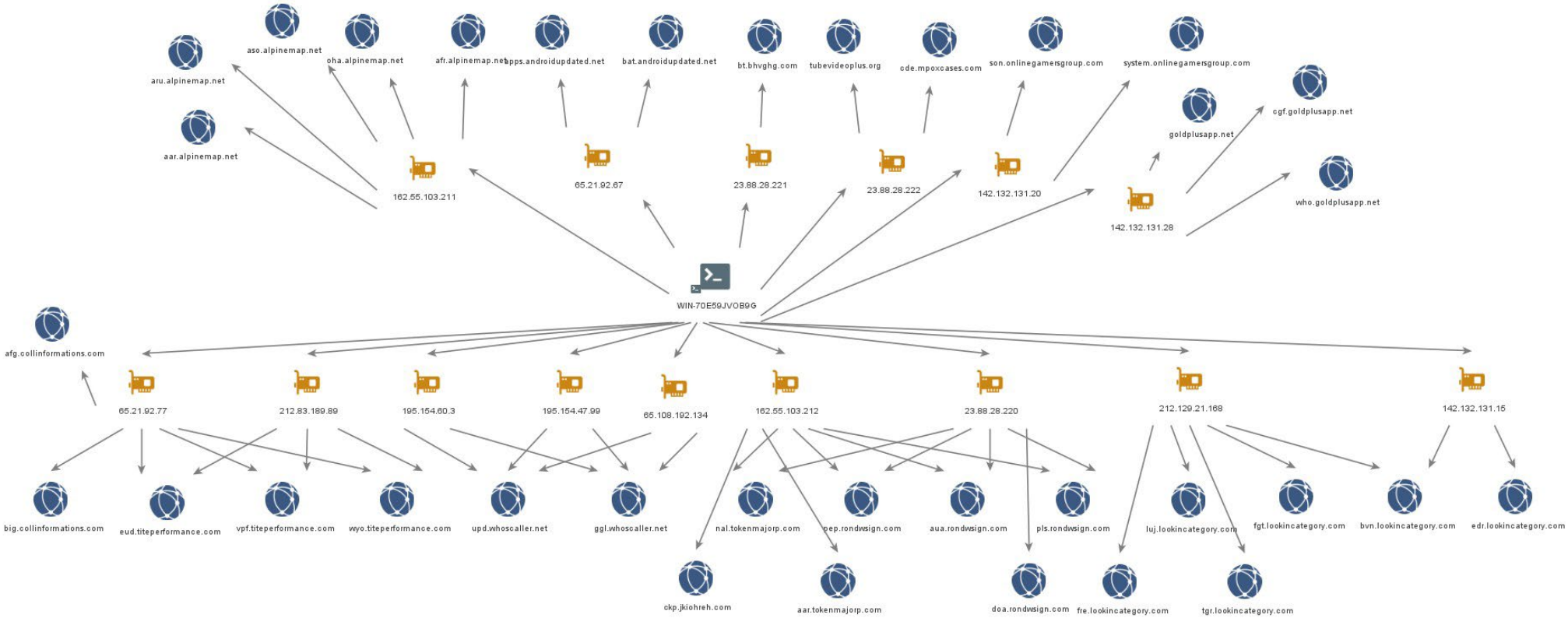
Image 5 – WHOIS links



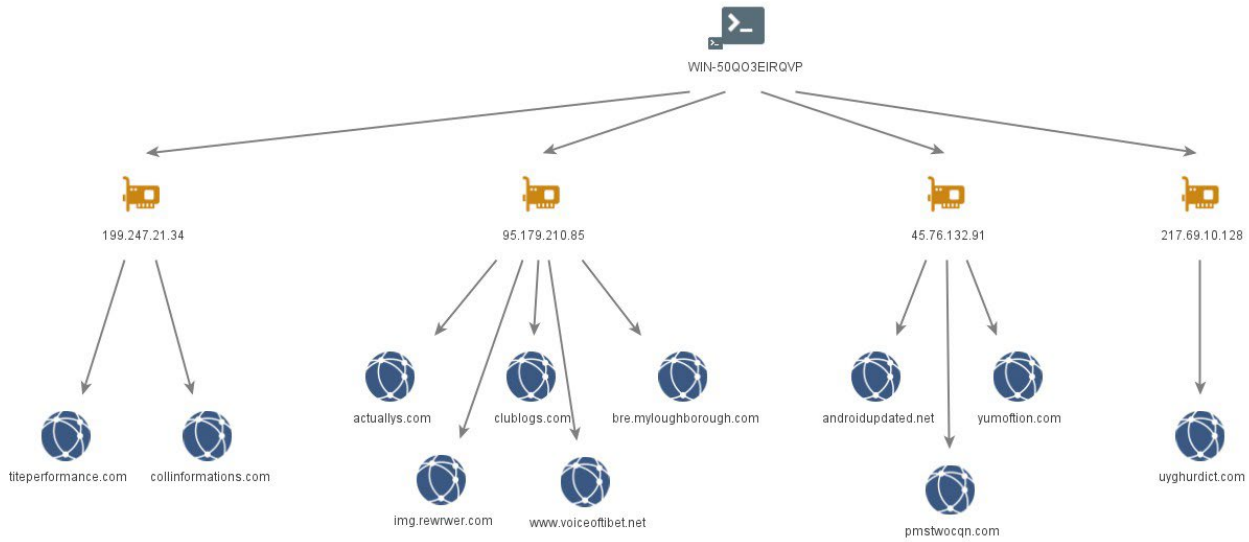
Imajen 6 – **WIN-EU0VLBL7TUJ**



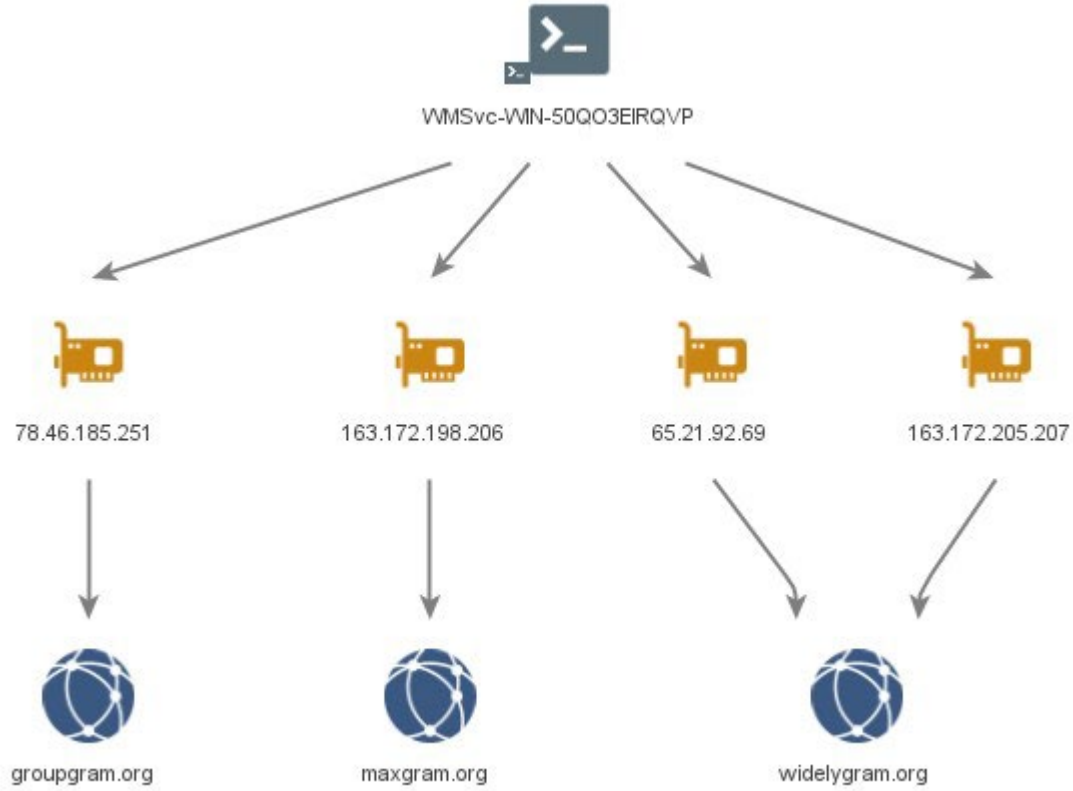
Imajen 7 – **WIN-70E59JVOB9G**



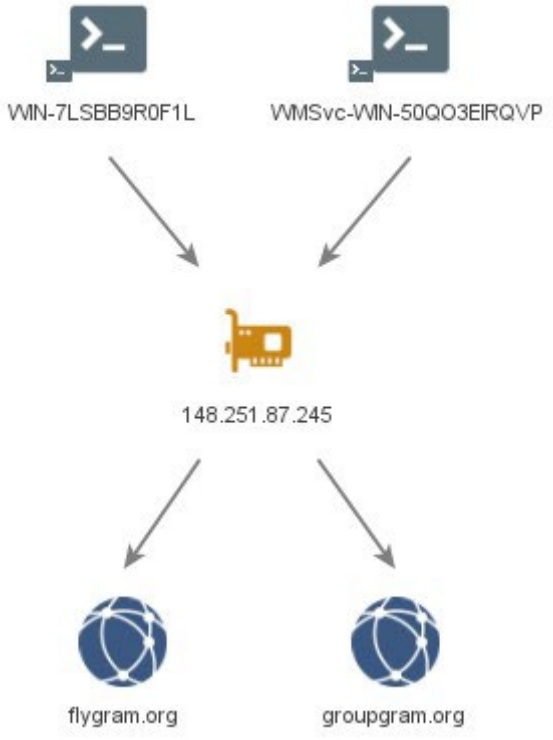
Imajen 8 - **WIN-50QO3EIRQVP**



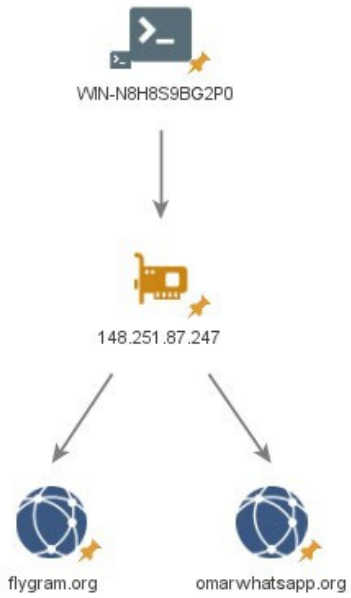
Imajen 9 - **VMSvc-WIN-50QO3EIRQVP**



Imajen 10 – **VMSvc-WIN-50QO3EIRQVP** and **WIN-7LSBB9R0F1L**



Imajen 11 - **WIN-N8H8S9BG2P0**



Imajen 12 – **WIN-I6VBN8MR92A**

Apendise B: Amostra MOONSHINE no BADBAZAAR ne'ebé observadu

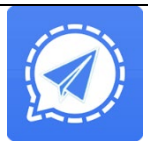
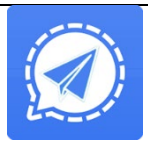
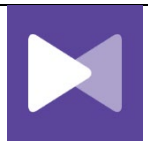
Tabela iha kraik ne'e lista aplikasaun sira mak uza iha kampaña MOONSHINE no BADBAZAAR iha tinan rua ikus.

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

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

AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	

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

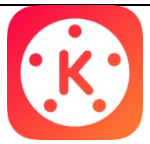
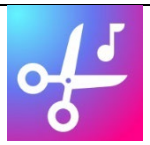
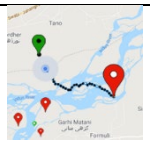
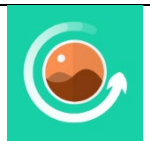
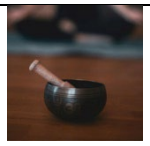
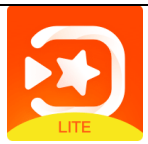
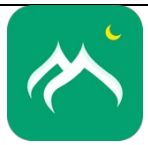
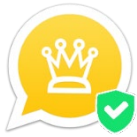
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

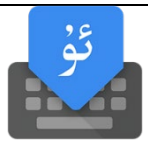
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	
Tibetan Divination System MO	net.rhombapp.mo	

Tibetan Prayer	com.chorig.tibetanprayer	
Translator AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Video Converter	com.inverseai.video_converter	
Video Cutter	com.naing.cutter	
Video Downloader	downloader.video.download.free	
Video Maker	com.bstech.slideshow.videomaker	

Video Player for Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Voice Recorder	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	

WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
WiFi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
YouTube Downloader	dentex.youtube.downloader	
Zom	im.zom.messenger	
iQuran Lite	com.guidedways.iQuran	

ئاۋازلىق ئەسەرلەر	com.ewlat.eserler	
ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى ئۇيغۇرچە APK	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	
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	

Leitura adisionál

Orientasaun husi Sentru Seguransa Sibernétika Austrália

- Relata kona-ba krime sibernétika, insidenti ka vulnerabilidade
- Oinsá seguru Ita-nia dispositivu
- 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 indivídual

Guia husi US NSA

- Prátika Melloria ba Dispositivu 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 indústria. 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.