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

Kamatata

BADBAZAAR ao MOONSHINE: Tuoan mwakurina ao kaokan arona

9 n Eberi 2025

BADBAZAAR ao MOONSHINE: Tuoan mwakurina ao kaokan arona

Kauarereke

Man ana boutoka te UK rinanon te Cyber League, te kamatata aei ea tia ni uaia ni karaoaki iroun te Botaki ni Kamanomano iaon te intanete i Buritan (NCSC-UK) ma raona nte aonnaba:

- **Ana tabo Aotiteria ni Kamanomano iaon te Intanete, mwangan Tauanimwin Tikino i Aotiteria**
- **Ana tabo Kanata ni Kamanomano iaon te Intanete, mwangan Boboti ibukin Kamanoan te Reitaki**
- **Ana Botaki n tibwai Tiaman**
- **Ana Aobiti Tiaman ibukin Kamanoan te Tua**
- **Ana tabo New Zealand ni Kamanomano iaon te Intanete, mwangan ana Botaki te Tautaeka ibukin Kamanoan Reitaki**
- **Ana Botaki ni Kakae Rongorongo Tautaeka n Amerika**
- **Botaki ibukin Kamanoan Aban Amerika**

Te kamatata aei e katauraoi rongorongon kakamaku aika boou ao ni barongaki raoi ibukin uoua tibwaiuea ae aranaki bwa BADBAZAAR ao MOONSHINE, ao e kairi naba taeka ni buobuoki ibukia nake aia bwai titoa ni burokuraem, taan kario ao kambwanan tabo n reitaki ibukin kamanoaia te koraki ake a kakabongana.

Te kamatata aei e boretiaki ni ikotaki ma te kamatata ibukia te koraki ake a rotaki ni mwauea aikai.

Te beba aio e kabonganai taeka ma nanoia man NCSC ibukin tibwaiuea: "Te aekaki n tibwaiuea are kona n rin n bwai n reitaki n akean ana kariaia te tia bwaibwai, e rikoi rongorongoia ao e manga kanakoi nakoia tabeman."

Te moan katoto: MOONSHINE

MOONSHINE ngaia te tibwaiuea nte Android are ribotinaki n 2019 iroun Citizen Lab bwa a tataketenia kurubu mai Tibet. MOONSHINE e katotongia burokuraem ake a kinaki ao e aneaia aomata bwa ana karinna n aia bwai n reitaki. E a tia n kabutaki iaon Telegram ao n rinki inanon WhatsApp.

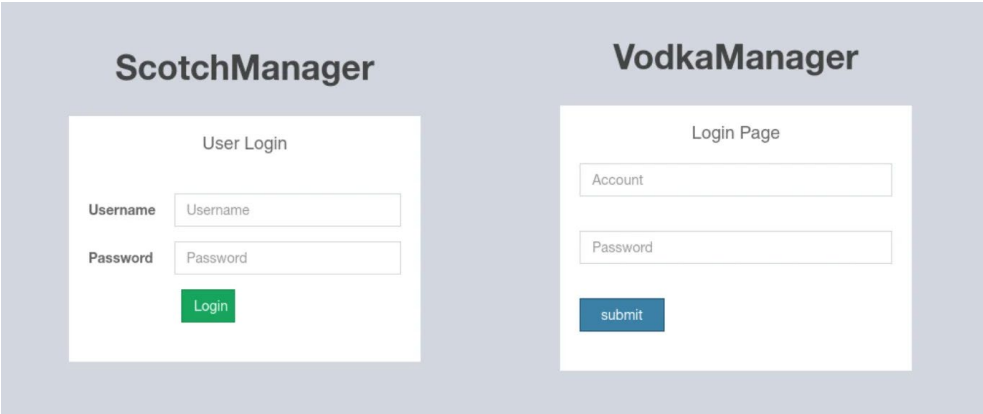
Ana ukeuke NCSC iaon MOONSHINE e kaoti aikai:

- MOONSHINE e kabonganai aron babaronga aika a bibitaki man te tai are moan ribotinaki iai.
- Aron barongana e kaotia ae e korakora ibukin taukiroaia aomata, iai naba ana kona ni kaotinakoi rongrongo man bwai n reitaki ao ni kona naba n rawei tamei aika maiu ao n rawea tamein te tikuriin.
- A tia ni kuneaki ana tiewa MOONSHINE ake a babarongaki mwakuria iai. Nnen babaronga aikai iai rekerekeia ma baeno ni karinrin ae rekereke ma UPSEC, e taku Te Tibwai Online bwa e rekereke ma te 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Nnen te babaronga

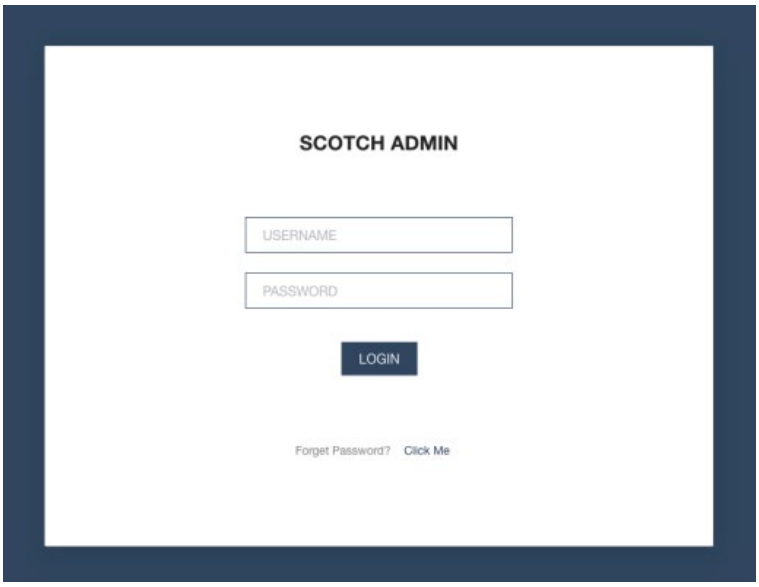
Te riboti iaon nnen barongan MOONSHINE e kaotia ae ea tia nikaraoki te bitaki nako iai, e kakoauaki ikai bwa ae bon tabe naba ngkai ni kamwakuraki.

Te moan katoto iaon te nne ni babaronga e kuneki inanon te Citizen Lab's 2019 ririboti.



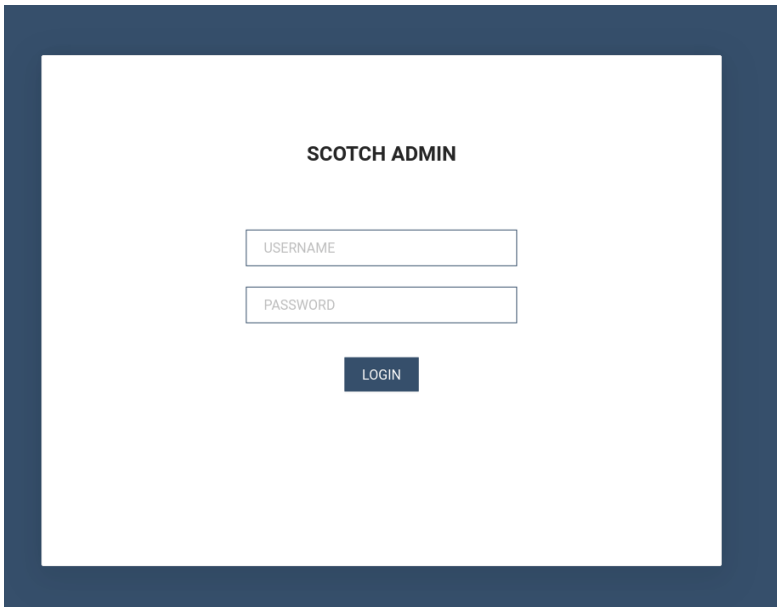
Nambwa 1: Nnen barongan MOONSHINE are kuneaki inanon ana riboti Citizen Lab's 2019 'Te Rinki ae Bua Kurubu mai Tibet a Taketenaki nte 1-Kiriki Aonikaian Tareboon'.

Ni moan 2022, e ribotinna Lookout bwa iai nnen babaronga aika a manga kabouaki karaoaia ao a katotongi aika i nano (onean mwin nnen babaronga ni kawai ane n figure 1):



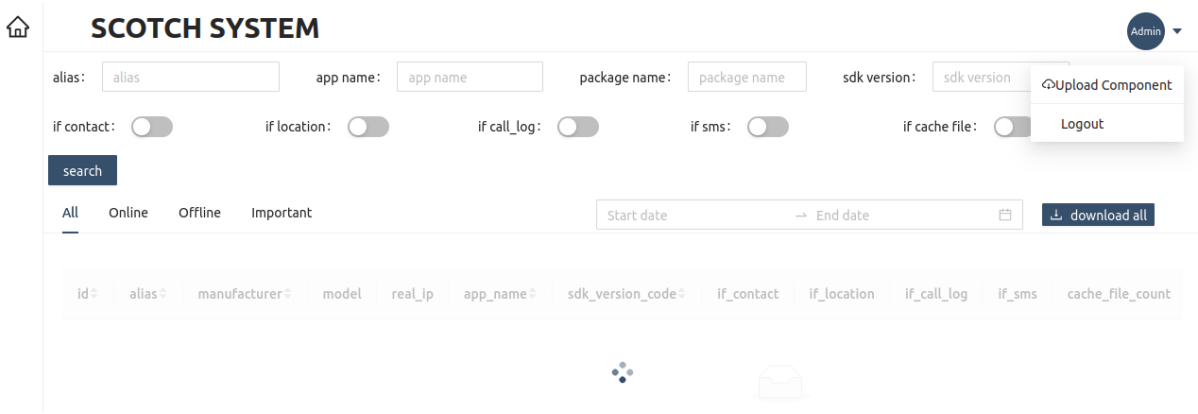
Nambwa 2: MOONSHINE nnen babarongana noria n Lookout 2022 riboti 'MOONSHINE: Bibitakin Bwai n Taukiro iaon Android mairoun te kambwana n China ae APT POISON CARP ibukin taketenakia kain Tibet ao taian Uyghurs'.

Inanon Aokati 2023, ao e kataratataraki aron MOONSHINE ni kairiraki ao n taubeakinaki (C2) e kaoti nnen babaronga ae titabo ma are n 2022 ma ai akea iai te konabwai ae te '**Mwaninga Taeka aika Raba**' n nambwa 2:



Nambwa 3: Nnen MOONSHINE ni barongaki e noraki n Aokati 2023 bwa ai akea iai te taeka ae 'Forget Password'.

Karaoan riki ukeran nnena ni barongaki ao a oti kanoan baeno are ea kaoti aron kawakinan rongorongon bwai n reitaki.



Nambwa 4: Baan te uebutiaiti ibukin karekean te rinnako n nnen barongan MOONSHINE.

Ana ukeuke Lookout e kaota aron tauan '**te bwi**' man aia bwai n reitaki te koraki ake a rotaki n ana tiewa MOONSHINE C2. Mwaitin 'te bwi' e irekereke ma mwaitin kariaiakan rinin te bwai ni kaikoaki n aia tareboon te koraki ake a rotaki.

Kaorum aikai 'if_contact', 'if_location', 'if_call_log' ao 'if_sms' nte itera ni ba aei e kaotia ae aki rin ni kabane ana kaikoaki MOONSHINE ibukin kumean ao tauan taekan bwai n reitaki. Atatai man kaorum aikai ao 'te bwi'' are anaki man bwai n reitaki nakon C2 e kaotia bwa aekita ni kakamaku aikai a kabongana te bwi ibukin atakin tian rinin te mwauea nte bwai n reitaki are a taua taekana ao n angania aekita ake a kakabonganai nnen babarongan te mwauea.

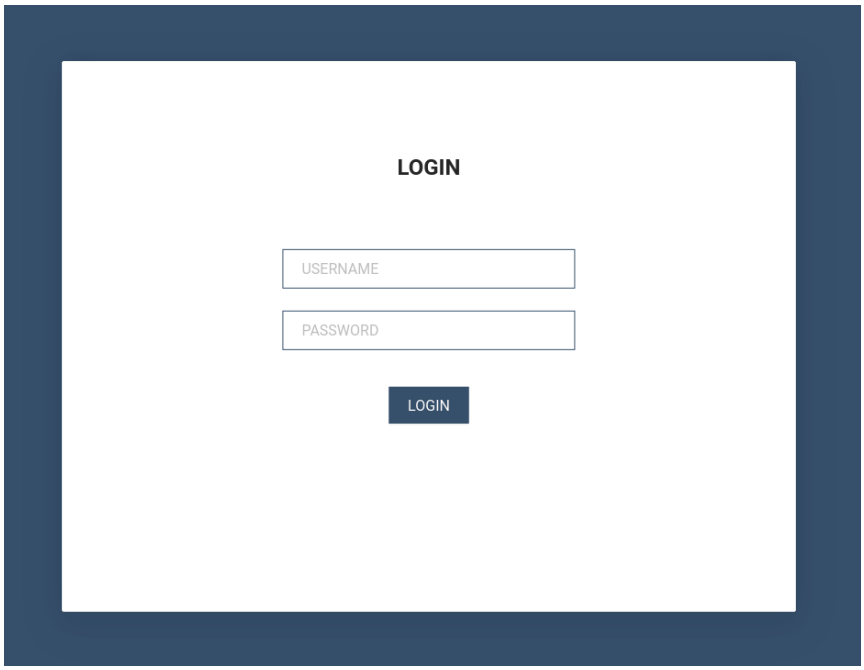
N teina ae ngkai, ao taeka n reirei ibukin aroaro aika mano ibukin totokoan burokuraem bwa ana anai rongorongo man bwai n reitaki kona tuia kariaia nakon burokuraem ibukin bwai ake kona karuoi ma te nano uoua. Ma e ngae n anne, ao MOONSHINE e ukori kariaia ake a botau ma mwakurin te burokuraem, bwa e aonga n aki tara ni kanano uoua, ma a bon kabonganai kariaia akanne ibukin rikoan rongorongo man te bwai n reitaki.

MOONSHINE iai naba Nnen Burokuraemian Burokuraem (API) are ea kaota naba rababan ana konabwai. Tein API aikai ake a oti nte beba ae koreaki nte Mandarin.

Tiewante intanete

Inanon kakaean ana baeno MOONSHINE, ao a noraki kabuanibwai ake nte tiewa. Te onrain tiewa e nanonaki iai are man teuana te IP aetureti ao e kawakini uebutiaiti aika mwaiti nte tai ae ti teuana. Te IP aetureti ibukin aonrain tiewa aikai ni ikotaki ma tomein ake i nanona a tuai n noraki n riki bwa katoton mwauea.

Taian kanganga ni bwain mwakuriaia e kakaokoro, ngkai atun itera niba bon '**LOGIN**' ao ai tiaki are nonoraki mai mwaina ae '**SCOTCH ADMIN**'.



Nambwa 5: MOONSHINE ana baeno ni babarongana e kakabongana te taeka ae LOGIN ao tiaki SCOTCH ADMIN.

Ni ikotaki ma anne, ao tein te baeno e kaokoro naba ma ane n nambwa 4, teina ane n nambwa 6.

Nambwa 6: Baan te uebutiaiti ibukin karekean te rinnako n tiewa ibukin barongan MOONSHINE.

Te baeno ane n nambwa 6 e tara n ae kauarereke-an te baeno are n tamnei 4. Irekereken tein baeno aikai e mena n aran kaorum aika ‘id’, ‘tia karao bwai’ ao ‘model’ inanon te taibora.

Bwai ake a reke n ana tiewa MOONSHINE bon:

Tomein	IP Aetureti
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

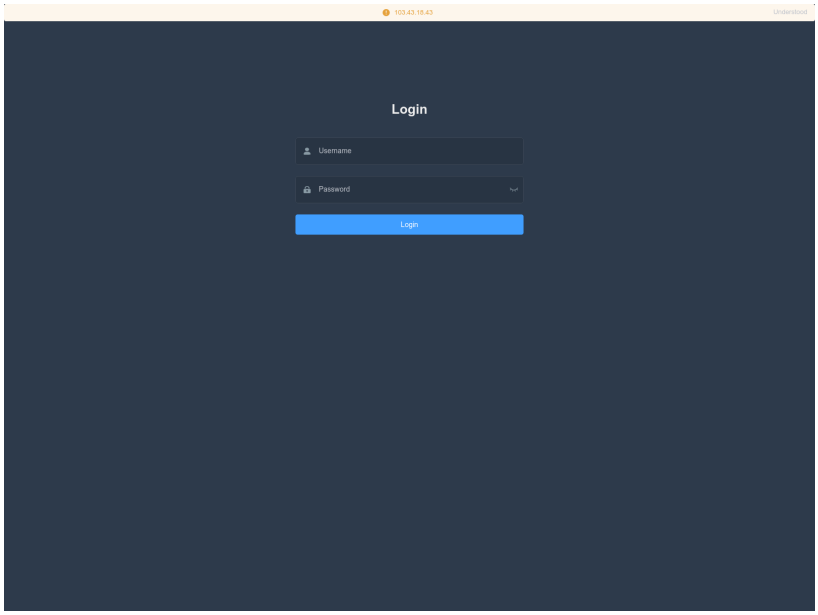
Tomein aikai a reke iroun Trend Micro ao a mena i nanona ana bwai MOONSHINE n karaoi ana aonikai, ibukin karaoani mwakuri n aonikai ao ibukin karinan mwauea inanon tareboon. Trend Micro e arana te mwauea aei bwa 'Dark Nimbus'.

Ibukin te kamatata, ao ana baeno ni babaronga MOONSHINE ngaia te tabo are a rereitaki iai mwauea, ao man kawakini naba iai rongorongoia konaia. Ana bwai MOONSHINE n aonikai are ribotinna Trend Micro, a kaokoro aron tein korakoraia n aonikai memere ibukin karinakin mwauea ao arana Dark Nimbus inanon bwai n reitaki. N reitia ma anne, Dark Nimbus ao MOONSHINE taian mwauea aia a rangi ni kaokoro.

Nnen babarongan MOONSHINE ao ana bwai n aonikai MOONSHINE a kuri n titabo taekan karaoaia ngaia are e kuri n titabo aron tein te rinako n nambwa 3 ao 5 ao ai arona naba ma kanoan itera ni ba inanon nambwa 4 ao 6. Iai naba te taeka aie ‘webpackJsonpreact-scotchui’ inanon manin burokuraem.

Taan kakamaku a karaoi URL rinki ake a toma nakon ana bwai n aonikai MOONSHINE ao mai ikanne are ea kaoti naba tamei ake a rekereke ma kain Tibet ao taian Uygurs, are rekereke ma taketenakin MOONSHINE.

Nikabane mwin bwai n reitaki ake iai ana bwai n aonikai MOONSHINE i nanona, ao iai te iteraniba ni karinrin ae aranaki bwa 'VLiteUI' iaon botu 444. Te itera ni ba anne e tataraki n tainako ao kuneakina inanon IPs e kaotia bwa iai rekerekena ma aia mwakuri taan kakamaku.



Nambwa 7: Baeno ni Karinrin nte HTML ae aranaki bwa 'VLiteUI' e nonoraki iaon IPs ake iai ana bwai n aonikai i nanona.

N tuoan Dark Nimbus iron Trend Micro ao e kaotaki bwa te mwauea e kona n rikoi rongorongon bwai n reitaki aika mwaiti, ao e rereitaki ma C2 nte XMPP.

E kaotia naba Trend Micro ae tabeua karinanin Dark Nimbus, ao aki toki n nonora te taeka ae 'DKNS' ni kakaoti.

'**ansec[.]com**' (e ataki bwa te Nimbus C2 iroun TrendMicro) e nonoraki naba n XMPP tieweti ni nnen bwai n reitaki ake a mwakuri ma taabo ake iai DKNS n araia:

- DKNS Android远程取证系统 (DKNS Ana Tititem ni Ukenako mai Kiraroa Android)
- DKNS云网侦控平台 (DKNS Tititem man Tiewa Ibukin Kakae ao Taraia taan aonrain)
- DKNS 云网侦控平台 (DKNS Tititem man Tiewa Ibukin Kakae ao Taraia taan aonrain)
- DKNS远程控制侦查系统 (DKNS Tititem ni Kakae mai Kiraroa)

Tebeua riki nnen bwai n reitaki ma '**ansec[.]com**' inanon te XMPP tieweti iai itera ni ba ae a atunaki n:

- UPSEC互联网控制指挥系统 (UPSEC Tititem ibukin Karaoan Taran te Intanete)
- UPSEC无线侦控系统 (UPSEC Tititem n Taukiroo ao Tararua ae akea Uaeana)
- UPSEC重点人数据还原系统 (UPSEC Tititem Ibukin Kaokan Aroia Mataniwi)

Ao iroun Intelligence Online, 'UPSEC' ae nonoraki n atun taian HTML uebutiaiti, bon kauarerekean te ara ae 'Sichuan Dianke Network Security Technology Co., Ltd'.

Ka Uoua ni Katoto: BADBAZAAR

BADBAZAAR bon mwauean tareboon ae iai nte iOS ao nte Android are ea tia n taketenia taian Uygurs, kain Tibet ao ai kain Tawan. Te tibwaiuea aio e kona ni butinako man tabo n reitaki ao titoan burokuraem. RRiboti aika boou man Volexity e kaoti aekakin nako BADBAZAAR, ake a tia ni kamaenakoaki bwa BadSolar, BADBAZAAR ao BadSignal. Ni kabane aekakina aika teniua aikai a titabo aia mwakuri ake a kakabonganaki ibukin rikoan rongorongon bwai n reitaki ao rangorongon te tia kabonganai.

Ana kamatebwai NCSC research iaon BADBAZAAR ao a oti aika i nano:

- Kakae iaon tomein aika C2 e kaotia ae iai rekerekeia ma rinki ake a tia ni kabonganaki ibukin kakamaku.
- C2 tiewa ao katoton mwauea a kaoti ara n rininako ake a rekereke ma aia bwai n aonrain aekita aikai.
- Aikai riki aron kinakia ake a kakabonganai aekita aikai ibukin anainano ao tibwakin aia mwauea i tinanikun titoa ni burokuraem.

WHOIS kakae / taan kabonakoi tomein

'UJYJYUJ'

Mwin ukoran ana rekoti WHOIS ibukin te tomein ae BADBAZAAR '**signalplus[.]org**' (e ribotinna ESET) e kaota te taeka ae '**UJYJYUJ**' inanon te marae ae '**State**'.

Kakae ibukin tomein ake titabo kanoaia e kaoti tomein aika a kakaongora aikai:

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

(Noora Anekiti A, tamnei 1)

Tomein aika **signalplus[.]org**, **tubevideoplus[.]org** ao **thetubeplus[.]com** a kaotaki bwa ana tomein BADBAZAAR C2, ao ESET e kaotia bwa te tiabu tomein ae **mail.pmumail[.]com** e mena inanon te FlyGram tiewa. FlyGram bon karinanin burokuraem ae BADBAZAAR ae karaoaki irouia taan kaikoaki aonrain. (Noora te Abentekiti ibukin karinanin ana burokuraem BADBAZAAR).

Kakaean taeka aika raba nte kibooti

Te NCSC ea tia naba n nonori kakae aikai n tomein ake a bwainaki iroun BADBAZAAR C2.

Te kabotau, tomein aikai iai kanoaia ae '**REWR**' ae noraki inanon te kaorum ae '**State**' (n aron kabonganana ngkoa):

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

(Noora Anekiti A, tamnei 2)

Tomein man 'FSDF' kanoan te kaorum ae state

Tabeua riki ana tomein BADBAZAAR C2 iai '**State**' inanon '**FSDF**':

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

(Noora Anekiti A, tamnei 3)

Ririboti ni ikawai iaon kakaean taeka aika raba nte kibooti

Kabonganan kakaean taeka aika raba nte kibooti inanon BADBAZZAR n ana rekoti WHOIS ao a kona n noraki n riboti ni kawai bwa a taketenaki boboti mai Tibet iroun TA413. Tauan mwin Taai aika ana roko ea tia n nonoria tomein ake a tauaki-mwiia ni kumei aia boboti kain Tibet ao ni kabongana te ara rinnakoi boboti akanne ae "**asfasf**".

clublogs[.]com

Katoton BADBAZAAR ake a reke iroun Lookout iai inanoia '**xle.clublogs[.]com**' ae ana tomein the C2. Wakan te tomein '**clublogs[.]com**' e mena iaon te IP aetureti '**95.179.210[.]85**' ao iai ana SSL beba ni kamano ma arana ao kanoana ae '**CN=WIN-50QO3EIRQVP**'. Te ware anne titabo raoi ma SSL beba ni kamano ake a kuneaki ni katoton BADBAZAAR are a kakabongana SSL ibukin totokoan kamangaoan te reitaki.

Rongorongon te IP aetureti ae **95.179.210[.]85** ao a kuneaki tomein aika kakaongora aikai:

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

(Nora Anekiti A, tamnei 4)

www.voiceoftibet[.]net

Te tomein ae '**www.voiceoftibet[.]net**' e tara ni kewe ni katotonga te rerio ae 'Bwanan Tibet', ae titabo ma te TTP are kabongana TA413.

Te tomein '**rewrwer[.]com**' e titabo ma kanoan '**State**' are atia ni kaotaki ae '**REWR**' are kuneaki inanon aia WHOIS rekoti taian BADBAZAAR tomein.

Taian tomein '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' ao '**myloughborough[.]com**' a bane n karaoaki man te imeeri ae '**tplutalova@list[.]ru**'.

actuallys[.]com

Ana rekoti WHOIS ibukin '**actuallys[.]com**' e kaotia bwa aia imeri aetureti tan rabakau ao tan mwakuria bon '**tplutalova@list[.]ru**' ma e karaoaki man te imeri ae '**ivan_s81@mail[.]ru**'.

Rongorongo ni kawai man WHOIS ibukin te tomein ae '**actuallys[.]com**' e kaotia ae e karaoaki man te imeri ae '**wangminghua6@gmail[.]com**' ae karaoke n 24 ni Beberuare 2016. N 11 ni Maati 2016, te imeri ea manga bitaki nakon '**ivan_s81@mail.ru**' e ngae ngke te tia karaoia ae boou aei e aki bita bongin namwakaina are ena toki iai taina.

wangminghua6@gmail[.]com

Te imeri aetureti ae '**wangminghua6@gmail[.]com**' e kabonganaki ibukin karaoan tomein ake a kuneaki i buakon kakae rongorongo ibukin ribotinakin kakamaku. Inanon 2015, Palo Alto e kaota te imeri are kabonganaki ibukin karaoan C2 tomein ibukin te mwauea ae, Cmstar. Inanon 2014, ao e kabonganaki naba

ibukin karaoan tomein ake a kuneaki iroun Mandiant ni karaoi kambein ni katairake ae karaoaki iroun APT3. Inanon 2013, ao e kabonganaki ibukin karaoan tomein ake a kuneaki iroun CrowdStrike inanon te mataroa mai buki ae iai koroboki n China iai inanon Rongorongon ana Burokuraem (PDB). Aio e kaotia bwa a karaoaki aikai n ana tititem China.

taoyujun@gmail[.]com

Te tomein ae '**hcjbtt[.]com**' e karaoaki nte imeri aetureti ae '**taoyujun@gmail[.]com**' ma taan mwakuriia a karaoaki aia akaunti man te imeri ae '**wangminghua6@gmail[.]com**'.

Akea mwakuri ni kaikoaki ae irekereke ma '**hcjbtt[.]com**', ma te imeri aetureti ae '**taoyujun@gmail[.]com**' ea tia ni kuneaki ni kakae rongorongo ibukin ribotinakin kakamaku. Inanon 2014, e kabonganaki ibukin karaoan te tomein ae kuneaki iroun Mandiant ni katoton '**Cueisfry Trojan**' ake a kabonganaki ibukin taketenaia aia boboti kain Japan.

Te imeri aetureti e karaoi naba tomein n aron '**iaea-international[.]org**' are e tara ni katotonga te **International Atomic Energy Agency** ao '**idc-ctbto[.]org**' are katotonga te **International Data Centre** nte **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

Ana rekoti ngkoa Whois ibukin te tomein ae '**iaea-international[.]org**' e kaota aran te imeri are karaoaki mai iai bwa '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Te tomein ae '**udtglobals[.]com**' e noraki ni kabongana te imeri ae '**wangminghua6@gmail[.]com**' ibukia taan mwakuriia ao '**ocean.nio@rediffmail[.]com**' ibukin karaoana. Rekoti man WHOIS ibukin te tomein aio, e kaota titabon te imeri ibukin karaoakiia ma aia akaunti taan mwakuria e karaoaki nte imeri ae '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' e tara ni katotonga '**UDT Global**' te runga nte aonnaba ibukia kambwana ibukin kamano ao otanga i marawa. Te ara ae '**ocean.nio**' are toma ma te imeri aetureti e kona n ae kataia ni katotonga te **National Institute of Oceanography (NIO)** te botaki ae tiraua mwangana n aba aika kakaokoro. E ngae ngke kabonganan te imeri service ae **Rediff**' (te kambwana mai-India) e kanamakinaki katotongan te **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

Te tomein ae '**djibdiplomatie[.]com**' e tara ni katotonga ana tieweti Djibouti ibukia kain tautaeka, ao iai naba ana rekoti nte WHOIS ae titabo ma '**utdglobals[.]com**'**.** Teuana te rekoti e tara ni kaota te tia karaoia '**ocean.nio@rediffmail[.]com**' ao taani mwakuria '**taoyujun@gmail[.]com**' ao rekoti ake tabeua a kaota '**wangminghua6@gmail[.]com**' bwa ana imeri te tia mwakuria ao '**ocean.nio@rediffmail[.]com**' ngaia ae karaoa te tomein.

Tomein aika uoua aikai iai mwin kakaean taeka aika raba irouia nte kibooti n ana rekoti WHOIS. Te kabotau, '**udtglobals[.]com**' e kabongana te taeka ae '**ASDF**' bwa te tabo are karaoaki mai iai ao '**djibdiplomatie[.]com**' e kabongana '**DAF DAGF**' bwa aran te tia karaooaia. A kuri n titabo tein aikai ma ake a nonoraki n ana tomein BADBAZAAR.

E ngae ngke iai mwin imeri aetureti aikai '**wangminghua6@gmail[.]com**' ao '**taoyujun@gmail[.]com**' ake a kuneaki n ana rekoti WHOIS bwa ngaia ake a kakatotongi **kamanoan kabin marawa nte aonnaba**, **Ana Tieweti Djibouti ibukia kain tautaeka** ao te **Botakin Aonnaba ibukin Korakora man te Atom**, ma taekaia iroun WHOIS ao tomein aikai aki-kaikoaki.

Ikotan tomein ni katoto ao tomein aika aki-kaikoaki e kona n tuangira ae iai ae kakaboi-nnen tomein ibukin aia mwakuri taan ioawa aonrain aikai.

Te imeri aetureti ae '**ocean.nio@rediffmail[.]com**' e bon ti kona ni kuneaki n tomein akana i eta. '**ivan_s81@mail[.]ru**' ao '**tplutalova@list[.]ru**' a tia ni karaoi tabeua taian tomein, ao tabeua mai buakon tomein akanne a tia ni kuneaki bwa a tiewa iroun BADBAZAAR. Taian imeri aetureti aika teniua aikai a kakoauaki bwa a nang kakabonganaki ibukin aia mwakuri buaka taan ioawa aonrain. Bukina bwa a rangi ni kakabonganaki riki n tomein ake a kakaraoaki iai taian mwakuri buaka, riki nakon taian imeri aikai '**wangminghua6@gmail[.]com**' ao '**taoyujun@gmail[.]com**'.

(Noona Anekiti A, tamnei 5)

Rinki nakoia taan kakamaku ake tabeman

Anuaia naba tomein ake a rinki ma-BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', ao '**voiceoftibet[.]net**' a karaoaki nte eNom ao a 'kateaki' n '**255.255.255[.]254**'.

Itera ni ba **14** man **15**

Mwiin ana ukeuke NCSC n taai aika nako, ao tomein ake tabeua a kaoti aekan naba anua akekei a rinki naki nakon **APT5** inanon 2019, ao **APT14** i marenan 2009 ao 2011.

Tomein ake a toma ma APT5- iai ana rekoti iai WHOIS are e ataki bwa te imeri ae '**taoyujun@gmail[.]com**' ngaia ae tia kakaraoi imeri.

Tomein ake a toma ma-APT14 iai teniua-reeta nte tiabu-tomein ae tara ni kaota ana takete te mwakuri ni ioawa. Te kabotau iaon aei bon '**bae.cisconline[.]net**', are kaotaki ikai bwa te takete bon ana Tititem BAE are kuneaki n '**Poison Ivy**' katotona.

Aekakin anua aikai a nonoraki n ana tomein BADBAZZAR are tiabutomein a irekereke ma aran burokuraem ake mataroa mai buki:

Atun Burokuraem	C2 URL
Boutokaia Motirim	**mpp**.pmstwocqn[.]com
Bwai n Tamei n Android	**vpf**.titeperformance[.]com
Tomein ae nanonaki riki	**bat**.androidupdated[.]net
Rerio mai Afghanistan	**afg**.collinformations[.]com
EN-UG Tekitinare Akea Boona	**eud**.titeperformance[.]com
Disk Kaokan Birim	**dvr**.collinformations[.]com
TextNgkai	**ttn**.titeperformance[.]com

E rangi ni kakawaki atakin ae mwakuri ake a irekereke ma APT5 ao APT14 a bongata ao iai riki tomein ake a karaoaki man eNOM ao ni katukaki n '**255.255.255.254**' aio are aki kona ni bukinaki ma mwakuri ni ioawa. Ngaia are tiaki kona ni kakoaua raoi bwa aekita ake a kakaraoi kambein aikai a okioki ke iai rekerekeia.

Aran Mitiin

Mwin ukeran BADBAZZAR C2s ao katotona ao e oti ae ara n rinnako akea kabonganaki bwa te 'Common Name' bane n titabo nte SSL beba ni kamano. Kakaean ara n rinnako iroun NCSC ake a nonoraki ni katoton BADBAZZAR ao ni nneia are a mena iai bwa ara n rinnako aikai a kabonganaki n taian IP aetureti aika mwaiti. Taian IP aetureti aikai e kawakinaki iai tomein ake a kuneaki ni katoton

nako BADBAZZAR. A bunraki riki rongorongoia nte mwakoro i nano ibukin ara ni karinrin, ao IP aetureti ake a kawakini ara ni karinrin ibukin ana tomein nako BADBAZZAR C2.

Angin te tai ao ena kaoti te beba ni kamano ma ara n rinako aika a titabo maniia ma IP ibukin nnen bwai n reitaki ibukia aran tomein ake a kaikoaki, a kaotaki naba taai are e aki riki aio.

WIN-EU0VLBL7TUJ

Te ara ae '**WIN-EU0VLBL7TUJ**' e noraki n IP aetureti aika kakaongora aikai:

- '**116.203.53[.]21**' e mena i nanona ana tomein BADBAZAAR C2 aika '**uyapkfinder[.]com**' ao '**thewestuniverse[.]com**'.

- '**95.216.169[.]27**' e mena i nanona ana tomein BADBAZAAR C2 aika '**adysfunction[.]com**' ao tiabu tomein '**download.apkbazar[.]biz**' are nonoraki bwa ngaia te rinki ibukin karuoan katoton BADBAZZAR.

(Noora Anekiti A, tamnei 6)

WIN-70E59JVOB9G

Te ara ae '**WIN-70E59JVOB9G**' e noraki nte IP aetureti aika kakaongora aikai:

- '**23.88.28[.]220**' e mena i nanona ana tiabu-tomein BADBAZAAR C2 aika, '**aua.rondwsign[.]com**', '**nal.tokenmajorp[.]com**', '**pep.rondwsign[.]com**', '**doa.rondwsign[.]com**', ao '**pls.rondwsign[.]com**'. Iai te maen ae uabong imarenan te tai are noraki iai te beba ni kamano ma te mitin, ao ngke tomein ni kaikoaki aikai a noraki n toma nakon te IP.

- '**23.88.28[.]221**' e mena i nanona tiabu-tomein ake a katomaki ma BADBAZAAR '**bt.bhvghg[.]com**'.

- ‘**23.88.28[.]222**’ e mena i nanona tomein ibukin BADBAZAAR C2 ‘**tubevideoplus[.]org**’ ao ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67**’ e mena i nanona tiabu-tomein ibukin BADBAZAAR C2 ‘**bat.androidupdated[.]net**’. E mena naba i nanona te tiabu-tomein aei ‘**apps.androidupdated[.]net**’ ae te Kauatabo n Tibwai ni mwauea C2.

- ‘**65.21.92[.]77**’ e mena i nanona ana tiabu-tomein BADBAZAAR C2 aikai ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ ao ‘**afg.collinformations[.]com**’.

- ‘**65.108.192[.]134**’ e mena i nanona ana tiabu-tomein BADBAZAAR C2 aika ‘**upd.whoscaller.net**’. ao ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ e mena i nanona ana tiabu-tomein BADBAZAAR C2 aika ‘**bvn.lookincategory[.]com**’ ao ‘**edr.lookincategory[.]com**’. Iai te maen ae tebwi ma teuana te bong imarenan te tai are noraki iai te beba ni kamano ma aran te mitin, ao ngke tomein ni kaikoaki aikai a noraki n toma nakon te IP.

- ‘**142.132.131[.]20**’ iai i nanona tiabu-tomein aika ‘**son.onlinegamersgroup[.]com**’ ao ‘**system.onlinegamersgroup[.]com**’, are a kakoauaki bwa taian BADBAZAAR C2s ngkai a kuneaki i nanona ni ikotaki ma SSL beba ni kamano a noraki naba inanon te IP.

- ‘**142.132.131[.]28**’ iai i nanona ana tomein BADBAZAAR C2 ae ‘**goldplusapp[.]net**’ ao tiabu-tomein aika ‘**who.goldplusapp[.]net**’ ao ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ iai i nanona ana tiabu-tomein BADBAZAAR C2 aika ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net**’, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, ao ‘**aar.alpinemap[.]net**’.

- ‘**162.55.103[.]212**’ iai i nanona ana tiabu-tomein BADBAZAAR C2 aika ‘**pep.rondwsign[.]com**’, ‘**ckp.jkiohreh[.]com**’, ‘**aar.tokenmajorp[.]com**’, ‘**nal.tokenmajorp[.]com**’, ‘**pls.rondwsign[.]com**’ ao ‘**aua.rondwsign[.]com**’.

- ‘**195.154.47[.]99**’ iai i nanona ana tiabu-tomein BADBAZAAR C2 aika ‘**ggl.whoscaller[.]net**’ ao ‘**upd.whoscaller.net**’. Iai te maen ae tenibong imarenan te tai are noraki iai te beba ni kamano ma aran te mitin, ao ngke tomein ni kaikoaki aikai a noraki n toma nakon te IP.

- ‘**195.154.60[.]3**’ iai i nanona ana tiabu-tomein BADBAZAAR C2 ae ‘**upd.whoscaller[.]net**’ ao ‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ iai i nanona ana tiabu-tomein BADBAZAAR C2 aika ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ ao ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ iai i nanona ana tomein BADBAZAAR C2 aika, ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ ao ‘**bvn.lookincategory[.]com**’.

(Noora Anekiti A, tamnei 7)

WIN-50QO3EIRQVP

Aran te tiewa ae ‘**WIN-50QO3EIRQVP**’ e noraki n IP Aetureti aika kakaongora aikai:

- ‘**45.76.132[.]91**’ iai i nanona tomein aikai, ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. Tomein aika uoua aikai a toma ma BADBAZAAR bwa taian tiabutomein ‘**fow.yumoftion[.]com**’ ao ‘**bat.androidupdated[.]net**’ ma bon taian tomein man BADBAZAAR C2. Irarikin anne ao te tiabu-tomein ae ‘**apps.androidupdated[.]net**’ bon te C2 tomein ae Kauatabo nTibwai. Ao iai naba i nanona te tomein ae ‘**pmstwocqn[.]com**’, ae toma ma BADBAZAAR rinanon ana rekoti WHOIS.

- ‘**95.179.210[.]85**’ iai i nanona ‘**clublogs[.]com**’, mai iai e reke ‘**xle.clublogs[.]com**’ ae ana tomein BADBAZAAR C2 ae iai naba inanon tomein ake a toma ma BADBAZAAR n aron ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, ‘**www.voiceoftibet[.]net**’ ao ‘**actuallys[.]com**’.

- ‘**199.247.21[.]34**’ iai i nanona ‘**titeperformance[.]com**’, ao ‘**collinformations[.]com**’ are taian sub-tomein iai bon taian tomein man BADBAZAAR C2.

- ‘**217.69.10[.]128**’ ana tiewa te tomein BADBAZAAR C2 ‘**uyghurdict[.]com**’.

(Noora Anekiti A, tamnei 8)

WMSvc-WIN-50QO3EIRQVP

Te ara ae ‘**WMSvc-WIN-50QO3EIRQVP**’ e noraki n IP aetureti aika kakaongora aikai:

- ‘**78.46.185[.]251**’ iai i nanona ana tomein BADBAZAAR C2 ae ‘**groupgram[.]org**’, are ribotinaki iroun Volexity bwa e kakabongana te botu ae 4432 ibukin katomatoma aika kaikoaki.

- ‘**65.21.92[.]69**’ ao ‘**163.172.205[.]207**’ e mena inanoia te tomein ae ‘**widelygram[.]org**’ are kakoauaki bwa te tomein man BADBAZAAR C2, ian ae ngkai a mena i nanona ao te botu 4432 e uki.

- ‘**163.172.198[.]206**’ iai i nanona te tomein ae ‘**maxgram[.]org**’ are kakoauaki bwa te tomein man BADBAZAAR C2 , ian ae ngkai a mena i nanona ao te botu 4432 e uki.

(Noora Anekiti A, tamnei 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Taian ara aika ‘**WMSvc-WIN-50QO3EIRQVP**’ ao ‘**WIN-7LSBB9R0F1L**’ a noraki nte IP aetureti aio nte tai ae ti teuana:

- ‘**148.251.87[.]245**’ e mena i nanona ana tomein BADBAZAAR C2 ‘**flygram[.]org**’ ao ‘**groupgram[.]org**’.

(Noora Anekiti A, tamnei 10)

WIN-N8H8S9BG2P0

Te ara ae ‘**WIN-N8H8S9BG2P0**’ e noraki nte IP aetureti aio:

- ‘**148.251.87[.]247**’ e mena i nanona ana tomein BADBAZAAR C2 ‘**omarwhatsapp[.]org**’ ao ‘**flygram[.]org**’.

(Noora Anekiti A, tamnei 11)

WIN-I6VBN8MR92A

Te ara ae ‘**WIN-I6VBN8MR92A**’ e noraki nte IP aetureti aio:

- ‘**148.251.87[.]197**’ e mena i nanona ana tomein BADBAZAAR C2 ‘**tryhrwserf[.]com**’.

(Noora Anekiti A, tamnei 12)

Man rongorongo aika kaboaki ao okiokin aran mitin aikai aonrain e kakaokoro mwaitiia. Tabeua mai buakoia a noraki n teuana te tai inanon IP aetureti aika kakaokoro are kaotia ikai bwa VMs a karaoaki man te tabo ae ti teuana. E kakawaki atakin ae ibukia tabeua ara ibukin rinnako, ao tiaki ni kabane IP ake a noraki iai a rekereke ma karaoan mwakuri ni kaikoaki. Nanona ngkanne bwa kabonganan ara n rinnano aikai tiaki ti ibukin karaoan kakamaku irouia aekita aikai.

Ma, okiokin ara n rinnako aikai n aran mitin n taian IP ake a mena i nanona ana tomein BADBAZZAR C2, e kona n tuangira te tia-kaboi e kabonganaki bwa ena kangaraoi mitin ibukin boutokan aia mwakuri ni kaikoaki taan ioawa aonrain.

Rokon Tabo n Reitaki

Riboti man Volexity e kaotia ae birim iaon YouTube (ake a kaungai kabonganan burokuraem aika kaikoaki) a kakaraoaki irouia taan kaikoaki aonrain. Birim aikai a airi ma reirei iaon kabonganan burokuraem ake a karaoaki.

Te NCSC ea tia ni kunei uoua riki Youtube akaunti ake a irekereke ma aia mwakuri taan aekitan te kakamaku aikai. Te YouTube akaunti ma ana URL te tia mwakuria

ae '**@josephjoey3499**' e tara ni kaungai kabonganan '**Maxgram**' ao iai riki te akaunti ae karaoaki iroun '**@uyghurapks3096**' ae kaunga kabonganan '**Uyghur APK Finder**'.

I rarikin anne ao, birim nte YouTube videos ake a katanoata '**Flygram**' ao '**Signal Plus**', showed the threat actors using visible phone numbers. Inanon te '**Flygram**' birim, nte tai ae 0:36 nambwan te tareboon ae '**+1 (570) 378-7250**' e kona n noiraki ao n tain te **Signal Plus**' birim, e kaotaki nambwan tareboon ae'**+1 (267) 298 4259**'.

Volexity e ribotini kewe man tabo ni kareke rongorongore ake a kaineti ma-Tibet ae '**ignitetibet[.]net**', are a kunea nte Telegram akaunti are a kakoauaki bwa a mwakuriaki irouia aekita ni kakamaku. Te imeri aetureti ae '**choekyi.wangmo@ignitetibet[.]net**' e nonoraki ni karaoi ana bwaebwaeti iaon katokatoka nte tomein ae '**tibetone.org**' are ea tia n ribotinaki nakoia aomata iroun Lookout bwa te C2 ae kabonganaki ibukin kabonganan BADBAZAAR iaon te iOS.

Te imeri aetureti aio e kakoauaki bwa a tauaki-taekaia irouia aekita, mani kabonganan te aomata ae '**Choekyi Wangmo**'.

Te Tutuo

BADBAZAAR ao MOONSHINE a kabonganai anga n bita aia iango aomata tabeman ibukin taketenakia taian Uygur, kain Tibet ao kain aiwan, araia:

- karaoan mataroa mai buki iananon burokuraem ake a nano iai koraki aikai, n aron te burokuraem ao Quran nte taetae ni Uygur, e bon ataaki bwa a karaooaki ibukia nake a taketenaki
- karinan mataroa mai buki aikai nanon titoan burokuraem ena bon karekea te iango bwa a kinaki, ao tibwatibwana n taabo ni maroro bon aia anga n aonikaia tangirakia irouia te koraki aikai

BADBAZAAR ao MOONSHINE a rikoi rongorongo ake ana bon nang bongana nakon te tautaeka n China. E ngae ngke BADBAZAAR ao MOONSHINE a tia n nooraki n taketenia taian Uyghur, ao kain Tibet ma Taiwan iai riki tabeua mwauea aika a taketenia koraki aika uarereke mwaitia iaon China. Aomata ake a irekereke-abaia, iaon China ao i tinaniku, ake a taraaki bwa a boutokai waaki aika ana karaoa te kanganga nakon raun te tautaeka, ngaia aika ana bon reke ni kakamaku n taian mwauea nte tareboon aika BADBAZAAR ao MOONSHINE. Aia konabwai n anai mwin am tabo, bwanaa, ao tamnei e kakoauaki bwa ena manga kangaraoa aron kakae ao karaoan mwakuri n aki rau n tai aika i mwaira man katauraoan rongorongo aika boni ngkai-naba nakon ana mwakuri ake a taketenia.

MITRE ATT&CK®

Te riboti aio e karaoaki ni kangaraoaki ma te tein te MITRE ATT&CK®, nnen te rabakau ibukin taobaran aia anga taan ioawa ae boboto iaon bwai aika nonoraki-aonnaba.

Angana	ID	Karaoana	Kawaina
Taukiroo	T1593.001	Search Open Websites/Domains: Taa bo n Reitaki	Actors find online groups and forums matching their intended victims to share the malware
Karikirakean Ritioti	T1583.001	Karekei Kateitei: Taian Tomein	Akita a karaoi taian tomein ibukin kairiran ao taubeakinan tiewa
Karikirakean Ritioti	T1587.001	Karikirakean Konabwai: Mwauea	Manin burokuraem aika kaikoaki a koreaki ibukin karinaia inanon burokuraem aika mataroa mai buki.
Karikirakean Ritioti	T1608.001	Karinan Mwauea: Katamwarakean Mwauea	Burokuraem aika mataroa mai buki a katamwarakeaki nako aonrain ni ikotaki ma titoa ni burokuraem
Karikirakean Ritioti	T1585.001	Karaoi Akaunti: Akaunti ni Bwai n Reitaki	Aekita a karaoi akaunti iaon uebutiaiti ao taabo n reitaki ibukin tibwan ao katanoatan te mwauea
Karikirakean Ritioti	T1585.002	Karaoi Akaunti: Imeri Akaunti	Aekita aikai a kakabonganai oin aia imeri ao imeri ake a kaboaki ibukin kawakinan ao tibwan te mwauea
Moan Rinnakoana	T1189	Karuoan-mwauea ni Urubwai	Manin burokuraem ni kaikoaki a karabaki inanon burokuraem aika kinaki ao mai ikanne a karinaki inanon titoa ni burokuraem.
Moan Rinnakoana	T1566.003	Katairake: Katairake ni kaikoaki nte imeri tieweti	Aekita a kakanakoi burokuraem ake mataroa mai buki n taketenia kurubu man bwai n reitaki aonrain ao Telegram

Katiana	T1204.002	Aron Karaoana: Rongorongo aika Kaikoaki	Nake a mwane a riai ni karuoi burokuraem ake mataroa mai buki ni kaotinakoan kanoana
Ekinakoan Totoko	T1027.009	Kamangaoan Bwaera ao Rongorongo: Kanoana ake i nanona	Kanoana are kaikoaki e karabaki inanon burokuraem ake a bon kinaki
Ekinakoan Totoko	T1036.005	Katotonga: Katitaboi ma Oin Ara ao Tabo	Rongorongo ake a riki bwa mataroa mai buki titabo araia, teia ao mwakuria ma burokuraem ake a bon kinaki.
Ekinakoan Totoko	T1656	Katotongaia aomata	Aekita aikai aki toki ni katotongia aomata ake a kinaki man karaoakin uebtiaiti ao ara ake a rekereke ma kurubu ake a teketeni
Te Boota	T1123	Rawe Bwana	Burokuraem ibukin karinrin mai buki a kona ni bubuti tokobitoan te mwaiki.
Te Boota	T1125	Rawe Birim	Burokuraem ibukin karinrin mai buki a kona ni bubuti tokobitoan te kaemera
Te Boota	T1005	Rongorongo man tititem i nanoa	Burokuraem ibukin karinrin mai buki a kona ni bubuti tokobitoan rongorongo ake ibukin maiun te kombiuta.
Kairiran ao Taubeakinan	T1071.001	Tuan te Reitaki i marenan Burokuraem: Tuan te reitaki Aonrain	Mwauea a toma nakon C2 man kabonganan HTTPS ao toman tiewa.
Kairiran ao Taubeakinan	T1509	Tiaki-Oin Botu	Tiaki Oin botu a kakabonganaki n aron botu 4432 ao 2333
Kimoan rongorongo	T1041	Kimoan rongorongo Rinanon C2.	Mwauea a kaotinakoi rongorongo mani kabonganan HTTPS ao man toman tiewa.
Ana Urubwai	T1565.002	Kunimwanian rongorongo: Kunimwanian rongorongo aika Maiu	Aekita a kakarekei rongorongoia konaia man kamaeuan burokuraem ake aki rangi ni kainanoaki ibukin mwakurin te burokuraem.

Kanikina

MOONSHINE:

- N 1 n Eberi 2025, kakae aonrain ibukin VLITEUI e kaoki aikai:

IP Aetureti	Botu	Moan Norana	Kabanean Norana
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

- N 1 n Eberi 2025, ao te kakae iaon te baeno ae SCOTCH ADMIN e kaoti aikai:

IP Aetureti	Botu	Moan Norana	Kabanean Norana
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

- N 14 ni Maati 2024, ao te kakae iaon te baeno ae SCOTCH ADMIN e kaoti aikai:

Tomein	IP Aetureti
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:

Te Kabwarabwara	SSI beba ni kamano a noraki iaon BADBAZZAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- N 1 n Eberi 2025, ao te kakae iaon ana beba ni kamano BADBAZZAR ane i eta e kaoti aikai:

IP Aetureti	Botu	Moan Norana	Kabanean Norana
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

Te Kabwarabwara	SSL beba ni kamano ae nooraki iaon BADBAZAAR C2s
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- N 1 n Eberi 2025, ao te kakae iaon ana beba ni kamano BADBAZZAR ane i eta e kaoti aikai:

IP Aetureti	Botu	Moan Norana	Kabanean Norana
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

- Tomein man WHOIS

I nano bon te taibora ibukin tomein ake iai ngkoa ao ake iai ngkai aia rekoti n WHOIS ma kanoaia ae titabo ma ake a nonoraki n ana tomein BADBAZAAR C2.

Kanoan WHOIS	Taian Tomein
Mwakoro are Karaoaki iai: UJYJYUJ **Te Aba are Karaoaki iai: Bolivia** **Tia Kabaeara: 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
Mwakoro are Karaoaki iai: REWR **Te Aba are Karaoaki iai: CF** **Tia Kabaeara: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

Mwakoro are Karaoaki iai: FSDF **Te Aba are Karaoaki iai: AL** **Tia Kabaeara: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

Imeri Aetureti
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

Taian rinki aikai a nakon taboo ni kamatata ibukin kinakin anga ni kamwane (IoCs) aika rekereke ma BADBAZAAR ao MOONSHINE. Te NCSC e aki kona ni kamatoai raoiroin rongorongo aika n rinki aikai ao a kaungaki taan wareware bwa ana ukeri i bon irouia etina ao riaina.

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

Kaokan arona

Te NCSC e kaungai karaoan taeka ni bau aika i nano ibukin kamanoam man kakamaku ake a kabwarabwaraki n taian katoto tabeua.

- **Taan taui mwin titoa ni burokuraem, ni ikotaki ma titoa ni burokuraem ake tabeua, a riai n ataia ae burokuraem ake irouia a mano ao a irii nanon Anua ni Mwakuri man te tautaeka.** Noora te Kamatata: 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

- **Mwaiti-taetae aika boutokaki**: Taan karaoi burokuraem a riai ni karaoi burokuraem ake a rangi ni kakabonganaki ena boutokai taetae aika mwaiti n aron te taetae ni Uyghur, taetae n Tibet, taetae n Taiwan Hokkien ao te Cantonese. Ana kamatata Apple ibukin karaoan burokuraem aika onoti: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Ana kamatata Google iaon burokuraem n raitaeka: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Kawakinan am bwai n reitaki aonrain bwa ana mano:** Kambwana ibukin reitaki aonrain a kona ni kamatoai angan rinia taan ioawa aonrain man aki kariaiakan akaunti ake a titibai rongorongo aika kaikoaki ke rinki nakon tabo n reitaki aika aki kinaki. Ngkana e kona, ao kambwana a riai n tibwai aron kinakin bwai n tokobito aonrain ma raoia ake tabeman e aonga n ae mwaiti te atatai ao te kona n totoko ao ni kamano.

- **Barongan mwakuri ni katamaroa ibukia katitamwa:** Boboti a riai ni iai irouia kawai ibukin kauringaia katitamwa ake a tia ni karuoi burokuraem ake a kaikoaki ao ni kabonganai aia tieweti. Kauring aikai a riai n rangi ni katitika ao ni bwarabwara raoi. Ngkana e riai, ao boboti a riai ni karaoi kamatata iaon aron kanakoan burokuraem ao ni kaungaia nake a mwane bwa ana riboti nakoia ake tabeia, n aron te NCSC nte UK.

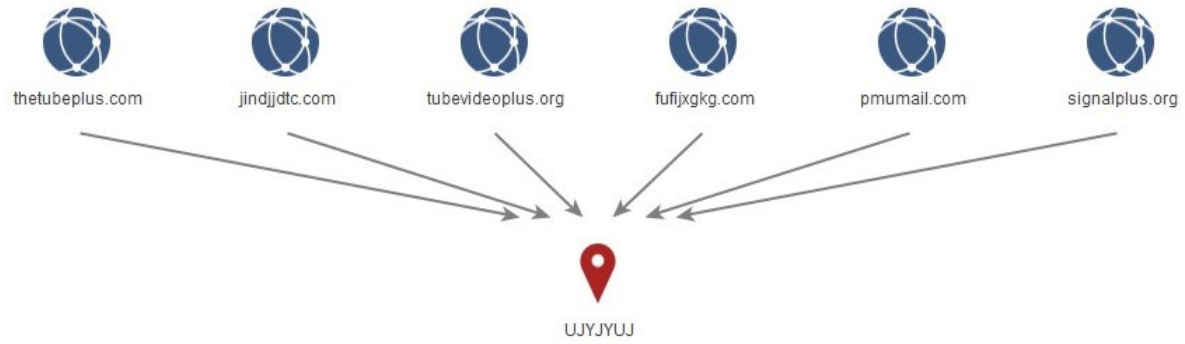
Noora te Titoa n Burokuraem ibukin Anua ni Mwakuri ibukin riki rongorongona: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Kurubu ni mwakuri ibukin te reitaki:** Kambwana ibukin te reitaki a kona ni karaoi aia kurubu ni mwakuri, ao ni kariaia bwa ana ibuobuoki n tabwai aron kinakin bwai ni kaikoaki, TTP ao kukune, e aonga ni kanganga ni karaoaki te kaikoaki n aia bwai n reitaki.

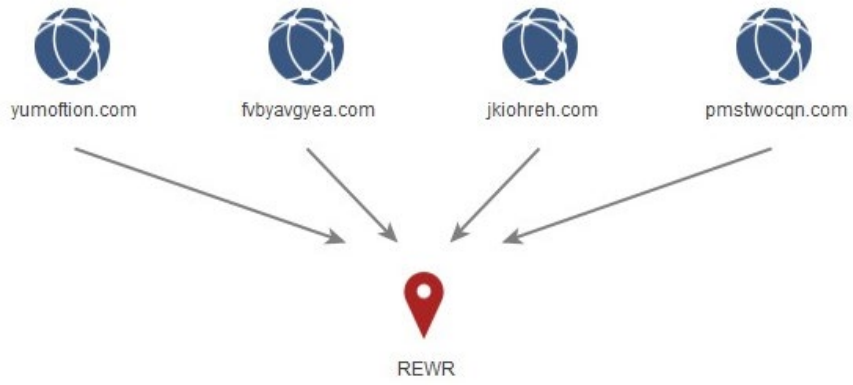
- **Kakaean burokuraem aika bitaki:** Ngkana e kona, taan karao burokuraem a riai ni kairi anga ake a kona n tuangia ake tabeia te kamano ngkana e karuoaki burokuraem ake 'aki kinaki', ibukin kamanoaia man bwai ni kaikoaki.

Abentekiti A: Tein bannan ibetutun BADBAZZAR WHOIS / rongorongo man tabo ni kabo tomein

Tamnei 1 - 'UKYJYUJ'

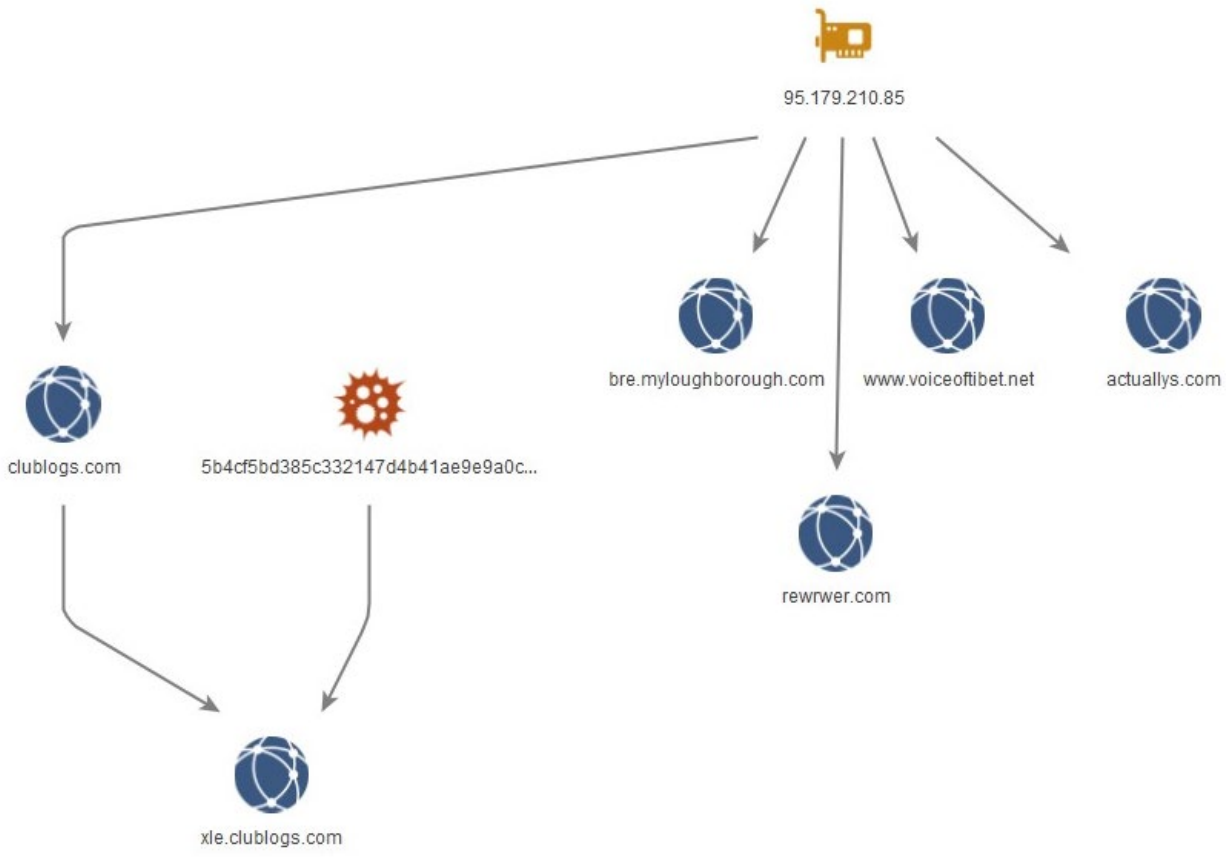


Tamnei 2 –Mwiin kakaean taeka aika raba nte kibooti

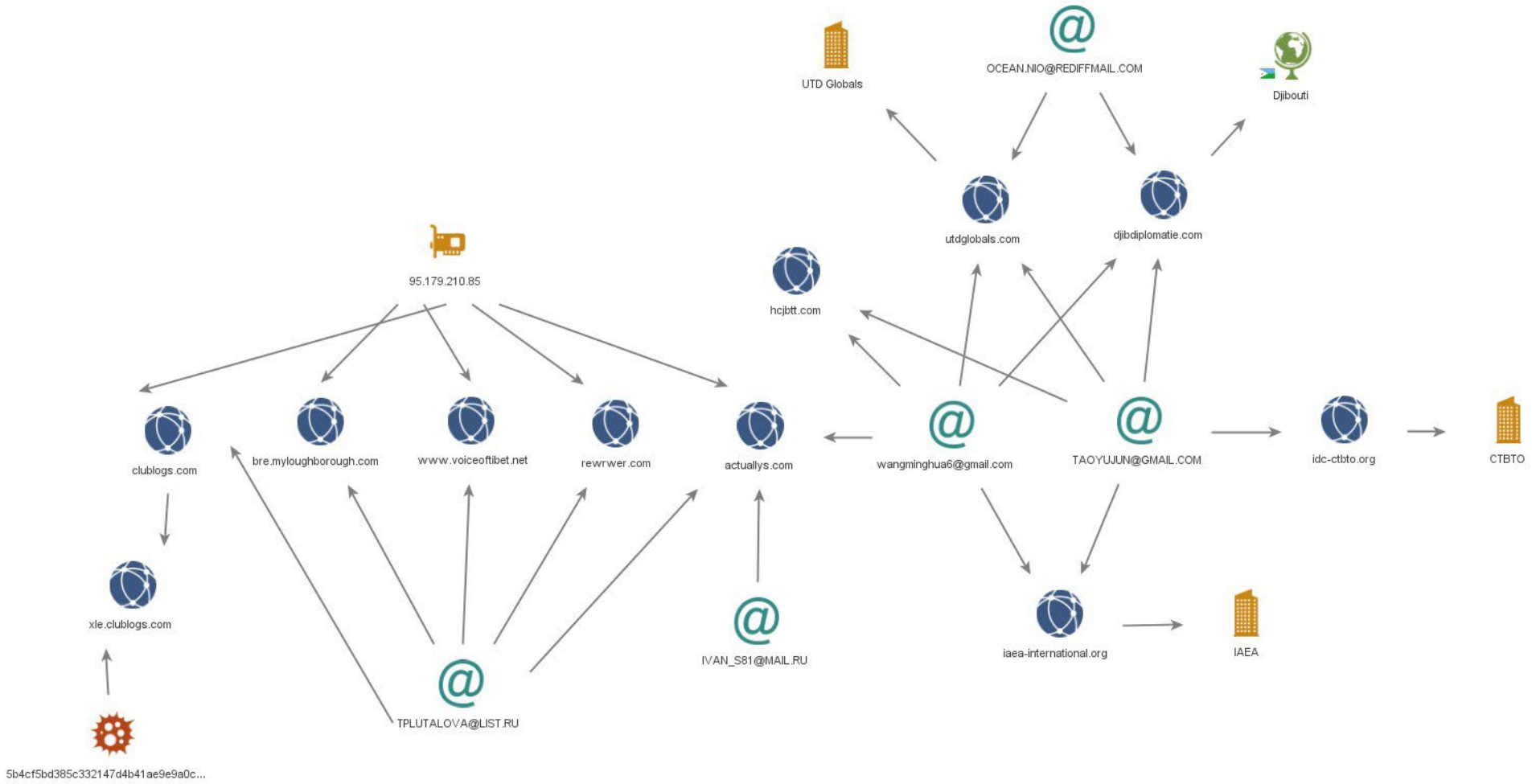


Tamnei 3 – Tomein riki ake iai 'FSDF' ibuakon kanoan te mwakoro

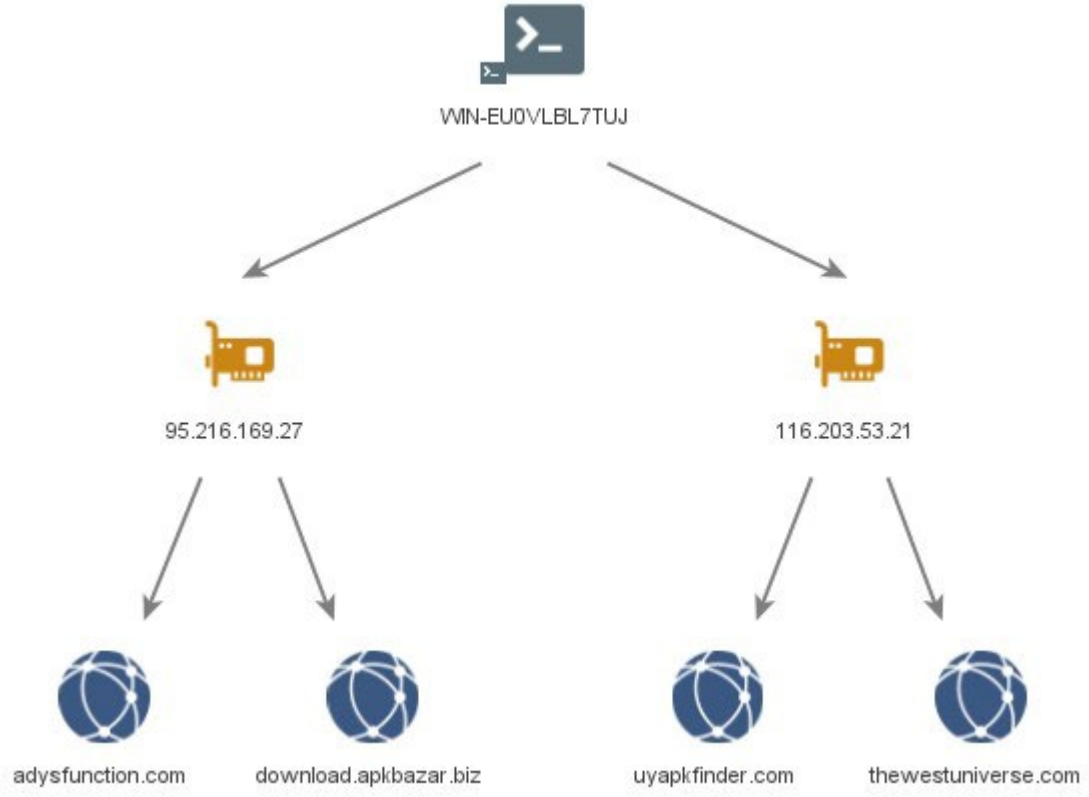
Tamnei 4 – **95.179.210[.]85**



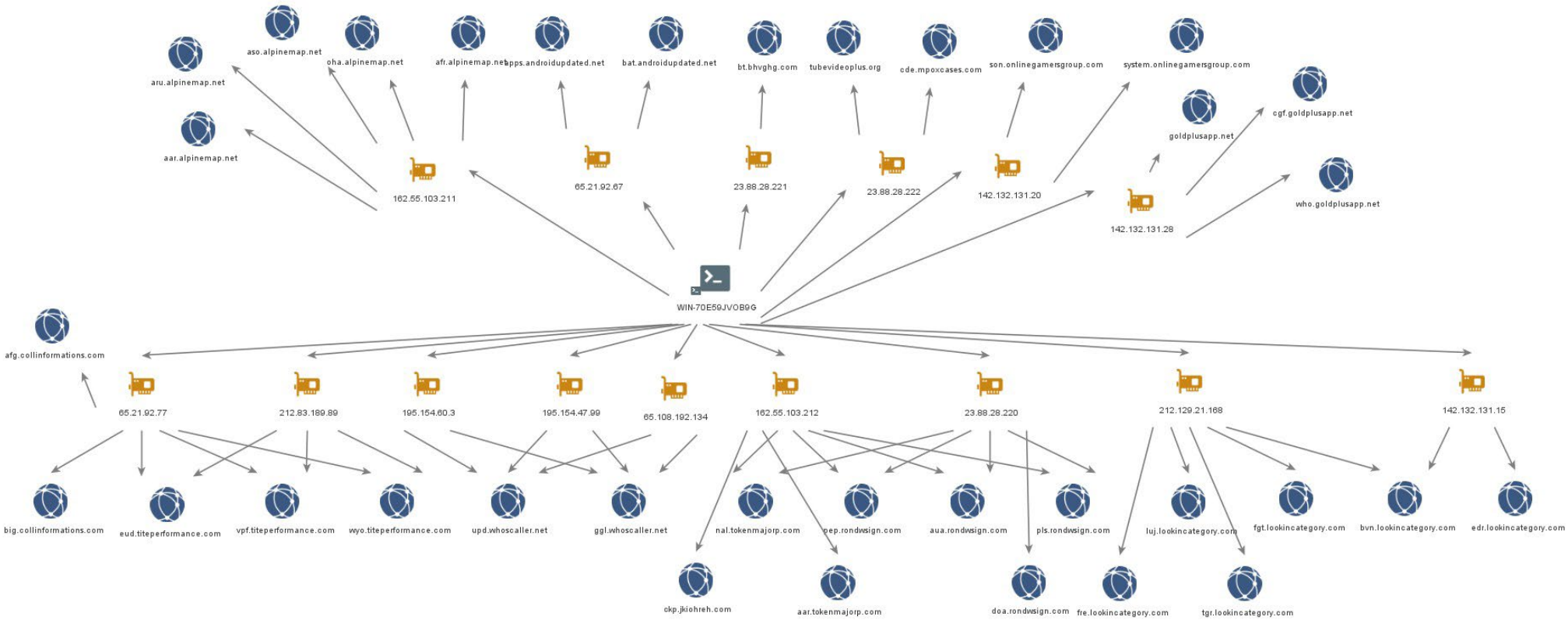
Tamnei 5 – WHOIS rinki



Tamnei 6 – **WIN-EU0VLBL7TUJ**

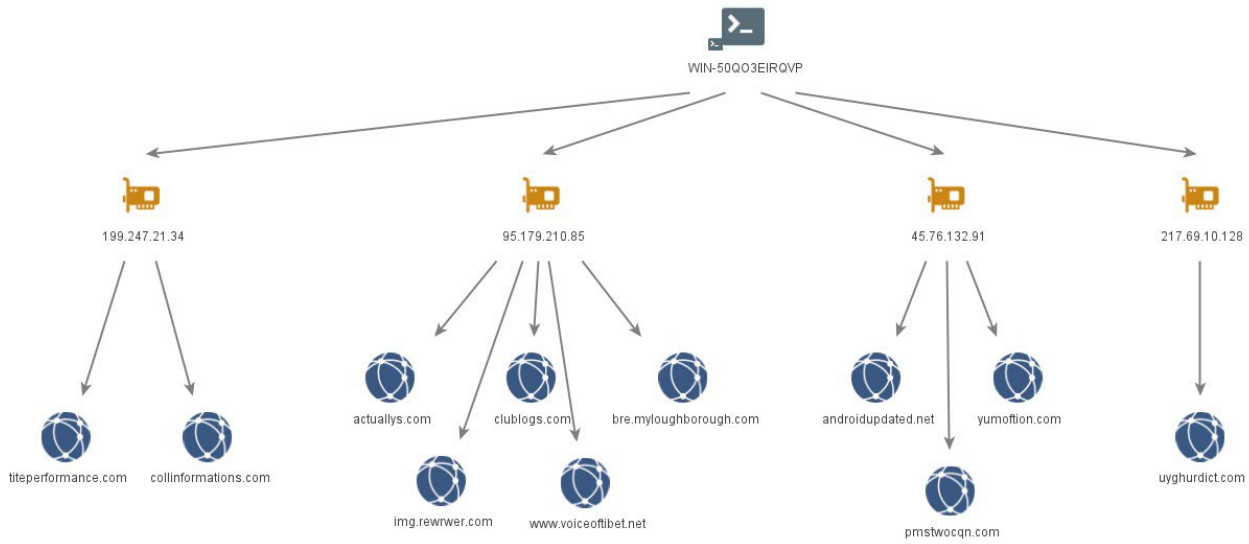


Tamnei 7 – **WIN-70E59JVOB9G**

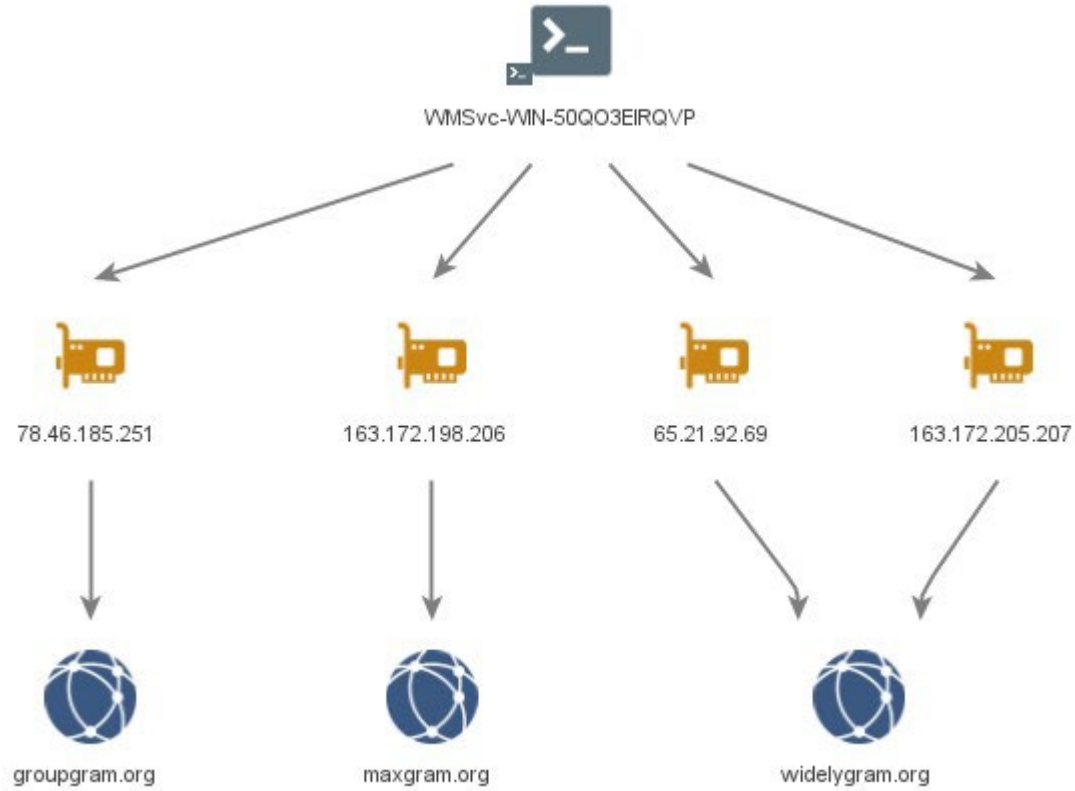


Itera ni ba **37** man **38**

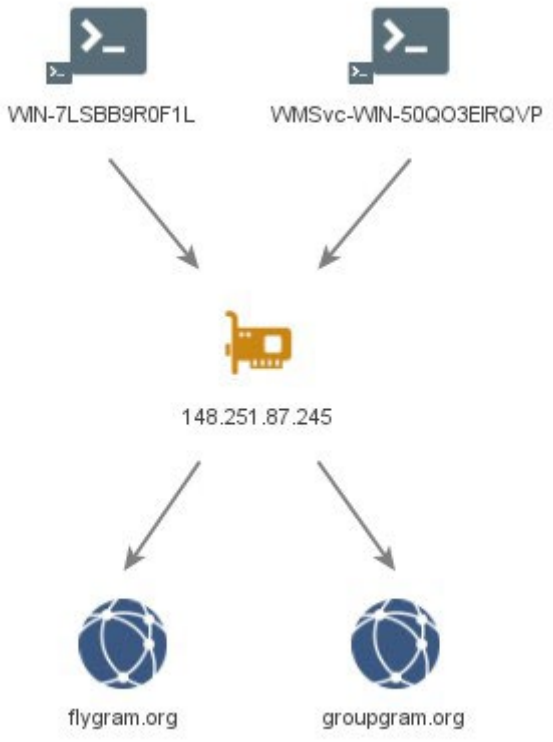
Tamnei 8 - **WIN-50QO3EIRQVP**



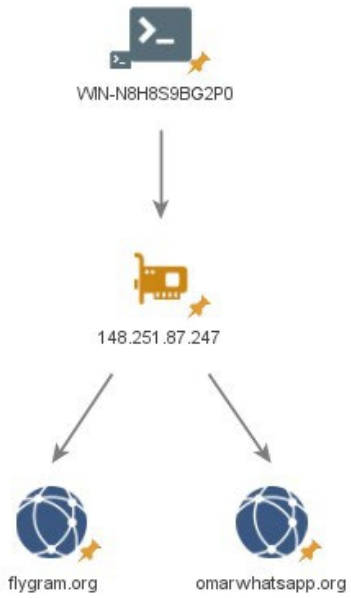
Tamnei 9 - **VMSvc-WIN-50QO3EIRQVP**



Tamnei 10 – **VMSvc-WIN-50QO3EIRQVP** ao **WIN-7LSBB9R0F1L**



Tamnei 11 - **WIN-N8H8S9BG2P0**



Tamnei 12 – **WIN-I6VBN8MR92A**

Abentekiti B: MOONSHINE & BADBAZAAR tarakin katoto tabeua

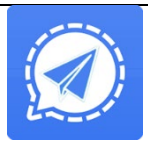
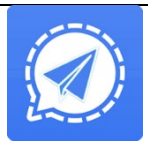
Te taibora ae i nano e karinani burokuraem ake a kabonganaki n ana kaembein MOONSHINE ao BADBAZAAR inanon uoua te ririki n nako.

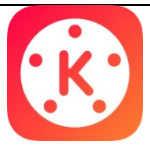
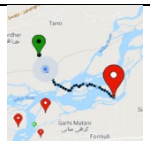
Angin burokuraem aikai a koata aron titaboia ma burokuraem ake a bon kinaki. E katautauaki aio bwa aia mwakuri naba aekita aikai n 'kaewei' kanikinaean karaobwai ake a nang-kinaki.

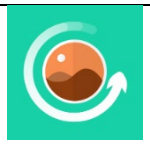
E kakawaki atakin ae, aran burokuraem, aran bakete, ao kanikinaean burokuraem a kona ni katotong ke ni katitaboaki ma ake bon oi ni burokuraem ao ea riai ngkanne n aki ti kabonganaki ibukin atakina bwa e man aoraki te bwai n reitaki ke aki.

Atun Burokuraem	Aran Bakete	Kanikinaean Burokuraem
99 Tikin Aran 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	
Kibooti n Arabia	com.arabic.keyboard.arabic.language.keyboard.app	
Bwain Korean Bwanan Birim	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Kunaia Buddhist (1)	com.bigkidsapps.buddhistsongs1	
Kaokureita	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Tekitinare Akea Boona	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

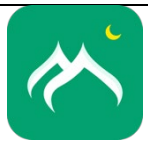
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
Tia Barongai Rongorongo +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Wifi Akea Boona	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Koran	com.golap.hefzquran	
Hijri Karenta	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	

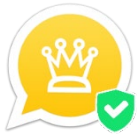
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
Korean MP3 & Tia Karaoi Tangin Tareboon	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Kakaean Abwaki nte Mwabe	com.routemap.mapdownload.gpsroute planner	
Kaokan Tamei Birim ao Anene	com.aaa.media.recovery.androidapp	
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	
Bwain Kunimwanian Tamnei	com.iudesk.android.photo.editor	
Kaokan Tamnei	recover.restore.undelete.photo.video.file	
Tabo n Rawe Tamnei	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Boki n Tataro	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Koraan	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Kaokan Tamnei ake a Kamaunaki	com.restore.deleted.pictures.video	

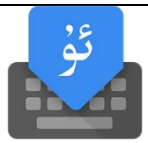
Tikino	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	

Telegram X	org.thunderdog.challegram	
Tititem ibukin Atakin Taai aika ana Roko i Tibet MO	net.rhombapp.mo	
Tataro n Tibet	com.chorig.tibetanprayer	
Te tia Raitaeka AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Kibooti n Uyghur	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Onei Tamei	com.inverseai.video_converter	
Korei Tamei	com.naing.cutter	

Karuoan Tamei	downloader.video.download.free	
Karao Birim	com.bstech.slideshow.videomaker	
Bwai n Tamei n Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Bwai n Rawe Bwana	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Taraan Kanoan Bong	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	
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	

Wareware Riki

Kamatata man ana Botaki ni Kamano Iaon Intanete mai Aotiteria

- Riboti iaon te kakamwarua nte intanete, kanganga ao memere
- Arom ni kamanoi am bwai n reitaki
- Kamanoa am tareboon
- Katairake
- Kewe
- Kamanoi am tabo n reitaki
- Kawai ni kamano ibukin bwai n reitaki ao burokuraem ni maroro

Kamatata man te UK NCSC ao NPSA

- Katanan te Tautaeka ni inaomata
- Tabo n reitaki: aron kabonganana ae mano
- Kamatata iaon kamanoan bwai n reitaki ibukin boboti ao tareboon
- Riboti iaon kakamakun titoa ni burokuraem.
- Maurim ao kamanoam ngkoe are ko kai-rotaki

Kamatata man te US NSA

- Aron Kabonganan am Tareboon ae tamaroa

Otanga

Taiaoka ni uringnga ae kamatata aikai e katauraoi rongorongo aika a koaua nte tai are a boretiaki iai.

Te riboti aei e anaki man rongorongo mairouia taan anga kariaia ao taian kambwana. Taian kukune ao taeka ni buobuoki aika a karaoaki aki katauraoaki ma te kantaninga bwa ena totokoi anga ni kaikoaki ao iran taeka n buobuoki aikai e aki kona ni kauarerekei ananga ni kaikoaki. Te bwaibwai n rongorongon kaikoaki e tiku i nanon bain te tia bwaibwai nte tititem ni katoa tai.

Nte UK, ao rongorongo aikai tiaki kona n bukintaeka iai iaan te Tua ae Inaomatan te Kareke Rongorongo 2000 (FOIA) ao ti kona naba n aki kona n rotaki iai iaaan te tua ibukin rongorongo nte UK.

Noora FOIA titiraki nakon ncscinfoleg@ncsc.gov.uk.