National Cyber Security Centre
a part of GCHQ

S

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

Advaesori

BADBAZAAR mo MOONSHINE: Teknikol analasis mo mitigesen

9 Eprel 2025

BADBAZAAR mo MOONSHINE: Teknikol analasis mo mitigesen

Samari

Wetem sapot blong UK Saeba Lig, advaesori ya National Cyber Security Centre (NCSC UK) i bin joen blong prodiusum mo ol intanasonal patna:

- **Australia Saeba Sekiuriti Senta, pat blong Australian Signol Daerektoret**
- **Canadian Senta blong Saeba Sekiuriti, pat blong Komunikesen Sekiuriti Establismen**
- **German Federol Inteligens Seves**
- **German Federol Ofis blong Proteksen blong Konstitusen**
- **New Zealand Nasenol Saeba Sekiuriti Senta, pat blong Gavman Komunikesen Sekiuriti Ofis**
- **United States Federol Ofis blong Investigesen**
- **United States Nasenol Sekiuriti Ejensi**

Advaesori ya i givim niu mo oda tret inteligens long tu fom blong spaewea we hemi BADBAZAAR mo MOONSHINE, mo i gat advaes blong app stoa opereta, developa mo sosol media kampani blong kipim ol yusa i sef.

Advaesori ya oli bin pablisim wetem wan advaesori blong ol viktim blong ol malwea ya.

Dokumen ya i yusum glosari defenisen blong NCSC spyware: “Wan kaen malwea we i instol long wan divaes witaot consent blong yusa, we i kolektem data mo afta sendem i go long nambatri pati.”

Keis stadi wan: MOONSHINE

MOONSHINE hem i wan Android spaewea we oli ripotem long 2019 tru long Citizen Lab we i tagetem Tibetan grup. MOONSHINE i jenisim hem olsem wan app blong pulum ol viktim blong instolem hem. Oli bin serem hem tru long Telegram janel mo tru ol link blong WhatsApp.

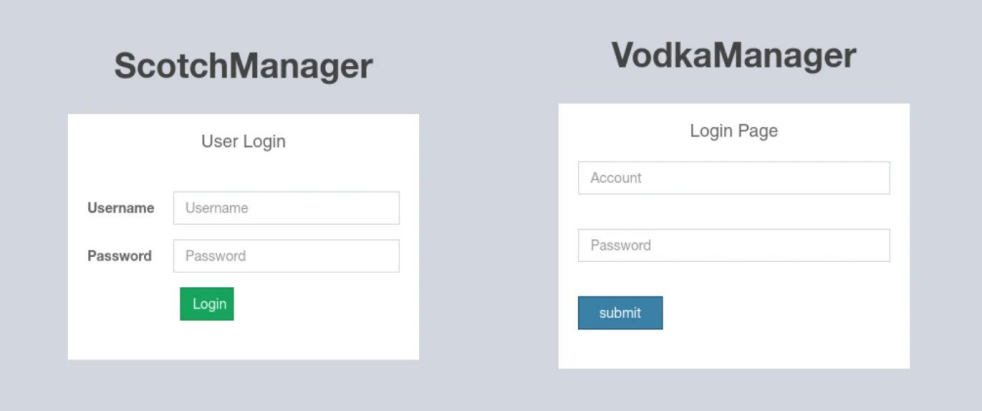
NCSC risej dip insaed long MOONSHINE mo talemaot se:

- MOONSHINE i yusum manejmen intafes we i bin go tru long ol jenis long stat we oli bin ripotem.
- Manejmen intafes ya i bin soem sam bigfala seveliens paoa, we i gat paoa blong witdroem ol fael aot long ol divaes mo kapjarem laef odio mo skrin rekoding.
- Wan set blong vituol manejmen intafes we MOONSHINE i bin hostem oli jes faenemaot. Ol intafes ya i gat infrastrakja we i krosem login panel we i joen wetem UPSEC, we i folem Intelligence Online i minim 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Manejmen intafes

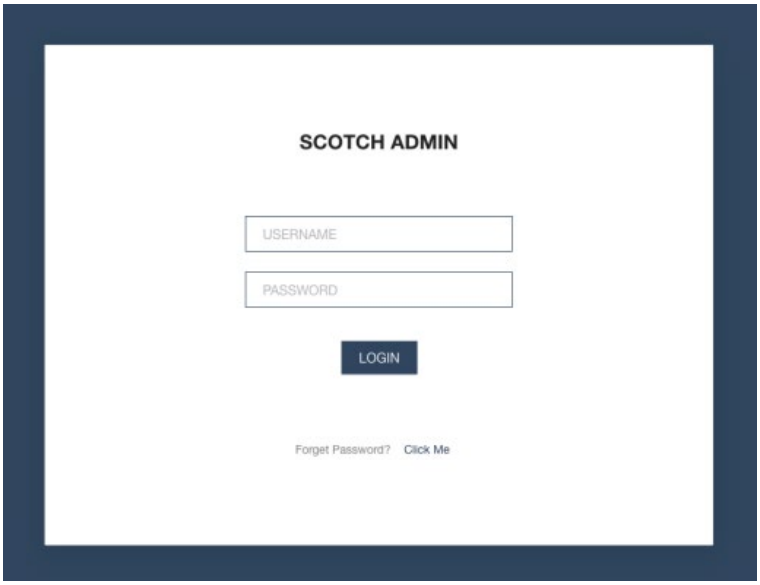
Ripot blong MOONSHINE manejmen intafes we i jes hapen i soem se hemi bin go tru long sam jenis, we i minim hemi stap develop yet.

Fas eksampol blong manejmen intafes oli faenem long Citizen's Lab's 2019 ripot.



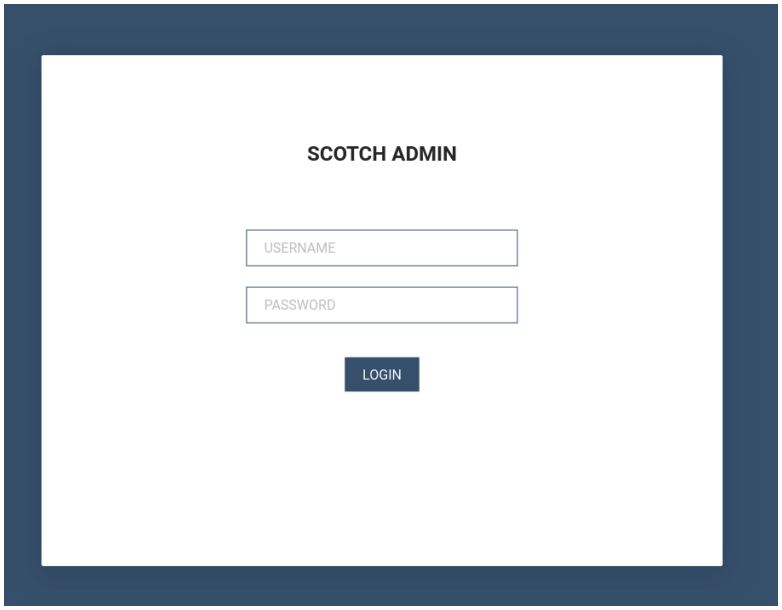
Pikja 1: MOONSHINE manejmen intafes we oli luk long Citizen Lab 2019 ripot 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'.

Long eli 2022, Lookout i bin ripotem wan defren manejmen intafes we oli bin ridisaenem blong luk olsem hemia andanit (i jenisim fas intafes long pikja 1):



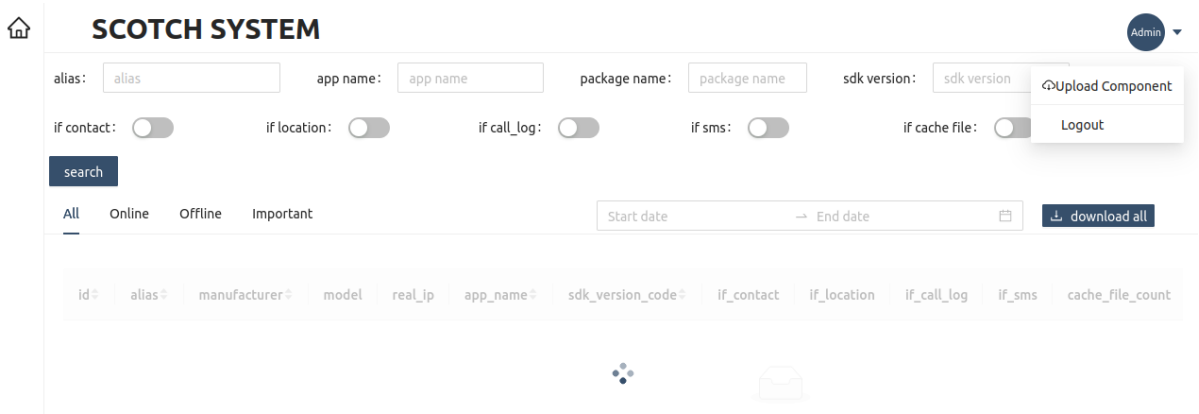
Pikja 2: MOONSHINE manejmen intafes we oli luk long Lookout 2022 ripot 'MOONSHINE: Evolving Android Surveillanceware tru long Chinese APT POISON CARP To Target Tibetans and Uyghurs'.

Long Ogis 2023, wan skan blong MOONSHINE koman mo kontrol (C2) we i soem wan intafes we i semak long intafes blong 2022 wetem '**Forget Password**' fangsen we i nomo avelebol olsem we i stap long pikja 2:



Namba 3: MOONSHINE manejmen intafes we oli faenem long Ogis 2023 we i nomo gat wan 'Forget Password' redi.

Moa investigesen blong manejmen intafes i soem konten insaed long panel we i soemaot hao ditel blong ol kompromaes divaes oli storem.



Pikja 4: Webpej bihaen long login pej blong MOONSHINE manejmen intafes.

Lookout risej i soem wan pas '**skoa**' aot long viktim divaes i go long MOONSHINE C2 seva. Valiu blong 'skoa' i bes long ol raet blong ol rabis sampol long divaes blong viktim.

Kolom 'if_contact', 'if_location', 'if_call_log' mo 'if_sms' insaed long pej i talem se i no evri MOONSHINE sampol oli gat ful akses long ol kompromaes divaes ya. Save blong ol kolom ya mo 'skoa' i pas long divaes i go long C2 i talem se ol tret akta oli stap yusum skoa blong talemaot level blong akses blong malwea i gat long kompromaes divaes long wanwan man we i aksesem manejmen intafes ya.

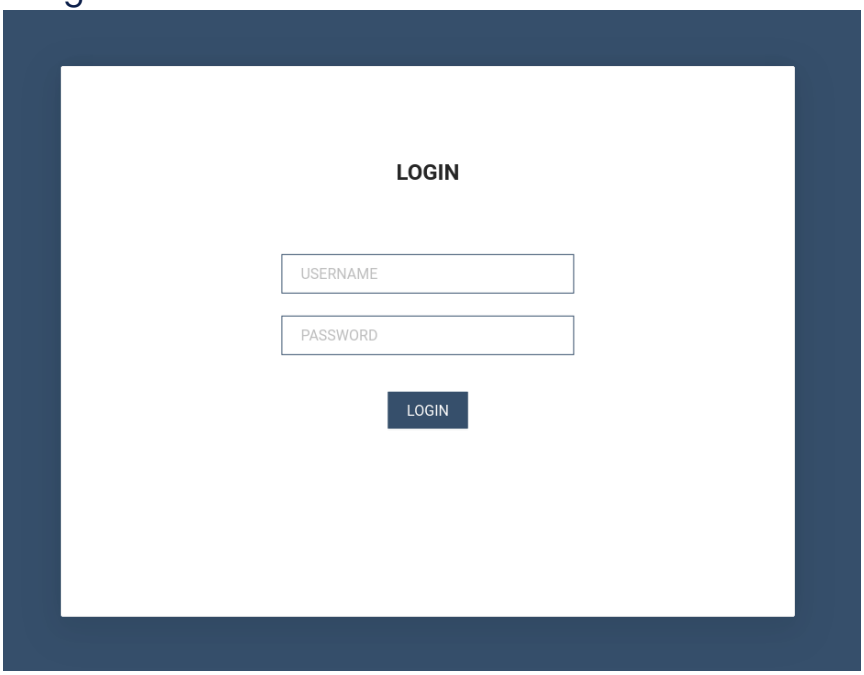
Lon jenerol, bes-praktis advaes blong stopem ol app blong tekemaot infomesen aot long divaes hemi blong inspektem ol raet blong app blong eni samting we i no stret bifo yu daonlod. Be, ol MOONSHINE sampol oli nidim raet we i stret long fangsen blong app, maet i luk defren smol, be olgeta tu oli yusum ol raet ya blong kolektem infomesen long ol divaes.

MOONSHINE i gat tu wan Application Programming Interface (API) we i talemaot saes blong ol abiliti ya. Eli vesen blong API dokumentesen i gat ol API nem long Mandarin lanwis.

Vituol host

Long ol sej blong MOONSHINE panel, oli bin faemenaot ol vituol host taem. Vituol hosting hem i taem wan IP adres i hostem maltipol websaet long wan taem. Ol IP adres blong ol vituol host taem ya mo ol domen we oli hostem oli no bin luk long eni malwea sampol.

Ol taem ya blong manejmen intafes oli defdefren, olsem taetol blong pej we hemi **'LOGIN'** insted long bifo we hemi '**SCOTCH ADMIN**'.



Pikja 5: MOONSHINE manejmen intafes we oli yusum LOGIN taetol insted long SCOTCH ADMIN.

Antap long hem, konten long panel oli defren long pikja 4, olsem we oli luk long pikja 6:

Pikja 6: Webpej bihaen long login pej blong vituol grup we i hostem MOONSHINE manejmen intafes.

Panel long pikja 6 i kamaot olsem wan smol vesen blong panel long pikja 4. Ol joen karakta blong ol panel hemi ol kolom nem 'id', 'manufaktara' mo 'model' long tebol.

Ol vituol host taem blong MOONSHINE we oli faenemaot hemi:

Domen	IP Adres
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

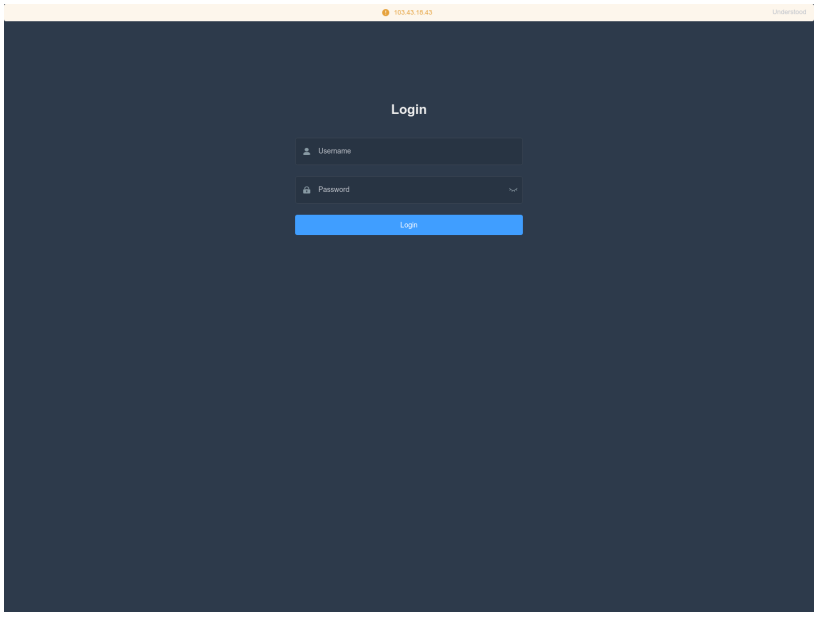
Ol domen ya we oli listim i kam long Trend Micro olsem ol wok kit blong MOONSHINE, we oli responsibol blong stopem braosa atak blong instolem malwea long ol mobael divaes. Trend Micro i nemem malwea ya 'Dark Nimbus'.

Blong klarifikesen, MOONSHINE manejmen intafes oli wanem MOONSHINE malwea sampol i toktok wetem, mo ples we oli storem viktim data long hem. MOONSHINE i banem ol kit we oli ripotem i kam long Trend Micro, hemi wan seperet paoa we i stopem braosa atak blong instolem wan malwea we oli kolem Dark Nimbus long ol mobael divaes. Moa tu, Dark Nimbus mo MOONSHINE oli tu defren malwea.

Tugeta MOONSHINE manejmen intafes mo MOONSHINE oli banem ol kit we oli gat kod we i ovalap mekem se tugeta i gat sem login prom long pikja 3 mo 5 mo tu konten blong pej long pikja 4 mo 6. Tufala tugeta i gat string ya 'webpackJsonpreact-scotchui' long sos kod.

Ol tret akta oli krietem URL link we i konek long MOONSHINE ban kit mo afta ridaerek long ol vidio we i go long ol man Tibet mo Uyghurs, we i ovalap wetem taget blong MOONSHINE.

Akros long plante IP adres hosting MOONSHINE i banem kit domen, i gat wan login pej we taetol blong hem 'VLiteUI' long pot 444. Pej ya oli no luksave fulwan mo presens blong hem long ol IP adres ya i soem wan posibol link long ol operesen blong ol akta ya.



Pikja 7: Login panel wetem HTML taetol 'VLiteUI' we oli faenem long ol IP we hem i wan hosting kit we MOONSHINE i yusum.

Analasis blong Trend Micro long Dark Nimbus i bin soemaot se malwea ya i save kolektem wan komplit lis blong infomesen long wan divaes, mo se i stap toktok wetem C2 mo i yusum wan XMPP protokol.

Trend Micro analasis i talemaot tu se long sam vesen blong Dark Nimbus, oli aedentifaem namba blong string 'DKNS'.

'**ansec[.]com**' (we oli listim olsem wan Dark Nimbus C2 we i kam long TrendMicro) oli bin faenem long ol seves blong XMPP we i blong ol narafala IP adres we oli sevem ol web pej wetem DKNS long taetol:

- DKNS Android远程取证系统 (DKNS Android Rimot Forensik Sistem)
- DKNS云网侦控平台 (DKNS Klaod Netwok Investigesen mo Kontrol Platfom)
- DKNS 云网侦控平台 (DKNS Klaod Netwok Investigesen mo Kontrol Platfom)
- DKNS远程控制侦查系统 (DKNS Rimot Kontrol Investigesen Sistem)

Nara set blong ol IP adres wetem '**ansec[.]com**' long seves blong XMPP we i gat ol pej wetem taetol ya:

- UPSEC互联网控制指挥系统 (UPSEC Intanet Kontrol Koman Sistem)
- UPSEC无线侦控系统 (UPSEC Waeales Sevelens mo Kontrol Sistem)
- UPSEC重点人数据还原系统 (UPSEC Ki Pesen Data Restoresen Sistem)

Folem Intelligence Online, 'UPSEC' i bin faenem long ol taetol blong ol HTML pej, we hemi 'Sichuan Dianke Network Security Technology Co., Ltd'.

Keis stadi tu: BADBAZAAR

BADBAZAAR hemi wan mobael malwea wetem iOS mo wan Android fom we i stap tagetem olgeta man blong Uyghur, Tibet mo wanwan man Taiwan. Spaewea ya hemi spred tru long sosol midia platfom mo ofisol app stoa. Risen ripot we i kam long Volexity i soem ol defren fom blong BADBAZAAR, we oli seperetem olsem BadSolar, BADBAZAAR mo BadSignal. Trifala fom ya oli link tugeta taem oli ovalapem ol fangsen we oli yusum blong kolektem divaes mo opereta infomesen.

Risej blong NCSC we i go insaed long BADBAZAAR i soem se:

- Grup blong ol C2 domen oli soem se i gat moa link long ol domen we oli ripotem long histri tret inteligens.
- C2 seva mo malwea sampol oli soem ol host nem we oli joen wetem akta infrastrakja.
- Moa profael ol tret akta oli yusum blong sosol enjiniring naoia oli yusum blong spredem malwea blong olgeta we i bitim ofisol app stoa.

WHOIS klastaring/domen broka

'UJYJYUJ'

Analasis blong WHOIS we i rekod blong BADBAZAAR domain '**signalplus[.]org**' (we ESET i ripot) i soem valiu blong '**UJYJYUJ**' long '**State**' fil.

Wan sej blong ol nara domen wetem sem valiu i soem ol domen blong intres:

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

(Luk Annex A, imej 1)

Ol domen ya **signalplus[.]org**, **tubevideoplus[.]org** mo **thetubeplus[.]com** oli ripotem olsem BADBAZAAR C2 domen, taem ESET i ripot long sab domen **mail.pmumail[.]com** olsem wan FlyGram proxi seva. FlyGram hemi wan app blong BADBAZAAR we oli developem tru long ol rabis saeba akta (luk long Appendix blong wan lis blong ol nara app blong BADBAZAAR).

Kibod woking valiu

NCSC i bin luk sem kibod woking paten long ol narafala rejista BADBAZAAR C2 domen.

Olsem eksampol, olgeta domen ya oli gat valiu ya '**REWR**' we oli faenem long '**State'** fil (we oli jes yusum):

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

(Luk Annex A, pikja 2)

Domen wetem 'FSDF' stet fil valiu

Nara set blong BADBAZAAR C2 domen we oli gat '**State**' valiu '**FSDF**':

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

(Luk Annex A, imej 3)

Ril ripoting wetem kibod woking valiu

Yus blong kibod woking valiu long WHOIS rekod blong BADBAZAAR domen i save kam olsem ril ripot taget blong ol man Tibet oganaesesen we i kam long TA413. Recorded Future we oli faenem se ol domen we ol akta oli kontrolem oli stap atakem ol oganaesen blong man Tibet mo yus blong wan rejistresen blong oganaesen valiu blong "**asfasf**".

clublogs[.]com

BADBAZAAR sampol we Lookout i kasem we i gat '**xle.clublogs[.]com'** olsem C2 domen. Rut domen '**clublogs[.]com**' i bin grup long wan IP adres ya '**95.179.210[.]85**' mo gat wan SSL setifiket wetem wan sabjek mo isua valiu blong '**CN=WIN-50QO3EIRQVP**'. Valiu i majem SSL setifiket we i stap long sampol blong BADBAZAAR we i yusum SSL pining blong avoidem intasepsen blong komunikesen.

Hosting histri blong IP address **95.179.210[.]85** i ritenem ol domen interes ya:

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

(Luk long Annex A, imej 4)

www.voiceoftibet[.]net

Domen ya '**www.voiceoftibet[.]net**' i kamaot mo jenis olsem 'Voice of Tibet' redio stesen, semak long TTP we TA413 i bin yusum.

Domen ya '**rewrwer[.]com**' hemi semak long hemia we oli faenemaot ya '**State**' valiu '**REWR**' we i stap long rekod blong WHOIS long domen blong BADBAZAAR.

Domen ya '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' mo '**myloughborough[.]com**' evriwan oli rejisterem wetem imel adres ya '**tplutalova@list[.]ru**'.

actuallys[.]com

Rekod blong WHOIS blong '**actuallys[.]com**' i soem wan taem we wan tek o admin imel adres we hemi '**tplutalova@list[.]ru**' be wan rejista imel i bin '**ivan_s81@mail[.]ru**'.

Tru infomesen blong WHOIS blong domen ya '**actuallys[.]com**' i soem rejistresen blong imel we hemi '**wangminghua6@gmail[.]com**' we oli listim long 24 Febwari 2016. Long Maj 11 2016, imel ya i jenis i go long '**ivan_s81@mail.ru**' nomata we rejistra blong rejistresen ekspaeresen deit hemi stap semak.

wangminghua6@gmail[.]com

Imel adres ya '**wangminghua6@gmail[.]com**' oli bin yusum blong rejistarem ol domen we i stap long tru tret inteligens ripoting. Long 2015, Palo Alto i faenemaot imel we oli yusum blong rejistarem ol C2 domen blong malwea, Cmstar. Long 2014, oli bin yusum tu blong rejistarem ol domen we oli bin faenem tru long Mandiant long fising kampen we APT3 i bin kondaktem. Long 2013, oli bin yusum blong rejistarem ol domen we i kam long CrowdStrike long wan malwea dropa wetem

wan Program Database (PDB) rod we i gat Chinese karakta long hem. Hemi i minim wan koleksen blong wan Chinese sistem.

taoyujun@gmail[.]com

Domen ya '**hcjbtt[.]com**' i rejista wetem imel adres ya '**taoyujun@gmail[.]com**' be administreta imel blong hem i rejista wetem '**wangminghua6@gmail[.]com**'.

I nogat eni rabis aktiviti we i joen wetem domen ya '**hcjbtt[.]com**', be, imel adres ya '**taoyujun@gmail[.]com**' oli faenem long tru tret inteligens ripot. Long 2014, oli bin yusum blong rejistarem wan domen we Mandiant i faenem long '**Cueisfry Trojan**' sampol we oli yusum blong tagetem ol Japanese oganaesesen.

Imel adres ya oli rejistarem olsem '**iaea-international[.]org**' wei i jenis olsem **International Atomic Energy Agency** mo '**idc-ctbto[.]org**' hemi jenis olsem **International Data Centre** long **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

Wan eli Whois rekod blong domen ya '**iaea-international[.]org**' i soem rejista imel ya '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Domen ya '**udtglobals[.]com**' oli faenem i stap yusum imel ya '**wangminghua6@gmail[.]com**' olsem administreta imel mo '**ocean.nio@rediffmail[.]com**' olsem rejista imel adres. Narafala WHOIS rekods blong domen ya, i soem sem rejistra imel be wetem administreta imel adres' **taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' i jenis olsem '**UDT Global**' we hemi wan globol iven blong andasi difens mo sekiuriti kampani. Yusanem ya '**ocean.nio**' long imel adres we i giaman se hemi **National Institute of Oceanography (NIO)** we i laef long plante kantri. Nomata yus blong '**Rediff**' imel seves (we i bes long India) i talem tu giaman blong **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

Domen ya '**djibdiplomatie[.]com**' we i kamaot olsem Djibouti diplomacy services, we i gat sem WHOIS rekod long '**utdglobals[.]com'.** Wan rekod i kamaot blong soem rejistra ya '**ocean.nio@rediffmail[.]com**' mo admin '**taoyujun@gmail[.]com**' be ol nara rekod oli soem

‘**wangminghua6@gmail[.]com**’ olsem admin imel wetem ‘**ocean.nio@rediffmail[.]com**’ olsem rejistra imel.

Tugeta domen ya oli gat tu kibod woking taeb valiu long ol rekod blong WHOIS. Eksampol, ‘**udtglobals[.]com**’ i gat valiu ya ‘**ASDF**’ olsem rejista siti blong hem mo ‘**djibdiplomatie[.]com**’ i gat ‘**DAF DAGF**’ olsem rejista nem valiu blong hem. Hemia i semak long ol valiu we oli bin faenem long ol narafala domen blong BADBAZAAR.

Nomata imel adres ya ‘**wangminghua6@gmail[.]com**’ mo ‘**taoyujun@gmail[.]com**’ oli faenem long ol rekod blong ol domen blong WHOIS we oli jenis olsem wan **globol andasi difens iven**, **Djibouti diplomasi seves** mo **Intanasenol Atomik Eneji Ejensi**, olgeta tu oli stap insaed long ol rekod blong WHOIS blong sam domen we oli gud.

Miks jenis blong ol domen mo gud domen i talem se i gat wan infrastrakja entiti we oli yusum blong sapotem rabis saeba akta operesen.

Imel adres ya ‘**ocean.nio@rediffmail[.]com**’ oli faenem nomo long ol niu domen we oli tokbaot antap ya. ‘**ivan_s81@mail[.]ru**’ mo ‘**tplutalova@list[.]ru**’ oli bin rejista olsem wan smol namba blong domen, mo sam long ol domen ya oli bin hostem long BADBAZAAR infrastrakja. Trifala imel adres ya oli bilif se oli moa klosap tugeta long ol rabis saeba akta operesen. Hemia from wan hae namba blong ol domen we oli joen wetem ol no nogud aktiviti, komperem wetem ol imel ya ‘**wangminghua6@gmail[.]com**’ mo ‘**taoyujun@gmail[.]com**’.

(Luk long Annex A, imej 5)

Link i go nara tret akta

Wan komon fasin blong old omen link we i go wetem BADBAZAAR ‘**actuallys[.]com**’, ‘**clublogs[.]com**’, ‘**myloughborough[.]com**’, ‘**rewrwer[.]com**’, mo ‘**voiceoftibet[.]net**’ hemi olgeta oli rejista wetem eNom mo oli bin pakem long ‘**255.255.255[.]254**’.

Folem ol fas investigesen blong NCSC, ol nara domen wetem ol fasin ya oli soem aktiviti wetem **APT5** long 2019, mo **APT14** bitwin 2009 mo 2011.

Ol domen we oli joen APT5 oli gat ol histri rekod wetem WHOIS we oli listim ‘**taoyujun@gmail[.]com**’ olsem rejistra imel adres.

APT14 we oli link domen oli gat tri sabdomen we i luk olsem blong ripresentem taget we oli wantem kasem long ol rabis operesen blong olgeta. Wan eksampol blong hemia hemi '**bae.cisconline[.]net**', we i talemaot taget we oli wantem kasem blong BAE Systems mo oli bin faenem long wan '**Poison Ivy**' sampol.

Sem karakta ya oli faenem long ol domen blong BADBAZAAR we ol sabdomen oli go wetem nem blong trojan app ya:

Aplikesen Taetol	C2 URL
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

Hemi impoten to notem se ol aktiviti we i rilet i go long APT5 mo APT14 oli ril mo i gat ol nara domen we oli rejista wetem eNom mo oli muv i go long '**255.255.255.254**' we oli no save linkem hem i go long ol rabis aktiviti. Mekem se hemi no stret se ol akta bihaen long ol kampen ya oli semak o oli famle.

Masin Nem

Analasis blong BADBAZAAR C2s mo sampol we oli faenem ol hostnem we oli yusum olsem 'Common Name' valiu long SSL setifiket. NCSC investigesen long ol hostnem oli faenem long ol sampol blong BADBAZAAR mo infrastrakja se ol hostnem ya oli yusum long plante IP adres. Ol IP adres ya oli stap hostem ol domen we i stap long ol sampol blong BADBAZAAR. I gat moa ditel long seksen andanit abaot ol hostnem, mo IP adres wetem hostnem we i hostem ol C2 domen blong BADBAZAAR.

Long evri keis presens blong ol setifiket wetem hostnem valiu we i joen wetem IP resolusen blong ol rabis spesel domen nem, long smol taem hemia i no bin keis ya we oli aotlaenem.

WIN-EU0VLBL7TUJ

Hostnem ya '**WIN-EU0VLBL7TUJ**' oli faenem long IP adres blong intres ya:

- '**116.203.53[.]21**' i hostem BADBAZAAR C2 domen ya '**uyapkfinder[.]com**' mo '**thewestuniverse[.]com**'.

- **'95.216.169[.]27**' i hostem BADBAZAAR C2 domen ya '**adysfunction[.]com'** mo sab-domen ya '**download.apkbazar[.]biz**' we oli ting se hemi wan daonlod link blong wan sampol blong BADBAZAAR.

(Luk long Annex A, imej 6)

WIN-70E59JVOB9G

Hostnem ya '**WIN-70E59JVOB9G**' oli bin faenem long ol IP adres blong interes ya:

- '**23.88.28[.]220**' i hostem BADBAZAAR C2 sab-domen, **'aua.rondwsign[.]com', 'nal.tokenmajorp[.]com', 'pep.rondwsign[.]com'** '**doa.rondwsign[.]com**', mo **'pls.rondwsign[.]com'.** I gat wan taem, blong tu dei bitwin taem setifiket wetem masin oli luk laswan, mo taem rabis domen oli bin luk fastaem i brok i go long IP.

- '**23.88.28[.]221**' i hostem BADBAZAAR link wetem sab-domen ya '**bt.bhvghg[.]com**'.

- **'23.88.28[.]222**' i hostem BADBAZAAR C2 domen ya '**tubevideoplus[.]org**' mo '**cde.mpoxcases[.]com**'.

- '**65.21.92[.]67**' i hostem BADBAZAAR C2 sab-domen ya '**bat.androidupdated[.]net**'. I hostem tu sab-domen ya '**apps.androidupdated[.]net**' we hemi wan DoubleAgent malwea C2.

- '**65.21.92[.]77**' i hostem BADBAZAAR C2 sab-domen '**wyo.titeperformance[.]com**',

‘**big.collinformations[.]com**’**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ mo ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ i hostem BADBAZAAR C2 sab-domen ya ‘**upd.whoscaller.net**’. mo ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ i hostem BADBAZAAR C2 sab-domen ya ‘**bvn.lookincategory[.]com’** mo ‘**edr.lookincategory[.]com’.** I gat wan taem blong ileven dei bitwin taem setifiket wetem masin nem oli bin luk laswan, mo taem rabis domen oli bin luk fastaem i brok i go long IP.

- **‘142.132.131[.]20’** i hostem sab-domen ya ‘**son.onlinegamersgroup[.]com’** mo ‘**system.onlinegamersgroup[.]com’**, oli bilif hemi BADBAZAAR C2s taem oli stap hostem tufala be BADBAZAAR i joen wetem SSL setifiket oli bin faenem long IP.

- ‘**142.132.131[.]28’** i hostem BADBAZAAR C2 domen ya ‘**goldplusapp[.]net**’ mo sab-domaen ya ‘**who.goldplusapp[.]net**’ mo ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ i hostem BADBAZAAR C2 sab-domen ya ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, mo ‘**aar.alpinemap[.]net**’.

- ‘**162.55.103[.]212**’ i hostem BADBAZAAR C2 sab-domen ya **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** mo **‘aua.rondwsign[.]com’.**

- ‘**195.154.47[.]99**’ i hostem BADBAZAAR C2 sab-domen ya ‘**ggl.whoscaller[.]net**’ mo ‘**upd.whoscaller.net**’. I gat wan taem blong tri dei bitwin taem setifiket wetem masin nem oli luk fastaem mo taem rabis domen oli bin luk laswan i brok i kam long IP.

- ‘**195.154.60[.]3**’ i hostem BADBAZAAR C2 sab-domen ya ‘**upd.whoscaller[.]net**’ ‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ i hostem BADBAZAAR C2 sab-domen ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ mo ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ i hostem BADBAZAAR C2 domen ya, ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ mo ‘**bvn.lookincategory[.]com**’.

(Luk long Annex A, imej 7)

WIN-50QO3EIRQVP

Hostnem ya ‘**WIN-50QO3EIRQVP**’ oli bin faenem long ol IP adres blong interes ya:

- ‘**45.76.132[.]91**’ i hostem ol domen ya, ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. Tugeta domen ya oli link go long BADBAZAAR olsem ol sab-domen ya ‘**fow.yumoftion[.]com**’ mo ‘**bat.androidupdated[.]net**’ oli ol BADBAZAAR C2 domen. Antap long hem sab-domen ya ‘**apps.androidupdated[.]net**’ hemi wan DoubleAgent C2 domen. Hemi hostem tu domen ya ‘**pmstwocqn[.]com**’, we i link long BADBAZAAR tru long ol WHOIS rekod.

- ‘**95.179.210[.]85**’ i hostem ‘**clublogs[.]com**’, we ‘**xle.clublogs[.]com**’ hemi wan BADBAZAAR C2 domen mo tu i hostem BADBAZAAR we i link wetem ol domen ya ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, '**www.voiceoftibet[.]net**' mo ‘**actuallys[.]com**’.

- ‘**199.247.21[.]34**’ i bin hostem ‘**titeperformance[.]com**’, mo ‘**collinformations[.]com’** we hemi ol sabdomen blong BADBAZAAR C2 domen.

- ‘**217.69.10[.]128**’ i hostem BADBAZAAR C2 domen ya ‘**uyghurdict[.]com**’.

(Luk long Annex A, imej 8)

WMSvc-WIN-50QO3EIRQVP

Hostnem ya '**WMSvc-WIN-50QO3EIRQVP**' oli bin faenem long ol IP adres blong interes ya:

- **'78.46.185[.]251'** i hostem BADBAZAAR C2 domen ya **'groupgram[.]org'**, we Volexity i ripotem se i stap yusum pot 4432 blong ol rabis koneksen.
- **'65.21.92[.]69'** mo **'163.172.205[.]207'** i hostem domen ya **'widelygram[.]org'** we oli se hemi wan BADBAZAAR C2 domen, semtaem oli hostem long tugeta IP, pot 4432 taem i bin open.
- **'163.172.198[.]206'** i hostem domen **'maxgram[.]org'** we hemi wan BADBAZAAR C2 domen, semtaem oli hostem be pot 4432 i bin open.

(Luk long Annex A, imej 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Hostnem ya '**WMSvc-WIN-50QO3EIRQVP**' mo '**WIN-7LSBB9R0F1L**' oli bin faenem long ol IP adres ya semtaem:

- '**148.251.87[.]245**' i bin hostem BADBAZAAR C2 domen ya '**flygram[.]org**' mo '**groupgram[.]org**'.

(Luk long Annex A, imej 10)

WIN-N8H8S9BG2P0

Ol hostnem ya '**WIN-N8H8S9BG2P0**' oli bin faenem long IP adres ya:

- '**148.251.87[.]247**' i hostem BADBAZAAR C2 domen '**omarwhatsapp[.]org**' mo '**flygram[.]org**'.

(Luk long Annex A, imej 11)

WIN-I6VBN8MR92A

Ol hostnem ya '**WIN-I6VBN8MR92A**' oli bin faenem long IP adres ya:

- '**148.251.87[.]197**' i hostem BADBAZAAR C2 domen ya '**tryhrwserf[.]com**'.

(Luk long Annex A, imej 12)

Beis long avelebol komesol data namba blong ol masin nem ya truaot long jenis blong intanet. Sam long olgeta oli faenem semtaem long fulap IP adres we i minim se ol VM oli bin krietem long sem model. Hem i impoten blong notem se sam long ol hostnem ya, evriwan long olgeta oli no link long ol rabis aktiviti wetem ol IP ya. Hemia i minim se yus blong ol hostnem oli no stap olgetawan long ol tret akta ya.

Be, namba blong sam long ol masin nem ya we oli krosem ol IP we oli bin hostem BADBAZAAR C2 domen, i talem se wan infrastrakja prokiua entiti oli bin yusum blong konfigarem ol masin blong sapotem rabis akta saeba operesen.

Sosael midia presens

Fas ripoting i kam long Volexity i soem se ol YouTube vidio (we oli promotem yus blong ol rabis aplikesen) oli krietem tru long ol rabis saeba akta. Ol vidio ya oli gat ol tutoriol long hao blong yusum ol aplikesen we oli developem ya.

NCSC i bin faenem tu moa YouTube janel we i joen wetem ol operesen blong ol tret akta ya. YouTube janel wetem URL handel ya '**@josephjoey3499**' i stap promotem yus blong '**Maxgram**' mo wan moa janel we oli rejistarem wetem '**@uyghurapks3096**' we i promotem '**Uyghur APK Finder**'.

Moa, YouTube vidio oli stap promotem '**Flygram**' mo '**Signal Plus**', we oli soem ol tret akta oli stap yusum klia ol fon namba. Long '**Flygram**' vidio, long 0:36 fon namba ya '**+1 (570) 378-7250**' yu save luk mo long taem blong '**Signal Plus**' vidio, fon namba ya '**+1 (267) 298 4259**' i bin kamaot.

Volexity i ripotem wan niufala giaman kalaTibet saet '**ignitetibet[.]net**', we oli faenem long ol Telegram janel we oli ting se ol tret akta oli stap operetem. Imel adres ya '**choekyi.wangmo@ignitetibet[.]net**' oli faenem se i stap livim ol komen pos long pej ya '**tibetone.org**' we oli bin faenem long pablik mo Lookout nao i ripotem olsem wan C2 pej we oli yusum long iOS olsem fom blong BADBAZAAR.

Imel adres ya oli faenem se wan akta i kontrolem, wetem yus blong wan man we nem blong hem i '**Choekyi Wangmo**'.

Asesmen

BADBAZAAR mo MOONSHINE i yusum sam sosol enjiniaring wei blong tagetem stret Uyghur, Tibetan mo ol komiuniti blong Taiwan, nem blong olgeta oli:

- Fasin blong trojanaesem ol app blong interes i go long ol komuniti ya, olsem wan Uyghur lanwis Quran app, oli mekem blong i tagetem viktim bes
- trajanaesesen app we oli ademap long ol ofisol app stoa oli save givim wan tru filing, mo blong stap serem long ol grup jat hemi save kam spolem wan gudfala rilesensip insaed long ol komuniti

BADBAZAAR mo MOONSHINE i kolektem infomesen we bae i gat moa valiu long Chinese stet. Nomata se BADBAZAAR mo MOONSHINE oli stap lukluk long tufala i stap tagetem man Uyghur, Tibetan mo Taiwan, i gat ol narafala malwea we oli tagetem smol grup long China. Ol sitisen blong ol nesen we oli joen, long China mo nara kantri, we oli stap traehad blong sapotem ol wok we i stap go agensem stabiliti blong gavman, kolosap evriwan oli stap anda long denja from mobael malwea olsem BADBAZAAR mo MOONSHINE. Ol skil blong tekem ples, odio mo foto infomesen kolosap oli givim ol janis blong letem fiuja seveilens mo ol operesen blong fasin nogud taem oli givim ril-taem infomesen long ol aktiviti blong ol taget.

MITRE ATT&CK®

Ripot ya oli bin putum tugeta wetem respek long MITRE ATT&CK® framwok, wan globoli akses save beis long ol nogud plan mo teknik beis long ril wol obsevesen.

Taktik	ID	Teknik	Rul
Rekonesons	T1593.001	Search Open Websites/Domains: Sosol Media	Akta oli faenem onlaen grup mo forom we i majem ol stret viktim blong oli serem malwea.
Risos Developmen	T1583.001	Kasem Infrastrakja: Domen (ol)	Akta oli rejistarem ol domen blong koman mo kontrol seva.
Risos Developmen	T1587.001	Developem ol Paoa: Malwea	Rabis kod oli raetem blong putum mesej blong app we oli trojanaesem.
Risos Developmen	T1608.001	Stej Paoa: Aploadem Malwea	Ol trojanaes app oli aploadem i go long onlaen platfom wetem ol app stoa.
Risos Developmen	T1585.001	Openem Akaon: Sosol Midia Akaon	Akta oli krietem akaon long websaet mo sosol midia blong serem mo advetaesem malwea.
Risos Developmen	T1585.002	Openem Akaon: Imel Akaon	Akta oli hostem ol praevet mo komesol imel akaon blong hostem mo serem malwea.
Fas Akses	T1189	Draev-bae Kompromaes	Rabis raeting oli haedem long ol tru app mo oli aplodem i go long ol app stoa.
Fas Akses	T1566.003	Fising: Spiafising tru long Seves	Akta oli sendem ol trojanaes app long taget grup tru long sosol midia iven Telegram.
Eksikusen	T1204.002	Yusa Eksikusen: Rabis Fael	Viktim i mas instolem trojanaes app ya blong kilim peilod.
Difens Evasen	T1027.009	Obfusketed Fael o Infomesen: Enklos Peilod	Rabis peilod oli haedem insaed long ol tru app.
Difens Evasen	T1036.005	Maskared: Majem Tru Nem o Lokesen	Ol trojan fael oli majem nem, fes mo fangsen blong ol tru app.

Difens Evasen	T1656	Imitesen	Akta tekem fes blong ol tru man mo krietem ol kova websaet mo yusum ol usanem we i go wetem ol taget grup.
Koleksen	T1123	Odio Kapja	Ol trojan app oli save rikwestem ol ekstra raet ingkludum maekrofon akses tu.
Koleksen	T1125	Vidio Kapja	Ol trojan app oli save rikwestem ol ekstra raet ingkludum kamera akses.
Koleksen	T1005	Data long Lokol Sistem	Ol trojan app oli save rikwestem ol ekstra raet ingkludum ol lokol fael.
Koman mo Kontrol	T1071.001	Aplikesen Leya Protokol: Web Protokol	Malwea konek i go long C2 yusum HTTPS mo WebSocket's.
Koman mo Kontrol	T1509	No-Standet Pot	Nostandet pot oli yusum olsem pot 4432 mo 2333.
Eksfiltresen	T1041	Eksfiltresen Ova C2 Janel	Malwea i karemaot data yusum HTTPS mo WebSocket koneksen.
Impak	T1565.002	Data Manipulesen: Transmit Data Manipulesen	Akta i kasem data long ol viktim tru long wan enabling app web we oli no nidim blong app ya i wok long hem.

Indiketa

MOONSHINE:

- Long 1 Eprel 2025, wan sej blong VliteUI panel i kambak wetem:

IP Adres	Pot	Fas Sin	Las Sin
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

- Long 1 Eprel 2025, wan sej blong SCOTCH ADMIN panem i kambak wetem:

IP Adres	Pot	Fas Sin	Las Sin
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

- Long 14 Maj 2024, wan sej blong vituol SCOTCH ADMIN panel i kambak wetem:

Domen	IP Adres
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:

Diskripsen	SSL setifiket we oli faenem long ol BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Long 1 Eprel 2025, wan sej blong hemia antap ya BADBAZAAR setifiket i kambak wetem:

IP Adres	Pot	Fas Sin	Las Sin
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

Diskripsen	SSL setifiket we oli faenem long ol BADBAZAAR C2s
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- Long 1 Eprel 2025, wan sej blong hemia antap ya BADBAZAAR setifiket i kambak wetem:

IP Adres	Pot	Fas Sin	Las Sin
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

- WHOIS domen

Andanit ya i gat wan tebol blong ol domen we naoia oli gat WHOIS rekod wetem ol valiu we i majem hemia we oli faenem long BADBAZAAR C2 domen.

WHOIS Valiu	Domen (ol)
Rejista Stet: UJYJYUJ **Rejista Kantri: Bolivia** **Rejista: 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
Rejista Stet: REWR **Rejista Kantri: CF** **Rejista: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

Rejista Stet: FSDF **Rejista Kantri: AL** **Rejista: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

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

Olgeta link ya oli joen wetem ol nara indiketa blong kompromaes (IoCs) we i joen wetem BADBAZAAR mo MOONSHINE. NCSC i no save konfemem sapos ol infomesen ya oli tru long ol link mo ol rida oli advaesem olgeta blong verifaem stret mo relevens blong olgeta:

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

Mitigesen

NCSC i enkarejem adopsen blong ol rekomendesen andanit ya blong stap agensem ol tret we oli tokbaot long ol keis stadi.

- **App stoa opereta, ingkludem nambatri pati app stoa, mo developa oli sud meksua se ol app long ol platfom blong olgeta oli sekiua mo se oli komplae wetem gavman Kod blong Praktis.** Luk Gaedens: 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

- **Maltae-lanwis sapot**: App developa oli sud inves long ol wok blong lokolaesem ol popula app blong ol yusa we oli toktok smol lanwis nomo long medel blong ol taget grup we i gat Uyghur, Tibetik, Taiwanis Hokien mo Cantonis. Apple gaedens blong lokolaesem ol app: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Google gaedens blong ol translesen app: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Kipim sosol midia platfom i sekiua:** Sosol midia kampani oli save mekem moa had blong ol rabis saeba akta blong krietem ol bokas akaon mo serem ol rabis fael o link long ol platfom blong olgeta long ol narafala tru onlaen komuniti. Wea i posibol, ol kampani oli sud serem ol rabis indiketa long ol bigfala indastri blong impruvum wanwan save long tret mo blong kasem proteksen mesa.

- **Rimidiasen plan blong ol kastoma:** Oganaesesen oli sud gat ol proses long ples blong notifaem kastoma we oli bin instolem ol rabis app taem oli yusum seves blong olgeta. Ol alet oli sud kasem atensen blong man mo gat daereksen. Wea i stret, oganaesesen oli mas givhan long hao blong karemaot sofwea mo enkarejem viktim blong ripot long ol atoriti blong olgeta olsem, NCSC long UK.

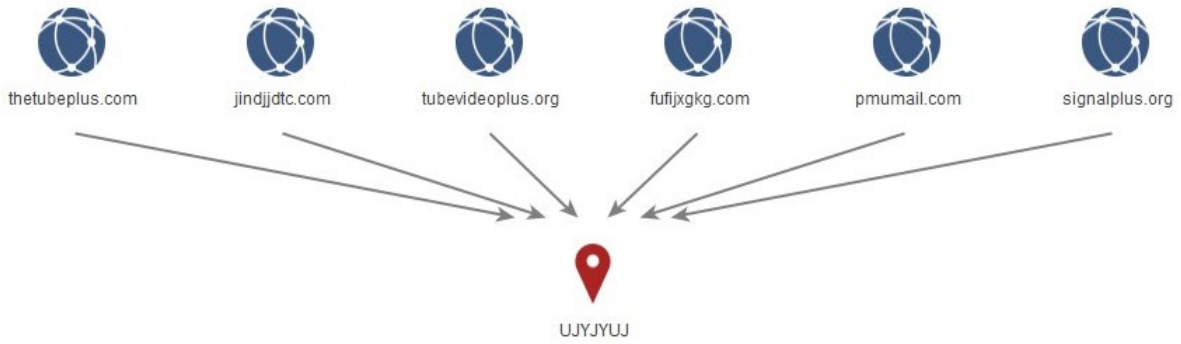
Luk long App Stoa Code of Practice blong moa infomesen: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Wok grup blong kolaboresen:** Sosol midia kampani oli save fomem wok grup, letem ol sekiuriti tim blong olgeta i serem ol rabis indiketa, TTP mo obsevesen, blong mekem i moa had blong ol akta blong yusum platfom blong olgeta blong sapotem ol rabis kampen.

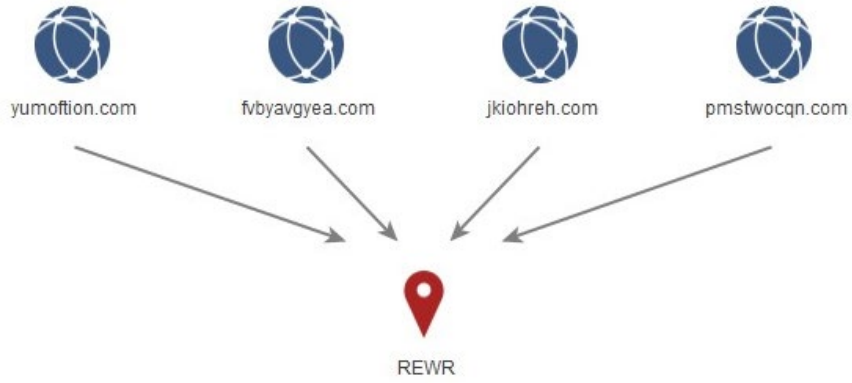
- **Luksave niu app:** Wea posibol, ol app developa oli sud gat wan fangsen blong letem yusa i save sapos oli bin daonlodem wan 'anofisol' vesen blong wan app, blong help stopem ol rabis kopi.

Apendex A: Graf blong BADBAZAAR WHOIS klasta / domen broka infomesen

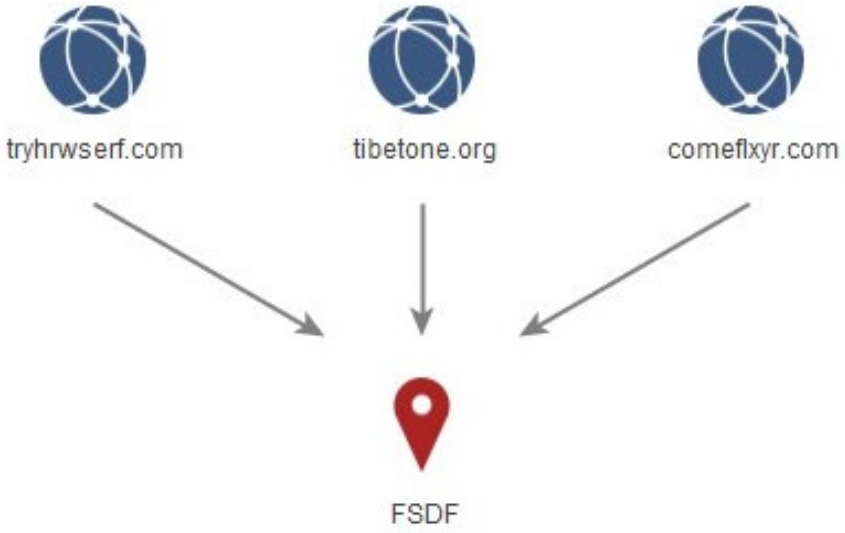
Imej 1 – 'UKYJYUJ'



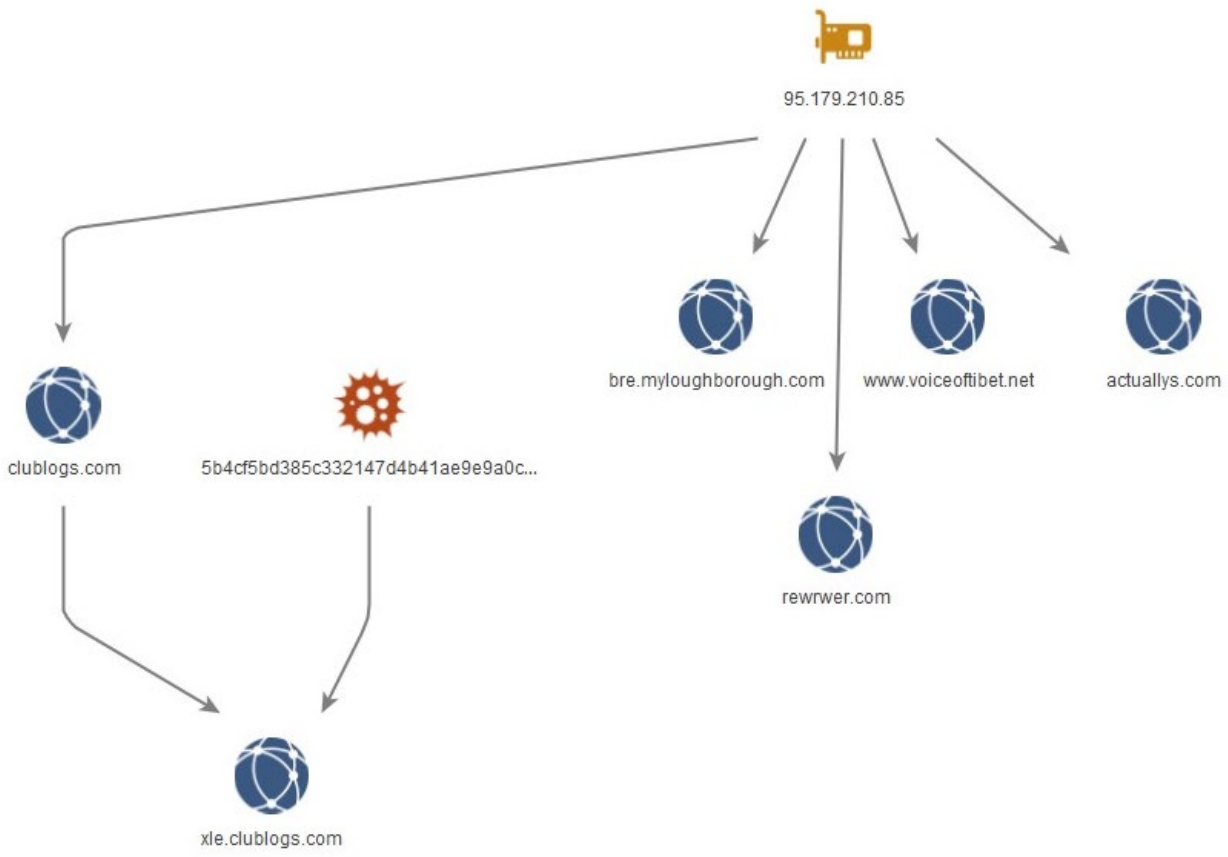
Imej 2 – Kibod woking valiu



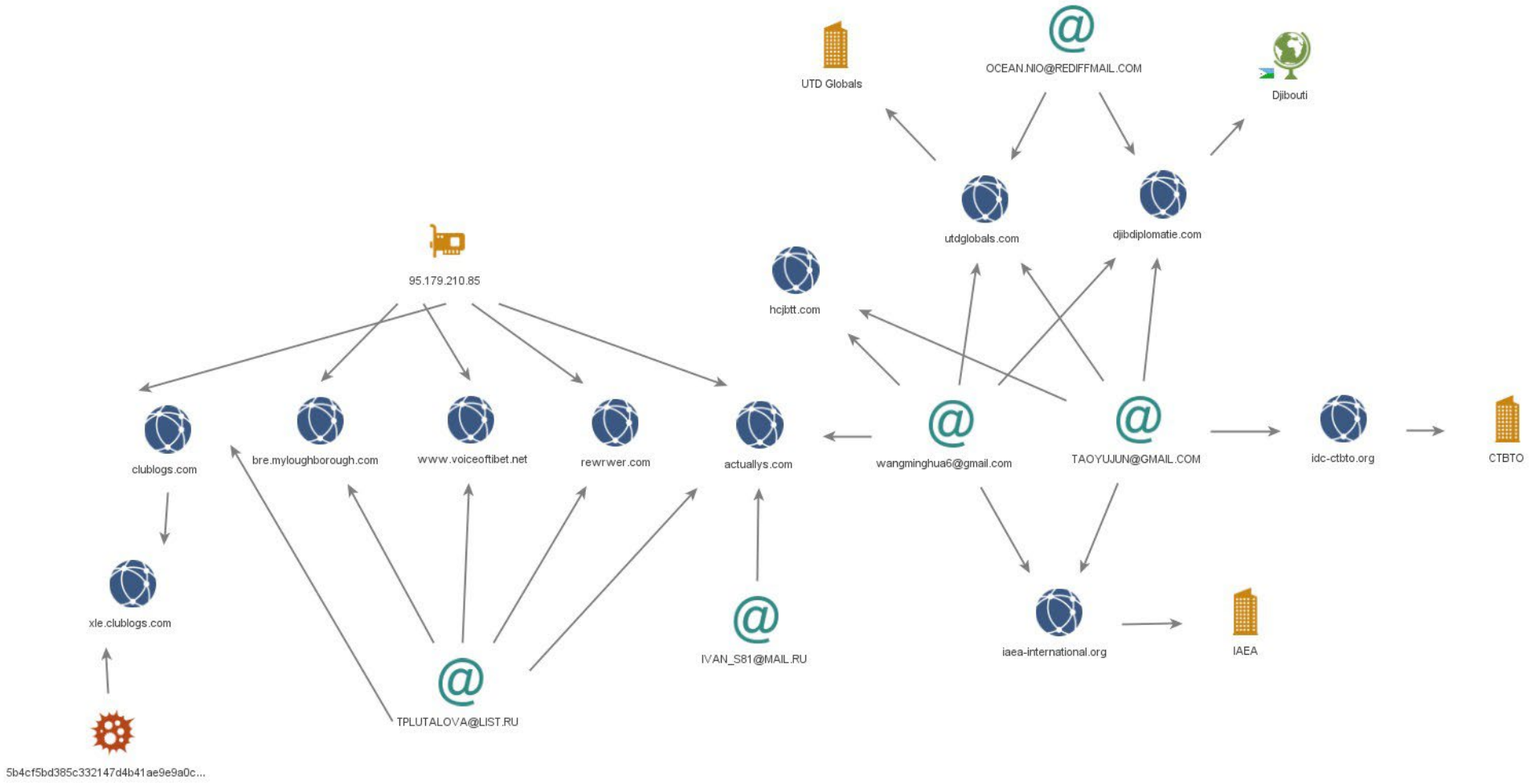
Imej 3 – Moa domen wetem 'FSDF' long stet fil valiu



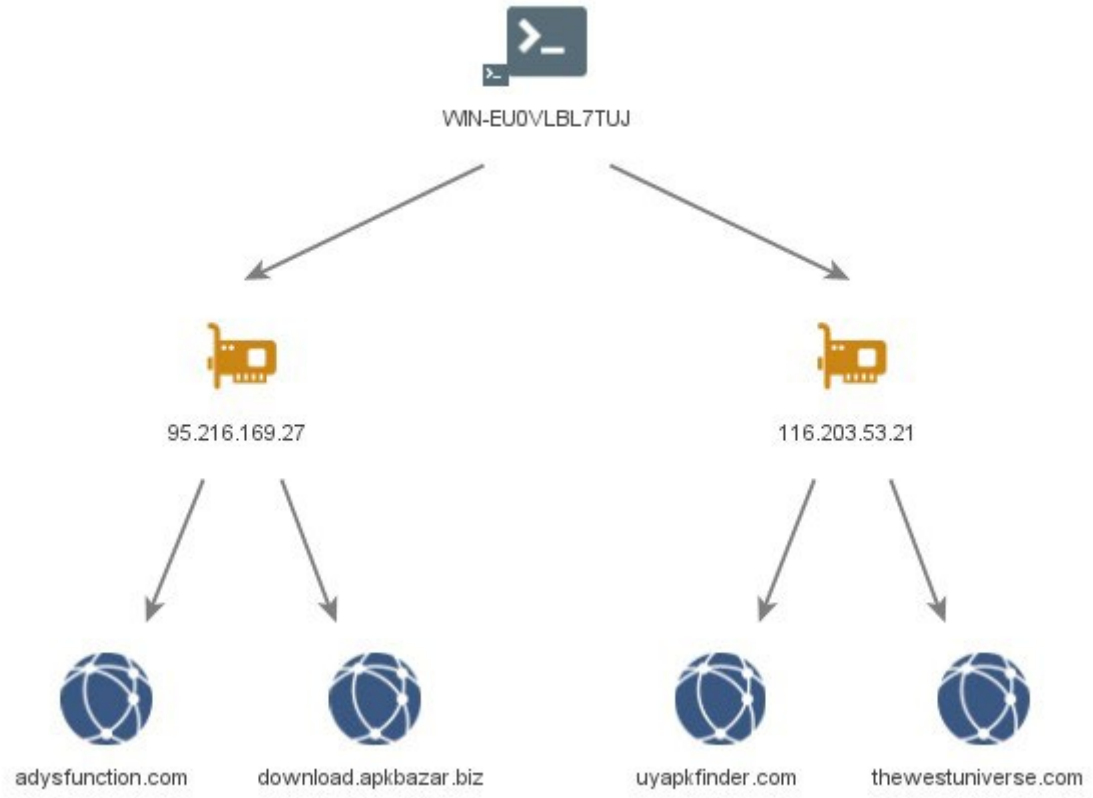
Imej 4 – **95.179.210[.]85**



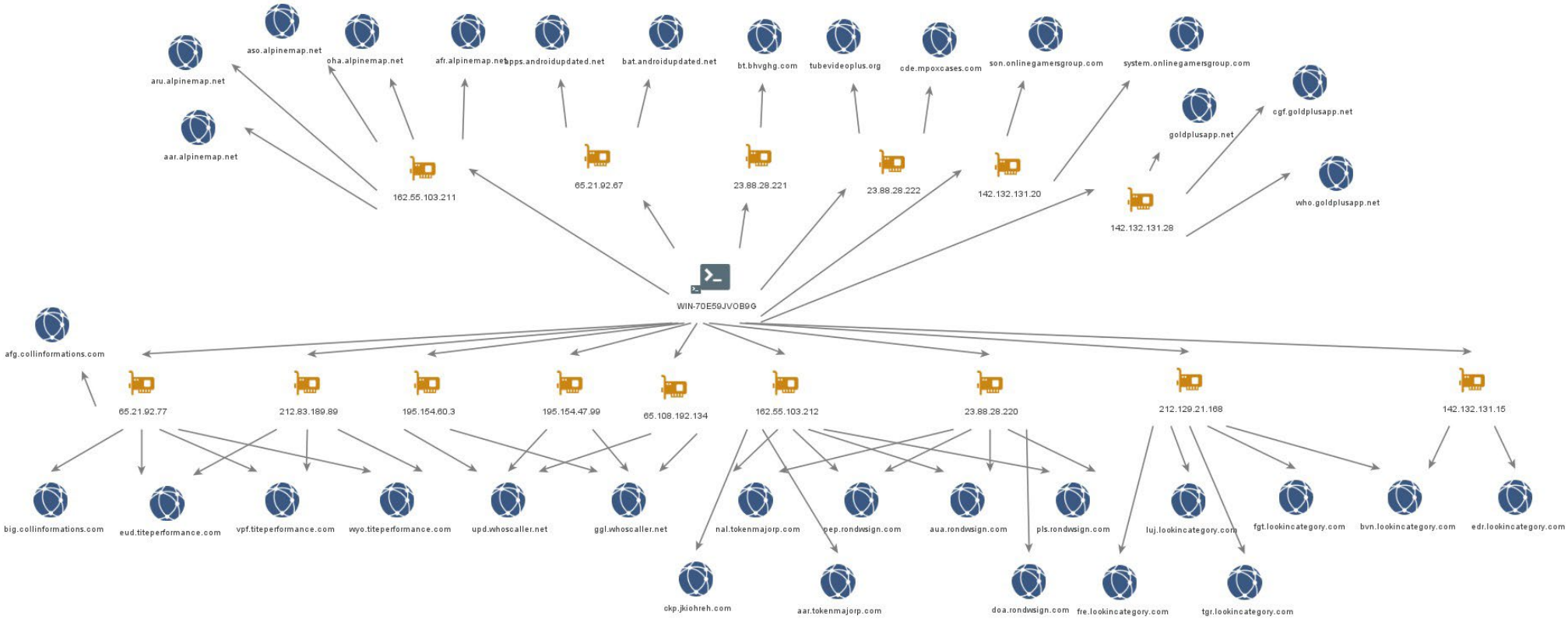
Imej 5 – WHOIS links



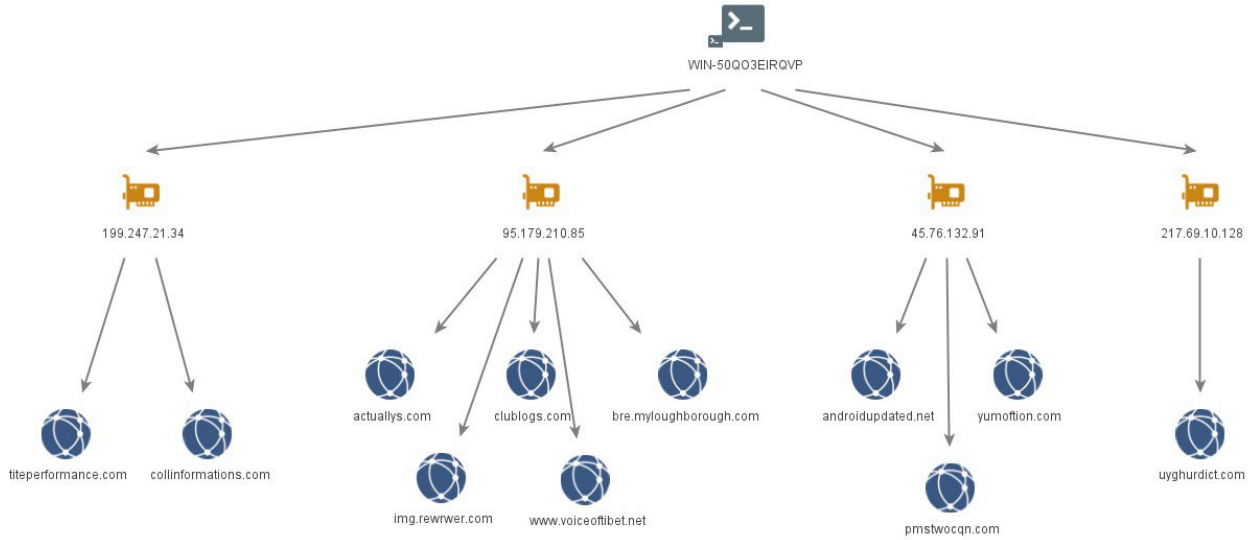
Imej 6 – **WIN-EU0VLBL7TUJ**



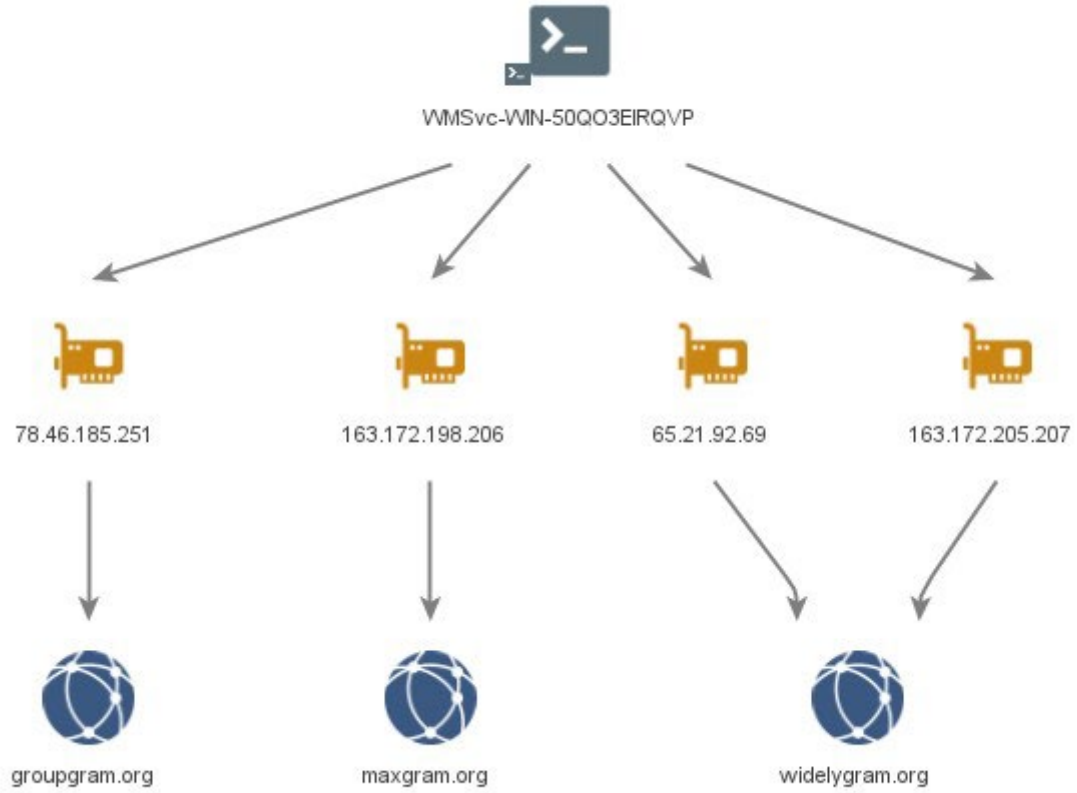
Imej 7 – **WIN-70E59JVOB9G**



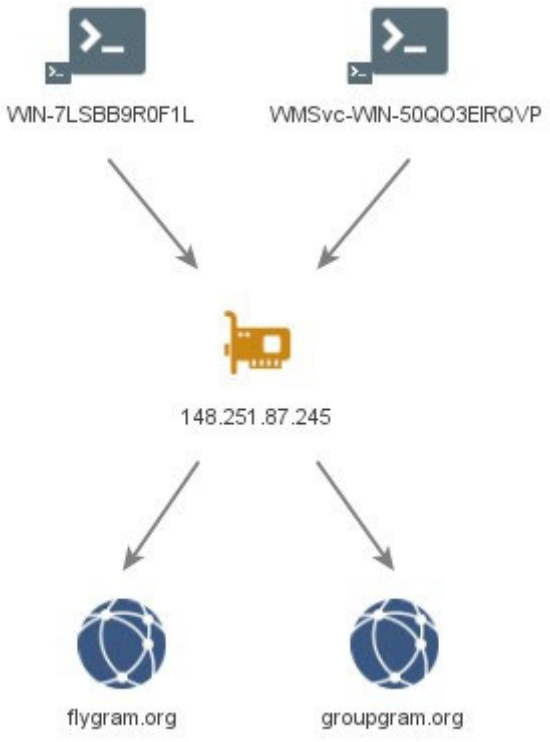
Imej 8 - **WIN-50QO3EIRQVP**



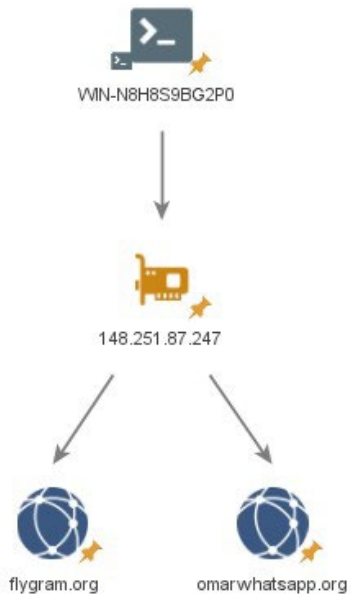
Imej 9 - **VMSvc-WIN-50QO3EIRQVP**



Imej 10 – **VMSvc-WIN-50QO3EIRQVP** mo **WIN-7LSBB9R0F1L**



Imej 11 - **WIN-N8H8S9BG2P0**



Imej 12 – **WIN-I6VBN8MR92A**

Apendex B: Sampol we oli faenem blong MOONSHINE & BADBAZAAR

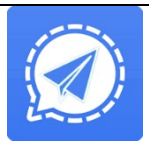
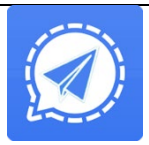
Tebol andanit i listim ol app we oli yusum long MOONSHINE mo BADBAZAAR kampen long las tu yia.

Plante long ol app ya oli soem wan klia lukluk blong mekem ol app ya. Hemia i gud blong mekem wan plan akta teknik blong 'trikim' ol bran we man i save.

Hemi impoten blong notem, app taetol, pakej nem, mo app aekon i save kopi o majem ril aplikesen mo no sud stap hemwan blong aedentifaem sapos wan divaes hem i nogud o no.

App taetol	Pakej nem	App aekon
99 Nem blong Alah	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobi Akrobat	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	
HARIAP	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	

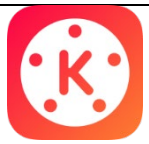
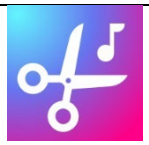
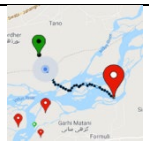
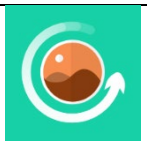
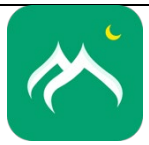
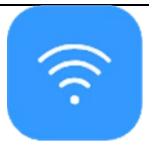
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

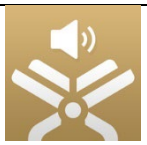
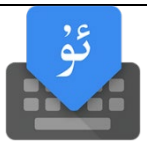
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

Ridim moa

Gaedens blong Australia Saeba Sekiuriti Senta

- Ripotem wan saebakraem, mistek o denja
- Hao blong protektem ol divaes blong yu
- Protektem mobael fon blong yu
- Fising
- Skam
- Protektem sosol media blong yu
- Tip blong protektem sosol media mo ol app blong mesej

Gaedens we i kam long UK NCSC mo NPSA

- Protektem Demokrasi
- Sosol Media: hao blong yusum gud
- Divaes Sekiuriti Gaed blong ol oganaesesen wetem mobael
- Ripotem tret long ol aplikesen stoa.
- Sefti blong yuwan mo sekiuriti blong ol hae risk man

Gaedens we i kam long US NSA

- Mobael Divaes Bes Praktis

Disklema

Plis tekem not se advaesori ya i givim infomesen we i stret long taem we oli pablisim.

Ripot ya i givim yu infomesen we i kam long atoriti ejensi mo olgeta long indastri sos. Eni samting we yu faenem mo ol rekomendesen we i stap oli no givim wetem tingting blong stap longwe long evri denja mo stap folem ol rekomendesen bae i no karemaot evri denja ia. Onasip blong ol infomesen denja i stap nomo wetem stret sistem ona evri taem.

Long UK, infomesen ya i fri anda long Freedom of Information Act 2000 (FOIA) mo maet bae i fri anda long ol nara UK infomesen legislesen.

Rifea eni FOIA kwestin long ncscinfoleg@ncsc.gov.uk.