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

Faufautua

BADBAZAAR ma MOONSHINE: Auiliiliga faatekonolosi ma le faaitiitia o le leaga tele

Aperila 9 2025

BADBAZAAR ma MOONSHINE: Auiliiliga faatekonolosi ma le faaitiitia o le leaga tele

Aotelega

Faatasi ai ma lagolagosua mai le UK Cyber League, o lenei faufautua na tuufaatasia le fausaga e le National Cyber Security Centre (NCSC UK) ma pa'aga faava-o-malo:

- **O le Australian Cyber Security Centre, vaega o le Australian Signals Directorate**
- **O le Canadian Centre mo Cyber Security, vaega o le Communications Security Establishment**
- **O le German Federal Intelligence Service**
- **O le German Federal Office mo le Protection of the Constitution**
- **O le New Zealand National Cyber Security Centre, vaega o le Government Communications Security Bureau**
- **O le United States Federal Bureau of Investigation**
- **O le United States National Security Agency**

O lenei faufautua e tuuina atu mea fou ma tomai o faamata'u na aoina mai i mea eseese e lua o polokalame komipiuta ua ta'ua o le BADBAZAAR ma le MOONSHINE, ma e aofia ai fautuaga mo tagata e fa'aaogaina app o faleoloa, i latou na faavaeina ma kamupani o ala o faasalalauga ina ia fesoasoani ai ia tausisia a latou tagata e fa'aaogaina auaunaga ia malu puipuia.

O lenei faufautua o loo ua faasalalauina ia ogatusa ma fautuaga mo i latou ua afaina i nei faagaoi i luga o komipiuta.

O lenei pepa o faatalaga e fa'aaogaina le faasologa o faamatalaga a le NCSC spyware: "O se ituaiga o polokalame komipiuta e faapipii i se masini e aunoa ma le faatagana a le tagata o loo fa'aaogaina, aoina mai ai faamaumauga ona lafo loa lea i se isi tagata lona tolu."

Suesuega o le mataupu muamua: MOONSHINE

O le MOONSHINE o se polokalame komipiuta Android na lipotia i le 2019 e Citizen Lab faapea na tulitulia kulupu mai Tibet. O le MOONSHINE e faatagā oso ane faapea o se app moni ina ia faasese ai tagata ua afaina ina ia lolomi ane ai i totonu. Ua faasoaina e ala i ala o faasalalauga faa-Telegram ma ala i sootaga na lafoina i le WhatsApp.

O suesuega a le NCSC i le MOONSHINE na iloa ai mea nei:

- E fa'aaoga e le MOONSHINE fesuiaiga o puleaga faapea na faia fesuiaiga talu mai le taimi muamua na lipotia ai.
- O fesuiaiga o puleaga na faailoa ai le tele nauā o le mafai ona maitauina faananā, e aofia ai le mafai ona aveesea faila mai masini komipiuta faapea foi le pu'eina o leo o loo fa'aali ma pu'eina ata o screens.
- O se veaga o puleaga faananā o loo faalafi e le MOONSHINE na faagaioi mamao mai na iloa ma mauaina. O nei faatalanoaga faananā e i ai fausaga e ova atu faatasi ai ma login vaega e login ai e fesootai ma le UPSEC, faapea e faatatau i Intelligence Online e faaliliu ifo faapea i le 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Puleaga vaega e lua o faatalanoaga

O lipoti talu ai o nofoaga e lua o faatalanoaga a le puleaga a le MOONSHINE na faailoa mai ai faapea sa fai fesuiaiga, faapea o loo faifaipea le atina'eina.

O le faataitaiga muamua o vaega e lua o faatalanoaga o puleaga na maua i le lipoti a le Citizen Lab 2019.

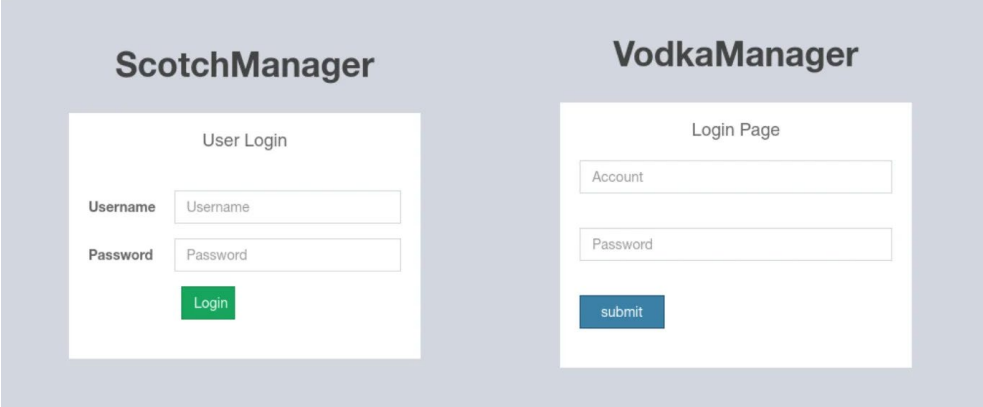


Figure 1: O vaega e lua o faatalanoaga a le puleaga a le MOONSHINE na iloa i le lipoti a le Citizen Lab 2019 'Missing Link Tibetan Groups Targeted faatasi ai ma le 1-Click Mobile Exploits'.

I le amataga o le 2022, na lipotia mai e le Lookout se puleaga e ese mai ai a vaega e lua o faatalanoaga a le puleaga faapea na toe sui le teuteuga ina ia foliga e pei o mea o i lalo ane (toe sui ai le vaega o faatalanoaga talu ai i le figure 1):

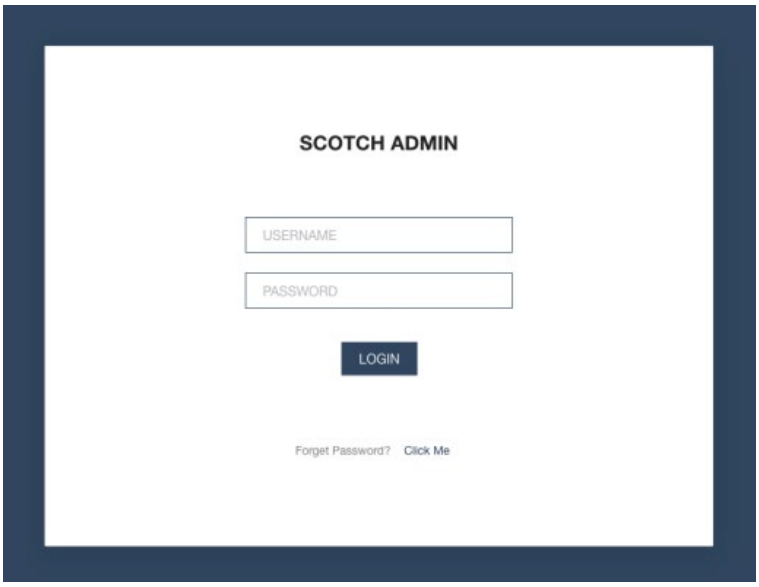


Figure 2: Nofoaga o faatalanoaga a le puleaga a le MOONSHINE e pei ona iloai i lipoti a le 2022 ***Lookout*** *'MOONSHINE: E aofia ai Android Surveillanceware mai le Chinese APT POISON CARP i le Target Tibetans ma Uyghurs'.*

Ia Aukuso 2023, o se scan o le MOONSHINE faatonuga ma le puleaina (C2) na iloa ai se vaega o faatalanoaga e tali tutusa i le vaega o faatalanoaga 2022 faatasi ai ma le gaioiga o le '**Forget Password**' ua le o toe maua e pei ona i ai i le figure 2:

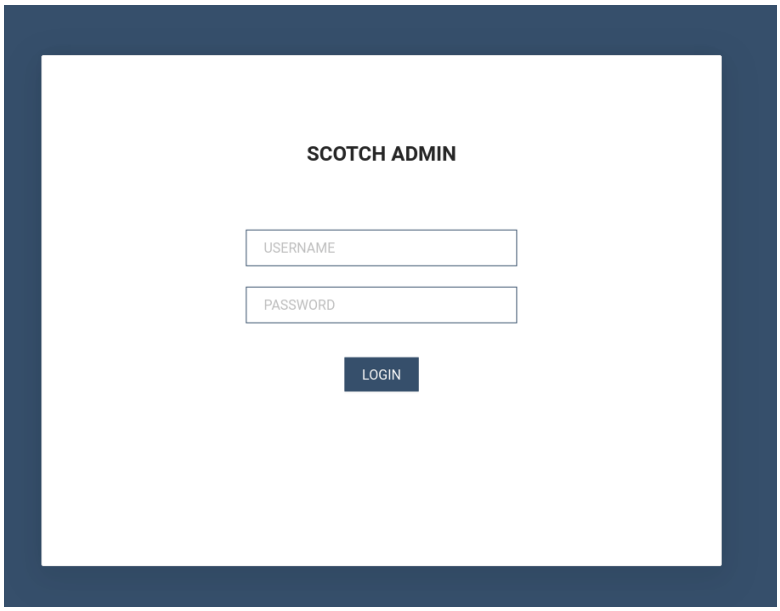


Figure 3: O nofoaga o faatalanoaga a pulega a le MOONSHINE na maitauina ia Aukuso 2023 faapea ua le o toe i ai le faamanatu o le 'Forget Password'.

I nisi o suesuega o nofoaga o faatalanoaga a le pulega na faailoa mai ai mea o i totonu o le faasologa na iloa ai auala o se fetuutuunaiga i masini o le a teuina.

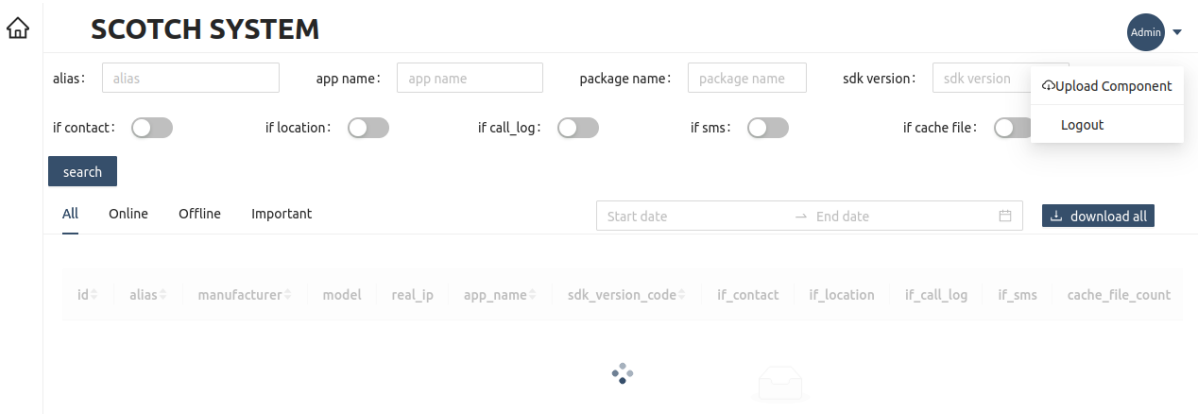


Figure 4: O le itulau upega tafailagi i tua o le itulau login o vaega e lua o faatalanoaga a le pulega a le MOONSHINE.

O suesuega a le Lookout na iloa ai le pasi atu o se '**score**' mai le masini ua afaina i polokalame komipiuta a le MOONSHINE C2. O le tau o le 'score' e fua i luga o le faatagana a le faataitaiga leaga tele i luga o le masini ua afaina.

O siata agai i luga ma lalo (columns) 'if_contact', 'if_location', 'if_call_log' ma le 'if_sms' o loo i totonu o le itulau o fautua mai faapea e lē o faataitaiga uma a le MOONSHINE e i ai atoa auala ina ia fetuutuunai uma i ai masini. O le iloaina o nei columns ma le 'score' e pasi mai le masini i le C2 ua fautuaina ai o le aufaamata'u o loo fa'aaogaina score ina ia faatalanoa ai le tulaga o loo maua ai le polokalame faaleaga komipiuta na i ai le masini ua afaina i tagata taitoatasi o loo faapea ona fetaui ai ma le isi itu o le puleaga.

Masani ai lava, o le fautuaga sili atu ina ia foia ai le aoina o faamatalaga mai masini o le siaki lea o faatagana a le app mo soo se mea e lē masani ai ae lei download. Ae ui i lea, o mea faataitai a le MOONSHINE e sailia faatagana faapea e talafeagai i gaioiga a le app, atonu la e foliga mai e masalomia, ae faapea foi ona fa'aaogaina faatagana nei ina ia aoina mai ai faamatalaga mai masini.

E i ai foi le Application Programme Interface (API) a le MOONSHINE o loo faailoa ai le lautele o lona mafai. O vaega muamua o le pepa o faamatalaga a le API o loo maua i igoa Mandarin i le API.

Nofoaga o loo faatonutonu mamao mai ai

I sailiiliga mo kava mo le MOONSHINE, o nofoaga e faatonutonu mamao atu ai na iloa ma mauaina. O le faatonutonu mamao atu e faapea e tasi le tuatusi IP e mafai ona faatonutonu mamao atu ai upega tafailagi e tele i le taimi e tasi. O tuatusi IP o mea nei e faatonutonu mamao atu ma kulupu o komipiuta e faatonutonu mamao atu ae lei maitauina i soo se faataitaiga o polokalame komipiuta.

O nei mea na tulai mai i nofoaga o faatalanoaga e puleaina e ese mai ai, e pei o le ulutala o itulau na '**LOGIN**' ae le o le igoa na iloa talu ai o le '**SCOTCH ADMIN**'.

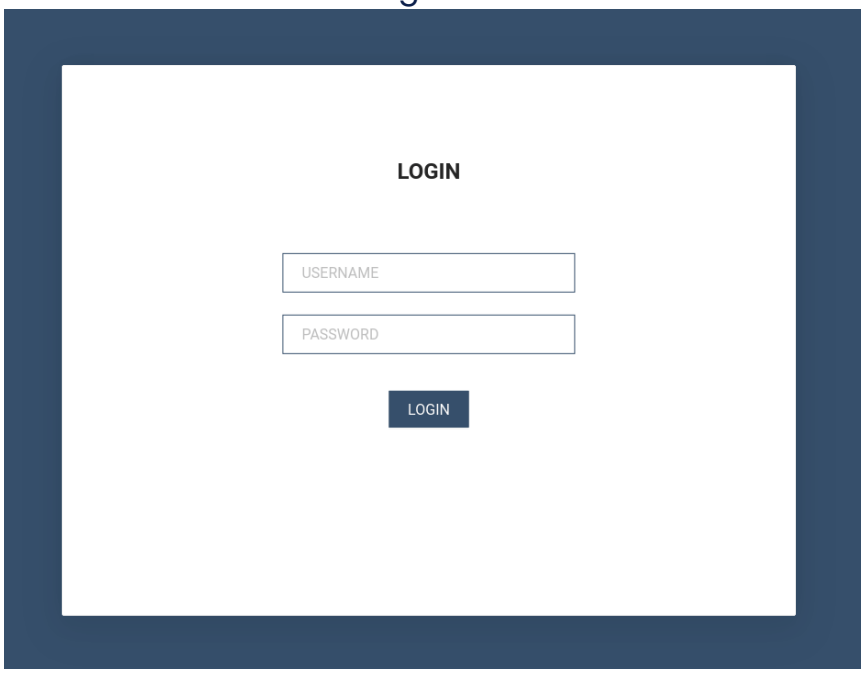


Figure 5: O pulega o faatalanoaga a le MOONSHINE e fa'aaogaina le ulutala o le LOGIN ae le o le SCOTCH ADMIN.

Faaopopo i ai, o mea o i totonu o le panel e ese foi mai le figure 4, pei ona vaai i ai i le figure 6:

Figure 6: O le upega tafailagi e i tua o le itulau e saini ai i totonu o le pulega faatonutonu a le MOONSHINE.

O le panel i le figure 6 e foliga mai o se vaega ua toesea ai ni mea o le panel i le figure 4. O mataitusi o loo ova mai ai o panels o igoa o column 'id', 'manufacturer' ma le 'model' i le fua faatatau.

O mea na maua i le faatonutonu mamao atu a le MOONSHINE na maua o:

Domain	Tuatusi IP
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

O nei kulupu o komipiuta o loo lisiina e Trend Micro faapea o mea laiti faataitai e faaleaga mea a le MOONSHINE, e fitoitonu i ai mo le faaleagaina o browser vaivai ina ia lolomi ai i totonu polokalame komiupiuta i luga o masini feaveai. Na faaigoa e Trend Micro o le 'Dark Numbus'.

Mo le faamaninoina, o pulega o faatalanoaga a le MOONSHINE faapea o faataitaiga o polokalame faaleaga masini a le MOONSHINE e faatalanoaina ai, ma i latou ua afaina i le aveesea o faamaumauga. O tamai kits faaleaga mea a le MOONSHINE na lipotia e Trend Micro, e ese mea e mafai ai faapea e faateia polokalame komipiuta vaivai ina ia lolomi ai i totonu polokalame faaleaga ua ta'ua o le Dark Nimbus i luga o masini feaveai. Fa'aopopo i ai, o le Dark Nimbus ma le MOONSHINE e matua tele lava le eseesega o polokalame komipiuta.

O mea uma e lua o le pulega o faatalanoaga a le MOONSHINE ma le kit faaleaga masini a le MOONSHINE e i ai igoa faalilolilo e ova teisi ai ae tali tutusa lava faamanatu o le saini i totonu i figures 3 ma le 5 faapea foi mea o i totonu o le itulau i figures 4 ma le 6. E i ai uma foi mea e lua o le so'oga o le 'webpackJsonpreact-scotchui' i totonu o le igoa faalilolilo i le mea e mafua mai ai.

O i latou e faatinoina faamata'u e gaosia sootaga URL links faapea e fesootai i kit faaleaga mea a le MOONSHINE ona toe faasino tuusa'o lea i video e talafeagai i le Tibetans ma le Uyghurs, faapea e ova atu kava i le tulituliloaina o le MOONSHINE.

I le tele o tuatusi IP o faatonutonu mamao atu kulupu komipiuta o kit faaleaga mea a le MOONSHINE, o loo i ai se itulau e saini ai i totonu ua ta'ua o le 'VLiteUI' i luga o le port 444. O lenei itulau e le maitauina faalauaitele ma lona tausisia o lona auai i nei IPs e faailoa mai ai o se sootaga e mafai i faatinoga a tagata e faatinoina.

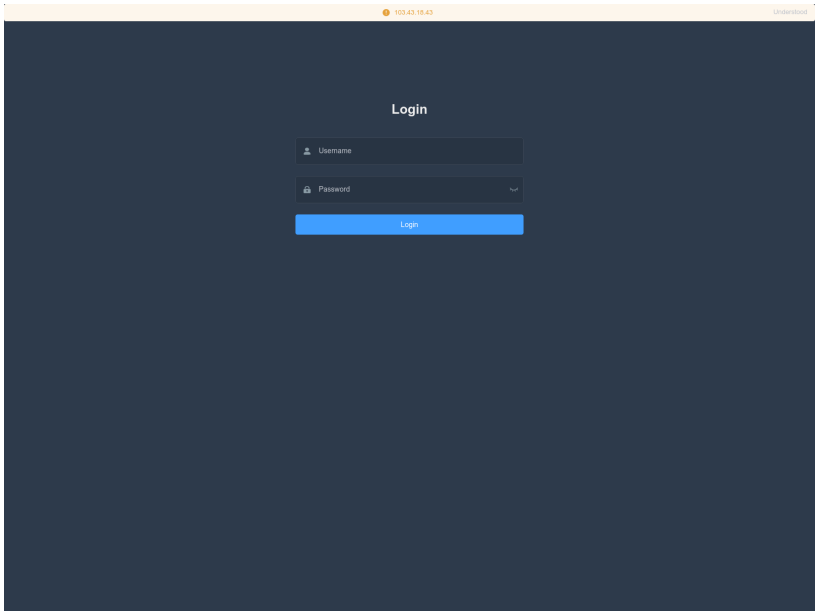


Figure 7: O le vaega e saini ai i totonu ma le HTML e ulutala o le 'VLiteUI' na maitauina i luga o IPs e faapea foi ona pulea faatonutonu mamao atu kits faaleaga mea a le MOONSHINE.

O auiliiliga a Trend Micro o le Dark Nimbus na iloa ai e mafai e le polokalame komipiuta ona aoina mai se lisi tele o faamatalaga i luga o le masini, ma faapea e fetalanoaa'i ma le C2 e fa'aaoga ai auala e fai ai o le XMPP.

Na iloaina foi e Trend Micro faapea o nisi o vaega o le Dark Nimbus, na latou faailoa mai le salalau tele ai o le sooga o le 'DKNS'.

‘**ansec[.]com**’ (na lisiina faapea o se Dark Nimbus C2 e TrendMicro) na maitauina foi i auaunaga XMPP mo isi tuatusi IP o loo tautuaina itulau upega tafailagi faatasi ai ma le DKNS i le ulutala:

- DKNS Android远程取证系统 (DKNS Android Remote Forensic System)
- DKNS云网侦控平台 (DKNS Cloud Network Investigation and Control Platform)
- DKNS 云网侦控平台 (DKNS Cloud Network Investigation and Control Platform)
- DKNS远程控制侦查系统 (DKNS Remote Control Investigation System)

O le isi seki o tuatusi IP faatasi ai ma le ‘**ansec[.]com**’ i le auaunaga XMPP e i ai itulau upega tafailagi faatasi ai ma le ulutala:

- UPSEC互联网控制指挥系统 (UPSEC Auala e Pulea Faatonutonu ai le Initaneti)
- UPSEC无线侦控系统 (UPSEC Maitauina Vavalalata e leai ni Uaea ma Auala e Faatonutonu ai)
- UPSEC重点人数据还原系统 (UPSEC Tagata Autū i Auala e Toe Mauaina ai Faamaumauga)

E faatatau i le Intelligence Online, ‘UPSEC’ na maitauina i ulutala o itulau HTML, na faasino i ai i le ‘Sichuan Dianke Network Security Technology Co., Ltd’.

Mataupu Suesue Lona lua: BADBAZAAR

O le BADBAZAAR o se polokalame na fausia e faaleaga ai telefoni feaveai faatasi ai ma e ese mai ai o le iOS ma le Android faapea e tulituliloaina Uyghurs, Tibetans ma tagata taitoatasi o Taiwan. O lenei polokalame e fa'aaoga ina ia maua mai ai faamatalaga o loo faasalalauina e ala i fata faatau o faasalalauga ma faleoloa aloaia e faatauina atu apps. O lipoti lata mai nei mai le Volexity o loo faailoa mai ai ituaiga eseese o BADBAZAAR, faapea o loo vavae'eseina faapea o le BadSolar, BADBAZAAR ma le BadSignal. O ituaiga eseese uma nei e tolu e foliga mai e soo faatasi e ala i le gaioiga o le isi i luga o le isi na fa'aaogaina mo le aoina mai o masini ma faamatalaga o le tagata o loo fa'aaogaina.

O le suesuega a le NCSC agai i le BADBAZAAR na iloa ai mea nei:

- Ia faailoa mea e tutusa C2 vaega komipiuta e iloa ai isi sootaga i kulupu o tuatusi na lipotia i faamata'u i tala'aga tomai.
- O polokalame C2 ma mea faataitai o polokalame faaleaga komipiuta na iloa ai igoa o fa'aaoga e faatatau i le tagata o faatinoina fausaga.
- O nisi foliga faapea e fa'aaoga e le aufaamata'u inisinia lautele i le va i fafo ina ia faasalalau ai a latou polokalame faaleaga komipiuta i tua atu o faleoloa apps aloaia.

WHOIS clustering / domain broker

'UJYJYUJ'

Auiliiliga o faamaumauga a le WHOIS mo le domain a le BADBAZAAR '**signalplus[.]org**' (na lipotia e ESET) na iloa ai le tau '**UJYJYUJ**' i le vaega o le '**State**'.

O se sailiga mo isi domains faatasi ai ma tau tutusa na iloa ai domains nei o fia iloaina:

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

(Tagai ane i le Annex A, image 1)

O domains **signalplus[.]org**, **tubevideoplus[.]org** ma le **thetubeplus[.]com** o loo lipotia domains a le BADBAZAAR C2, a o ESET e lipotia le domain laitiiti **mail.pmumail[.]com** faapea o se server faafoliga FlyGram. O FlyGram o se app na fausia e BADBAZAAR e ala ia i latou e faatino gaoi leaga i luga o initaneti (tagai ane i le Appendix mo se lisi o isi apps a le BADBAZAAR).

Keyboard walking values

O le NCSC sa faapea foi ona iloa ai fausaga o keyboard walking i isi domains lesitala a le BADBAZAAR C2.

Mo se faataitaiga, o domains nei e i ai uma tau '**REWR**' na maitauina i le vaega o le '**State**' (e pei ona fa'aaogaina talu ai):

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

(Tagai ane i le Annex A, image 2)

Domains e i ai le 'FSDF' tau o vaega i le setete

O le isi seki domains o le BADBAZAAR C2 e i ai le tau '**State**' '**FSDF**':

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

(Tagai ane i le Annex A, image 3)

Lipoti o tala'aga faatasi ai ma keyboard walking values

O le fa'aaogaina o keyboard walking values i faamaumauga a le WHOIS i le domain a le BADBAZAAR e mafai foi ona vaai i ai faatala'aga na lipotia i taulai i faalapotopotoga i Tibet e ala i le TA413. Lumanai Faamaumauina na maitauina i domains na faateia ai tagata faatino na pulea faalapotopotoga i Tibet ma le fa'aaogaina o se lesitala o le tau o se faalapotopotoga o "**asfasf**".

clublogs[.]com

O mea faataitai a le BADBAZAAR na maua mai e ala i le Lookout na i ai mea nei '**xle.clublogs[.]com**' faapea o le domain C2. O le autū o domain '**clublogs[.]com**' sa faailoaina tuatusi IP '**95.179.210[.]85**' ma se tusi faamaonia SSL faatasi ai ma le mataupu ma tau o le mea na faamatuuina mai ai '**CN=WIN-50QO3EIRQVP**'. O le tau lenei e tutusa ma le tusi pasi o le SSL na maua i mea faataitai a le BADBAZAAR faapea na fa'aaogaina e le SSL faapipii ina ia foia ai le mauaina o faatalanoaga.

O le tala'aga o le masini o loo faasoaina auaunaga mo tuatusi IP **95.179.210[.]85** e toe faafoi domains nei e fia iloaina:

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

(Tagai ane i le Annex A, image 4)

www.voiceoftibet[.]net

O le domain '**www.voiceoftibet[.]net**' e foliga mai o loo fealua'i solo faapea o le 'Voice of Tibet' le ofisa o leitio, e tutusa TTP na fa'aaogaina e TA413.

O le domain '**rewrwer[.]com**' e tali tutusa i lea na iloa talu ai '**State**' le tau '**REWR**' na maua i faamaumauga a le WHOIS o domains a le BADBAZAAR.

O domains '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' ma'**myloughborough[.]com**' na lesitala uma faatasi mai ma tuatusi imeli '**tplutalova@list[.]ru**'.

actuallys[.]com

O faamaumauga a le WHOIS mo '**actuallys[.]com**' na iloa ai se mea na tupu faapea o le tekonolosi ma tuatusi imeli o galuega ofisa sa '**tplutalova@list[.]ru**' ae o le imeli na lesitalaina sa '**ivan_s81@mail[.]ru**'.

O faamatalaga o le tala'aga o le WHOIS mo le domain '**actuallys[.]com**' na iloa ai le imeli na lesitala ai '**wangminghua6@gmail[.]com**' na lisiina ia Fepuari 24 2016. I le aso 11 Mati 2016, na sui ai le imeli ina ua uma le '**ivan_s81@mail.ru**' e ui o le lesitala i le ofisa lesitala e uma aso e aogā ai o loo tumau lava i le mea e tasi.

wangminghua6@gmail[.]com

O le tuatusi imeli '**wangminghua6@gmail[.]com**' sa fa'aaoga e lesitala ai domains na maua i le faamata'u o tala'aga lipotia tomai. I le 2015, na faailoa e Palo Alto le imeli sa fa'aaoga e lesitala ai domains C2 mo le polokalame komipiuta, Cmstar. I le 2014, na faapea ona fa'aaoga e lesitala ai domains na iloa e Mandiant i le faalauiloa o imeli pepelo na faatautaia e ala i le APT3. I le 2013, sa fa'aaoga e lesitala ai domains na maua e CrowdStrike i se mea na faapa'u mai le polokalame komipiuta faatasi ai ma se auala o le Program Database (PDB) o loo i ai mataitusi Chinese. O lea e iloa ai se tuufaatasiga i luga o se auala o galuega Chinese.

taoyujun@gmail[.]com

O le domain '**hcjbtt[.]com**' o loo lesitalaina faatasi ai ma le tuatusi imeli '**taoyujun@gmail[.]com**' ae o le imeli a galuega ofisa na lesitala i le '**wangminghua6@gmail[.]com**'.

E le o i ai se gaioiga leaga tele e fesootai i le domain '**hcjbtt[.]com**', ae ui i lea o le tuatusi imeli '**taoyujun@gmail[.]com**' sa maua i tala'aga faamata'u i lipoti o tomai. I le 2014, sa fa'aaoga e lesitala ai se domain na maua e Mandiant i le '**Cueisfry Trojan**' i mea faataitai na fa'aaoga i le tulituliloaina o faalapotopotoga Japanese.

O le tuatusi imeli na lesitala ai foi domains e pei o '**iaea-international[.]org**' faapea na foliga mai na fealuai faapea o le **International Atomic Energy Agency** ma le '**idc-ctbto[.]org**' fealuai faapea o le **International Data Centre** i le **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

O se faamaumauga muamua atu o le Whois mo le domain '**iaea-international[.]org**' na iloa ai le imeli na lesitala ai ina ia faapea o le '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

O le domain '**udtglobals[.]com**' sa maitauina o fa'aaoga '**wangminghua6@gmail[.]com**' faapea o le imeli ofisa ma le '**ocean.nio@rediffmail[.]com**' faapea o le imeli lesitala o le tuatusi imeli. O isi faamaumauga a le WHOIS mo le domain lenei, na iloa ai o le imeli lesitala e tasi ae faatasi ai ma le tuatusi imeli ofisa '**taoyujun@gmail[.]com**'.

‘**udtglobals[.]com**’ na alia’e faapea na fealuai faapea o le ‘**UDT Global**’ faapea o se mea na tupu i le lalolagi mo puipuiga o lalo o le sami ma kamupani o puipuiga. O le igoa e saini ai ‘**ocean.nio**’ i totonu o le tuatusi imeli na mafai ona faataitaia le **National Institute of Oceanography (NIO)** faapea o loo i ai pea i le tele o atunuu. E ui o le fa’aaoga o le ‘**Rediff**’ auaunaga imeli (faapea e i ai i India) na mafai ona fautuaina le faataitaia o le **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

O le domain ‘**djibdiplomatie[.]com**’ na aliali ane o loo fealuai Djibouti i auaunaga e vaavaaia tagata, faapea e i ai faamaumauga tali tutusa o WHOIS i le ‘**utdglobals[.]com**’**.** O se tasi o faamaumauga na aliali ane ai ua iloa ai le lesitala ‘**ocean.nio@rediffmail[.]com**’ ma galuega ofisa ‘**taoyujun@gmail[.]com**’ faapea ai o isi faamaumauga na iloa ai ‘**wangminghua6@gmail[.]com**’ faapea o le tuatusi imeli ofisa i le ‘**ocean.nio@rediffmail[.]com**’ faapea o le imeli lesitala.

O domains uma nei e lua e i ai foi le tau i keyboard walking type i faamaumauga a le WHOIS. Mo se faataitaiga, ‘**udtglobals[.]com**’ e i ai le tau ‘**ASDF**’ faapea o lona lesitala i le taulaga ma le ‘**djibdiplomatie[.]com**’ e i ai ‘**DAF DAGF**’ faapea o le tau o le igoa lesitala. O lea e faatusatusa i tau na maitauina i isi domain BADBAZAAR.

E ui o tuatusi imeli ‘**wangminghua6@gmail[.]com**’ ma le ‘**taoyujun@gmail[.]com**’ o loo maua i faamaumauga a WHOIS mo domains o fealuai faapea o le **global undersea defence event**, **Djibouti diplomacy services** ma le **International Atomic Energy Agency**, o loo i ai foi i latou i faamaumauga a le WHOIS mo le tele o domains e le matu’ia le leaga.

O le fefiloi o domains feoai ma domains e le matu’ia na mafai ona fautuaina le i ai pea o se fausaga o se faalapotopotoga e maua ai mea na fa’aaoga e lagolago ai gaioiga a le augaoi i luga o initaneti.

O le tuatusi imeli ‘**ocean.nio@rediffmail[.]com**’ o loo maua na o domains o loo feoai na faamatalaina atu i luga. ‘**ivan_s81@mail[.]ru**’ ma le ‘**tplutalova@list[.]ru**’ na lesitala i se numera laitiiti faalausoso’o o domains, ma o nisi o nei domains na mautu ai fausaga a le BADBAZAAR. O nei tuatusi imeli e tolu ua talitonuina e sili atu le fesootaiga i gaioiga matu’ia a le augaoi i luga o initaneti. O lea ona o le numera o domains e maualuga atu latou te faifaimea faatasi ma

fesootaiga i gaoiga matu'ia, i le faatusatusa atu i imeli '**wangminghua6@gmail[.]com**' ma le '**taoyujun@gmail[.]com**'.

(Tagai ane i le Annex A, image 5)

Fesootaiga i isi aufaamata'u

O le isi amio masani o sootaga o domains a le BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', ma le '**voiceoftibet[.]net**' e faapea na latou lesitala uma i le eNom ma na 'paka' i le '**255.255.255[.]254**'.

Mulimulitai ai i suesuega talu ai a le NCSC, o isi domains e i ai mataitusi nei na iloa ai gaioiga na fesootai i le **APT5** i le 2019, ma le **APT14** i le va o le 2009 ma le 2011.

O le APT5-na fesootai domains sa i ai faamaumauga o tala'aga WHOIS faapea na lisiina '**taoyujun@gmail[.]com**' faapea o le tuatusi imeli lesitala.

O le APT14-o domains fesootai na i ai mataitusi e fa o domains laiti faapea na iloa na tuuina atu le taulai faamoemoe i a latou gaioiga matu'ia. O se faataitaiga o le mea lea o le '**bae.cisconline[.]net**', faapea na fautuaina na taulai faamoemoe o BAE Systems ma na maua i se mea faataitai '**Poison Ivy**'.

O se ituaiga e tali tutusa na maitauina i domains a le BADBAZAAR faapea e faatatau i domains laiti i le igoa o le trojanised app:

Ulutala o le Talosaga	C2 URL
Muslim Pro	**mpp**.pmstwocqn[.]com
Video Player mo Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Leitio Afghanistan	**afg**.collinformations[.]com
EN-UG Dictionary Free	**eud**.titeperformance[.]com
Disk Video Recovery	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

E tāua ina ia manatua faapea o gaioiga e faatatau i le APT5 ma le APT14 o tala'aga ma sa i ai foi isi domains na lesitala i le eNom ma faaleleia i le '**255.255.255.254**' faapea e le mafai ona fesootai i gaioiga matu'ia. O le mea lea e le mautinoa faapea o i latou e faatinoina o i tua o nei faalauiloa e tutusa pe fetaui i ai.

Igoa o Masini

Auiliiliga o le BADBAZAAR C2s ma mea faataitai na iloa ai igoa o faafoeina na fa'aaoga faapea o le tau o 'Common Name' i tusipasi a le SSL. O suesuega a le NCSC i igoa o masini fesootai na maitauina o mea faataitai i le BADBAZAAR ma fausaga na iloa ai faapea o masini fesootai nei na fa'aaoga i le tele i tuatusi IP. O nei tuatusi IP o loo fesootai domains na maua i mea faataitai a le BADBAZAAR. O loo tele nisi faamatalaga i le vaega o i lalo e uiga i igoa o hostnames, ma tuatusi IP faatasi ai igoa o faasalalauina domains a le BADBAZAAR C2.

I le tele o mataupu e i ai tusi faamaonia ai le tau o igoa e sili atu i luga o faaiuga IP mo igoa matu'ia o domain faapitoa, o nai mea faapea e, o le mataupu lenei na auiliili mai.

WIN-EU0VLBL7TUJ

O le igoa o le komipiuta '**WIN-EU0VLBL7TUJ**' sa maitauina i tuatusi IP nei e fia iloaina:

- '**116.203.53[.]21**' hosted BADBAZAAR C2 sub-domains '**uyapkfinder[.]com**' ma le '**thewestuniverse[.]com**'.

- '**95.216.169[.]27**' na faasoa domains BADBAZAAR C2 '**adysfunction[.]com**' ma domain laiti '**download.apkbazar[.]biz**' na maitauina faapea o se feaootaiga e download ai mo se mea faataitai a le BADBAZAAR.

(Tagai ane i le Annex A, image 6)

WIN-70E59JVOB9G

Hostname '**WIN-70E59JVOB9G**' na maitauina i luga o tuatusi IP nei e fia iloaina:

- '**23.88.28[.]220**' na faamau ai domains laiti a le BADBAZAAR C2, '**aua.rondwsign[.]com**', '**nal.tokenmajorp[.]com**', '**pep.rondwsign[.]com**' '**doa.rondwsign[.]com**', ma le '**pls.rondwsign[.]com**'. Sa i ai se taimi e lua

aso e va ai faapea na iloa mulimuli ai le tusi faamaonia o le masini, ma ina ua iloa muamua domains matu'ia ua iu atu i le IP.

- '**23.88.28[.]221**' na tali atu e le BADBAZAAR fesootaiga o domain laiti '**bt.bhvghg[.]com**'.

- '**23.88.28[.]222**' na tali atu domains a le BADBAZAAR C2 '**tubevideoplus[.]org**' ma le '**cde.mpoxcases[.]com**'.

- '**65.21.92[.]67**' hosted BADBAZAAR C2 sub-domain '**bat.androidupdated[.]net**'. Na faapea foi ona talimalo i domain laiti '**apps.androidupdated[.]net**' faapea o se DoubleAgent polokalame leaga C2.

- '**65.21.92[.]77**' hosted BADBAZAAR C2 sub-domains '**wyo.titeperformance[.]com**', '**big.collinformations[.]com**' '**vpf.titeperformance[.]com**', '**eud.titeperformance[.]com**' ma '**afg.collinformations[.]com**'

- '**65.108.192[.]134**' hosted BADBAZAAR C2 sub-domains '**upd.whoscaller.net**'. ma '**ggl.whoscaller[.]net**'.

- '**142.132.131[.]15**' hosted BADBAZAAR C2 sub-domains '**bvn.lookincategory[.]com**' ma '**edr.lookincategory[.]com**'**.** Sa i ai se taimi e fitu a o va ai ina ua iloa mulimuli ai le tusi faamaonia ma le igoa o le masini, ma ina ua iloa muamua masini matu'ia le leaga na iu i le IP.

- '**142.132.131[.]20**' hosted sub-domains '**son.onlinegamersgroup[.]com**' ma le '**system.onlinegamersgroup[.]com**', na talitonuina ina ia faapea o le BADBAZAAR C2s faapea na latou talimalo aia o faifaimea le BADBAZAAR ma tusi faamaonia SSL na maitauina i luga o le IP.

- '**142.132.131[.]28**' na taliaina le domain BADBAZAAR C2 '**goldplusapp[.]net**' ma domain laiti '**who.goldplusapp[.]net**' ma le '**cgf.goldplusapp[.]net**'.

- '**162.55.103[.]211**' hosted BADBAZAAR C2 sub-domains '**oha.alpinemap[.]net**', '**aru.alpinemap[.]net**', '**aso.alpinemap[.]net**', '**afr.alpinemap[.]net**', ma le '**aar.alpinemap[.]net**'.

- ‘**162.55.103[.]212**’ hosted BADBAZAAR C2 sub-domains ‘**pep.rondwsign[.]com**’, ‘**ckp.jkiohreh[.]com**’, ‘**aar.tokenmajorp[.]com**’, ‘**nal.tokenmajorp[.]com**’, ‘**pls.rondwsign[.]com**’ ma le ‘**aua.rondwsign[.]com**’.

- ‘**195.154.47[.]99**’ hosted BADBAZAAR C2 sub-domains ‘**ggl.whoscaller[.]net**’ ma le ‘**upd.whoscaller.net**’. Sa i ai se taimi e tolu aso e va ai ina ua muamua iloa le igoa o le masini ma le tusi faamaonia ma ina ua iloa ai domains matu’ia le leaga na mautu atu i le IP.

- ‘**195.154.60[.]3**’ na teuina domains laiti BADBAZAAR C2 ‘**upd.whoscaller[.]net**’, ‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ na teuina BADBAZAAR C2 domains laiti ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ ma le ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ na teuina domains BADBAZAAR C2, ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ ma le ‘**bvn.lookincategory[.]com**’.

(Tagai ane i le Annex A, image 7)

WIN-50QO3EIRQVP

Teuina i le igoa ‘**WIN-50QO3EIRQVP**’ na maitauina i luga o tuatusi IP nei e fia iloaina:

- ‘**45.76.132[.]91**’ teuina i masini, ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. O masini uma e lua o loo fesootai atu i le BADBAZAAR faapea o se masini laititi ‘**fow.yumoftion[.]com**’ ma le ‘**bat.androidupdated[.]net**’ o masini BADBAZAAR C2. Fa’aopopo i ai o domain laiti ‘**apps.androidupdated[.]net**’

o se DoubleAgent C2 domain. E fa'aalia ai foi domain '**pmstwocqn[.]com**', e feoootai i le BADBAZAAR e ala i faamaumauga a le WHOIS .

- '**95.179.210[.]85**' na faalauiloaina '**clublogs[.]com**', e faapea o le '**xle.clublogs[.]com**' o se polokalame autu a le BADBAZAAR C2 ma faapea foi ona faalauiloaina le BADBAZAAR e fesootai ma polokalame autu '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**www.voiceoftibet[.]net**' ma le '**actuallys[.]com**'.

- '**199.247.21[.]34**' hosted '**titeperformance[.]com**', ma '**collinformations[.]com**' faapea o subdomains a le BADBAZAAR C2 domains.

- '**217.69.10[.]128**' hosted BADBAZAAR C2 domain '**uyghurdict[.]com**'.

(Tagai ane i le Annex A, image 8)

WMSvc-WIN-50QO3EIRQVP

Hostname '**WMSvc-WIN-50QO3EIRQVP**' sa maitauina i luga o tuatusi IP nei:

- '**78.46.185[.]251**' hosted BADBAZAAR C2 domain '**groupgram[.]org**', na lipotia e Volexity na fa'aaogaina port 4432 mo fesootaiga leaga.

- '**65.21.92[.]69**' **ma le** '**163.172.205[.]207**' hosted domain '**widelygram[.]org**' faapea e talitonuina o se domain a le BADBAZAAR C2 , a o hosted i ai i luga o Ips uma e lua, port 4432 sa Tatala .

- '**163.172.198[.]206**' hosted domain '**maxgram[.]org**' faapea na talitonuina o le BADBAZAAR C2 domain, faapea sa i ai 4432 sa tatala.

(Tagai ane i le Annex A, image 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Hostnames '**WMSvc-WIN-50QO3EIRQVP**' ma '**WIN-7LSBB9R0F1L**' na maitauina i luga o tuatusi IP nei faalausoso'o:

- '**148.251.87[.]245**' hosted BADBAZAAR C2 domains '**flygram[.]org**' ma '**groupgram[.]org**'.

(tagai ane i leAnnex A, image 10)

WIN-N8H8S9BG2P0

Hostnames '**WIN-N8H8S9BG2P0**' na maitauina i luga o tuatusi IP nei:

- '**148.251.87[.]247**' hosted BADBAZAAR C2 domains '**omarwhatsapp[.]org**' ma '**flygram[.]org**'.

(Tagai ane i le Annex A, image 11)

WIN-I6VBN8MR92A

Hostnames '**WIN-I6VBN8MR92A**' na maitauina i luga o le tuatusi IP lenei:

- '**148.251.87[.]197**' hosted BADBAZAAR C2 domain '**tryhrwserf[.]com**'.

(Tagai ane i le Annex A, image 12)

E fua i luga o faamaumauga faapisinisi o loo maua le salalau o igoa o masini nei faalauaitele i le initaneti e eseese. O nisi o i latou o loo maitauina faasolosolo i le tele o tuatusi IP faapea e iloa ai na faavaeina VMs mai i se pepa o faamatalaga ua uma ona fafauina e tasi. E tāua ina ia maitau mai faapea o nisi o igoa o masini tumau, e le o IPs uma faapea na maitauina i latou e mafai ona fesootai i gaioiga matu'ia le leaga. O le uiga o lea e mafai faapea o le fa'aaogaina o igoa o masini tumau e le faapea e aofia uma ai i faamata'u nei.

Ae ui i lea, o le salalau o nisi o igoa o masini nei i le lautele o IPs faapea na taliina domains a le BADBAZAAR C2, e mafai ona fautuaina faapea ina ia maua mai se mea i fausaga o faalapotopoptoga o loo fa'aaogaina ina ia faatulaga ai masini ia lagolagoina ai faatinoga leaga a le augaoi i luga o initaneti.

O le i ai o ala o faasalalauga

O lipoti talu ai e Volexity na iloa ai faapea o ata video YouTube (faamalosia ai le fa'aaoga o talosaga matu'ia) na fafauina e i latou e faatinoina matu'ia i luga o initaneti. O nei videos e aofia ai le a'oa'oina pe faapefea ona fa'aaoga talosaga na faavaeina.

Na iloa e le NCSC e lua ala o faasalalauga fa'aopopo a le YouTube e faatatau i faatinoga o faamata'u a i latou e faatinoina. O auala o faasalalauga a le YouTube faatasi ai ma le URL taulimaina '**@josephjoey3499**' na alia'e ai faapea a faalauiloa ai le fa'aaogaina o le '**Maxgram**' ma se fa'aopopoga o channel na lesitala i le '**@uyghurapks3096**' faalauiloa '**Uyghur APK Finder**'.

Fa'aopopo i ai, O videos YouTube o loo Faalauiloa ai le '**Flygram**' ma le '**Signal Plus**', na iloa ai gaioiga faamata'u o loo fa'aaogaina e i latou o faatinoina e fa'aaoga ai numera telefoni o iloa atu ai. i le '**Flygram**' video, e 0:36 numera telefoni '**+1 (570) 378-7250**' o iloa atu ma taimi o le '**Signal Plus**' video, o le numera telefoni '**+1 (267) 298 4259**' o loo faailoa ai.

Na lipotia e Volexity se upega tafailagi o tala fou e le moni i Tibet '**ignitetibet[.]net**', faapea na latou mauaina i ala o faasalalauga o Telegram na talitonuina na faatinoina e le vaega faamata'u. Tuatusi imeli '**choekyi.wangmo@ignitetibet[.]net**' o loo maitauina o loo tuu mai ai manatu fa'aalia i mea o tuuina atu i luga o le itulau '**tibetone.org**' faapea na lipotia faalauaitele e le Lookout faapea o se itulau C2 na fa'aaoga mo le eseesega iOS o mea a le BADBAZAAR.

O lenei tuatusi imeli ua talitonuina sa pulea e se tagata o faatinoina, e fa'aaoga ai faafoliga ia '**Choekyi Wangmo**'.

Suesuega

BADBAZAAR ma MOONSHINE e fa'aaoga nai metotia fa'ainisinia lautele ina ia taulai faapitoa ai komiuniti Uyghur, Tibetan ma Taiwanese, faaigoaina:

- o le polokalame taufaasesē o apps e fia iloa e komiuniti nei, e pei o gagana Uyghur ma le app Quran, e toeitiiti a mautinoa na faasoaina e fua e taulai i tagata ua afaina
- o le fa'aopopoina o polokalame taufaasesē o apps nei i faleoloa aloaia o app e maualuga atonu na tuuina atu se lagona o le mea moni, ma le faasoa i faatalanoaga i kulupu e maualuga e ono faamoemoe ina ia faaleaga ai mafutaga faatuatuaina i totonu o nei komiuniti

BADBAZAAR ma le MOONSHINE e aoina faamaumauga faapea e faia toeitiiti lava mautinoa faapea o le tau o le setete Chinese. E ui o le BADBAZAAR ma le MOONSHINE na maitauina tulituliloaina tagata taitoatasi Uyghur, Tibetan ma Taiwanese, o loo i ai isi polokalame faapea e tuliloaina isi kulupu laiti i totonu o China. O tagata sitiseni mai atunuu o loo faamauina pepa o faamatalaga, i totonu o China ma tua atu, faapea o loo talitonu ina ia lagolagoina mafua'aga faapea e faamata'u ai le mautū o le puleaga, toeitiiti a mautinoa o i lalo o faamata'u mai polokalame o telefoni feaveai e pei o BADBAZAAR ma le MOONSHINE. O le mafai ona ia maua mai nofoaga, ata, ma faamaumauga pu'e leo e mafai ona tu'uina mai le avanoa i le mata'ituina ma gaioiga faasoesā i le lumanai, i le tuuina atu o faamatalaga sa'o i le taimi o gaioiga taula'i.

MITRE ATT&CK®

O lenei lipoti na tuufaatasia ma le manatu amanaia i le faavae o fausaga a le MITRE ATT&CK®, o se silafia e maua uma i le lalolagi ma le iloa o gaioiga faaleaga ma auala e fai ai e fua i luga mea na maitauina i le lalolagi moni.

Gaioiga	ID	Faiga e faatino ai	Auala aloaia e fai ai se mea
Siakiina o se tulaga	T1593.001	Saili Tatala Upega tafailagi/Polokalame Komipiuta: Ala o Faasalalauga	O i latou e faatinoina e sailia kulupu i luga o initaneti ma faatalanoaga e tutusa i a latou tagata ua afaina ina ia faasoa ai le polokalame faaleaga masini
Atia'e Alaga'oa	T1583.001	Ia maua Fausaga: Domains	E lesitala se vaega o komipiuta e tagata e faatinoina mo auala o a latou komipiuta e faatonutonu ma pulea
Atia'e Alaga'oa	T1587.001	Faavae Mea Eseese o le mafai ma faatino ai: Polokalame komipiuta e matu'ia le leaga	O se code matu'ia o loo tusia mo le tuuina i totonu o se app faafoliga
Atia'e Alaga'oa	T1608.001	Tulaga o Agavaa: Upload Malware	Polokalame faafoliga o loo upload i luga o auala o komipiuta e aofia ai faleoloa o apps
Atia'e Alaga'oa	T1585.001	Faavae ni Accounts: Accounts o Ala o Faasalalauga	E faavae e i latou e faatinoina accounts i luga o upega tafailagi e faasoa ma faasalalau ai polokalame matuia o komipiuta
Atia'e Alaga'oa	T1585.002	Faavae ni Accounts: Account Imeli	E fa'aaoga e latou o faatinoina imeli accounts e taliaina tuma'oti ma faapisinisi mo le taliaina ma le faasoaina o polokalame matu'ia o komipiuta
Avanoa Muamua	T1189	O se auala e faaleaga ai se komipiuta e ala i le login	O tusitusiga matu'ia o loo faanana i totonu o apps moni ma upload i faleoloa o apps

Avanoa Muamua	T1566.003	Lafoina o Imeli e le moni: O se ituaiga o le lafona o imeli pepelo e tuliloaina se tagata po o kulupu e ala i auaunaga	E lafo e le aufaasese apps faafoliga i kulupu mataituina e ala i auala o faasalalauga e aofia ai Telegram
O le faia o se fuafuaga ina ia mae'a ai	T1204.002	O se Tulaga faapea e faaleaga ai e le au osofai gaioiga a se tagata o loo fa'aaogaina ina ia maua ai se code e faauma ai: O se Faila ua fafauina ina ia faaleaga ai komipiuta po o fesootaiga	Ua faapipii e tagata ua afaina apps o polokalame faalafi ina ia faataunuuina ai faasologa o totogi
Auala e fa'aoga e le au osofa'iga e 'aua ai ne'i iloa	T1027.009	O Faila e Faalilolilo po o Faamatalaga: Faatumuina Faalilolilo o Faamaumauga	O le code faaleaga mea o loo faalafi i totonu o apps moni
Auala e fa'aoga e le au osofa'iga e 'aua ai ne'i iloa	T1036.005	Faafoliga: Faatutusa Igoa Moni po o Nofoaga	O faila faafoliga e tutusa igoa, foliga ma faatinoga o apps faamaoni.
Auala e fa'aoga e le au osofa'iga e 'aua ai ne'i iloa	T1656	Faafoliga i se isi	O i latou nei e faatinoina e faafoliga i tagata faatuatuaina e ala i le faia o kava o upega tafailagi ma fa'aaoga ai username e fesootai ma kulupu o loo tulituliloaina
Aoina mai	T1123	Pu'eina o leo	O apps faafoliga e ono talosagaina faatagana lē talafeagai e aofia ai auala e maua ai mea e faaleotele ai
Aoina mai	T1125	Faaliliuina o Ata Video	O apps faafoliga e ono talosagaina ni faatagana e lē talafeagai e aofia ai le mauaina o mea pu'e ata
Aoina mai	T1005	Faamaumauga mai Accounts e Pulea Auala o Puna'oa	O apps faafoliga e ono talosagaina ni faatagana e lē talafeagai e aofia ai faila faalotoifale.

Puleaga ma Faatonuga	T1071.001	Faatulagana o Tulafono ma tulaga e manino ai faatalanoaga a polokalame Tulaga o Tulafono e pulea faamaumauga	O le polokalame faaleaga komipiuta ua koneti i le C2 e fa'aaoga ai le HTTPS ma le WebSocket's.
Puleaga ma Faatonuga	T1509	O se numera TCP po o le UDP e le fesootai i se auaunaga faapitoa	O se numera port e le fesootai ma auaunaga e pei o le 4432 ma le 2333
Aveesea Faagaoi o Faamaumauga	T1041	Aveeseina o C2 Channels	Polokalame faaleaga na aveesea faamaumauga e fa'aaoga ai le HTTPS ma fesootaiga WebSocket.
Aafiaga	T1565.002	Faaliliuina o Faamaumauga i se tulaga ina ia mafai ai ona fa'aaoga: O le fesuiaiga o faamaumauga i le ui atu mai le isi agai i le isi masini	E maua mai e ala e faatino ai faamaumauga mai ia i latou ua afaina e ala i le mafai e apps fegasoloai i upega tafailagi faapea e le tatau ai mo le faatinoina o le app

Faailoilo

POLOKALAME KOMIPIUTA MOONSHINE:

- O le aso 1 Aperila 2025, o se sailiga mo kava o le VLiteUI na maua mai ai mea nei:

Tuatusi IP	Port	Na Vaaia Muamua	Na Vaaia Mulimuli
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

- I le aso 1 Aperila 2025, o se sailiga mo kava mo SCOTCH ADMIN na maua mai ai mea nei:

Tuatusi IP	Port	Na Vaaia Muamua	Na Vaaia Mulimuli
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

- I le aso 14 Mati 2024, o se sailiga mo kava faatonutonu SCOTCH ADMIN na maua mai ai mea nei:

Domain	Tuatusi IP
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:

Faamatalaga	SSL tusi faamaonia na maitauina i luga o le BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- O le aso 1 Aperila 2025, o se sailiga mo le tusi faamaonia o le BADBAZAAR na maua mai ai mea nei:

Tuatusi IP	Port	Na Vaaia Muamua	Na Vaaia Mulimuli
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

Faamatalaga	SSL tusi faamaonia na maitauina o le BADBAZAAR C2s
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- O le aso 1 Aperila 2025, o se sailiga mo le tusi faamaonia o le BADBAZAAR na maua mai ai mea nei:

Tuatusi IP	Port	Na Vaaia Muamua	Na Vaaia Mulimuli
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

- Fausaga faaofisa a le WHOIS

I lalo ifo o i ai se folasaga o fausaga faaofisa faapea o i ai i le taimi nei po o le tala'aga e i ai faamaumauga o le WHOIS faatasi ai ma tau faapea e tutusa ma i latou na maitauina i fausaga faaofisa a le BADBAZAAR C2.

WHOIS Value	Domains
Setete na Lesitala ai: UJYJYUJ **Atunuu na Lesitala ai: Bolivia** **Tagata Aloaia e Tausia Faamaumauga o Lesitala: 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
Setete na Lesitala ai: REWR **Atunuu na Lesitala ai: CF** **Tagata Aloaia e Tausia Faamaumauga o Lesitala: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com

	• tooenabled[.]com • suguestions[.]com • searching2[.]com
Setete na Lesitala ai: ASDF **Atunuu na lesitala ai: AL** **Tagata Aloaia e Tausia Faamaumauga o Lesitala: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

Ala o Faasalalauga YouTube
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

O mea nei o fesootaiga i isi faailoilo o faaletonu (IoCs) e faatatau i le BASBAZAAR ma le MOONSHINE. E le mafai e le NCSC ona faamautū le aogā o faamatalaga uma i fesootaiga nei ma ua fautuaina le aufaitau ina ia faamaonia tuma'oti lo latou sa'o lelei ma talafeagai ai.

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

Faaitiitia

E faamalosia e le NCSC le fa'aaoga o fautuaga o i lalo ina ia tete'e atu ai faamata'u o loo faamatalaina mai i suesuega o mataupu.

- **O i latou e faatautaia App faleoloa, e aofia ai se isi faleoloa e lona tolu i ai, ma e tatau i tagata atia'e ona fai ia mautinoa faapea o apps i luga o a latou fata o loo puipuia ma latou te usitaia tulaga a le malo o le Code of Practice.** Tagai ane i le Taiala: 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

- **Lagolagosua i Gagana e Tele**: O i latou e atia'eina Apps e tatau ona inivesi i taumafaiga ina ia i ai i lotoifale apps tauta'ua mo i latou e fa'aaogaina faapea e laiti gagana e tautatala ai i le tele o kulupu tulituliloaina e aofia Uyghur, Tibetic, Taiwanese Hokkien ma Cantonese. Taiala a le Apple mo le faaliliuina o apps: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Taiala a le Google i le faaliliuina o apps: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Tausisia lou Tulaga i Auala o Faasalalauga ia Puipuia:** O kamupani i auala o faasalalauga e mafai ona faia ia sili atu le faigata mo le augaoi i luga o initaeti ina ia faia accounts pepelo ma faasoa i ai faila faaletonu po o fesootaiga i luga o a latou fata i se isi itu e moni komiuniti i luga o upega tafailagi. I tulaga e mafai ai, e tatau i kamupani ona faasoa faailoilo leaga faatasi ai ma pisinisi lautele ina ia faaleleia ai le malamalama tuufaatasi i le faamata'u ma fesoasoani ai ina ia i ai tulaga o puipuiga.

- **Fuafuaga e Faaleleia ai mo tagata faatau:** O faalapotopotoga e tatau ona fai auala ia faatulaga e fai ina ia faailoa ai tagata faatau faapea na faapipii ai apps leaga e fa'aaoga a latou auaunaga. O nei faailoilo e tatau ona uai atu i le maua mai o faamatalaga e iloa ai. I tulaga e talafeagai ai, e tatau i faalapotopotoga ona tuuina atu taiala pe faapefea ona aveesea

polokalame komipiuta ma faamalosia i latou ua afaina ina ia lipotia i a latou pule, e pei o le NCSC i le UK.
Tagai ane i le App Store Code of Practice mo nisi faamatalaga: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Kulupu Galulue mo le Tuufaatasiga:** O kamupani i ala o faasalalauga e mafai ona tuufaatasi kulupu faigaluega, e faataga ai a latou vaega puipuia ia faasoa faailoilo faaleaga mea, o TTPs ma le maitauina, faia ia sili atu ona faigatā mo le au faatino e fa'aaoga a latou tulaga e lagolagoina ai faalauiloa faaleaga mea.

- **Mauaina o apps ua fesuia'i:** I tulaga e mafai ai, o i latou e atia'eina app e tatau ona aofia ai faagaioiga faapea e faailoa ai le tagata e fa'aaogaina pe afai na latou downloaded se vaega e le aloaia o se app, ina ia fesoasoani ai i le puipuiga e faasaga i kopi e leaga ai.

Appendix A: Graphs of BADBAZAAR WHOIS clustering / domain broker faamatalaga

Image 1 - 'UKYJYUJ'

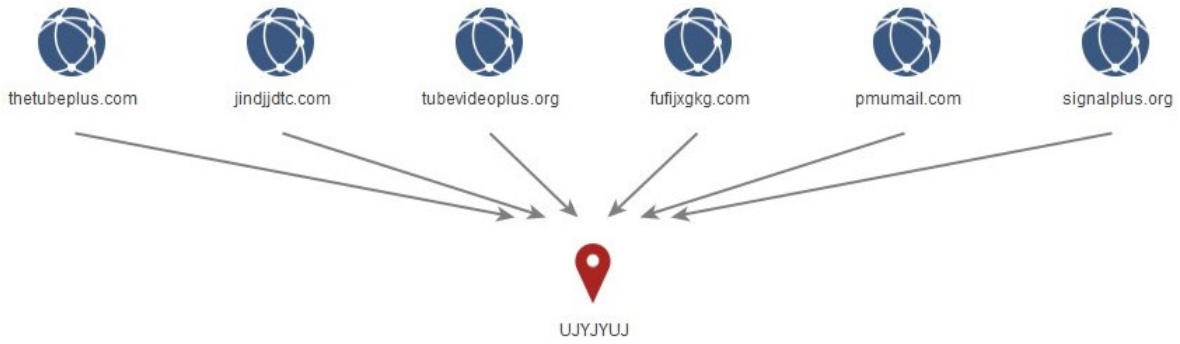


Image 2 – Keyboard walking values

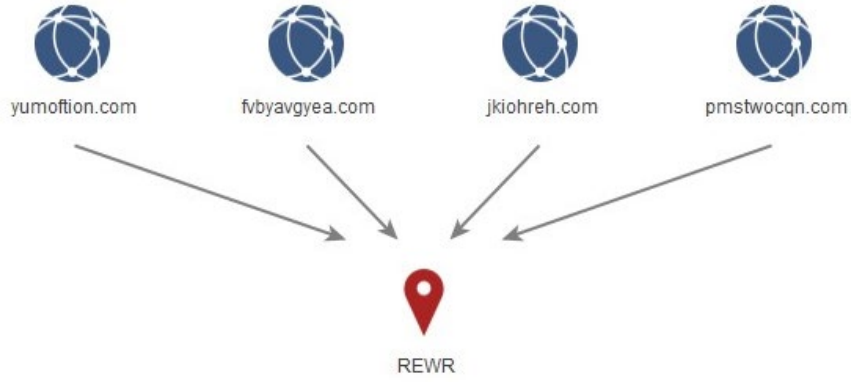


Image 3 – Additional domains with 'FSDF' state field values

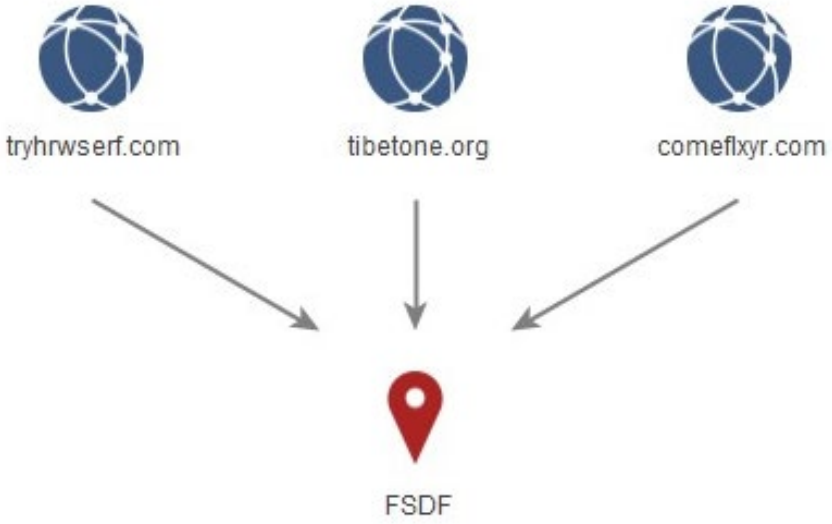


Image 4 – **95.179.210[.]85**

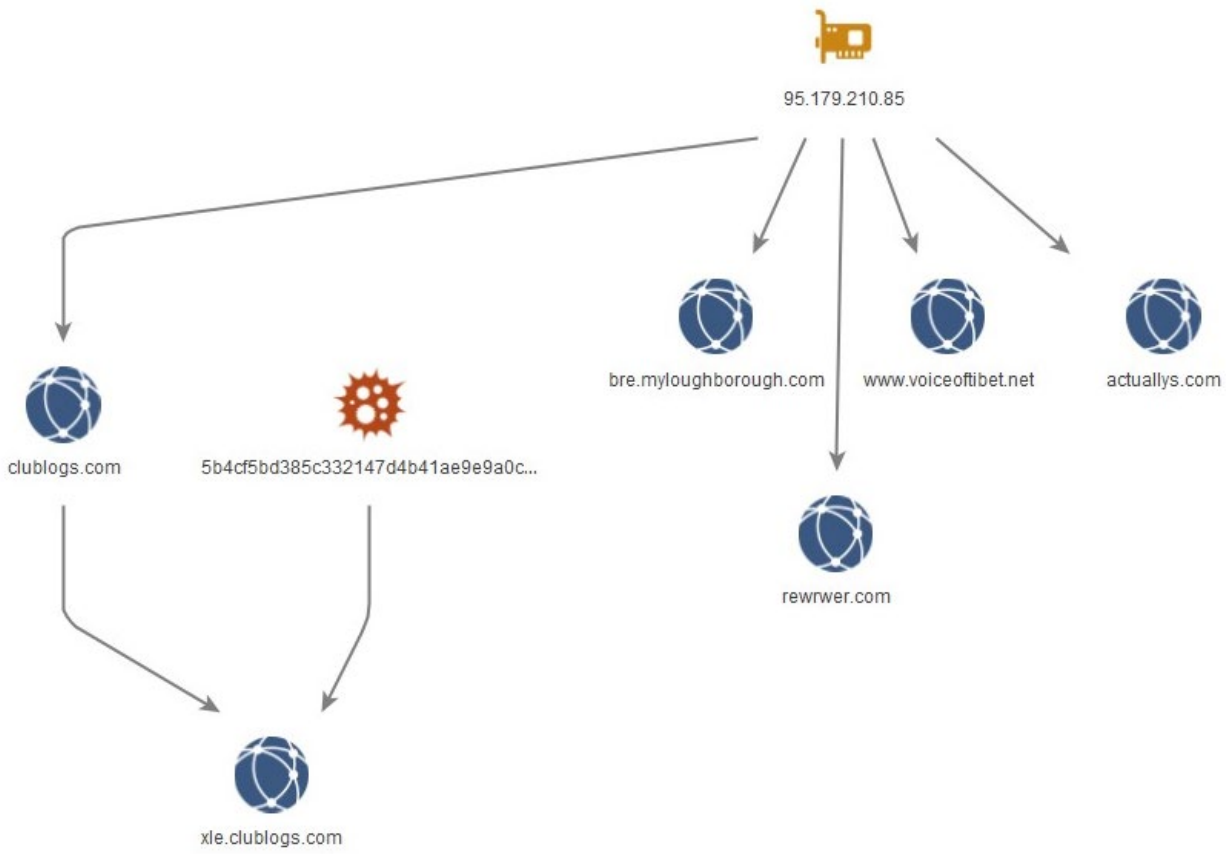


Image 5 – WHOIS links

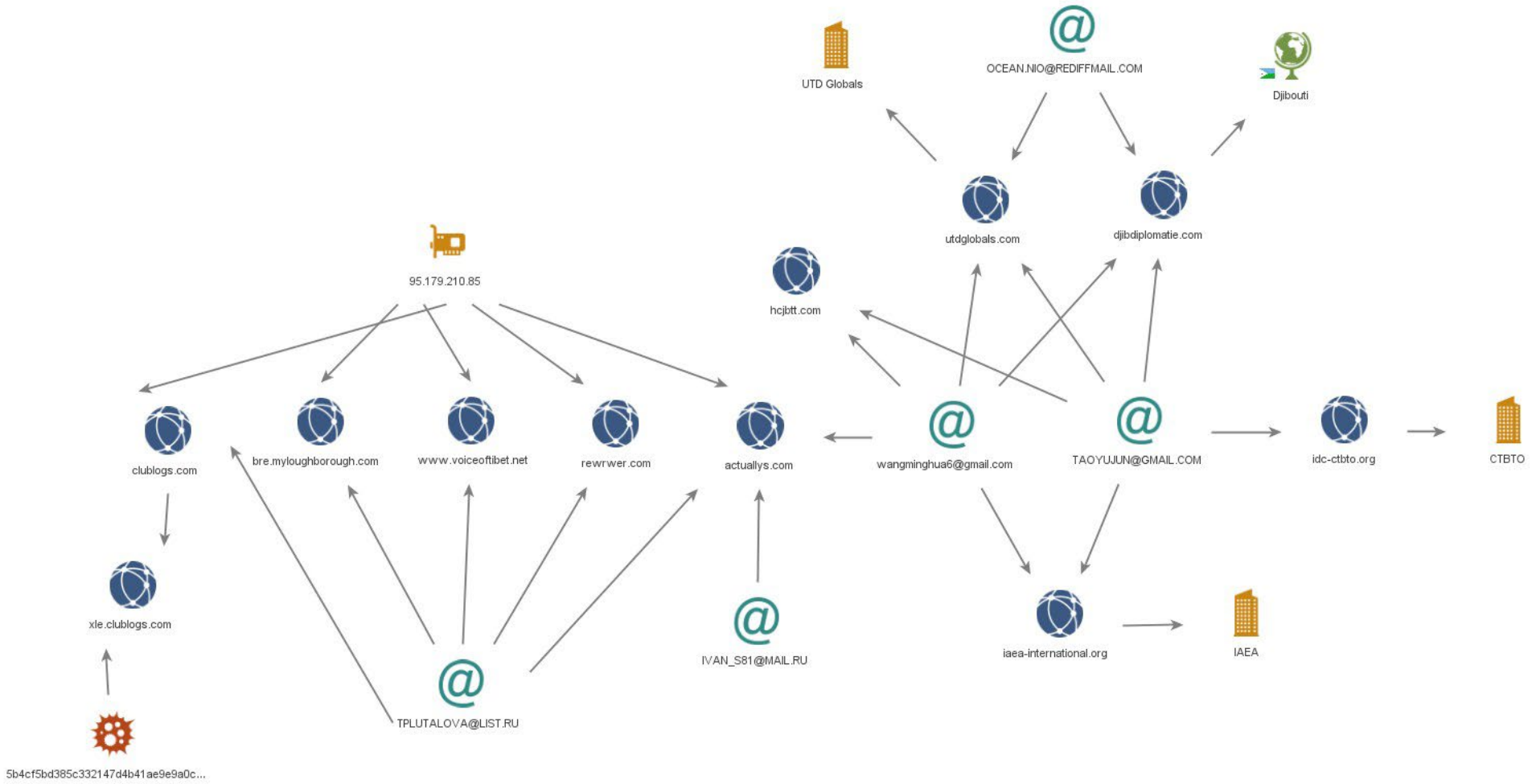


Image 6 – **WIN-EU0VLBL7TUJ**

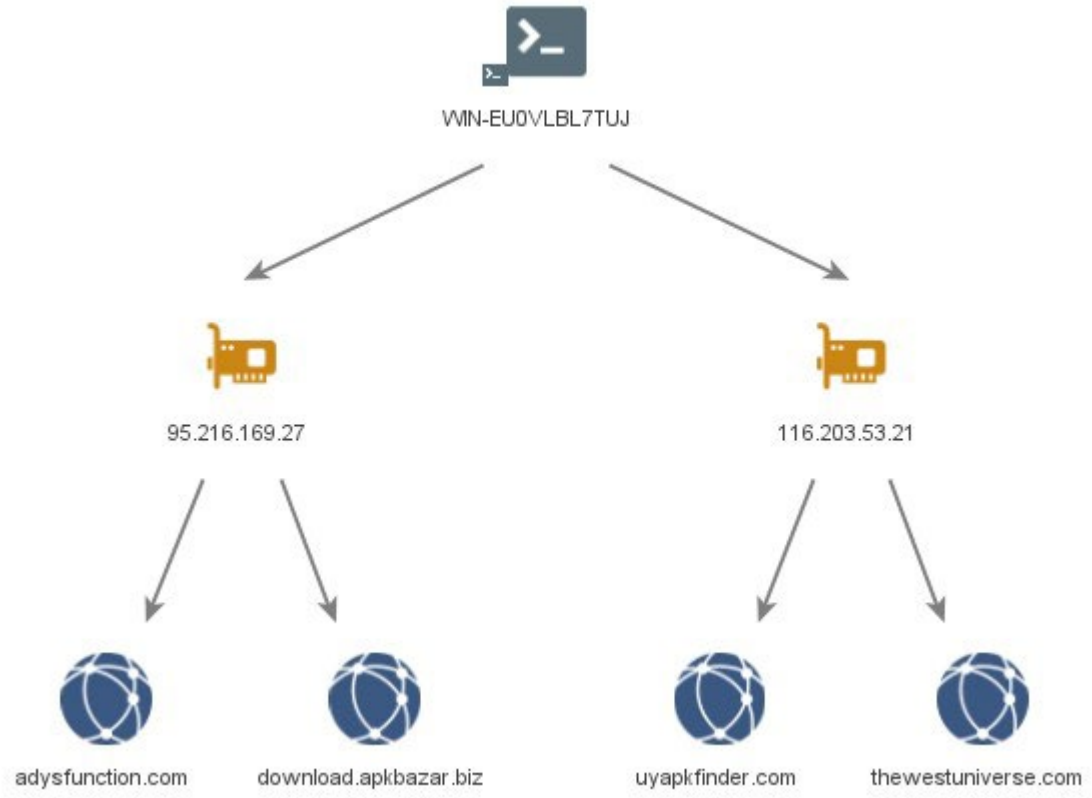


Image 7 – **WIN-70E59JVOB9G**

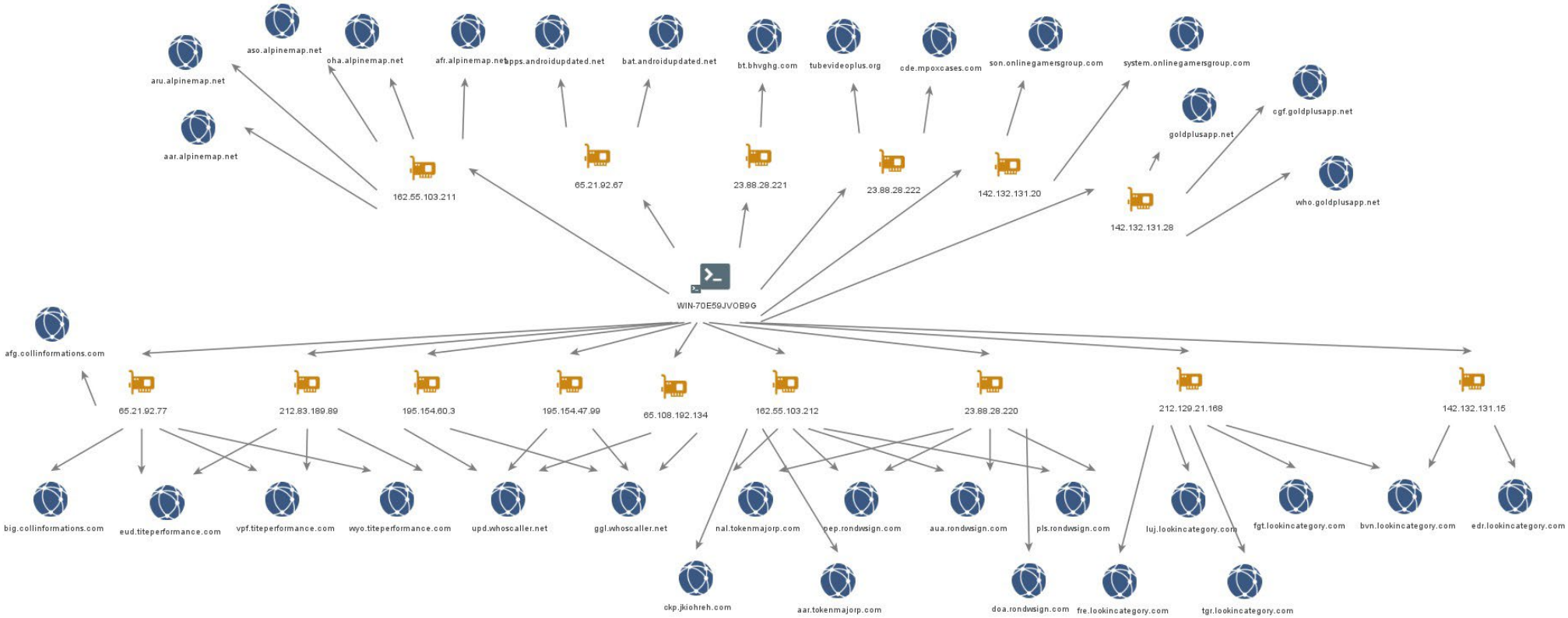


Image 8 - **WIN-50QO3EIRQVP**

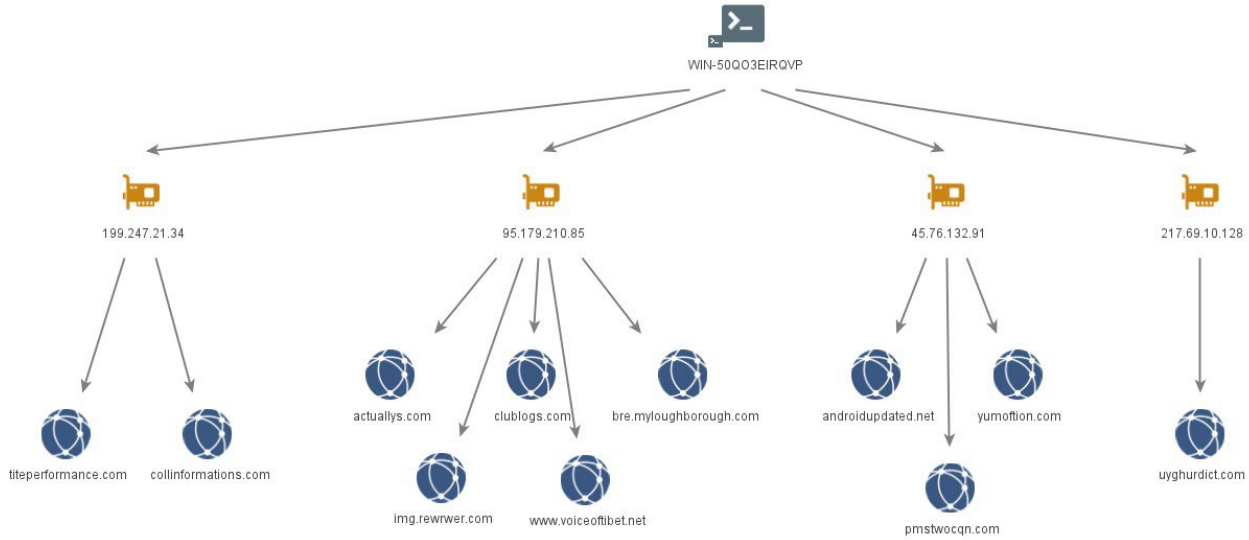


Image 9 - **VMSvc-WIN-50QO3EIRQVP**

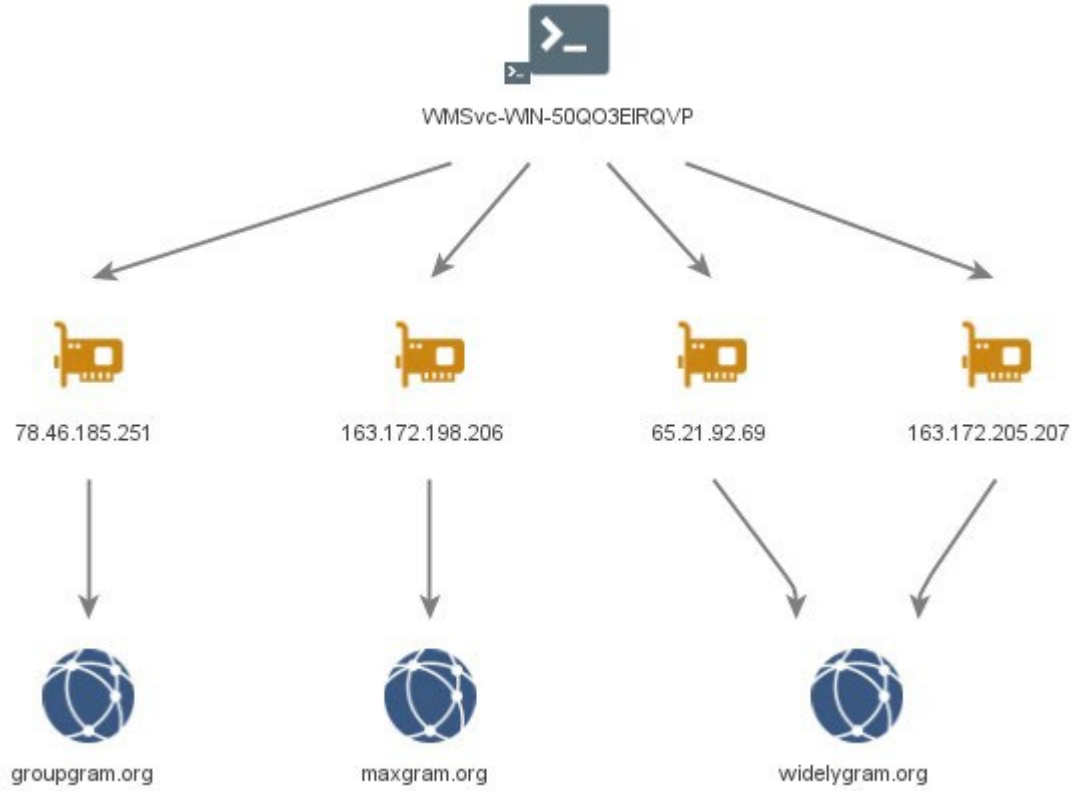


Image 10 – **VMSvc-WIN-50QO3EIRQVP** ma **WIN-7LSBB9R0F1L**

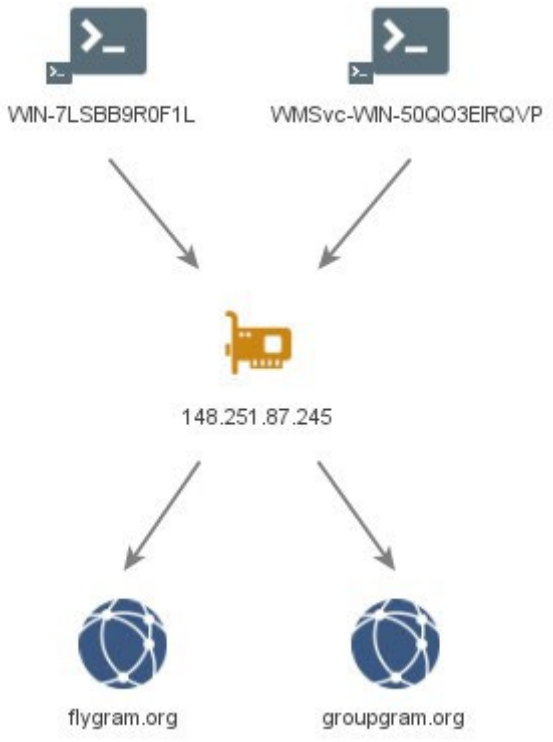


Image 11 - **WIN-N8H8S9BG2P0**

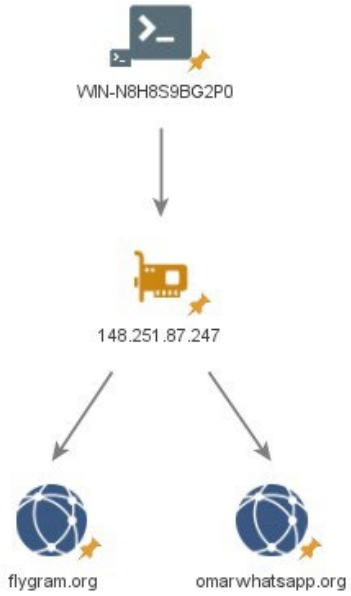


Image 12 – **WIN-I6VBN8MR92A**

Appendix B: MOONSHINE & BADBAZAAR o faataitaiga na maitauina

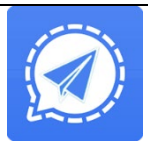
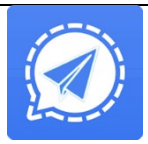
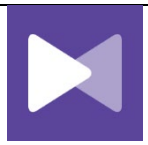
O le fua faatatau o i lalo o loo lisiina ai apps na fa'aaoga i faalauiloa a MOONSHINE ma BADBAZAAR i tausaga e lua ua te'a atu.

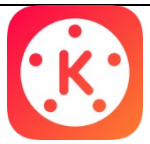
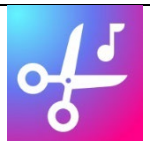
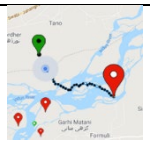
O le tele o nei apps e fa'aalia ai se manino o fa'ata'ita'iga i apps faavaeina. O le mea lea e ono avea ma auala faamoemoeina a le au faatino e faatei ai ituaiga ua iloa lelei.

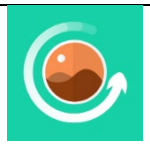
E tāua ina ia manatua, le ulutala o le app, igoa o le package, ma le app icon e mafai uma ona faataitai pe faatusa i talosaga moni ma tatau le so'ona tele le fa'aaoga ia iloa ai po ua pisia se masini.

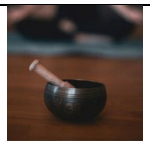
App title	Igoa o le Afifi	App icon
99 Igoa o ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistssongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
VAVE	com.netflix.Speedtest	

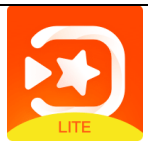
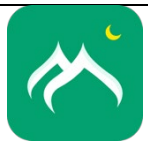
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot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

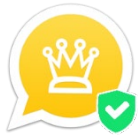
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

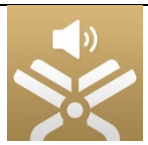
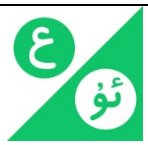
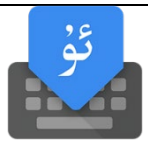
Fesuia'i ai Ata	com.iudesk.android.photo.editor	
Toe Maua Mai Ata	recover.restore.undelete.photo.video.file	
Fale Pu'e Ata	com.kvadgroup.photostudio	
Fa'aopopo	org.telegram.pluspro	
Tusi Tatalo	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Toe Maua Mai Ata na Tapē Ese	com.restore.deleted.pictures.video	
Faailoilo	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	
Uaealesi	org.zhifeijihj.messenger	
Uaealesi	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	
Masini Faaliliu ai Video	com.inverseai.video_converter	
Tipi ai Video	com.naing.cutter	
Lolomi ai I totonu ata video	downloader.video.download.free	
Faiga o ata video	com.bstech.slideshow.videomaker	

Video Player mo Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Masini Pu'eleo	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Tala o le Tau	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	

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

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

Alaga’oa fa’aopopo

Taiala mai le Ofisa Tutotonu i le Malu Puipuia o Tulaga tau Komipiuta Ausetalia

- Lipoti se solitulafono i luga o komipiuta, mea e tupu faafuasei po o le faigofie ona afaina gofie
- Pe faapefea ona malu puipuia au masini
- Malu puipuia lau telefoni feaveai
- Lafoina o imeli pepelo
- Faagaoi
- Malu puipuia au ala o faasalalauga
- Fautuaga pupuu mo le saogalemu i ala o faasalalauga apps o fe’au

Taiala mai le NCSC UK ma le NPSA

- Puipui mai le Faatemokarasi
- Ala o Faasalalauga Faalauaitele: auala e fa’aaoga ai ma le saogalemu
- Taiala i le Malu Puipuia o Masini mo faalapotopotoga e aofia ai telefoni feaveai
- Lipoti o faamata’u i luga o apalai i faleola.
- Saogalemu o le tagata lava ia ma le malupuipuia o tagata taitoatasi e maualuga le lamatia

Taiala mai le NSA US

- Faataitaiga Sili mo Telefoni Feaveai

O se Faamatalaga e te’ena ai

Faamolemole ia utagia mai faapea o lenei faufautua e tuuina atu faamatalaga e moni i le taimi na lomia ai.

O lenei lipoti e maua mai faamatalaga na aumai mai le faalapotopotoga e fausia ma tusia ma punaoa faapisinisi. Soo se mea na mauaina ma fautuaina e lei tuuina atu ma le faamoemoe e foia ai lamatiaga uma ma usitaia fautuaga o le a lē aveesea ai lamatiaga uma. O le tagata e ana faamatalaga e tumau le lamatia faatasi ai ma le tagata e ana auala talafeagai e fai ai i taimi uma.

I le UK, o lenei faamatalaga o loo faasaoina mai lalo o le Freedom of Information Act 2000 (FOIA) ma atonu e sao mai lalo o isi faamatalaga faaletulafono a le UK.

Faasino ane soo se faafesili FOIA i le ncscinfoleg@ncsc.gov.uk.