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

Fale‘i

BADBAZAAR mo e MOONSHINE: ‘Analaiso fakatekinikale mo e ngaahi fakasi‘isi‘i uesia

9 ‘Epeleli 2025

BADBAZAAR mo e MOONSHINE: ʻAnalaiso fakatekinikale mo e ngaahi fakasiʻisiʻi uesia

Fakalukufua

Ko e faleʻi ko ʻení kuo faʻu ia ʻi he poupou mai ʻa e UK Cyber League, fakataha mo e National Cyber Security Centre (NCSC UK) mo e ngaahi hoangāue fakavahaʻapuleʻangá:

- **The Australian Cyber Security Centre, ko e konga ʻo e Australian Signals Directorate**
- **The Canadian Centre for Cyber Security, ko e konga ʻo e Communications Security Establishment**
- **The German Federal Intelligence Service**
- **The German Federal Office for the Protection of the Constitution**
- **The New Zealand National Cyber Security Centre, ko e konga ʻo e Government Communications Security Bureau**
- **The United States Federal Bureau of Investigation**
- **The United States National Security Agency**

ʻOku tuku atu ʻe he faleʻi ko ʻení ha maʻuʻanga fakamatala fakamanamana ʻoku foʻou mo fakatahataha ʻi ʻo kau ki he liuanga ʻe ua ʻo e spyware ʻa ia ʻoku ʻiloa ko e BADBAZAAR mo e MOONSHINE, pea kau ki ai mo e faleʻi maʻa e kau fakalele falekoloa app, kinautolu ʻokú nau faʻú mo e ngaahi kautaha mītia sōsialé ke tokoni ki hono tauhi ke malu ʻenau kakai ʻokú nau ngāue ʻakí.

ʻOku pulusi ʻa e faleʻi ko ʻení ʻo ʻi he taimi tatau mo ha faleʻi maʻa e niʻihi mamahi ʻo e ongo melouea ko ʻení.

ʻOku ngāue ʻaki ʻe he tohi ngāue ko ʻení ʻa e ʻa e ʻuhingaʻi lea meí he lisi ʻo e ngaahi lea ʻa e NCSC ki he spyware: "Ko ha faʻahinga ʻo e meloueá ʻa ia ʻokú ne fokotuʻu ia ʻe ia ke ngāue ʻaki ʻi ha meʻangāue ʻo ʻikai ha fakangofua ʻa e taha ʻokú ne ngāue ʻakí, ʻo ne tānaki fakamatala mo ʻave ia ki ha faʻahi hono tolu."

Keisi ako ʻuluakí: MOONSHINE

Ko e MOONSHINE ko ha spyware ʻi he Android ʻa ia naʻe lipōti ʻi he 2019 ʻe he Citizen Lab ʻokú ne tāketi ʻa e ngaahi kulupu Tibet. ʻOku fakapuli ʻa e MOONSHINE ko ha app ʻoku fakalao ke ne tauheleʻi ʻa e niʻihi mamahí kenau ʻinisitolo ia. Kuo vahevahe fakaʻilekitulōnika ia ʻi he ngaahi sēnolo Telegram pea fou ʻi he ngaahi fehokotakiʻanga ʻinitaneti ʻoku seni ʻi he WhatsApp.

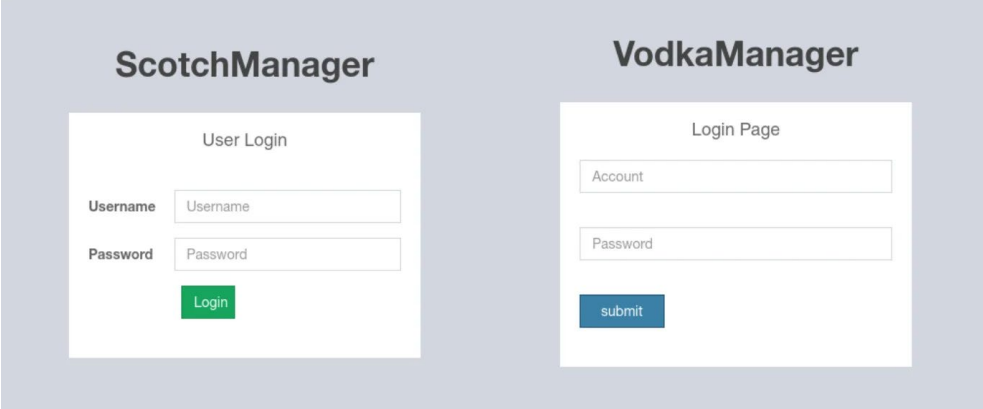
Ko e fakatotolo ʻa e NCSC ki he MOONSHINE ʻokú ne tala ʻa e ngaahi meʻa ko ʻení:

- ʻOku ngāue ʻaki ʻe he MOONSHINE ha management interface ʻa ia kuo hoko ki ai ha ngaahi liliu talu mei hono fuofua lipōtí.
- ʻOku hā meí he manangement interface ʻa e ngaahi ivi ngāue siofi ʻoku lahi, kau ai ʻa e malava ke toʻo ʻa e ngaahi faile meí he ngaahi meʻangāué kae pehē ki hono puke ʻo e ngaahi hiki ʻi he taimi pē ko iá ʻo e ongó mo e ngaahi hiki meí he sikuliní.
- Kuo ʻiloʻi ha seti ʻo e ngaahi management interface ʻa e MOONSHINE ʻa ia kuo housi fakaʻilekitulōnika. Ko e ngaahi interface ko ʻení ʻoku ʻi ai ʻa e fepakifapki ʻi he faʻunga meʻangāue ʻoku ʻi ai ʻenau ngaahi pēnolo hū ʻoku fekauʻaki mo e UPSEC, ʻa ia ʻo fakatatau ki he Intelligence Online ʻoku ʻuhinga ki he ‘Sichuan Dianke Network Security Technology Co., Ltd.’.

Management interface

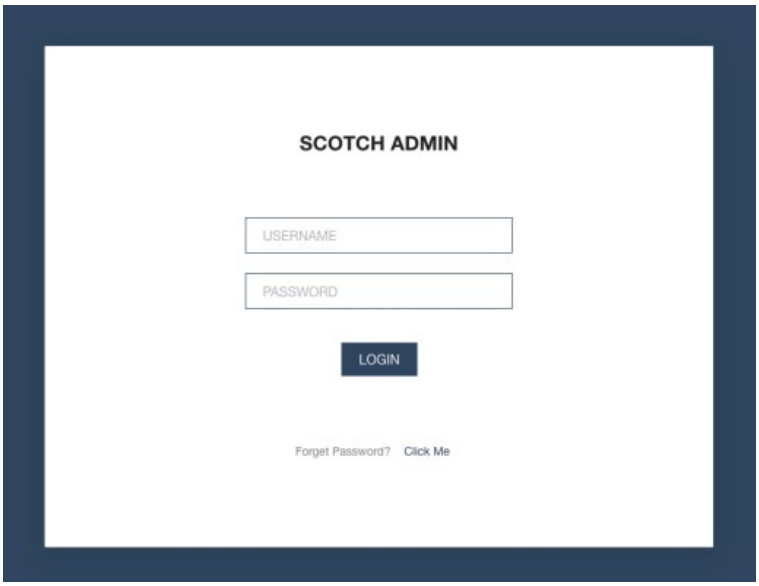
ʻOku fakahā ʻe he lipōti kimuʻa ʻo e management interfaces ʻa e MOONSHINE kuo hoko ki ai ha ngaahi liliu, ʻa ia ʻokú ne tala mai ʻa e hokohoko atu ʻo e fakalakalaka ki aí.

Ko e ʻuluaki fakatātā ʻo e manangement interface ʻoku maʻu ia ʻi he lipōti ʻa e Citizen Lab 2019.



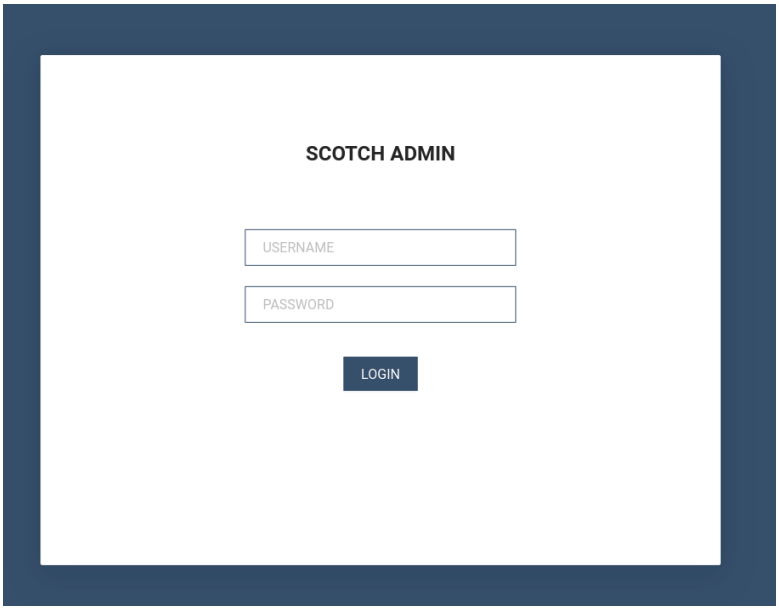
Fakatātā 1: Ko e ngaahi management interfaces ʻa e MOONSHINE ʻa ia ʻoku asi ʻi he lipōti ʻa e Citizen Lab's 2019 ko e 'Fehalāki meí he Fehokotaki ki he Ngaahi kulupu Tibet naʻe Tāketiʻí ʻaki ʻa e Ngaahi Naunau ʻOhofi 1-Click Mobile '.

ʻI he konga kimuʻa ʻo e 2022, naʻe lipōti ʻe he Lookout ha management interface kehe ʻa ia naʻe toe faʻu ke fōtunga ʻo hangē ko ia ʻoku hā atu ʻi laló (ke ne fetongi ʻa e ngaahi interfaces kimuʻa ʻi he Fakatātā 1):



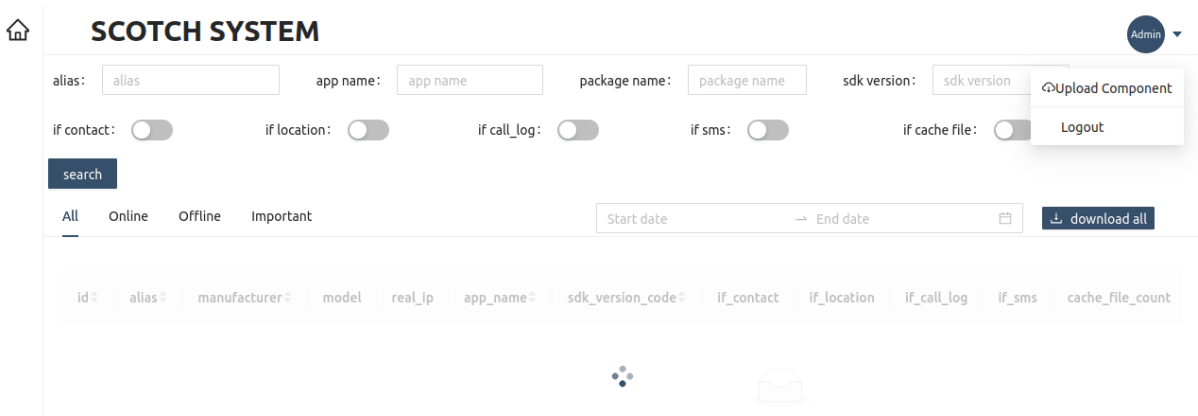
Fakatātā 2: Ko e management interface ʻa e MOONSHINE ʻa ia ʻoku ʻiloʻi ʻi he 2022 lipōti ʻa e Lookout ko e 'MOONSHINE: Liliu ʻa e Surveillanceware ki he Android naʻe faʻu ʻe he kau Siainá ko e APT POISON CARP Ke Tāketi Ki he Kakai Tibet mo e Uyghur.

ʻI ʻAokosi 2023, naʻe hā mei hono sikeni ʻo e fekau mo puleʻi (C2) ʻo e MOONSHINE ha interface ʻoku faitatau mo e interface 2022 ʻaki ʻa e ʻikai toe lava ʻo ngāue ʻaki ʻa e ngāue '**Forget Password**' ʻo hangē ko ia ʻi he Fakatātā 2:



Fakatātā 3: Ko e management interface ʻa e MOONSHINE naʻe ʻiloʻi ʻi ʻAokosi 2023 ʻa ia naʻe ʻikai toe ʻi ai ha fakatokanga 'Forget Password'.

Naʻe hā meí he fakatotolo makehe ʻo e management interface ʻa e koniteni ʻi loto ʻi he pēnoló ʻo hā mei ai ʻa e founga ʻe tauhi ai ʻa e ngaahi fakaikiiki ʻo e ngaahi meʻangāue kuo uesiá.



Fakatātā 4: Ko e peesi uepisaiti ʻi he tuʻa ʻo e peesi hū ʻo e management interface ʻo e MOONSHINE.

ʻOku hā ʻi he fakatotolo ʻa e Lookout ʻa hono ʻave ʻo e **'score'** meí he meʻangāue ʻa e taha mamahí ki he ngaahi seeva ʻa e MOONSHINE C2. Ko e mahuʻinga ʻo e 'score' ʻoku tuʻunga ia ʻi he ngaahi fakangofua ʻa e semipolo kovi ʻoku ʻi he meʻangāue ʻa e taha mamahí.

ʻOku tala ʻe he ngaahi kōlomu 'if_contact', 'if_location', 'if_call_log' mo e 'if_sms' ʻi loto ʻi he peesí ʻoku ʻikai maʻu ʻe he kotoa ʻo e ngaahi semipolo MOONSHINE ʻa e

aʻu kakato ki he ngaahi meʻangāue kuo uesiá. ʻOku tala ʻe he ʻilo ki he ngaahi kōlomu ko ʻení mo e ʻscoreʻ kuo ʻomai meí he meʻangāué ki he C2 ʻa hono ngāue ʻaki ʻe he kakai ngāue kovi fakamanamaná ʻa e score ke fakafetuʻutaki ʻa e tuʻunga aʻu ʻo e meloueá ki he meʻangāue kuo uesiá pea ki he kakai ʻa ia ʻokú nau ngāue ʻaki ʻa e management interface.

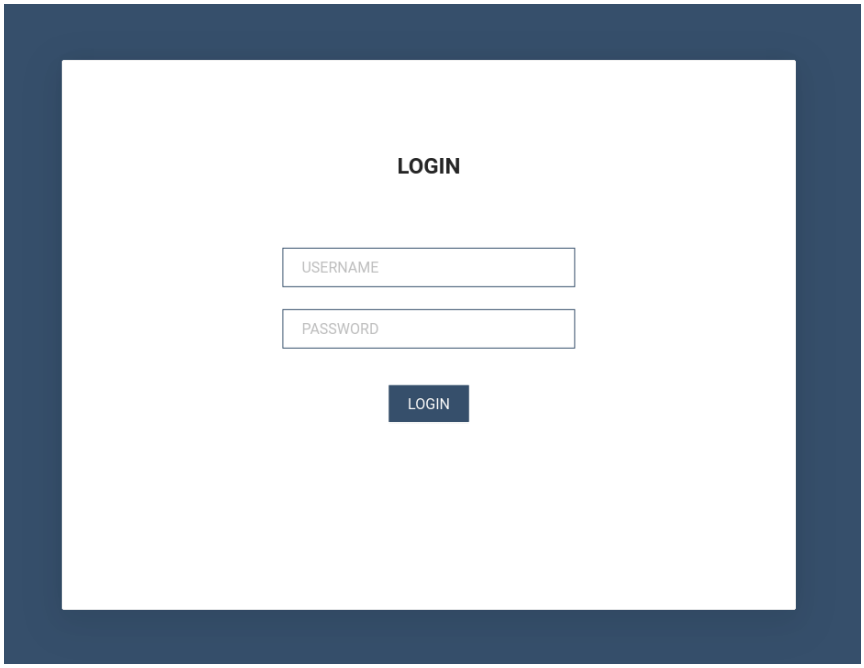
ʻI he fakalukufuá, ko e faleʻi ki he founga lelei taha ki hono taʻofi ʻo e tānaki faamatala ʻa e apps meí he ngaahi meʻangāué ko hono sivi ʻo e ngaahi fakangofua ʻa e app ki ha meʻa ʻoku ʻikai angamaheni kimuʻa pea toki tauniloutí. Neongo iá, ʻoku kumi ʻe he ngaahi semipolo MOONSHINE ʻa e ngaahi fakangofua ʻa ia ʻoku felāveʻi mo e ngāue ʻa e app, koeʻuhí ke ʻoua ʻe asi ngalikehe, ka ʻokú nau ngāue ʻaki foki ʻa e ngaahi fakangofua ko ʻení ke tānaki ʻa e fakamatala meí he ngaahi meʻangāué.

ʻOku ʻi ai foki ʻa e Application Programming Interface (API) ʻa e MOONSHINE ʻa ia ʻokú ne fakahā ʻa e loloto ʻo hono ngaahi ivi ngāué. Ko e ngaahi fuofua tatau ʻo e tohi ngāue API naʻe ʻi ai ʻa e ngaahi hingoa API ʻi he lea Mandarin.

Ngaahi housi fakaʻilekitulōniká

ʻI he ngaahi kumi ki he ngaahi pēnolo MOONSHINE, naʻe ʻilo ai ha ngaahi taimi naʻe hoko ai ha ngaahi housi fakaʻilekitulōniká. Ko e housi fakaʻilekitulōniká ko e taimi ia ʻoku lava ai ʻe he tuʻasila IP ʻe taha ʻo housi ʻa e ngaahi uepisaiti kehekehe ʻi he taimi pē ʻe taha. Naʻe ʻikai ʻiloʻi ʻa e ngaahi tuʻasila IP ʻo e ngaahi meʻa ko ʻeni naʻe housi fakaʻilekitulōniká mo e ngaahi tōmeini naʻe housí i ha taha ʻo e ngaahi semipolo meloueá ʻoku ʻiloʻí.

Naʻe kehekehe ʻa e ngaahi meʻa ko ʻení ʻi he management interface, ʻa ia ko e hingoa ʻo e ngaahi peesí ko e **‘LOGIN’** kae ʻikai ko ia naʻe ʻasi kimuʻá ko e **‘SCOTCH ADMIN’**.



Fakatātā 5: Ngāue ʻaki ʻe he management interface ʻa e MOONSHINE ʻa e hingoa ʻo e LOGIN kae ʻikai ko e SCOTCH ADMIN.

ʻIkai ngata aí, ko e koniteni ʻi he pēnoló naʻe kehe foki ia meí he fakatātā 4, hangē ko ia ko ʻene hā ʻi he fakatātā 6:

Fakatātā 6: Ko e peesi uepisaiti ʻi he tuʻa ʻo e peesi hū ʻo e management interface ʻo e MOONSHINE ʻa ia naʻe housi fakaʻilekitulōnika.

Ko e pēnolo ʻi he fakatātā 6 ʻoku hangē ha tatau kuo fakasiʻisiʻi ʻo e pēnolo ʻi he fakatātā 4. Ko e ngaahi naunau ʻo e pēnoló ʻa ia ʻoku fepakipakí ko e ngaahi hingoa kōlomu ko e ‘id’, ‘manufacturer’ mo e ‘model’ ʻi he tēpilé.

Ko e ngaahi taimi naʻe ʻiloʻi ai hono housi fakaʻilekitulōnika ʻa e MOONSHINE ko e:

Tōmeini	Tuʻasila 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

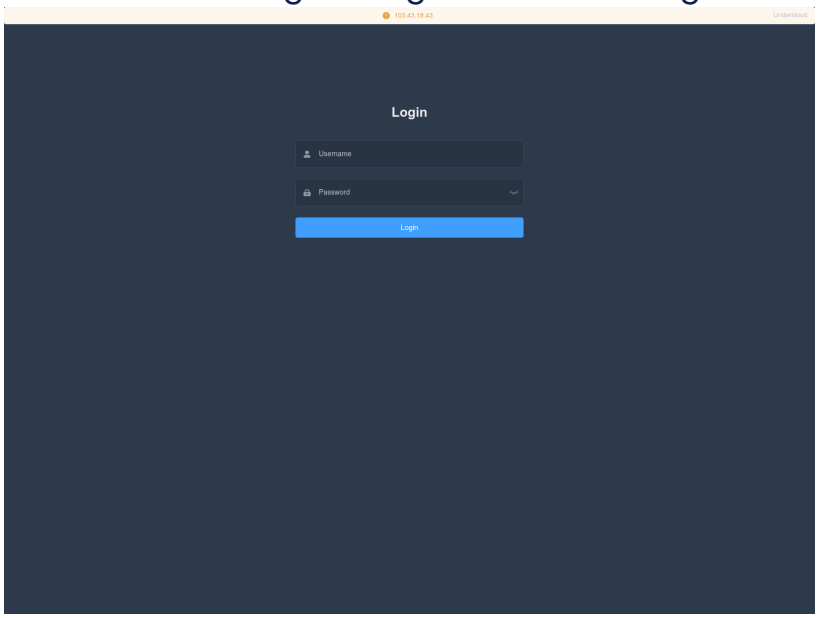
ʻOku lisi ʻa e ngaahi tōmeini ko ʻení ʻe he Trend Micro ko e ngaahi naunau ngāue ʻohofi ʻa e MOONSHINE, ʻa ia ʻokú ne ngāue ʻaki ʻa e ngaahi matavaivai ʻo e polokalama ʻinitanetí ke ʻinisitolo ʻaki ʻa e meloueá ʻi he ngaahi meʻangāue toʻotoʻó. Naʻe fakahingoa ʻe he Trend Micro ʻa e melouea ko ʻení ko e 'Dark Nimbus'.

Ke mahino angé, ko e MOONSHINE management interfaces ʻoku fetuʻutaki mo e ngaahi semipolo melouea MOONSHINE, peá ne toʻo ki ai ʻa e teita ʻa e taha mamahí. Ko e ngaahi naunau ngāue ʻohofi ʻa e MOONSHINE ʻa ia kuo lipōti ʻe he Trend Micro, ko ha ivi makehe ia ʻokú ne ʻohofi ʻa e ngaahi matavaivai ʻo e polokalama ʻinitanetí ke ʻinisitolo ʻaki ha melouea ʻoku ui ko e Dark Nimbus ʻi he ngaahi meʻangāue toʻotoʻó. ʻIkai ko ia pē, ko e Dark Nimbus mo e MOONSHINE ko e ongo melouea mātuʻaki kehekehe pē.

ʻOku ʻi ai ʻa e fepakipaki ʻi he MOONSHINE management interface mo e naunau ngāue ʻohofi ʻa e MOONSHINE fakatouʻosi ʻo tuʻunga ai ʻa e ngaahi fakatokanga tatau ʻi he huú ʻi he fakatātā 3 mo e 5 kae pehē ki he kakano ʻo e peesí ʻi he fakatātā 4 mo e 6. Naʻe ʻi ai fakatouʻosi foki ʻa e string ‘webpackJsonpreact-scotchui’ ʻi he source code.

Naʻe faʻu ʻe he kakai ngāue kovi fakamanamaná ʻa e ngaahi fehokotakiʻanga ʻinitaneti URL ʻa ia naʻe fakafehokotaki ki he naunau ngāue ʻohofi ʻa e MOONSHINE ʻo afeʻi ʻaki ʻa e ngaahi vitiō felaveʻi mo e kakai Tibet mo Uyghur, ʻa ia ʻoku fepakipaki mo e tāketi ʻa e MOONSHINE.

ʻI he lahi taha ʻo e ngaahi tuʻasila IP ʻokú nau housi ʻa e tōmeini naunau ngāue ʻohofi ʻa e MOONSHINE, ʻoku ʻi ai ʻa e peesi hū ʻoku ui ko e ʻVLiteUIʼ ʻi he pooti 444. Ko e peesi ko ʻení ʻoku ʻikai ke ʻilolahia pea ko ʻene ʻasi ʻi he ngaahi IP ʻokú ne tala ha ala fakafehokotaki ʻi ai ki he ngaahi ngāue ʻa e kakai ngāue koví.



Fakatātā 7: ʻOku ʻiloʻi ʻa e pēnolo hū ʻoku ʻi ai ʻa e hingoa HTML ko e 'VLiteUI' ʻi he ngaahi IP ʻa ia ʻokú nau toe housi ʻa e ngaahi naunau ngāue ʻohofi ʻa e MOONSHINE.

Kuo hā meí he ʻanalaisio ʻe he Trend Micro ʻa e Dark Nimbus ʻoku lava ʻa e meloueá ʻo tānaki ha lisi lahi ʻo e fakamatala ʻi he meʻangāué, pea ʻokú ne fetuʻutaki mo e C2 ʻo ngāue ʻaki ʻa e founga XMPP.

ʻOku fakahā foki ʻe he Trend Micro ʻoku ʻi ai ha ngaahi tatau ʻe niʻihi ʻo e Dark Nimbus, ʻokú nau tala ʻa e lahi ʻi ai ʻa e string ʻDKNSʼ.

ʻ**ansec[.]com**ʼ (naʻe lisi ʻe he TrendMicro ko e Dark Nimbus C2) ʻa ia naʻe ʻiloʻi foki ʻi he ngaahi sēvesi XMPP ki he ngaahi tuʻasila IP ʻokú ne ngāue maʻa e ngaahi peesi uepisaiti ʻoku ʻi ai ʻa e DKNS ʻi he hingoá:

- 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)

Ko ha seti ʻe taha ʻo e ngaahi tuʻasila IP ʻoku ʻi ai ʻa e ʻ**ansec[.]com**ʼ ʻi he sēvesi XMPP ʻoku ʻi ai ʻenau ngaahi peesi uepisaiti ko e hingoá ko e:

- UPSEC互联网控制指挥系统 (UPSEC Internet Control Command System)
- UPSEC无线侦控系统 (UPSEC Wireless Surveillance and Control System)
- UPSEC重点人数据还原系统 (UPSEC Key Person Data Restoration System)

Fakatatau k i he Intelligence Online, ko e ʻUPSECʼ naʻe ʻiloʻi ʻi he ngaahi hingoa ʻo e ngaahi peesi HTML, naʻe ʻuhinga ki he ʻSichuan Dianke Network Security Technology Co., Ltdʼ.

Keisi ako hono uá: BADBAZAAR

BADBAZAAR ko ha meloua toʻotoʻo ʻoku ʻi ai hono ongo liuanga iOS mo Android ʻa ia kuó ne tāketiʻi ʻa e kakai Uyghur, Tibet mo Taiwan. Ko e melouea ko ení kuo fakamafola ia ʻo fou ʻi he ngaahi peletifoomu mītia sōsialé mo e ngaahi falekoloa app fakaʻofisialé. ʻOku hā ʻi he lipōti fakamuimui ʻa e Volexity ʻa e ngaahi liuanga kehekehe ʻo e BADBAZAAR, ʻa ia ʻoku fakamavahevaheʻi kinautolu ko e BadSolar, BADBAZAAR mo e BadSignal. Ko e ngaahi liuanga kotoá ʻe tolu ʻoku fakafehokotaki fakataha ʻe he ngaahi fatongia ʻoku fepakipaki ʻa ia ʻoku ngāue ʻaki ki hono tānaki ʻo e fakamatala ʻo kau ki he meʻangāué mo e taha ʻokú ne ngāue ʻakí.

Naʻe fakahā ʻe he fekumi ʻa e NCSC ki he BADBAZAAR ʻa e ngaahi meʻa ko ʻení:

- Ko hono fakatahataha‘i ʻo e ngaahi tōmeini C2 naʻe fakahā ai ʻa e ngaahi fehokotakiʻanga makehe ki he ngaahi tōmeini kuo lipōti ʻi he hisitōlia maʻuʻanga fakamatala fakamanamaná.
- Fakahā ʻe he ngaahi seeva C2 mo e ngaahi semipolo meloueá ʻa e ngaahi hingoa housi ʻoku fekauʻaki mo e faʻunga meʻangāue ʻa e kakai ngāue koví.
- Ngaahi polōfaile makehe ʻa ia naʻe ngāue ʻaki ʻe he kakai ngāue kovi fakamanamaná ki he ʻenisia fakasōsiale ke fakamafola ʻenau meloueá ke mahili atu meí he ngaahi falekoloa app fakaʻofisialé.

WHOIS fakatahataha‘i / polouka tōmeini

‘UJYJYUJ’

ʻAnalaisio ʻo e ngaahi lekōti WHOIS maʻa e tōmeini BADBAZAAR ‘**signalplus[.]org**’ (lipōti ʻe he ESET) fakahā ʻa e tuʻunga ‘**UJYJYUJ**’ ʻi he konga ʻo e ‘**State**’.

Ko ha fekumi ki ha ngaahi tōmeini kehe ʻoku ʻi ai hanau tuʻunga tatau ʻo maʻu ai ʻa e ngaahi tōmeini mahuʻinga ko ʻení:

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

(Vakai ki he Annex A, ʻīmisi 1)

Ko e tōmeini **signalplus[.]org**, **tubevideoplus[.]org** mo e **thetubeplus[.]com** kuo lipōti ko e ngaahi tōmeini BADBAZAAR C2, lolotonga ia ʻoku lipōti ʻe he ESET ʻa e

tōmeini iiki **mail.pmumail[.]com** ko ha seeva polokisī FlyGram. Ko e FlyGram ko ha app BADBAZAAR naʻe faʻu ʻe he kakai ngāue kovi ʻi he ʻinitanetí (Vakai ki he appendix ki ha lisi ʻo e apps BADBAZAAR kehé).

Ngaahi tuʻunga hokohoko ʻi he kīpootí

Kuo vakai foki ʻa e NCSC ki ha ngaahi pēteni hokohoko tatau ʻi he kīpootí ʻi he ngaahi tōmeini BADBAZAAR C2 kehe kuo lesisitá.

Hangē ko ʻení, ko e ngaahi tōmeini ko ʻení ʻoku ʻi ai kotoa honau tuʻunga ko e '**REWR**' ʻoku ʻiloʻi ʻi he konga ko e '**State**' (ʻi hono ngāue ʻaki ki muʻá):

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

(Vakai ki he Annex A, ʻīmisi 2)

Ngaahi tōmeini fakataha mo e ngaahi tuʻunga konga state ʻo e 'FSDF'

Ko ha seti ʻe taha ʻo e ngaahi tōmeini BADBAZAAR C2 ʻoku ʻi ai ʻa e tuʻunga '**State**' ko e '**FSDF**':

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

(Vakai ki he Annex A, ʻīmisi 3)

Lipōti fakahisitōlia fakataha mo e ngaahi tuʻunga hokohoko ʻi he kīpootí

Ko hono ngāue ʻaki ʻo e ngaahi tuʻunga hokohoko ʻi he kīpootí ʻi he ngaahi lekōti WHOIS ʻo e ngaahi tōmeini BADBAZAAR ʻe lava ke toe vakai ki ai ʻi he lipōti fuoloa hono tāketi ʻo e ngaahi kautaha Tibet ʻe he TA413. Kuo ʻiloʻi ʻe he Recorded Future ʻa e ngaahi tōmeini naʻe puleʻi ʻe he kakai ngāue kovi ʻenau spoofing ʻa e ngaahi kautahaTibet mo hno ngāue ʻaki ʻo ha tuʻunga kautaha ʻo ha taha lesisita ko e "**asfasf**".

clublogs[.]com

Ko e ngaahi semipolo BADBAZAAR naʻe maʻu ʻe he Lookout ʻoku ʻi ai ʻa e '**xle.clublogs[.]com'** ko e tōmeini C2. Ko e tefitoʻi tōmeini '**clublogs[.]com**' naʻe housi ia ʻi he tuʻasila IP '**95.179.210[.]85**' pea naʻe ʻi ai ʻa e tohi fakamoʻoni SSL fakataha mo e kaveinga mo e tuʻunga ʻo e taha foakí ko e '**CN=WIN-50QO3EIRQVP**'. Naʻe tatau ʻa e tuʻunga ko ʻení mo e ngaahi tohi fakamoʻoni SSL ʻa ia naʻe maʻu ʻi he ngaahi semipolo BADBAZAAR ʻa ia naʻe ngāue ʻaki ʻa e SSL ke taʻofi ʻa hono fakamoveuveu ʻo e ngaahi fetuʻutakí.

Ko e hisitōlia housi ʻo e tuʻasila IP **95.179.210[.]85** naʻe hā ai ʻa e ngaahi tōmeini mahuʻinga ko ʻení:

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

(Vakai ki he Annex A, ʻīmisi 4)

www.voiceoftibet[.]net

Ko e tōmeini '**www.voiceoftibet[.]net**' hangē ʻokú ne fakapuli ko e letiō 'Voice of Tibet' ia, ke faitatau mo e TTP naʻe ngāue aki ʻe he TA413.

Ko e tōmeini '**rewrwer[.]com**' ʻoku faitatau mo e tuʻunga '**State**' naʻe ʻiloʻi kimuʻá '**REWR**' ʻa ia naʻe maʻu ʻi he ngaahi lekōti WHOIS ʻo e ngaahi tōmeini BADBAZAAR.

Ko e ngaahi tōmeini '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' mo e '**myloughborough[.]com**' naʻe lesisita kotoa ʻaki ʻa e tuʻasila ʻīmeili '**tplutalova@list[.]ru**'.

actuallys[.]com

Naʻe hā ʻi he ngaahi lekōti WHOIS ki he '**actuallys[.]com**' ha taimi ko e ngaahi tuʻasila ʻīmeilie ki he tekí mo e ʻetiminí ko e '**tplutalova@list[.]ru**' ka ko e ʻīmeili ʻa e taha lesisitá ko e '**ivan_s81@mail[.]ru**'.

Naʻe fakahā ʻe he fakamatala WHOIS fakahisitōliá ki he tōmeini '**actuallys[.]com**' ʻa e ʻīmeili lesisitá ko e '**wangminghua6@gmail[.]com**' ʻa ia naʻe lisi ʻi he ʻaho 24 Fepueli 2016. ʻI he 11 Maʻasi 2016, naʻe faifai pea liliu ʻa e ʻīmeilí ki he

‘**ivan_s81@mail.ru**’ neongo naʻe kei tatau pē ʻa e ʻaho naʻe ngata ki ai ʻa e lesisita ʻa e taha failesisitá.

wangminghua6@gmail[.]com

The tuʻasila ʻīmeili ‘**wangminghua6@gmail[.]com**’ naʻe ngāue ʻaki ke lesisita ʻa e ngaahi tōmeinī naʻe maʻu ʻi he ngaahi lipōti hisitōlia maʻuʻanga fakamatala fakamanamaná ʻI he 2015, naʻe ʻiloʻi ʻi Palo Alto ʻa e ʻīmeili naʻe ngāue ʻaki ke lesisita ʻa e ngaahi tōmeini C2 ki he meloueá, Cmstar. ʻI he 2014, naʻe ngāue ʻaki foki ia ke lesisita ʻa e ngaahi tōmeini naʻe ʻiloʻi ʻe he Mandiant ʻi he ngaahi kemipeini phishing naʻe fakahoko ʻe he APT3. ʻI he 2013, naʻe ngāue ʻaki ia ke lesisita ʻa e ngaahi tōmeini naʻe ʻilo ʻe he CrowdStrike ʻi hano tukuange ʻo ha meloued fakataha mo ha halanga Teitapeisi Polokalama (PDB) ʻoku ʻi ai ha ngaahi mataʻitohi Siaina. ʻOku fokotuʻu atu ʻi heni hono fakatahataha‘i ʻi ha sisitemi Siaina.

taoyujun@gmail[.]com

Ko e tōmeini ‘**hcjbtt[.]com**’ ʻoku lesisita ʻaki ʻa e tuʻasila ʻīmeili ‘**taoyujun@gmail[.]com**’ ka ko hono ʻīmeili ʻetiminí ʻoku lesisita ia ʻi he ‘**wangminghua6@gmail[.]com**’.

ʻOku ʻikai ha ʻekitivitī kovi ʻe fehokotaki mo e tōmeini ‘**hcjbtt[.]com**’, neongo iá naʻe maʻu ʻa e tuʻasila ʻīmeili ‘**taoyujun@gmail[.]com**’ ʻi he ngaahi lipōti hisitōlia maʻuʻanga fakamatala fakamanamaná. ʻI he 2014, naʻe ngāue ʻaki ke lesisita ha tōmeini naʻe maʻu ʻe Mandiant ʻi he ngaahi semipolo ‘**Cueisfry Trojan**’ oku ngāue ʻaki ke tāketi ʻa e ngaahi kautaha Siapaní.

Naʻe lesisita foki ʻe he tuʻasila ʻīmeilí ʻa e ngaahi tōmeini hangē ko e ‘**iaea-international[.]org**’ ʻa ia naʻe hangē ʻokú ne fakapuli ko e **International Atomic Energy Agency** ia mo e ‘**idc-ctbto[.]org**’ naʻá ne fakapuli ko e **International Data Centre** ia ʻi he **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

Naʻe hā ʻi ha lekōti fuoloa ʻo e WHOIS ki he tōmeini ‘**iaea-international[.]org**’ ʻa e ʻīmeili ʻo e taha lesisitá ko e ‘**wangminghua6@gmail[.]com**’.

udtglobals[.]com

Naʻe ʻiloʻi ʻa e tōmeini ‘**udtglobals[.]com**’ ʻokú ne ngāue ʻaki ʻa e ‘**wangminghua6@gmail[.]com**’ ko e īmeili ʻetiminí mo e ‘**ocean.nio@rediffmail[.]com**’ ko e tuʻasila ʻīmeili ʻo e taha lesisitá. Ko e ngaahi

lekōti WHOIS kehe ki he tōmeini ko ʻení, naʻe hā ai ʻa e ʻīmeili ʻo e taha lesisita tatau ka ko e tuʻasila ʻīmeili ʻetiminí ko e '**taoyujun@gmail[.]com**'.

Ko e '**udtglobals[.]com**' hangē ʻokú ne fakapuli ko e '**UDT Global**' ia ʻa ia ko ha ʻiveni fakamāmānilahi maʻa e ngaahi kautaha maluʻi mo ngāue maluʻi ʻo kilisitahí. Ko e username '**ocean.nio**' ʻi loto ʻi he tuʻasila ʻīmeilí ʻe ala ke ne faʻifaʻitaki ʻa e **National Institute of Oceanography (NIO)** ʻa ia ʻoku ʻi he ngaahi fonua lahi. Neongo ko hono ngāue ʻaki ʻo e sēvesi ʻīmeili '**Rediff**' (ʻa ia ʻoku tuʻu ʻi ʻInitiá) ʻe ala tala ai ʻa hono faʻifaʻitaki ʻo e **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

Ko e tōmeini '**djibdiplomatie[.]com**' naʻe hangē ʻokú ne fakapuli ko e ngaahi sēvesi fakatipilomētika Djibouti ia, ʻa ia naʻe ʻi ai hono lekōti WHOIS ʻoku faitatau mo e '**utdglobals[.]com**' Naʻe ʻasi ʻa e lekōti ʻe taha ke fakahā ʻe taha lesisitá '**ocean.nio@rediffmail[.]com**' mo e ʻetiminí '**taoyujun@gmail[.]com**' kae fakahā ʻe he ngaahi lekōti kehé ʻa e '**wangminghua6@gmail[.]com**' ko e tuʻasila ʻīmeili ʻetiminí mo e '**ocean.nio@rediffmail[.]com**' ko e ʻīmeili ʻo e taha lesisitá.

Ko e ongo tōmeini ko ʻení fakatouʻosi naʻe ʻi ai hona ngaahi tuʻunga hokohoko ʻi he kīpootí ʻi he ngaahi lekōti WHOIS. Hangē ko ʻení, ko e '**udtglobals[.]com**' ko hono tuʻungá ʻa e '**ASDF**' ko hono kolo lesisitá pea ko e '**djibdiplomatie[.]com**' ko e '**DAF DAGF**' ʻa hono tuʻunga hingoa lesisitá. ʻOku lava ʻeni ʻo fakahoa ki he ngaahi tuʻunga kuo ʻilo ʻi he ngaahi tōmeini BADBAZAAR kehé.

Neongo ʻoku maʻu ʻa e tuʻasila ʻīmeilí '**wangminghua6@gmail[.]com**' mo e '**taoyujun@gmail[.]com**' ʻi he ngaahi lekōti WHOIS ki he ngaahi tōmeiní ʻoku fakapuli ko ha '**iveni maluʻi fakamāmānilahi ʻo e kilisitahí**, **ngaahi sēvesi fakatipilomētika Djibouti** mo e **International Atomic Energy Agency**, ʻoku toe maʻu foki kinautolu ʻi he ngaahi lekōti WHOIS ʻo e ngaahi tōmeini lahi ʻoku ʻikai koví.

Ko e tuifio ʻa e ngaahi tōmeini fakapulí mo e ngaahi tōmeini ʻoku ʻikai koví ʻe ala tala ai ʻa e ʻi ai ʻa e sino ʻokú ne maʻu mai ʻa e faʻunga meʻangāue naʻe ngāue ʻaki ke poupou ki he ngaahi ngāue ʻa e kakai ngāue kovi ʻi he ʻinitanetí.

The tuʻasila ʻīmeili '**ocean.nio@rediffmail[.]com**' ʻoku toki maʻu pē ʻi he ngaahi tōmeini fakapuli ʻoku fakamatalaʻi ʻi ʻolungá. Kuo lesisita ʻe he '**ivan_s81@mail[.]ru**' mo e '**tplutalova@list[.]ru**' ha toko siʻi ʻaupito ʻo e ngaahi

tōmeiní takitaha, pea ko e niʻihi ʻo e ngaahi tōmeini ko ʻení kuo housi kinautolu ʻi he faʻunga meʻangāue BADBAZAAR. Ko e ngaahi tuʻasila ʻīmeili ʻe tolu ko ʻení ʻoku ʻi ai ʻa e tui ʻoku ʻi ai ʻenau fehokotaki ofi ange mo e ngaahi ngāue ʻa e kakai ngāue kovi ʻi he ʻinitanetí. Ko e ʻuhingá ʻoku ʻi ai ha fika lahi ange ʻo e ngaahi tōmeini ʻokú nau fekauʻakí ʻoku fehokotaki ki he ʻekitivitī koví, ʻi hono fakafehoanaki ki he ʻīmeili '**wangminghua6@gmail[.]com**' mo e '**taoyujun@gmail[.]com**'.

(Vakai ki he Annex A, ʻīmisi 5)

Ngaahi fehokotaki ki he ngaahi kakai ngāue kākā fakamanamana kehé

Ko e ʻulungaanga angamaheni ʻo e ngaahi tōmeini ʻoku fehokotaki mo e BADBAZZAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', mo e '**voiceoftibet[.]net**' naʻe lesisita kotoa kinautolu ʻaki ʻa e eNom mo hono 'tau' ʻi he '**255.255.255[.]254**'.

Hili ʻa e ngaahi fakatotolo NCSC kimuʻá, kuo fakahā ʻe he ngaahi tōmeini kehe ʻoku ʻi ai honau ngaahi ʻulungaanga pehé ní ʻa e ʻekitivitī ʻoku fehokotaki ki he **APT5** ʻi he 2019, mo e **APT14** ʻi he vahaʻa ʻo e 2009 mo e 2011.

Ko e ngaahi tōmeini ʻa ia ʻoku fehokotaki ki he APT5- ʻoku ʻi ai honau ngaahi lekōti WHOIS fakahikistōlia ʻa ia ʻoku lisi ai ʻa e '**taoyujun@gmail[.]com**' ko e tuʻasila ʻīmeili ia ʻo e taha lesisitá.

Ko e ngaahi tōmeini ʻa ia ʻoku fehokotaki ki he APT14 naʻe ʻi ai hono ngaahi tōmeini iiki mataʻitohi ʻe tolu ʻa ia naʻe hangē ʻokú nau fakafofongaʻi ʻa e tāketi ʻoku taumuʻa ki ai ʻenau ngaahi ngāue koví. Fakatātā ʻaki ʻeni ko e '**bae.cisconline[.]net**', ʻa ia naʻá ne fakahā ʻa e tāketi ʻoku fakataumuʻa ki ai ʻa e Ngaahi Sisitemi BAE pea naʻe ʻilo ia ʻi ha semipolo '**Poison Ivy**'.

Ko e ngaahi ʻulungaanga tatau kuo ʻiloʻi ʻi he ngaahi tōmeini BADBAZAAR ʻa ia ʻoku felāveʻi ʻa e ngaahi tōmeini iikí ki he hingoa ʻo e app kuo trojanised:

Hingoa Faʻu ʻo e Polokalama	C2 URL
Muslim Pro	**mpp**.pmstwocqn[.]com
Meʻa Hulu Vitiō ʻa e Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Letiō Afghanistan	**afg**.collinformations[.]com
EN-UG Dictionary Free	**eud**.titeperformance[.]com
Toe Maʻu ʻo e Vitiō Tisi	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

ʻOku mahuʻinga ke ʻiloʻi ko e ngaahi ʻekitivitī ʻa ia ʻoku felaveʻi mo e APT5 mo e APT14 naʻe fakahisitōlia pea naʻe ʻi ai foki mo e ngaahi tōmeini kehe naʻe lesisita ki he eNom pea fakapapauʻi ki he '**255.255.255.254**' ʻa ia ʻoku ʻikai lava ʻo fakafehotaki ki ha ʻekitivtī kovi. Ko ia ai ʻoku ʻikai ke fakapapauʻi pe ko e kakai ngāue kovi ʻi he tuʻa ʻo e ngaahi kemipeini ko ʻení ko ha kakai tatau pe felāveʻi.

Ngaahi Hingoa Mīsini

Naʻe maʻu ʻi hono ʻanalaisio ʻo e ngaahi BADBAZAAR C2 mo e ngaahi seimipoló ʻa e ngaahi hingoa housi kuo ngāue ʻaki ko e tuʻunga 'Common Name' ʻi he ngaahi tohi fakamoʻoni SSL. ʻOku hā ʻi he ngaahi fakatotolo NCSC ki he ngaahi hingoa housi kuo ʻiloʻiʻiloʻi ʻi he ngaahi semipolo BADBAZAAR mo e faʻunga meʻangāué ʻa hono ngāue ʻaki ʻo e ngaahi hingoa housi ko ʻení ʻi he ngaahi tuʻasila IP lahi. Ko e ngaahi tuʻasila IP ko ʻení ko e ngaahi tōmeini housi ʻa ia ʻoku maʻu ʻi he ngaahi semipolo BADBAZAAR. ʻOku lahi ʻi he fakaikiiki ʻi he konga ʻi laló ʻo fekauʻaki mo e ngaahi hingoa housí, mo e ngaahi tuʻasila IP fakataha mo e hingoa housi ʻokú ne housi ʻa e ngaahi tōmeini BADBAZAAR C2.

ʻI he meimei meʻa kotoa pē ʻoku fepakipaki ʻa e ʻi ai ʻa e ngaahi tohi fakamoʻoní fakataha mo e tuʻunga hingoa housí mo e ngaahi solova IP ki he ngaahi hingoa tōmeini kovi kuo fakamahino paú, ʻa ia ko e ngaahi meʻa ia ʻe niʻihi ʻa ia naʻe fakamamafaʻi ai naʻe ʻikai ko e meʻa ʻeni naʻe hokó.

WIN-EU0VLBL7TUJ

Hingoa housi ko e '**WIN-EU0VLBL7TUJ**' naʻe ʻiloʻi ia ʻi he ngaahi tuʻasila IP mahuʻinga ko ʻení:

- '**116.203.53[.]21**' naʻá ne housi ʻa e ngaahi tōmeini BADBAZAAR C2 '**uyapkfinder[.]com**' mo e '**thewestuniverse[.]com**'.

- **'95.216.169[.]27**' naʻá ne housi ʻa e ngaahi tōmeini BADBAZAAR C2 '**adysfunction[.]com'** mo e tōmeini siʻisiʻi '**download.apkbazar[.]biz**' naʻe ʻiloʻiʻiloʻi ia ko ha fehokotakiʻanga taunilouti ki ha semipolo BADBAZAAR.

(Vakai ki he Annex A, ʻīmisi 6)

WIN-70E59JVOB9G

Hingoa housi ko e '**WIN-70E59JVOB9G**' naʻe ʻiloʻi ia ʻi he ngaahi tuʻasila IP mahuʻinga ko ʻení:

- '**23.88.28[.]220**' naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2, **'aua.rondwsign[.]com', 'nal.tokenmajorp[.]com', 'pep.rondwsign[.]com'** '**doa.rondwsign[.]com**', mo e **'pls.rondwsign[.]com'.** Naʻe ʻi ai ʻa e vahaʻa taimi ko e ʻaho ʻe ua ʻi he vahaʻa ʻo e taimi naʻe ʻiloʻi fakamuimui ai ʻa e tohi fakamoʻoní fakataha mo e mīsiní, mo e taimi naʻe fuofua ʻiloʻi ai ʻa e ngaahi tōmeini koví ʻi he tali ʻo e IP.

- '**23.88.28[.]221**' naʻá ne housi ʻa e tōmeini iiki ʻoku fehokotaki ki he BADBAZAAR **bt.bhvghg[.]com**'.

- **'23.88.28[.]222**' naʻá ne housi ʻa e ngaahi tōmeini BADBAZAAR C2 '**tubevideoplus[.]org**' mo e '**cde.mpoxcases[.]com**'.

- '**65.21.92[.]67**' naʻá ne housi ʻa e tōmeini iiki BADBAZAAR C2 '**bat.androidupdated[.]net**'. Naʻá ne housi foki ʻa e tōmeini iiki '**apps.androidupdated[.]net**' ʻa ia ko ha DoubleAgent melouea C2.

- ‘**65.21.92[.]77**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ mo e ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**upd.whoscaller.net**’. mo e ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**bvn.lookincategory[.]com’** mo e ‘**edr.lookincategory[.]com’.** Naʻe ʻi ai ʻa e vahaʻa taimi ko e ʻaho ʻe hongofulu mā taha ʻi he vahaʻa ʻo e taimi naʻe ʻiloʻi fakamuimui ai ʻa e tohi fakamoʻoní fakataha mo e mīsiní, mo e taimi naʻe fuofua ʻiloʻi ai ʻa e ngaahi tōmeini koví ʻi he tali ki he IP.

- **‘142.132.131[.]20’** naʻá ne housi ʻa e ngaahi tōmeini iiki ‘**son.onlinegamersgroup[.]com’** mo e ‘**system.onlinegamersgroup[.]com’**,ʻa ia ʻoku ʻi ai ʻa e tui ko ha ngaahi BADBAZAAR C2 ʻi hono housi kinautolu lolotonga ʻiloʻiʻoku ʻiloʻi ʻa e ngaahi tohi fakamoʻoni ʻo e BADBAZAAR ʻoku fekauʻaki mo e SSL ʻi he IP.

- ‘**142.132.131[.]28’** naʻá ne housi ʻa e tōmeini BADBAZAAR C2 ‘**goldplusapp[.]net**’ mo e ngaahi tōmeini iiki ‘**who.goldplusapp[.]net**’ mo e ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, mo e ‘**aar.alpinemap[.]net**’.

- ‘**162.55.103[.]212**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** mo e **‘aua.rondwsign[.]com’.**

- ‘**195.154.47[.]99**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**ggl.whoscaller[.]net**’ mo e ‘**upd.whoscaller.net**’. Naʻe ʻi ai ʻa e vahaʻa taimi ko e ʻaho ʻe tolu ʻi he vahaʻa ʻo e taimi naʻe fuofua ʻiloʻi ai ʻa e tohi fakamoʻoní fakataha mo e hingoa ʻo e mīsiní mo e taimi naʻe ʻiloʻi fakamuimui ai ʻa e ngaahi tōmeini koví ʻi he tali ki he IP.

- ‘**195.154.60[.]3**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**upd.whoscaller[.]net**’
‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ naʻá ne housi ʻa e ngaahi tōmeini iiki BADBAZAAR C2 ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ mo e ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ naʻá ne housi ʻa e ngaahi tōmeini BADBAZAAR C2, ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ mo e ‘**bvn.lookincategory[.]com**’.

(Vakai ki he Annex A, ʻĪmisi 7)

WIN-50QO3EIRQVP

Ko e hingoa housi ko e ‘**WIN-50QO3EIRQVP**’ naʻe ʻiloʻi ia ʻi he ngaahi tuʻasila IP mahuʻinga ko ʻení:

- ‘**45.76.132[.]91**’ naʻá ne housi ʻa e tōmeini, ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. Ko e ongo tōmeiní fakatouʻosi ʻokú na fehokotaki ki he BADBAZAAR ko e ongo tōmeini iiki ‘**fow.yumoftion[.]com**’ mo e ‘**bat.androidupdated[.]net**’ ko e ongo tōmeini BADBAZAAR C2. ʻIkai ko ia pē ka ko e tōmeini iiki ‘**apps.androidupdated[.]net**’ ko ha tōmeini DoubleAgent C2. Naʻá ne housi foki ʻa e tōmeini ‘**pmstwocqn[.]com**’, ʻa ia ʻoku fehokotaki ki he BADBAZAAR ʻo fou ʻi he ngaahi lekōti WHOIS.

- ‘**95.179.210[.]85**’ naʻá ne housi ʻa e ‘**clublogs[.]com**’, ʻa ia ko e ‘**xle.clublogs[.]com**’ ko ha tōmeini BADBAZAAR C2 pea naʻá ne housi foki ʻa e ngaahi tōmeini fehokotaki ki he BADBAZAAR ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, '**www.voiceoftibet[.]net**' mo e ‘**actuallys[.]com**’.

- ‘**199.247.21[.]34**’ naʻá ne housi ʻa e ‘**titeperformance[.]com**’, and ‘**collinformations[.]com’** ʻa ia ko e ngaahi tōmeini iikí ko e ongo tōmeini BADBAZAAR C2.

- ‘**217.69.10[.]128**’ naʻá ne housi ʻa e BADBAZAAR C2 Tōmeini ‘**uyghurdict[.]com**’.

(Vakai ki he Annex A, ʻīmisi 8)

WMSvc-WIN-50QO3EIRQVP

Hingoa housi ko e ‘**WMSvc-WIN-50QO3EIRQVP**’ naʻe ʻiloʻi ia ʻi he ngaahi tuʻasila IP mahuʻinga ko ʻení:

- **’78.46.185[.]251’** naʻá ne housi ʻa e tōmeini BADBAZAAR C2 **‘groupgram[.]org’**, kuo lipōti ʻe he Volexity ʻokú ne ngāue ʻaki ʻa e pooti 4432 ki he ngaahi fehokotaki kovi.

- **‘65.21.92[.]69’** mo e **‘163.172.205[.]207’** naʻá ne housi ʻa e tōmeini **‘widelygram[.]org’** ʻa ia ʻoku ʻi ai ʻa e tui ko ha tōmeini BADBAZAAR C2, ʻa ia ʻi he lolotonga hono housi ʻi he ongo IP fakatouʻosí, naʻe ava ʻa e pooti 4432.

- **‘163.172.198[.]206’** naʻá ne housi ʻa e tōmeini **‘maxgram[.]org’** ʻa ia ʻoku ʻi ai ʻa e tui ko e tōmeini BADBAZAAR C2, ʻa ia ʻi he lolotonga hono housi iá naʻe ava ʻa e pooti 4432.

(Vakai ki he Annex A, ʻīmisi 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Ko e ngaahi hingoa housi ko e ‘**WMSvc-WIN-50QO3EIRQVP**’ mo e ‘**WIN-7LSBB9R0F1L**’ naʻe ʻiloʻiʻiloʻi fakataha ʻi he tuʻasila IP ko ʻení:

- ‘**148.251.87[.]245**’ naʻá ne housi ʻa e tōmeini BADBAZAAR C2 ‘**flygram[.]org**’ mo e ‘**groupgram[.]org**’.

(Vakai ki he Annex A, ʻīmisi 10)

WIN-N8H8S9BG2P0

Ko e ngaahi hingoa housi ko e '**WIN-N8H8S9BG2P0**' naʻe ʻiloʻiʻiloʻi ia ʻi he tuʻasila IP ko ʻení:

- '**148.251.87[.]247**' naʻá ne housi ʻa e tōmeini BADBAZAAR C2 '**omarwhatsapp[.]org**' mo e '**flygram[.]org**'.

(Vakai ki he Annex A, ʻīmisi 11)

WIN-I6VBN8MR92A

Ko e ngaahi hingoa housi '**WIN-I6VBN8MR92A**' naʻe ʻiloʻiʻiloʻi ia ʻi he tuʻasila IP ko ʻení:

- '**148.251.87[.]197**' naʻá ne housi ʻa e BADBAZAAR C2 tōmeini '**tryhrwserf[.]com**'.

(Vakai ki he Annex A, ʻīmisi 12)

Tuʻunga ʻi he teita kōmesiale ʻoku maʻú ko e lahi ʻa e ngaahi hingoa mīsini ko ʻení ʻi he ʻinitanetí ʻoku fetōʻaki. Ko e niʻihi ʻoku ʻiloʻi kehekehe pē ʻi he ngaahi tuʻasila IP lahi ʻa ia ʻokú ne tala mai ʻa hono faʻu ʻo e ngaahi VM meí he temipeleti tataú. ʻOku mahuʻinga ke ʻiloʻi ko e niʻihi ʻo e ngaahi hingoa housí, ʻoku ʻikai lava ʻo fakafehokotaki ʻa e kotoa ngaahi IP ʻa ia naʻe ʻiloʻi ai kinautolú ki ha ʻekitivitī kovi. ʻOku ala ʻuhinga ʻeni ʻoku ʻikai tāfataha ʻa hono ngāue ʻaki ʻo e ngaahi hingoa housí ki he ngaahi kakai ngāue kovi fakamanamana ko ʻení.

Neongo iá, ko e lahi ʻa e niʻihi ʻo e ngaahi hingoa mīsini ko ʻení ʻi he ngaahi IP ʻa ia kuó nau housi ʻa e ngaahi tōmeini BADBAZAAR C2, ʻokú ne ala tala ʻa hono ngāue ʻaki ʻo ha sino ʻokú ne maʻu ʻa e faʻunga meʻangāué ke fokotuʻutuʻu ʻaki ʻa e ngaahi mīsini ʻoku tokoniʻi ʻaki ʻa e ngaahi ngāue kovi ʻa e kakai ngāue koví ʻi he ʻinitanetí.

ʻI he mītia sōsialé

Ko e lipōti kimuʻa ʻa e Volexity naʻe hā ai ʻa hono faʻu ʻe he kakai ngāue kovi ʻi he ʻinitanetí ʻa e ngaahi vitiō YouTube (ʻokú ne tuʻuaki hono ngāue ʻaki ʻo e ngaahi polokalama koví). Ko e ngaahi vitiō ko ʻení ʻoku kau ai ʻa e ngaahi lēsoni ki he founga hono ngāue ʻaki ʻo e ngaahi polokalama kuo faʻú.

Kuo ʻilo ʻe he NCSC ha sēnolo YouTube makehe ʻe ua ʻoku fekauʻaki mo e ngaahi ngāue ʻa e kakai ngāue kovi fakamanamaná. Ko e sēnolo YouTube mo e henitolo

URL ‘**@josephjoey3499**’ ʻoku hangē ʻokú ne tuʻuaki hono ngāue ʻaki ʻo e ‘**Maxgram**’ mo ha sēnolo makehe kuo lesisita ʻi he ‘**@uyghurapks3096**’ ʻokú ne tuʻuaki ʻa e ‘**Uyghur APK Finder**’.

ʻIkai ko ia pē, ko e ngaahi vitiō YouTube ʻoku tuʻuaki ai ʻa e ‘**Flygram**’ mo e ‘**Signal Plus**’, ʻoku hā ai ʻa e kakai ngāue kovi fakamanamaná ʻokú nau ngāue ʻaki ʻa e ngaahi fika telefoni ʻoku lava ʻo ʻiloʻi. ʻI he vitiō ‘**Flygram**’, ʻi he 0:36 ko e fika telefoni ‘**+1 (570) 378-7250**’ ʻoku ʻasi ʻo ʻiloʻi ‘**Signal Plus**’ vitiō, ʻoku ʻasi ʻa e fika telefoni ‘**+1 (267) 298 4259**’.

Naʻe lipōti ʻe he Volexity ha saiti ongoongo loi ʻo kaveinga ʻaki ʻa Tibet ‘**ignitetibet[.]net**’, ʻa ia naʻá nau ʻiloʻi ʻi he ngaahi sēnolo Telegram ʻoku ʻi ai ʻa e tui ʻoku fakalele ʻe he kakai ngāue kovi ʻoku fakamanamaná. Ko e tuʻasila ʻīmeili '**choekyi.wangmo@ignitetibet[.]net**' kuo ʻiloʻi ʻe ne tuku ʻa e ngaahi komeni ʻi he ngaahi pousi ʻi he peesi '**tibetone.org**' ʻa ia kuo lipōti fakahāhā ia ʻe he Lookout ko ha peesi C2 ʻa ia ʻoku ngāue ʻaki ki he liuanga iOS ʻo e BADBAZAAR.

ʻOku ʻi ai ʻa e tui ko e tuʻasila ʻīmeili ko ʻení ʻoku puleʻi ia ʻe he kakai ngāue kovi, ʻo ngāue ʻaki ʻa e sīpinga ʻo ‘**Choekyi Wangmo**’.

Sivi

Ko e BADBAZAAR mo e MOONSHINE ʻokú na ngāue ʻaki ʻa e ngaahi founga ʻenisinia sōsiale kehekehe ke tāketi fakapatonu ʻa e ngaahi komiunitī Uyghur, Tibet mo e Taiwan, ʻa ia ko e:

- ko hono trojanisation ʻo e ngaahi apps ʻoku mahuʻinga ki he ngaahi komiunitī ko ʻení, ʻo hangē ko e polokalama Quran lea Uyghur, ʻa ia ʻoku ʻosi fakapatonu ia ki he peisi ʻo e kakai mamahi ʻoku tāketí
- ko hono tānaki atu ʻa e app kuo trojanise ki he ngaahi falekoloa app fakaʻofisialé ʻoku lahi ʻaupito ai ʻa e faingamālie ke ʻi ai ʻa e ongoʻi ʻoku fakalao, pea ko hono vahevahe fakaʻilekitulōnika atu ʻi he ngaahi kulupu fepōtalanoaʻakí ʻoku lahi ʻaupito ʻa ʻene taumuʻa ke ngāue ʻaki ʻa e ngaahi vā falalaʻanga ʻi loto ʻi he ngaahi komiunitī ko ʻení

Ko e BADBAZAAR mo e MOONSHINE ʻokú na tānaki ʻa e teita ʻa ia ʻe mei mahuʻinga ki he puleʻanga Siainá. Neongo ko e BADBAZAAR mo e MOONSHINE kuo ʻiloʻi ʻena tāketi ʻa e kakai Uyghur, Tibet mo Taiwan, ʻoku ʻi ai ha ngaahi melouea kehe ʻokú nau tāketi ʻa e ngaaahi kulupu toko siʻi kehe ʻi Siaina. Ko e kakai meí he ngaahi fonua kaungā silá, ʻi Siaina mo tuʻapuleʻanga, ʻa ia ʻoku pehē ʻokú nau poupouʻi ʻa e ngaahi ngāue ʻoku fakamanamana ki he tuʻumaʻu ʻa e puleʻangá, ʻokú nau mei kau ʻi hono fakamanaʻi meí he melouea toʻotoʻó ʻo hangē ko e BADBAZAAR mo e MOONSHINE. Ko e malava ke maʻu ʻa e feituʻú, ongó mo e teita tā ʻoku mei maʻu ai pē ʻa e faingamālie ke ʻaputeiti ʻa e ngaahi ngāue siofi mo fakakina ʻi he kahaʻú ʻaki hono ʻoatu ʻo e fakamatala ʻi he taimi pē ʻoku hoko aí ʻo kau ki he ʻekitivitī ʻa e tāketí.

MITRE ATT&CK®

Ko e lipōti ko ʻení kuo fakatahataha‘i ʻo fekau‘aki fa‘unga ʻo e MITRE ATT&CK®, ʻa ia ko ha ma‘u‘anga fakamatala ʻoku ʻatā ke ngāue ʻaki fakamāmanilahi ʻo kau ki he ngaahi founga ʻa e fakafepakí ʻo makatu‘unga ʻi he ngaahi me‘a mo‘oni kuo ʻilo ʻi he māmaní.

Fakalakalaka Founga	ID	Founga	Founga ngaue
Reconnaissance	T1593.001	Kumi ʻo e Ngaahi Uepisaiti ʻoku ʻAtā/Ngaahi Tōmeini: Mitia Sōsialé	Ma‘u ʻe he kakai ngāue koví ʻa e ngaahi kulupu ʻi he ʻinitanetí mo e ngaahi fōlomu ʻoku hoa mo ʻenau ni‘ihi mamahí kenau vahevahe faka‘ilekitulōnika ʻa e meloueá
Fakalakala ʻo e Naunaú	T1583.001	Ma‘u Mai ʻo e Fa‘unga Me‘angāué Ngaahi Tōmeini	Lesisita ʻe he kakai ngāue koví ʻa e ngaahi tōmeini ki he ʻenau ngaahi seeva fekau mo pule‘í
Fakalakala ʻo e Naunaú	T1587.001	Fakalahi ʻo e Ngaahi Ivi Ngāué Melouea	ʻOku hiki ʻa e ngaahi fika koví ke fakahū ki he ngaahi app kuo trojanised
Fakalakala ʻo e Naunaú	T1608.001	Fakanofonofó: ʻApulouti ʻo e Meloueá	ʻOku ʻapulouti ʻa e apps kuo trojanised ki he ngaahi peletifoomu ʻi he ʻinitanetí ʻo kau ai ʻa e ngaahi falekoloa app
Fakalakala ʻo e Naunaú	T1585.001	Fokotu‘u ʻa e Ngaahi ʻAkauni: Ngaahi ʻAkauni Mītia Sōsialé	ʻOku fa‘u ʻe he kakai ngāue koví ʻa e ngaahi ʻakauni ʻi he ngaahi uepisaití mo e mītia sōsialé ke vahevahe faka‘ilekitulōnika ai mo tu‘uaki ʻa e meloueá
Fakalakala ʻo e Naunaú	T1585.002	Fokotu‘u ʻa e Ngaahi ʻAkauni: Ngaahi ʻAkauni ʻĪmeili	ʻOku ngāue ʻaki ʻe he kakai ngāue koví ʻa e ngaahi ʻakauni ʻīmeili ʻoku housi tāutaha mo fakakomēsiale ki hono housi mo e vahevahe faka‘ilekitulōnika ʻo e meloueá
Fuofua A‘ú	T1189	Drive-by Compromise	Ko ha ngaahi tohi kovi ʻa ia ʻoku fufū ʻi he apps ʻoku ʻikai

			fakalao pea kuo ʻapulouti ki he ngaahi falekoloa app
Fuofua Aʻú	T1566.003	Phishing: Spearphishing ʻo fou ʻi he Sēvesí	ʻOku seni ʻe he kakai ngāue koví ʻa e apps kuo trojanise ki he ngaahi kulupu kuo tāketiʻí ʻo fou ʻi he mītia sōsialé ʻo kau ai ʻa e Telegram
Fakahoko ʻo e ʻohofí	T1204.002	Fakahoko ʻe he Taha Ngāue ʻAkí Faile Kovi	Kuo ʻinisitolo ʻe kinautolu mamahí ʻa e app kuo trojanise ke ne fakahoko ʻa e payload
Kalofi ʻo e Maluʻí	T1027.009	Ngaahi Faile pe Fakamatala kuo Fufū: Ngaahi payload kuo Fakanofonofo ke Puli	ʻOku fūfū ʻa e payload koví ʻi loto ʻi he apps ʻoku ʻikai fakalao
Kalofi ʻo e Maluʻí	T1036.005	Fakapuli: Fakatauhoa ki he Hingoa pe Feituʻu Fakalao	ʻOku fakatauhoa ʻe he ngaahi faile kuo trojanise ʻa e hingoa, fōtunga mo e fatongia ʻo e apps ʻokufakalao.
Kalofi ʻo e Maluʻí	T1656	Faʻifaʻitaki ha taha	ʻOku faʻifaʻitaki ʻe he kakai ngāue koví ʻa e kakai falalaʻangá ʻaki hono faʻu ʻo e ngaahi uepisaiti fakapuli ʻo ngāue ʻaki ʻa e ngaahi username ʻoku fekauʻaki mo ha ngaahi kulupu ʻoku tāketiʻí
Tānaki	T1123	Maʻu ʻo e Ongó	ʻE ala kole ʻe he app kuo trojanise ʻa e ngaahi fakangofua ʻoku ʻikai fie maʻu ʻo kau ai ʻa e aʻu ki he meʻa fakaongo leʻó
Tānaki	T1125	Puke ʻo e Vitiō	ʻE ala kole ʻe he app kuo trojanise ʻa e ngaahi fakangofua ʻoku ʻikai fie maʻu ʻo kau ai ʻa e aʻu ki he meʻafaitaá
Tānaki	T1005	Teita mei he Sisitemi Lōkoló	ʻE ala kole ʻe he app kuo trojanise ʻa e ngaahi fakangofua ʻoku ʻikai fie maʻu ʻo kau ai ʻa e ngaahi faile lōkoló.

Fekau mo e Pule‘i	T1071.001	Lao ‘i he Leia ‘Olunga ‘o e Polokalamá: Ngaahi Lao ‘i he Uepí	‘Oku fakafehokotaki ‘a e meloueá ki he C2 ‘o ngāue ‘aki ‘a e HTTPS mo e WebSocket.
Fekau mo e Pule‘i	T1509	Pooti ‘Ikai Angamaheni	‘Oku ngāue ‘aki ‘a e ngaahi pooti ‘ikai angamahení ‘o hangē ko e pooti 4432 mo e 2333
To‘o ‘ikai fakamafai‘i	T1041	To‘o ‘ikai fakamafai‘i ‘o e Sēnolo C2	To‘o ‘ikai fakamafai‘i ‘e he meloueá ‘a e teitá ‘o ngāue ‘aki ‘a e ngaahi fakafehokotaki HTTPS mo e WebSocket.
Uesiá	T1565.002	Fokotu‘utu‘u ‘o e Teitá: Fokotu‘utu‘u ‘o e Teita Fe‘ave‘aki Holó	‘Oku ma‘u ‘e he kakai ngāue koví ‘a e teitá meia kinautolu mamahí ‘aki hono faka‘atā ‘o e fefononga‘aki ‘a e app ‘i he ‘initanetí ‘a ia ‘oku ‘ikai fie ma‘u ki he ngāue ‘a e app

Ngaahi meʻa fakaʻilongá

MOONSHINE:

- ʻI he ʻaho 1 ʻEpeleli 2025, naʻe maʻu ʻa e ngaahi meʻa ko ʻení ʻi ha fekumi ki he ngaahi pēnolo VLiteUI:

Tuʻasila IP	Pooti	Fuofua ʻAsi	ʻAsi Fakamuimui
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

- ʻI he ʻaho 1 ʻEpeleli 2025, naʻe maʻu ʻa e ngaahi meʻa ko ʻení ʻi ha fekumi ki he ngaahi pēnolo SCOTCH ADMIN ʻi he ʻinitanetí:

Tuʻasila IP	Pooti	Fuofua ʻAsi	ʻAsi Fakamuimui
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

- ʻI he ʻaho 14 Maʻasi 2024, naʻe maʻu ʻa e ngaahi meʻa ko ʻení ʻi ha fekumi ki he ngaahi pēnolo SCOTCH ADMIN ʻi he ʻinitanetí:

Tōmeini	Tuʻasila 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:

Fakamatala	Tohi fakamoʻoni SSL naʻe ʻiloʻi ʻi he BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- ʻI he ʻaho 1 ʻEpeleli 2025, naʻe maʻu ʻa e ngaahi meʻa ko ʻení ʻi ha fekumi ki he tohi fakamoʻoni BADBAZAAR ʻi ʻolungá:

Tuʻasila IP	Pooti	Fuofua ʻAsi	ʻAsi Fakamuimui
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

Fakamatala	Tohi fakamoʻoni SSL naʻe ʻiloʻi ʻi he BADBAZAAR C2s
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- ʻI he ʻaho 1 ʻEpeleli 2025, naʻe maʻu ʻa e ngaahi meʻa ko ʻení ʻi ha fekumi ki he tohi fakamoʻoni BADBAZAAR ʻi ʻolungá:

Tuʻasila IP	Pooti	Fuofua ʻAsi	ʻAsi Fakamuimui
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

- Ngaahi tōmeini WHOIS

ʻOku hā ʻi he tēpile ʻi laló ʻa e ngaahi tōmeini ʻai a ʻoku lolotonga ʻi ai pe ʻoku ʻi he hisitōliá naʻe ʻi ai honau ngaahi lekōti WHOIS fakataha mo e ngaahi tuʻunga ʻa ia ʻoku faitatau mo ia kuo ʻiloʻi ʻi he ngaahi tōmeni BADBAZAAR C2.

Tuʻunga ʻo e WHOIS	Ngaahi Tōmeini
Siteiti ʻo e Taha Lesisitá: UJYJYUJ **Fonua ʻo e Taha Lesisitá: Bolivia** **Failesisita: 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
Siteiti ʻo e Taha Lesisitá: REWR **Fonua ʻo e Taha Lesisitá: CF** **Failesisita: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com

	• tooenabled[.]com • suguestions[.]com • searching2[.]com
Siteiti ʻo e Taha Lesisitá: FSDF **Fonua ʻo e Taha Lesisitá: AL** **Failesisita: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

Ngaahi Tuʻasila ʻĪmeilí
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

Ko e ngaahi fehokotakiʻanga ʻinitaneti ko ʻení ki he ngaahi meʻa fakaʻilonga kehe ʻo e uesia (IoCs) ʻa ia ʻoku fekauʻaki mo e BADBAZAAR mo e MOONSHINE. ʻOku ʻikai lava ʻe he NCSC ʻo fakapapauʻi ʻa e fakalao ʻo e kotoa ʻo e ngaahi fakamatala ʻi he ngaahi fehokotakiʻanga ʻinitaneti ko ʻení pea ʻoku faleʻi ʻa e kau laukongá ke fakamoʻoniʻi ʻiate kinautolu pē ʻenau tonú mo e ʻaongá:

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

Fakasiʻisiʻi Uesia

ʻOku poupouʻi ʻe he NCSC ʻa hono ngāue ʻaki ʻo e ngaahi fokotuʻu fakakaukau ʻi laló ke matatali ʻaki ʻa e ngaahi fakamanamana kuo fakamatalaʻi ʻi he ongo keisi akó.

- **ʻOku totonu ke fakapapauʻi ʻe he kau pule App store, kau ai ʻa e ngaahi falekoloa app faʻahi hono tolu, mo e kau faʻu app ʻoku malu ʻa e apps ʻi he ʻenau peletifoomú pea ʻokú nau faipau ki he Tuʻutuʻuni Ngāue fakapuleʻangá.** Vakai ki he Fakahinohinó: 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

- **Tokoni maʻa e lea fakafonua kehekehé**: ʻOku totonu ke ʻinivesi ʻa e kau faʻu app ʻi he ngaahi ngāue ke liliu lea ʻa e apps manakoá maʻa kinautolu ʻokú nau ngāue ʻaki ʻokú nau lea ʻi he ngaahi lea fakafonua ʻoku ʻikai tokolahi ʻi he ngaahi kulupu ʻoku tāketiʻí kau ai ʻa e Uyghur, Tibetic, Taiwanese Hokkien mo e Cantonese. Fakahinohino ʻa e Apple ki he liliu lea ʻi he apps: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Fakahinohino ʻa e Google ʻo kau ki he apps liliu leá: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Tauhi malu hoʻo peletifoomu mītia sōsialé:** ʻE lava ʻe he ngaahi kautaha mītia sōsialé ʻo fakafaingatāʻiaʻi lahi ange ke faʻu ʻe he kakai ngāue kovi ʻi he ʻinitainetí ha ngaahi ʻakauni loi pe vahevahe fakaʻilekitulōnika ʻa e ngaahi faile pe fehokotakiʻanga ʻinitaneti kovi ʻi he ʻenau ngaahi peletifoomú ʻi he ngaahi komiunitī ʻikai fakalao ʻi he ʻinitanetí. Kapau ʻe lava, ʻoku totonu ke vahevahe fakaʻilekitulōnika ʻe he ngaahi kautahá ʻa e ngaahi meʻa fakatokanga ʻekitivitī kovi ki he ngaahi ngāueʻanga lahi ange ke fakalelei ʻi ʻa e mahino fakalukufua ki he fakamanamaná mo tokoni ʻi he ngaahi founga maluʻí.

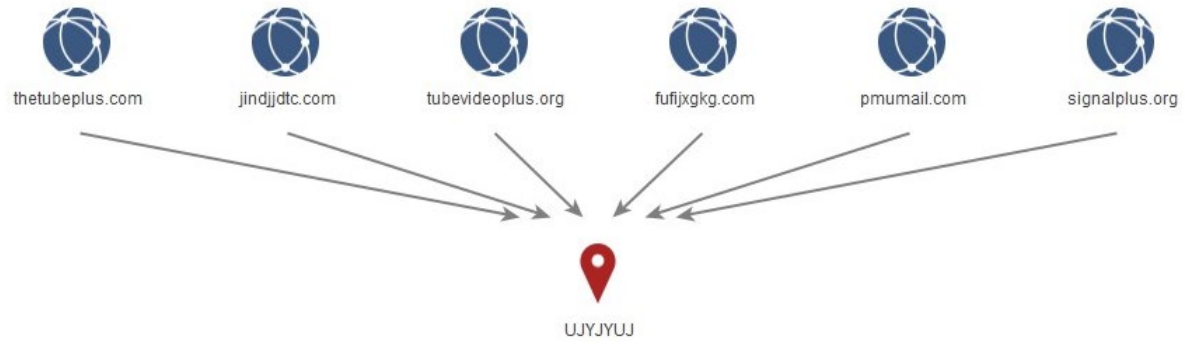
- **Palani founga fakalelei maʻa e kau kasitomaá:** ʻOku totonu ke ʻi ai ha ngaahi founga ngaue ʻa e ngaahi kautahá ke fakahā ʻaki ki he kau kasitomā ʻa ia kuó nau ʻinisitolo ʻa e app koví ʻo ngāue ʻaki ʻenau ngaahi sēvesí. Ko e ngaahi fakatokanga ko ʻení ʻoku totonu ke ne tohoakiʻi ʻa e tokangá pea ʻaonga. Kapau ʻoku fie maʻu, ʻoku totonu ke tuku atu ʻe he ngaahi kautahá ha fakahinohino ki he founga ʻe toʻo ʻaki ʻa e polokalamá mo fakalotolahi ki he niʻihi mamahí ke lipōti ki heʻenau kau maʻumafaí, ʻo hangē ko e NCSC ʻi he UK.
  Vakai ki he Tuʻutuʻuni Ngāue ʻa e App Store ki ha fakamatala lahi ange: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Ngaahi kulupu ngāue ke ngāue fakatahá:** ʻE lava ʻa e ngaahi kautaha mītia sōsialé ʻo faʻu ha ngaahi kulupu ngāue, ʻo fakangofua ʻenau ngaahi timi maluʻi takitaha ke vahevahe fakaʻilekitulōnika ʻa e ngaahi meʻa fakatokanga ʻekitivitī koví, ngaahi TTP mo e ngaahi siofí, ʻo faingataʻa ange ai ke ngāue ʻaki ʻe he kakai ngāue koví ʻenau ngaahi peletifoomú ke poupou ki he ngaahi kemipeini koví.

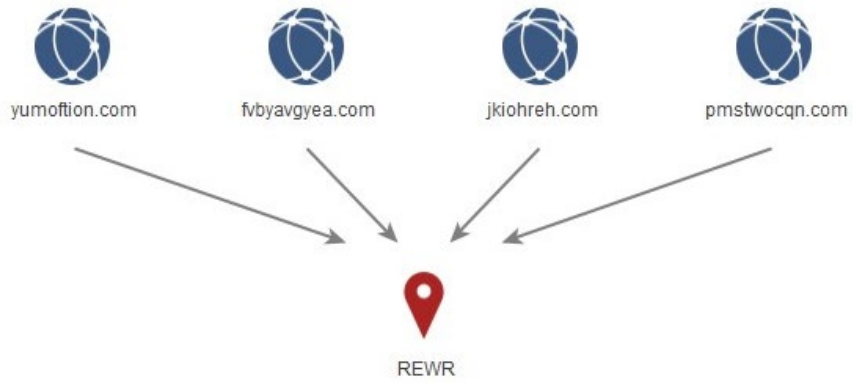
- **Kumi ʻo e apps kuo liliu:** Kapau ʻoku lava, ʻoku totonu ke fakakau ʻe he kau faʻu app ha fatongia ʻokú ne tala ki he taha ʻokú ne ngāue ʻakí kapau kuó nau taunilotu ha tatau ʻoku ʻʻikai fakaʻofisialeʻ ʻo ha app, ke tokoni ki he maluʻi meí he ngaahi tatau koví.

Appendix A: Ngaahi kalafi ʻo e BADBAZAAR WHOIS fakatahataha‘i / fakamatala ʻo e tōmeini polouká

ʻĪmisi 1 – ‘UKYJYUJ’

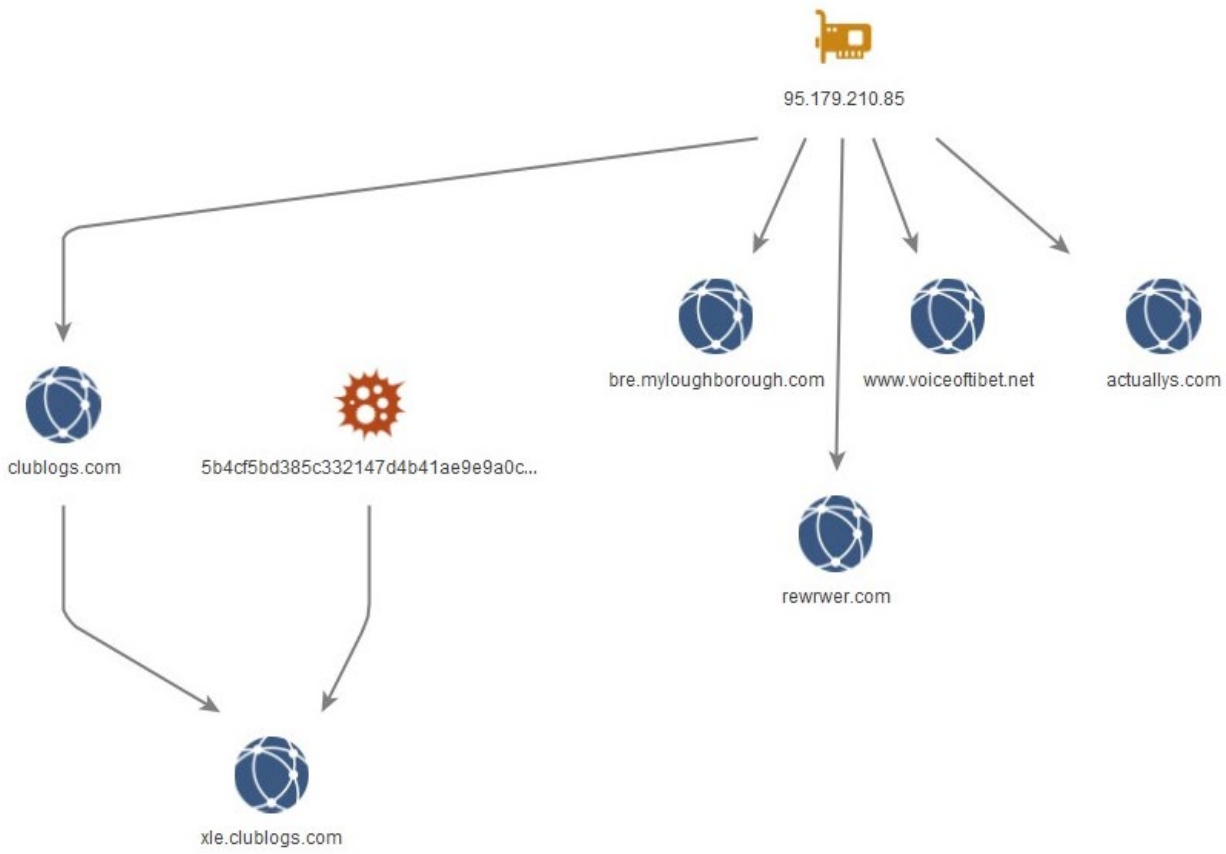


ʻĪmisi 2 – Ngaahi tu‘unga hokohoko ʻi he kīpootí

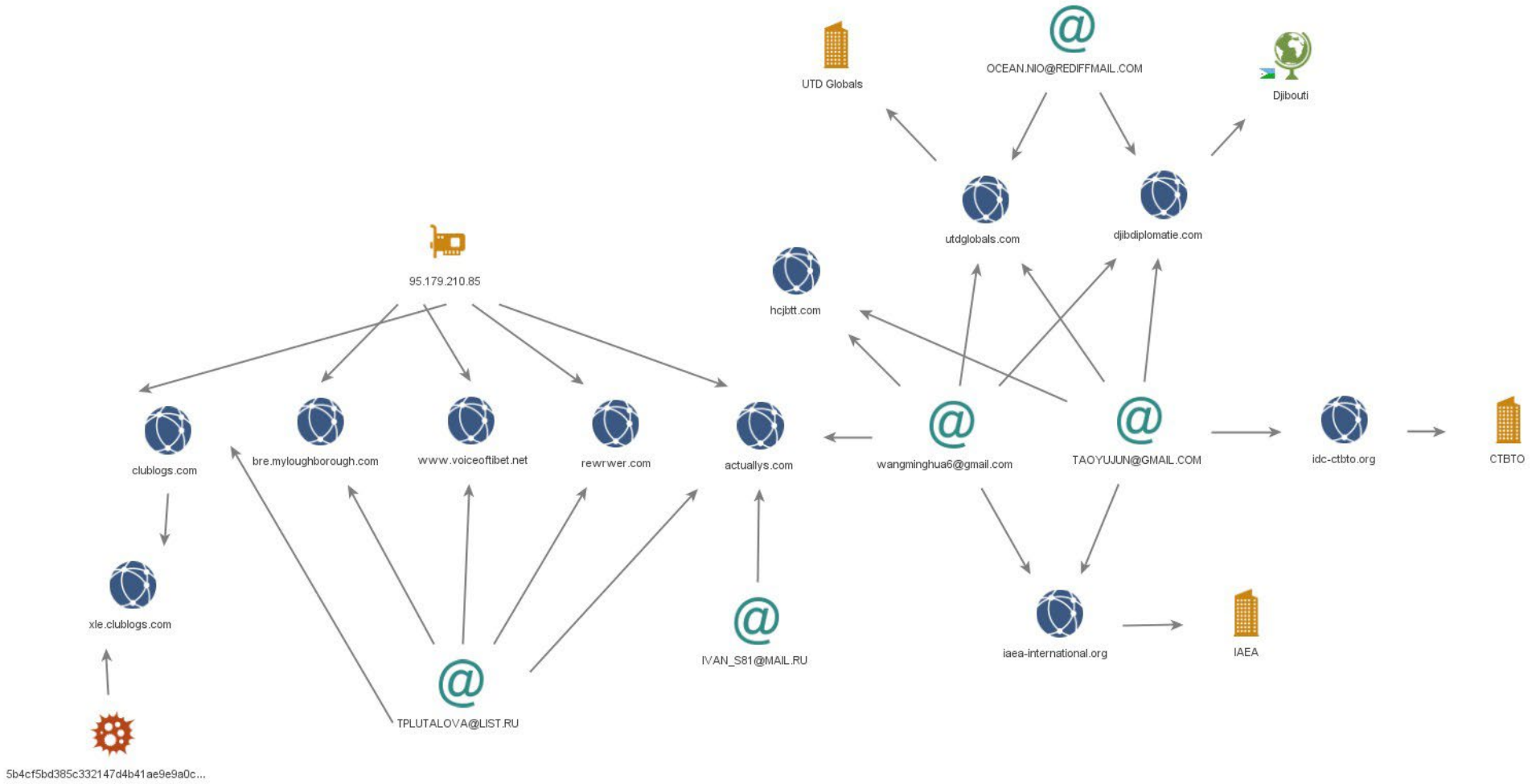


ʻĪmisi 3 – Ngaahi tōmeini makehe fakataha mo e ngaahi tu‘unga state konga ʻo e ‘FSDF’

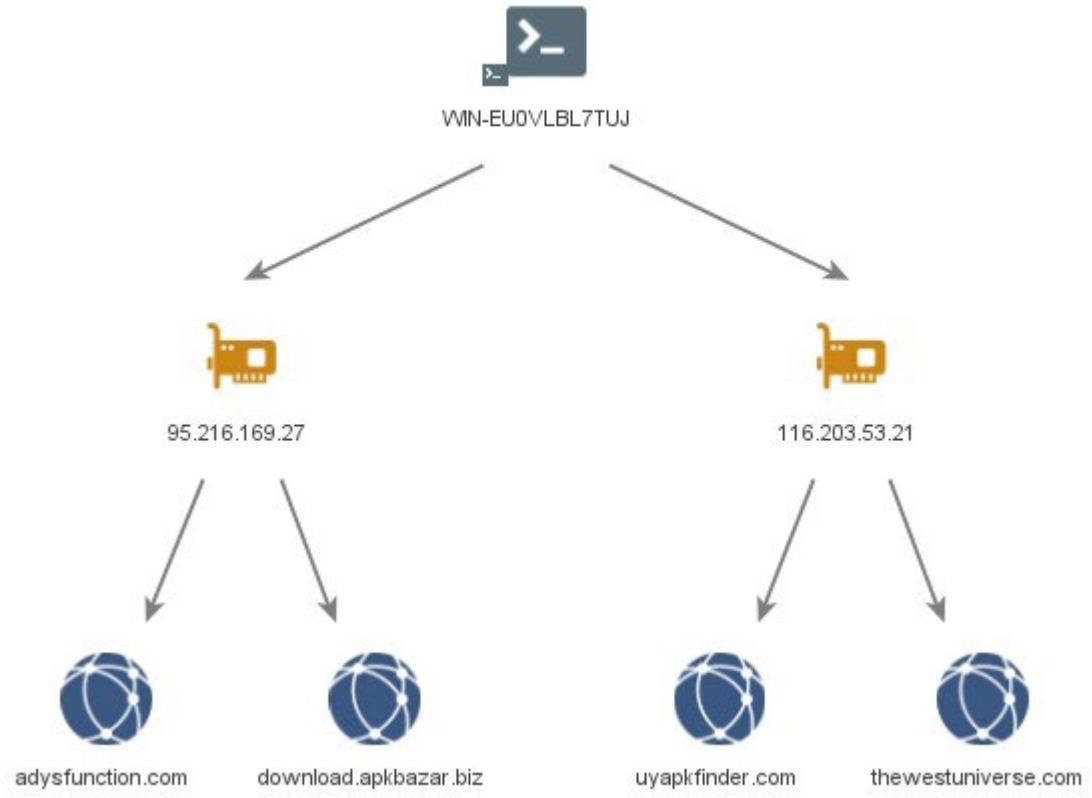
ʻĪmisi 4 – **95.179.210[.]85**



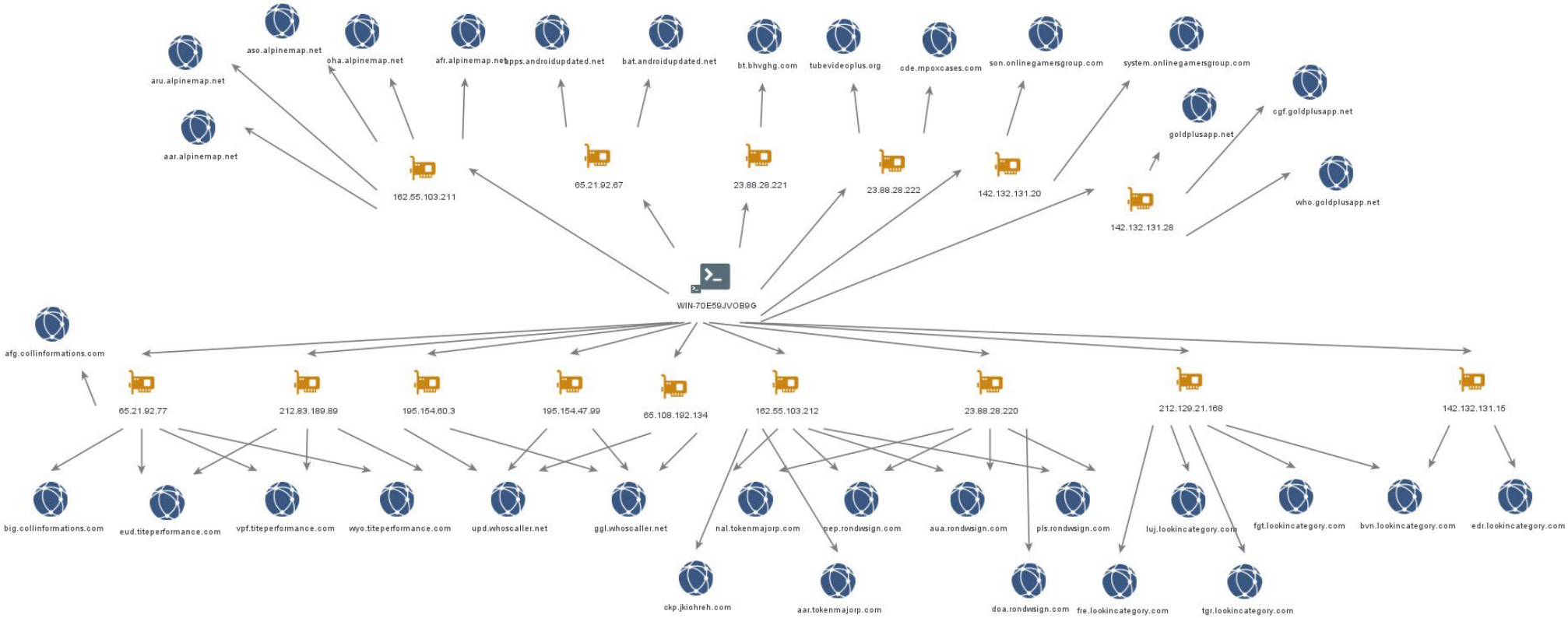
‘Īmisi 5 – ngaahi fehokotaki‘anga ‘initaneti WHOIS



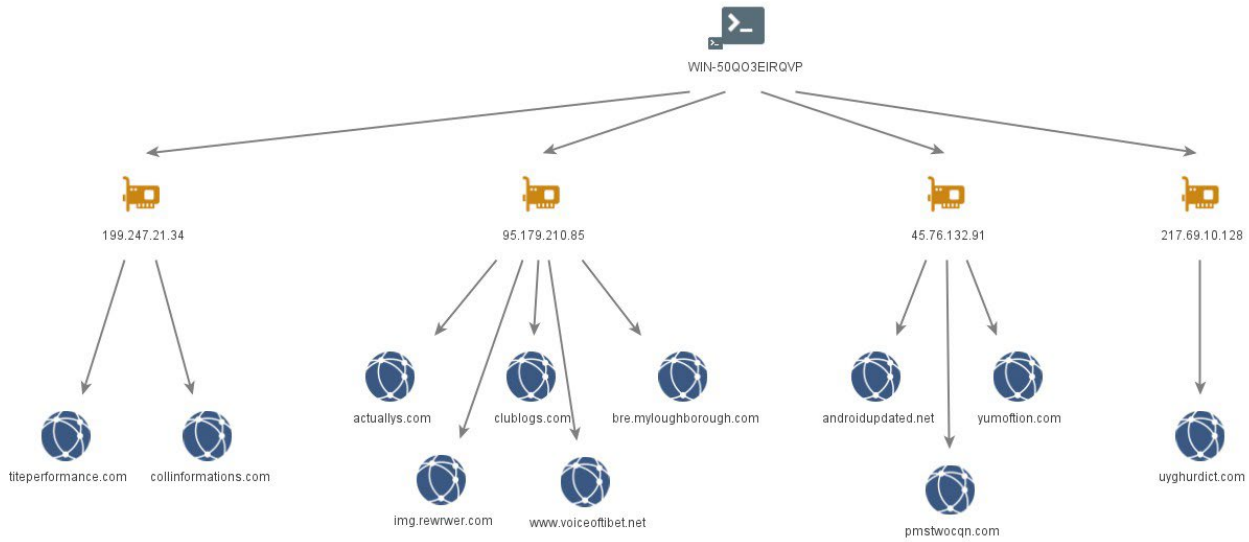
ʻĪmisi 6 – **WIN-EU0VLBL7TUJ**



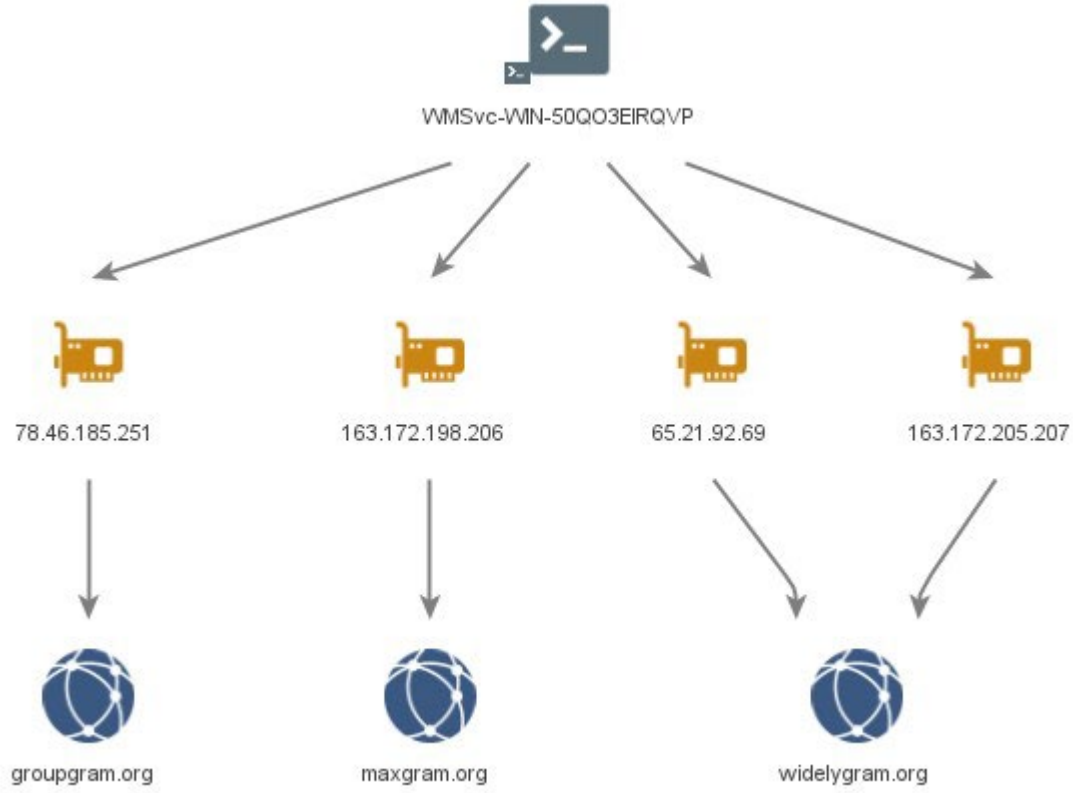
‘Īmisi 7 – **WIN-70E59JVOB9G**



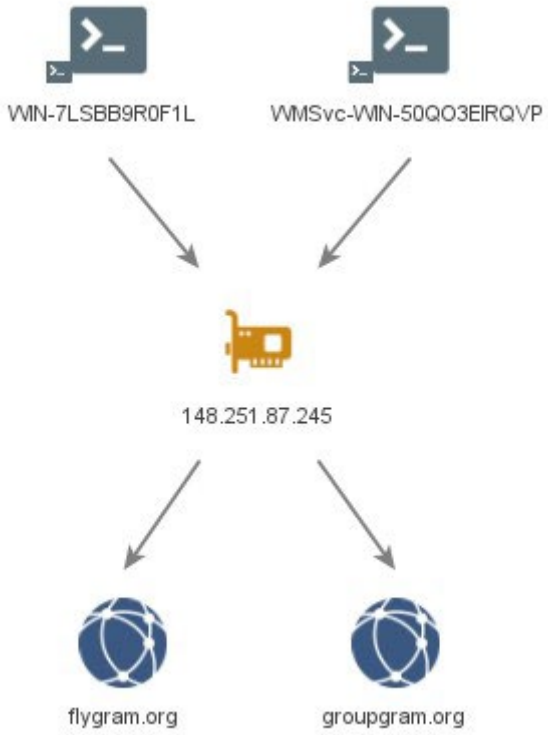
ʻĪmisi 8 - **WIN-50QO3EIRQVP**



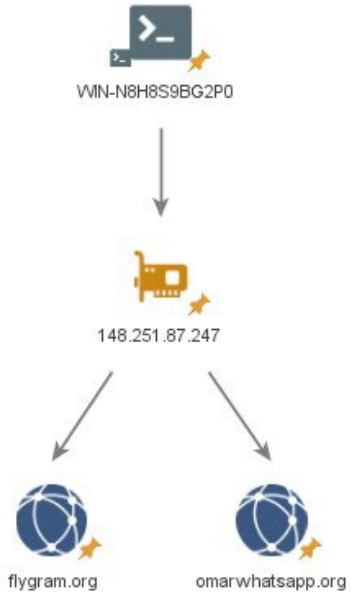
ʻĪmisi 9 - **VMSvc-WIN-50QO3EIRQVP**



‘Īmisi 10 – **VMSvc-WIN-50QO3EIRQVP** mo e **WIN-7LSBB9R0F1L**



ʻĪmisi 11 - **WIN-N8H8S9BG2P0**



ʻĪmisi 12 – **WIN-I6VBN8MR92A**

Appendix B: Siofi ʻo e ngaahi semipolo MOONSHINE & BADBAZAAR

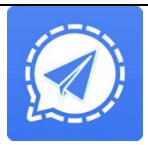
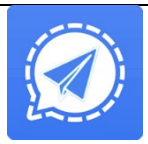
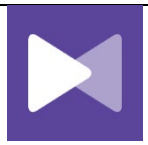
ʻOku lisi ʻi he tēpile ʻi laló ʻa e ngaahi app ʻoku ngāue ʻaki ʻi he ngaahi kemipeini ʻi he MOONSHINE mo e BADBAZAAR ʻi he taʻu ʻe ua kuo ʻosi.

Ko e lahi taha ʻo e ngaahi apps ko ʻení ʻokú ne fakahā ha faitatau mahino ki he apps kuo fokotuʻu. ʻOku ngalingali ko ha founga eni ʻa ha taha ngāue kovi naʻá ne taumuʻa ke 'spoof' ʻa e ngaahi kalasi ʻiloá.

ʻOku mahuʻinga ke ʻiloʻi, ko e hingoa ʻo e app, hingoa ʻo e package, mo e ʻaikoní ʻe lava ke ne fakapuli pe tatau mo e polokalama moʻoní pea ʻoku totonu ke ʻoua ʻe ngāue ʻaki ʻiate ia pē ke tala ʻaki pe kuo uesia ha meʻangāue.

Hingoa ʻo e App	Hingoa ʻo e Package	ʻAikoni ʻo e App
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

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

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

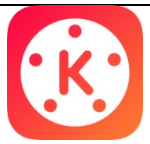
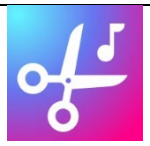
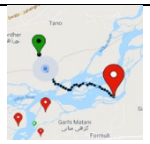
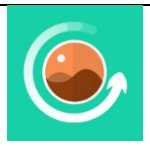
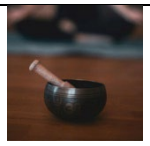
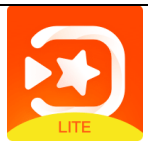
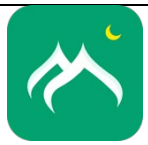
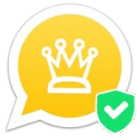
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

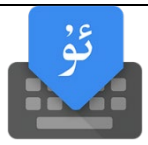
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

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

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

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

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

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

Laukonga makehe

Fakahinohino meí he Australian Cyber Security Centre

- Lipōti ha hia ʻinitaneti, meʻa naʻe hoko pe tuʻunga
- Founga ke maluʻi ʻaki hoʻo ngaahi meʻangāué
- Maluʻi hoʻo telefoni toʻotoʻó
- Phishing
- Scams
- Maluʻi hoʻo mītia sōsialé
- Ngaahi fakahinohino founga malu ki he mītia sōsialé mo e apps fetohiʻakí

Fakahinohino meí he UK NCSC mo e NPSA

- Taukapoʻi ʻo e Temokālatí
- Mītia Sōsialé: founga ki hono ngāue ʻaki ʻoku malú
- Fakahinohino ki he Malu ʻa e Meʻangāué maʻa e ngaahi kautahá kau ai ʻa e telefoni toʻotoʻó
- Lipōti ʻo e fakatuʻutāmaki ki he ngaahi falekoloa polokalamá.
- Malu fakatāutahá mo e maluʻi ʻo e kakai ʻoku tuʻu laveangofua ʻaupitó

Fakahinohino meí he US NSA

- Ngaahi Founga Lelei Taha ki hono Ngāue ʻAki ʻo e Telefoni Toʻotoʻó

Fakamatala Fakaʻataʻatā

Kātaki ʻo fakatokangaʻi ʻoku tuku atu ʻe he faleʻi ko ʻení ha fakamatala ʻa ia ʻoku fakalao ʻi he taimi naʻe pulusi aí.

ʻOku makatuʻunga ʻa e lipōti ko ʻení ʻi he fakamatala kuo maʻu meí he kautaha faʻu faleʻí mo e ngaahi maʻuʻanga fakamatala ngāueʻangá. Ko ha ngaahi ola mo ha faleʻi kuo fakahoko naʻe ʻikai tuku atu ia ʻaki ha taumuʻa ke fakaʻehiʻehi meí he kotoa ʻo e ngaahi faingamālie ke hoko ha fakatuʻutāmaki pea ko e muimui ki he ngaahi faleʻí ʻe ʻikai ke toʻo ai ʻa e kotoa ʻo e ngaahi faingamālie ko iá. Ko e ngaahi faingāmālie ke hoko ha fakatuʻutāmaki ki he taha ʻoʻona ʻo e fakamatalá ʻoku ʻi he taha ʻoʻona pē ia ʻo e sisitemi takitaha ʻi he kotoa ʻo e ngaahi taimí.

ʻI he UK, ʻoku fakaʻatā ʻa e fakamatala ko ʻeni ʻi he Lao ki he Tauʻatāina ki he Fakamatalá (FOIA) 2000 pea ʻe ala fakaʻatā ʻi ha lao fakamatala kehe ʻi UK.

ʻAve ha ngaahi fakaʻekeʻeke FOIA ki he ncscinfoleg@ncsc.gov.uk.