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

Patnubay

BADBAZAAR at MOONSHINE: Teknikal na pagsusuri at mga pagpapagaan o mitigasyon

ika-9 ng Abril 2025

BADBAZAAR at MOONSHINE: Teknikal na pagsusuri at mga pagpapagaan o mitigasyon

Buod

Sa tulong ng UK Cyber League, ang patnubay na ito ay magkatuwang na inihanda ng National Cyber Security Center (NCSC UK) at mga internasyonal na katuwang:

- **Ang Australian Cyber Security Centre, bahagi ng Australian Signals Directorate**
- **Ang Canadian Center for Cyber Security, bahagi ng Communications Security Establishment**
- **Ang German Federal Intelligence Service**
- **Ang German Federal Office**
- **Ang New Zealand National Cyber Security Center, bahagi ng Government Communications Security Bureau**
- **Ang Federal Bureau of Investigation ng Estados Unidos**
- **Ang National Security Agency ng Estados Unidos**

Nagbibigay ang patnubay na ito ng bago at pinagsama-samang impormasyon ukol sa banta ng intelihensya (threat intelligence) mula sa dalawang uri ng spyware na kilala bilang BADBAZAAR at MOONSHINE, at may kasamang payo para sa mga operator ng app store, developer at mga kumpanya ng social media upang mapanatiling ligtas ang kanilang mga user.

Inilathala ang patnubay na ito kasabay ng patnubay para sa mga biktima ng mga malware na ito.

Ginagamit ng dokumentong ito ang kahulugan ng spyware mula sa glossary ng NCSC: "Isang uri ng malware na ini-install sa isang device nang walang pahintulot ng user, nangongolekta ng mga datos at pagkatapos ay ipinapadala sa third party."

Unang case study: MOONSHINE

Ang MOONSHINE ay isang Android spyware na iniulat noong 2019 ng Citizen Lab na nagta-target ng mga grupong Tibetan. Ang MOONSHINE ay nagpapanggap bilang isang lehitimong app upang akitin ang mga biktima na i-install ito. Isini-share ito sa pamamagitan ng mga channel ng Telegram at sa pamamagitan ng mga link na ipinadala sa WhatsApp.

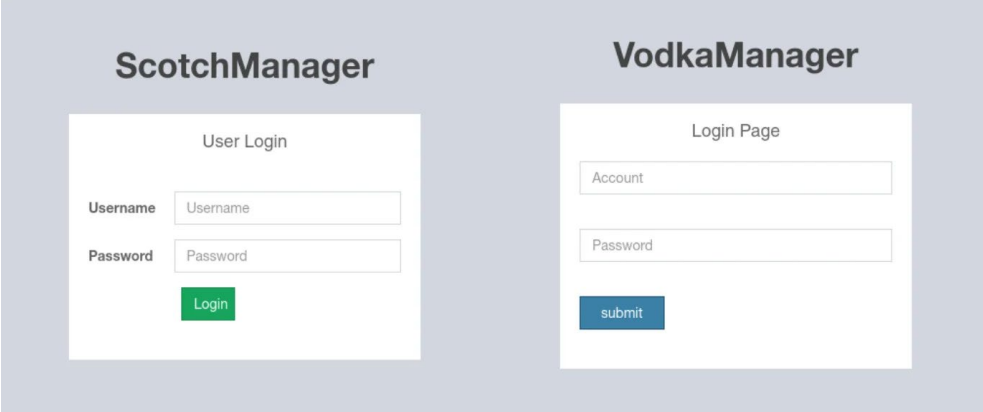
Ang pananaliksik ng NCSC sa MOONSHINE ay nagpapahiwatig ng mga sumusunod:

- Gumagamit ang MOONSHINE ng management interface na sumailalim sa mga pagbabago mula noong una itong naiulat.
- Ang management interface ay nagpapakita ng malawak na mga kakayahan sa pagsubaybay (surveillance), kabilang ang kakayahang mag-exfiltrate ng mga file mula sa mga device pati na rin ang pag-record ng live na audio at mga nasa screen.
- May natuklasang ilang mga MOONSHINE management interface na virtually hosted. Ang mga interface na ito ay may magkatulad na imprastruktura sa mga login panel na nauugnay sa UPSEC, na ayon sa Intelligence Online ay tumutukoy sa 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Management interface

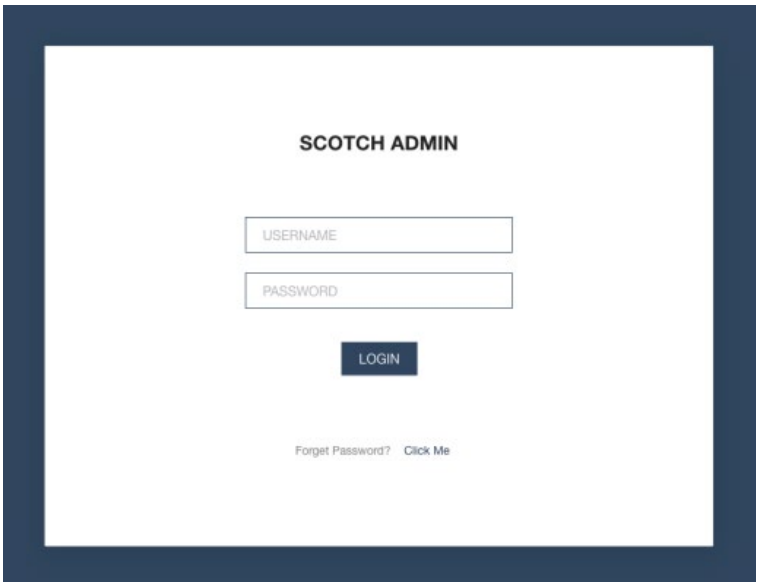
Ipinapakita ng mga naunang ulat tungkol sa mga MOONSHINE management interface na sumailalim ito sa mga pagbabago, na nagpapahiwatig ng patuloy na pag-unlad.

Ang unang halimbawa ng management interface ay makikita sa ulat ng Citizen Lab noong 2019.



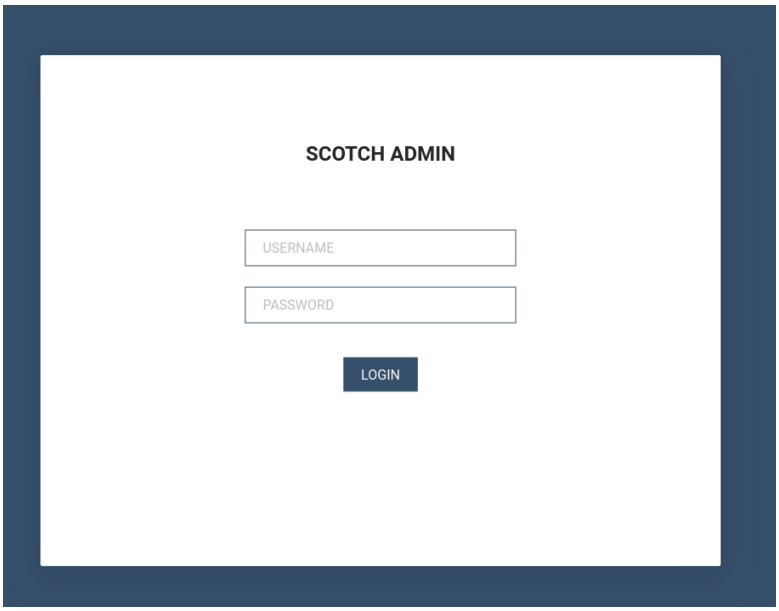
Larawan 1: May nakitang mga Moonshine management interface sa ulat ng Citizen Lab noong 2019 na 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'.

Noong unang bahagi ng 2022, nag-ulat ang Lookout ng ibang management interface na muling idinisenyo upang magmukhang nasa ibaba (pinapalitan ang mga nakaraang interface sa larawan 1):



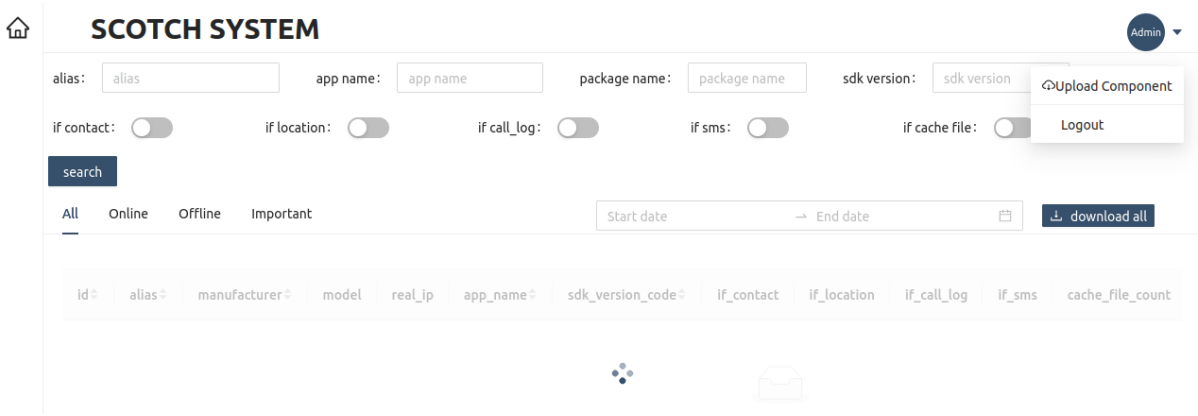
Larawan 2: Moonshine management interface na makikita sa ulat 2022 ng Lookout na 'MOONSHINE: Nagbabagong Android Surveillanceware ng Chinese APT POISON CARP Upang Targetin ang mga Tibetan at Uyghur.

Noong Agosto 2023, isang scan command and control ng MOONSHINE (C2) ang nagpakita ng isang interface na katulad ng 2022 interface kung saan ang function na **'Forget Password'** ay hindi na available gaya ng nasa larawan 2:



Larawan 3: Ang MOONSHINE management interface ay nakita noong Agosto 2023 na wala nang prompt na 'Forget Password'.

Ang karagdagang pagsisiyasat sa management interface ay nagsiwalat ng content sa loob ng panel na nagpapakita kung paano itatabi ang mga detalye ng mga nakompromisong device.



Larawan 4: Webpage sa likod ng login page ng MOONSHINE management interface.

Ipinakita ng pananaliksik sa Lookout ang pagpasa ng '**score**' mula sa device ng biktima patungo sa mga server ng MOONSHINE C2. Ang value ng 'score' ay batay sa mga permiso ng malicious sample sa device ng biktima.

Ang mga column na 'if_contact', 'if_location', 'if_call_log' at 'if_sms' sa loob ng page ay nagpapahiwatig na hindi lahat ng sample ng MOONSHINE ay may ganap na access sa mga nakompromisong device. Ang kaalaman sa mga column na ito at ang 'score' na ipinasa mula sa device patungo sa C2 ay nagpapahiwatig na ginagamit ng mga threat actor ang score upang ipaalam ang antas ng pag-access ng malware sa nakompromisong device sa mga indibidwal na nag-a-access sa management interface.

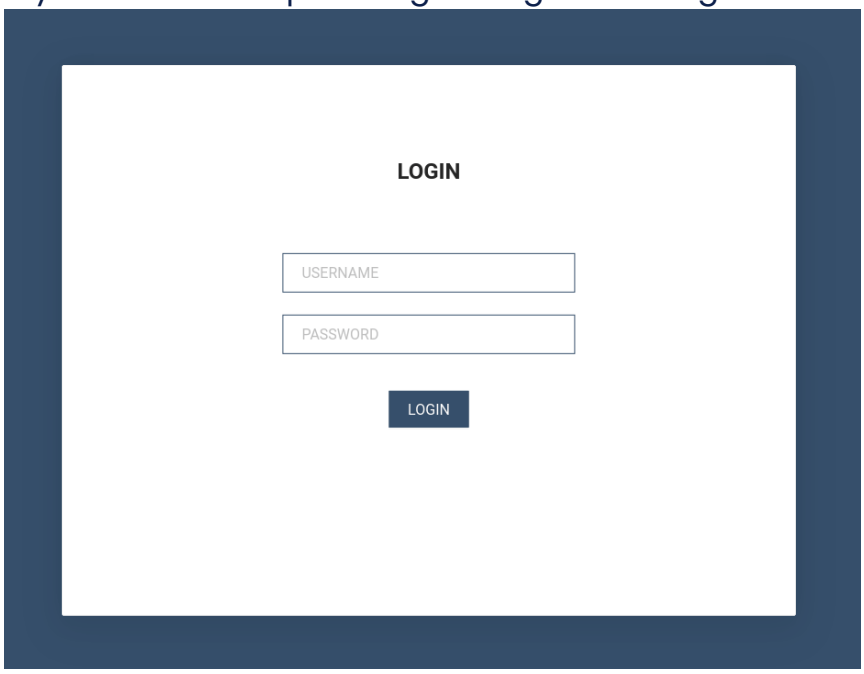
Sa pangkalahatan, ang payo kung ano ang pinakamahusay na gawi upang mapigilan ang mga app na mangalap ng impormasyon mula sa mga device ay ang pagsuri kung may anumang hindi pangkaraniwan sa mga app permission bago mag-download. Gayunpaman, ang mga sample ng MOONSHINE ay humihingi ng mga permiso na nauugnay sa functionality ng app, kaya maaaring mukhang hindi kahina-hinala, ngunit ginagamit din nila ang mga permiso na ito upang mangolekta ng impormasyon mula sa mga device.

Ang MOONSHINE ay mayroon ding Application Programming Interface (API) na nagpapakita ng lawak ng mga kakayahan nito. Ang mga unang bersyon ng dokumentasyon ng API ay naglalaman ng mga pangalan ng API sa Mandarin.

Virtual host

Sa mga pag-search sa mga panel ng MOONSHINE, natuklasan ang mga pagkakataong virtually hosted. Ang virtual hosting ay kapag ang isang IP address ay maaaring mag-host ng maramihang mga website nang sabay-sabay. Ang mga IP address ng mga pagkakataong virtually hosted na ito at ang mga domain hosted ay hindi naobserbahan sa anumang kilalang mga sample ng malware.

Ang mga pagkakataong ito ng management interface ay naiiba, dahil ang title ng mga page ay **'LOGIN'** sa halip na ang dating nakikitang **'SCOTCH ADMIN'**.



Larawan 5: MOONSHINE management interface gamit ang LOGIN na title sa halip na SCOTCH ADMIN.

Bilang karagdagan, ang nilalaman sa panel ay naiiba din sa figure 4, tulad ng nakikita sa figure 6:

Larawan 6: Webpage sa likod ng login page ng MOONSHINE management interface na virtually hosted.

Ang panel sa larawan 6 ay mukhang stripped-down na bersyon ng panel sa larawan 4. Ang nag-o-overlap na mga katangian ng mga panel ay ang mga pangalan ng column na 'id', 'manufacturer' at 'model' sa talahanayan.

Ang mga pagkakataong natuklasan na virtually hosted ang MOONSHINE ay:

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

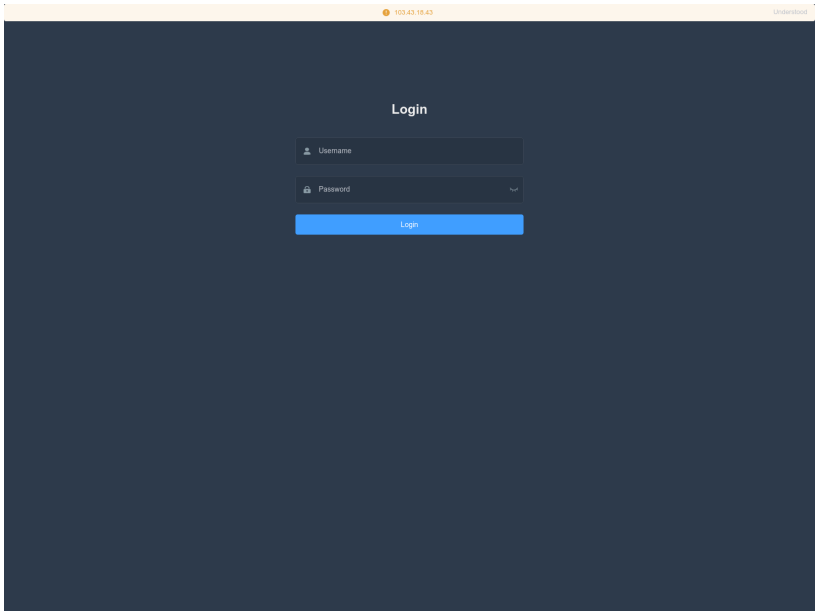
Ang mga domain na ito ay nakalista ng Trend Micro bilang MOONSHINE exploit kit, na responsable sa pagsasamantala sa mga kahinaan ng browser upang makapag-install ng malware sa mga mobile device. Pinangalanan ng Trend Micro ang malware na ito na 'Dark Nimbus'.

Para malinaw, ang mga MOONSHINE management interface ay kung saan nakikipag-ugnayan ang mga sample ng malware ng MOONSHINE, at ine-exfiltrate ang mga datos ng biktima. Ang mga MOONSHINE exploit kit na iniulat ng Trend Micro, ay hiwalay na capability na nagsasamantala sa mga kahinaan ng browser upang makapag-install ng malware na tinatawag na Dark Nimbus sa mga mobile device. Higit pa rito, ang Dark Nimbus at MOONSHINE ay ganap na magkaibang malware.

Parehong may overlap sa code ang MOONSHINE management interface at Moonshine exploit kit kaya magkatulad ang prompt sa pag-login na nasa larawan 3 at 5 pati na rin ang content ng page sa larawan 4 at 6. Pareho rin silang naglalaman ng string na 'webpackJsonpreact-scotchui' sa source code.

Ang mga threat actor ay bumuo ng mga URL link na nakakonekta sa exploitation kit ng MOONSHINE at pagkatapos ay ire-redirect sa mga video na nauugnay sa mga Tibetan at Uyghurs, na nag-o-overlap sa pag-target sa MOONSHINE.

Sa karamihan ng mga IP address na nagho-host ng MOONSHINE exploit kit domain, mayroong isang login page na may title na 'VLiteUI' sa port 444. Ang page na ito ay hindi malawak na naoobserbahan at ang presensya nito sa mga IP na ito ay nagpapahiwatig ng isang posibleng link sa mga operasyon ng mga (threat) actor.



Larawan 7: Login panel na may HTML na title na 'VLiteUI' na naobserbahan sa mga IP na nagho-host din ng mga MOONSHINE exploit kit.

Ang pagsusuri ng Trend Micro sa Dark Nimbus ay nagpakita na ang malware ay magagawang mangolekta ng isang kumpletong listahan ng impormasyon sa device, at ito ay ibabahagi sa C2 gamit ang XMPP protocol.

Binabalangkas din ng Trend Micro na sa ilang bersyon ng Dark Nimbus, natukoy nila ang paglaganap ng string na 'DKNS'.

Ang **'ansec[.]com'** (nakalista bilang isang Dark Nimbus C2 ng TrendMicro) ay naobserbahan din sa mga serbisyo ng XMPP para sa iba pang mga IP address na nagse-serve sa mga web page na may DKNS sa title na:

- 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)

Isa pang hanay ng mga IP address na may '**ansec[.]com**' sa XMPP service ay may mga web page na may title na:

- 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)

Ayon sa Intelligence Online, naobserbahan ang 'UPSEC' sa mga title ng mga HTML page, na tinutukoy sa 'Sichuan Dianke Network Security Technology Co., Ltd'.

Ikalawang case study: BADBAZAAR

Ang BADBAZAAR ay isang mobile malware na may mga variant ng iOS at Android na nagta-target sa mga indibidwal na Uyghur, Tibetan at Taiwanese. Ang spyware na ito ay kumakalat sa pamamagitan ng mga social media platform at mga official app store. Ang kamakailang pag-uulat mula sa Volexity ay nagpapakita ng iba't ibang mga variant ng BADBAZAAR, na pinaghihiwalay bilang BadSolar, BADBAZAAR at BadSignal. Ang tatlong variant ay naka-link sa isa't isa sa pamamagitan ng nag-o-overlap na mga function na ginagamit para sa pagkolekta ng impormasyon ng device at operator.

Ang pananaliksik ng NCSC ukol sa BADBAZAAR ay nagsiwalat ng mga sumusunod:

- Ang pag-cluster ng mga C2 na domain ay nagpapakita ng higit pang mga link sa mga domain na iniulat sa historical threat intelligence.
- Ang mga C2 server at mga sample ng malware ay nagpapakita ng mga hostname na nauugnay sa actor infrastructure.
- Mga karagdagang profile na ginagamit ng mga threat actor para sa social engineering upang maikalat ang kanilang malware sa kabila ng mga official app store.

WHOIS clustering/domain broker

'UJYJYUJ'

Ang pagsusuri sa mga tala ng WHOIS para sa domain ng BADBAZAAR na **'signalplus[.]org**' (iniulat ni ESET) ay nagpapakita ng value na '**UJYJYUJ**' sa field na '**State**'.

Ang paghahanap para sa iba pang mga domain na may parehong value ay nagpapakita ng mga sumusunod na domain of interest:

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

(Tingnan ang Annex A, larawan 1)

Ang mga domain na **signalplus[.]org, tubevideoplus[.]org** at **thetubeplus[.]com** ay iniulat na mga domain ng BADBAZAAR C2, habang iniuulat ng ESET ang sub domain na **mail.pmumail[.]com** bilang isang FlyGram proxy server. Ang FlyGram ay isang BADBAZAAR app na binuo ng mga malicious cyber actor (tingnan ang Appendix para sa listahan ng iba pang BADBAZAAR app).

Mga keyboard walking value

Nakakita rin ang NCSC ng mga katulad na keyboard walking pattern sa iba pang nakarehistrong mga domain ng BADBAZAAR C2.

Halimbawa, lahat ng mga sumusunod na domain ay may value na '**REWR**' na naobserbahan sa field na '**State**' (tulad ng ginamit dati):

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

(Tingnan ang Annex A, larawan 2)

Mga domain na may MGA 'FSDF' state field value

Ang isa pang hanay ng mga domain ng BADBAZAAR C2 ay mayroong '**State**' value '**FSDF**':

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

(Tingnan ang Annex A, larawan 3)

Makasaysayang pag-uulat (historical reporting) na may mga keyboard walking value

Ang paggamit ng mga keyboard walking value sa mga talaan ng WHOIS ng mga domain ng BADBAZAAR ay makikita rin sa historically reported na pag-target ng mga organisasyong Tibetan ng TA413. Naobserbahan ng Recorded Future ang mga domain na kontrolado ng actor na nanggagaya sa mga organisasyong Tibetan at ang paggamit ng value ng organisasyong nagparehistro na **"asfasf".**

clublogs[.]com

Ang mga sample ng BADBAZAAR na nakuha ng Lookout ay naglalaman ng **'xle.clublogs[.]com'** bilang C2 domain. Ang root domain na **'clublogs[.]com'** ay naka-host sa IP address na **'95.179.210[.]85'** at may SSL certificate na may subject at issuer value na **'CN=WIN-50QO3EIRQVP'**. Ang value na ito ay tumugma sa mga SSL certificate na makikita sa mga sample ng BADBAZAAR na gumamit ng SSL pinning upang maiwasan ang pagharang ng mga komunikasyon.

Ang hosting history para sa IP address **95.179.210[.]85** ay nagbabalik ng mga sumusunod na domain of interest:

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

(Tingnan ang Annex A, larawan 4)

www.voiceoftibet[.]net

Ang domain na **'www.voiceoftibet[.]net'** ay lumilitaw na nagpapanggap bilang ang 'Voice of Tibet' na istasyon ng radyo, katulad ng TTP na ginamit ng TA413.

Ang domain na **'rewrwer[.]com'** ay katulad ng dati nang natukoy na **'State'** value na **'REWR'** na makikita sa mga talaan ng WHOIS ng mga domain ng BADBAZAAR.

Ang mga domain na **'clublogs[.]com', 'rewrwer[.]com'**, **'voiceoftibet[.]net'** at **'myloughborough[.]com'** ay nakarehistro lahat sa email address na **'tplutalova@list[.]ru'**.

actually[.]com

Ang mga tala ng WHOIS para sa **'actuallys[.]com'** ay nagpakita ng isang pagkakataon kung saan ang mga tech at admin na email address ay **'tplutalova@list[.]ru'** ngunit ang email ng nagparehistro ay **'ivan_s81@mail[.]ru'**.

Ang historical na impormasyon ng WHOIS para sa domain na **'actuallys[.]com'** ay nagsiwalat ng email sa pagpaparehistro na **'wangminghua6@gmail[.]com'** na nakalista noong ika-24 ng Pebrero 2016. Noong ika-11 ng Marso 2016, ang email ay kasunod na binago sa **'ivan_s81@mail.ru'** kahit na ang petsa ng pag-expire ng pagpaparehistro ng registrar ay nanatiling pareho.

wangminghua6@gmail[.]com

Ginamit ang email address na **'wangminghua6@gmail[.]com'** para irehistro ang mga domain na makikita sa historical threat intelligence reporting. Noong 2015, tinukoy ng Palo Alto ang email na ginamit para irehistro ang mga C2 na domain para sa malware, Cmstar. Noong 2014, ginamit din ito upang irehistro ang mga domain na natukoy ng Mandiant sa mga kampanyang phishing na isinagawa ng APT3. Noong 2013, ginamit ito para irehistro ang mga domain na natagpuan ng CrowdStrike sa isang malware dropper na may Program Database (PDB) path na naglalaman ng mga Chinese character. Ito ay nagpapahayag ng compilation sa isang Chinese system.

taoyujun@gmail[.]com

Ang domain na **'hcjbtt[.]com'** ay nakarehistro sa email address na **'taoyujun@gmail[.]com'** ngunit ang administrator email nito ay nakarehistro sa **'wangminghua6@gmail[.]com'**.

Walang malicious activity na naka-link sa domain na **'hcjbtt[.]com'**, gayunpaman, ang email address na **'taoyujun@gmail[.]com'** ay natagpuan sa mga ulat ng historical threat intelligence. Noong 2014, ginamit ito upang irehistro ang isang domain na natagpuan ng Mandiant sa mga sample ng **'Cueisfry Trojan'** na ginamit sa pag-target ng mga organisasyong Hapon.

Ang email address ay nagrehistro din ng mga domain tulad ng **'iaea-international[.]org'** na lumilitaw na nagpapanggap bilang **International Atomic Energy Agency** at **'idc-ctbto[.]org'** na nagpapanggap bilang **International Data Center** sa **Comprehensive-B Nuclear Organization (BTOCT).**

Ang naunang Whois record para sa domain na **'iaea-international[.]org'** ay nagpakita ng email ng nagparehistro na **'wangminghua6@gmail[.]com'.**

udtglobals[.]com

Ang domain na **'udtglobals[.]com'** ay naobserbahan gamit ang **'wangminghua6@gmail[.]com'** bilang administrator email at **'ocean.nio@rediffmail[.]com'** bilang email address ng nagparehistro. Ang ibang mga tala ng WHOIS para sa domain na ito, ay nagpakita ng parehong email ng nagparehistro ngunit may email address ng administrator na **'taoyujun@gmail[.]com'.**

Ang '**udtglobals[.]com**' ay lumilitaw na nagpapanggap bilang '**UDT Global**' na isang pandaigdigang kaganapan para sa mga kumpanya sa pagtatanggol at seguridad sa ilalim ng dagat. Ang username na **'ocean.nio'** sa loob ng email address ay maaaring ginagaya ang **National Institute of Oceanography (NIO)** na umiiral sa maraming bansa. Bagama't ang paggamit ng email service na '**Rediff**' (na nakabase sa India) ay maaaring magpahiwatag ng imitasyon ng **Indian National Institute of Oceanography.**

Djibdiplomatie[.]com

Ang domain na **'djibdiplomatie[.]com'** ay lumilitaw na nagpapanggap na mga serbisyo ng diplomasya ng Djibouti, na may katulad na WHOIS record sa **'utdglobals[.]com'**. Isang talaan ang lumabas upang ipakita ang nagparehistrong **'ocean.nio@rediffmail[.]com'** at admin na **'taoyujun@gmail[.]com'** samantalang ang ibang mga tala ay nagpakita ng **'wangminghua6@gmail[.]com'** bilang admin email address na may **'ocean.nio@rediffmail[.]com'** bilang email ng nagparehistro.

Ang parehong mga domain na ito ay mayroon ding mga keyboard walking type value sa mga talaan ng WHOIS. Halimbawa, ang **'udtglobals[.]com'** ay may value na '**ASDF**' bilang registrant city nito at ang **'djibdiplomatie[.]com'** ay may **'DAF DAGF**' bilang registrant name value nito. Ito ay maihahambing sa mga value na naobserbahan sa ibang mga domain ng BADBAZAAR.

Bagama't ang mga email address na **'wangminghua6@gmail[.]com'** at **'taoyujun@gmail[.]com'** ay matatagpuan sa mga talaan ng WHOIS para sa mga domain na nagpapanggap bilang isang **global undersea defence event**, **Djibouti diplomacy services** at ang **International Atomic Energy Agency**, ang mga ito ay nasa mga talaan din ng WHOIS para sa maraming non-malicious na domain.

Ang magkahalong masquerading domain at non-malicious domain ay maaaring magpahiwatig ng pag-iral ng infrastructure-procuring entity na ginagamit upang suportahan ang mga operasyon ng mga malicious cyber actor.

Ang email address na **'ocean.nio@rediffmail[.]com'** ay matatagpuan lamang sa mga masquerading domain na inilarawan sa itaas. Ang **'ivan_s81@mail[.]ru'** at **'tplutalova@list[.]ru'** ay nagrehistro ng napakaliit na bilang ng mga domain ayon sa pagkakasunod, at ang ilan sa mga domain na ito ay na-host sa imprastraktura ng BADBAZAAR. Ang tatlong email address na ito ay pinaniniwalaang mas malapit na nauugnay sa mga operasyon ng malicious cyber actor. Ito ay dahil ang mas mataas na bilang ng mga domain na nauugnay sa kanila ay naka-link sa malicious activity, kumpara sa mga email na **'wangminghua6@gmail[.]com'** at '**taoyujun@gmail[.]com**'.

(Tingnan ang Annex A, larawan 5)

Mga link sa iba pang mga threat actor

Ang isa pang karaniwang katangian ng mga domain na naka-link sa BADBAZAAR na **'actuallys[.]com', 'clublogs[.]com', 'myloughborough[.]com', 'rewrwer[.]com'**, at **'voiceoftibet[.]net'** ay ang lahat ng ito ay nakarehistro sa eNom at 'naka-park' sa '**255.255.255[.]254**'.

Kasunod ng mga nakaraang pagsisiyasat ng NCSC, ang ibang mga domain na may ganitong mga katangian ay nagsiwalat ng aktibidad na naka-link sa **APT5** noong 2019, at **APT14** sa pagitan ng 2009 at 2011.

Ang APT5-mga naka-link na domain ay may mga historical na talaan ng WHOIS na nakalista sa **'taoyujun@gmail[.]com'** bilang email address ng nagparehistro.

Ang mga domain na naka-link sa APT14 ay may tatlong titik na mga subdomain na lumalabas na kumakatawan sa nilalayong target ng kanilang mga malicious na operasyon. Ang isang halimbawa nito ay ang **'bae.ciscoline[.]net'**, na nagmungkahi ng nilalayong pag-target sa BAE Systems at natagpuan sa isang sample na '**Poison Ivy**'.

May katulad na katangian ang nakikita sa mga domain ng BADBAZAAR kung saan nauugnay ang mga subdomain sa pangalan ng trojanised app:

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

Mahalagang tandaan na ang mga aktibidad na nauugnay sa APT5 at APT14 ay historical at mayroon ding iba pang mga domain na nakarehistro sa eNom at naresolba sa **'255.255.255.254'** na hindi maaaring maiugnay sa malicious activity. Samakatuwid, hindi tiyak na ang mga actor sa likod ng mga kampanyang ito ay pareho o magkakaugnay.

Mga Pangalan ng Machine

Ang pagsusuri sa mga BADBAZAAR C2 at mga sample ay nagsiwalat ng mga hostname na ginamit bilang value ng 'Common Name' sa mga SSL certificate. Ang mga pagsisiyasat ng NCSC sa mga hostname na naobserbahan sa mga sample at imprastraktura ng BADBAZAAR ay nagpakita na ang mga hostname na ito ay ginagamit sa maraming IP address. Ang mga IP address na ito ay nagho-host ng mga domain na matatagpuan sa mga sample ng BADBAZAAR. Mayroong higit pang detalye sa seksyon sa ibaba tungkol sa mga hostname, at mga IP address na may hostname na nagho-host ng mga domain ng BADBAZAAR C2.

Sa halos lahat ng kaso, ang pagkakaroon ng mga certificate na may value ng hostname ay nag-o-overlap sa mga IP resolution para sa mga malicious domain name na tinukoy, ang ilang mga pagkakataon kung saan hindi ito ang kaso ay nakabalangkas.

WIN-EU0VLBL7TUJ

Ang hostname na **'WIN-EU0VLBL7TUJ'** ay naobserbahan sa mga sumusunod na IP address of interest:

- Nag-host ang '**116.203.53[.]21'** ng BADBAZAAR C2 na domain na '**uyapkfinder[.]com'** at **'thewestuniverse[.]com'**.

- Nag-host ang **'95.216.169[.]27'** ng mga domain ng BADBAZAAR C2 na **'adysfunction[.]com'** at sub-domain na **'download.apkbazar[.]biz'** na naobserbahan bilang download link para sa sample ng BADBAZAAR.

(Tingnan ang Annex A, larawan 6)

WIN-70E59JVOB9G

Ang hostname na **'WIN-70E59JVOB9G'** ay naobserbahan sa mga sumusunod na IP address of interest:

- Nag-host ang '**23.88.28[.]220'** ng mga sub-domain ng BADBAZAAR C2, **'aua.rondwsign[.]com', 'nal.tokenmajorp[.]com', 'pep.rondwsign[.]com'** '**doa.rondwsign[.]com**', at **'pls.rondwsign[.]com'.** May tagal ng dalawang araw sa pagitan ng huling nakita ang certificate na may pangalan ng machine, at noong unang nakitang nagre-resolve ang mga malicious domain sa IP.

- Nag-host ang '**23.88.28[.]221'** ng naka-link na sub-domain ng BADBAZAAR na '**bt.bhvghg[.]com'**.

- Nag-host ang '**23.88.28[.]222'** ng mga domain ng BADBAZAAR C2 na '**tubevideoplus[.]org'** at **'cde.mpoxcases[.]com'**.

- Nag-host ang '**65.21.92[.]67'** ng BADBAZAAR C2 sub-domain na '**bat.androidupdated[.]net'**. Nag-host din ito ng sub-domain na **'apps.androidupdated[.]net'** na isang DoubleAgent malware C2.

- Nag-host ang **'65.21.92[.]77'** ng BADBAZAAR C2 sub-domain na '**wyo.titeperformance[.]com', 'big.collinformations[.]com' 'vpf.titeperformance[.]com', 'eud.titeperformance[.]com'** at **'afg.coll]cominformations'**

- Nag-host ang '**65.108.192[.]134'** ng mga sub-domain ng BADBAZAAR C2 na '**upd.whoscaller.net'**. at **'ggl.whoscaller[.]net'.**

- Nag-host ang **'142.132.131[.]15'** ng BADBAZAAR C2 sub-domain na '**bvn.lookincategory[.]com'** at '**edr.lookincategory[.]com'**. May tagal ng labing-isang araw sa pagitan ng huling nakita ang certificate na may pangalan ng machine, at noong unang nakitang nagre-resolve ang mga malicious domain sa IP.

- Nag-host ang '**142.132.131[.]20'** ng mga sub-domain na '**son.onlinegamersgroup[.]com'** at '**system.onlinegamersgroup[.]com'**, na pinaniniwalaang mga BADBAZAAR C2 dahil naka-host ang mga ito habang naobserbahan sa IP ang mga SSL certificate na nauugnay sa BADBAZAAR.

- Nag-host ang **'142.132.131[.]28'** ng BADBAZAAR C2 domain na '**goldplusapp[.]net'** at mga sub-domain na **'who.goldplusapp[.]net'** at **'cgf.goldplusapp[.]net'**.

- Nag-host ang '**162.55.103[.]211**' ng mga sub-domain ng BADBAZAAR C2 na **'oha.alpinemap[.]net', 'aru.alpinemap[.]net', 'aso.alpinemap[.]net', 'afr.alpinemap[.]net',** at **'aar.alpinemap'.**

- Nag-host ang '**162.55.103[.]212'** ng mga sub-domain ng BADBAZAAR na **'pep.rondwsign[.]com', 'ckp.jkiohreh[.]com', 'aar.tokenmajorp[.]com', 'nal.tokenmajorp[.]com', 'pls.rondwsign[.]com'** at **'aua.rondwsign[.]com'**

- Nag-host ang '**195.154.47[.]99'** ng mga sub-domain ng BADBAZAAR C2 na **'ggl.whoscaller[.]net'** at **'upd.whoscaller.net'.** May tagal ng tatlong araw sa pagitan ng unang nakita ang certificate na may pangalan ng machine at noong huling nakita ang mga malicious domain na nagre-resolve sa IP.

- Nag-host ang **'195.154.60[.]3**' ng mga sub-domain ng BADBAZAAR C2 na '**upd.whoscaller[.]net'**
'ggl.whoscaller[.]net'.

- Nag-host ang '**212.83.189[.]89**' ng mga sub-domain ng BADBAZAAR C2 na '**wyo.titeperformance[.]com', 'eud.titeperformance[.]com', 'vpf.titeperformance[.]com'** at **'afg.collinformations[.]com'.**

- Nag-host ang '**212.129.21[.]168'** ng mga domain ng BADBAZAAR C2, '**fre.lookincategory[.]com**', '**tgr.lookincategory[.]com**', '**fgt.lookincategory[.]com**' '**luj.lookincategory[.]com**' at '**bvn.lookincategory[.]com**'.

(Tingnan ang Annex A, larawan 7)

WIN-50QO3EIRQVP

Ang hostname na **'WIN-50QO3EIRQVP'** ay naobserbahan sa mga sumusunod na IP address of interest:

- Nag-host ang **'45.76.132[.]91'** ng mga domain na **'yumoftion[.]com'**, **'androidupdated[.]net'**. Ang parehong mga domain ay naka-link sa BADBAZAAR bilang mga subdomain na **'fow.yumoftion[.]com'** at **'bat.androidupdated[.]net'** ay mga BADBAZAAR C2 domain. Bukod pa rito, ang sub-domain na **'apps.androidupdated[.]net'**ay isang DoubleAgent C2 domain. Nagho-host din ito ng domain na **'pmstwocqn[.]com'**, na naka-link sa BADBAZAAR sa pamamagitan ng mga talaan ng WHOIS.

- Nag-host ang **‘95.179.210[.]85’** ng **‘clublogs[.]com’**, kung saan ang **‘xle.clublogs[.]com**’ ay isang domain ng BADBAZAAR C2 at nagho-host din ng mga naka-link na domain ng BADBAZAAR na ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, **‘www.voiceoftibet[.]net‘** at ‘**actuallys[.]com**’.

- Nag-host ang ‘**199.247.21[.]34’** ng **‘titeperformance[.]com**’, at ‘**collinformations[.]com’** kung saan ang mga subdomain ay mga domain ng BADBAZAAR C2.

- Nag-host ang ‘**217.69.10[.]128**’ ng domain ng BADBAZAAR C2 na ‘**uyghurdict[.]com**’.

(Tingnan ang Annex A, larawan 8)

WMSvc-WIN-50QO3EIRQVP

Ang hostname na **‘WMSvc-WIN-50QO3EIRQVP’** ay naobserbahan sa mga sumusunod na IP address of interest:

- Nag-host ang **‘78.46.185[.]251’** ng BADBAZAAR C2 domain na **‘groupgram[.]org’**, na iniulat ng Volexity na gumagamit ng port 4432 para sa mga malicious na koneksyon.

- Nag-host ang **‘65.21.92[.]69’** at **‘163.172.205[.]207’** ng domain na **‘widelygram[.]org’** na pinaniniwalaang isang domain ng BADBAZAAR C2, dahil habang naka-host sa parehong mga IP, nakabukas ang port 4432.

- Nag-host ang **‘163.172.198[.]206’** ng domain na **‘maxgram[.]org’** na pinaniniwalaang isang domain ng BADBAZAAR C2, dahil habang ito ay naka-host, nakabukas ang port 4432.

(Tingnan ang Annex A, larawan 9)

WMSvc-WIN-50QO3EIRQVP at WIN-7LSBB9R0F1L

Ang mga hostname na **‘WMSvc-WIN-50QO3EIRQVP’** at **‘WIN-7LSBB9R0F1L’** ay naobserbahan sa sumusunod na IP address nang sabay-sabay:

- Nag-host ang **‘148.251.87[.]245’** ng mga domain ng BADBAZAAR C2 na ‘**flygram[.]org’** at ‘**groupgram[.]org’**.

(Tingnan ang Annex A, larawan 10)

WIN-N8H8S9BG2P0

Ang mga hostname na **‘WIN-N8H8S9BG2P0’** ay naobserbahan sa sumusunod na IP address:

- Nag-host ang ‘**148.251.87[.]247’** ng mga domain ng BADBAZAAR C2 na ‘**omarwhatsapp[.]org’** at ‘**flygram[.]org’**.

(Tingnan ang Annex A, larawan 11)

WIN-I6VBN8MR92A

Ang mga hostname na **‘WIN-I6VBN8MR92A’** ay naobserbahan sa sumusunod na IP address:

- Nag-host ang ‘**148.251.87[.]197’** ng domain ng BADBAZAAR C2 na **‘tryhrwserf[.]com’**.

(Tingnan ang Annex A, larawan 12)

Batay sa available na komersyal na datos, nag-iiba-iba ang paglaganap ng mga machine name na ito sa internet. Ang ilan sa mga ito ay naobserbahang sabay-sabay sa maraming IP address na nagpapahiwatig ng mga VM na nililikha mula sa parehong template. Mahalagang tandaan na para sa ilan sa mga hostname, hindi lahat ng IP kung saan naobserbahan ang mga ito ay maaaring maiugnay sa malicious activity. Ito ay maaaring mangahulugan na ang paggamit ng mga hostname ay hindi eksklusibo sa mga threat actor na ito.

Gayunpaman, ang paglaganap ng ilan sa mga machine name na ito sa mga IP na nagho-host ng mga domain ng BADBAZAAR C2, ay maaaring magpahiwatig na isang infrastructure-procuring entity ay ginagamit upang i-configure ang mga machine upang suportahan ang mga cyber operation ng mga malicious actor.

Presensya sa social media

Ang nakaraang pag-uulat ng Volexity ay nagpakita na ang mga video sa YouTube (na nagpo-promote ng paggamit ng mga malicious application) ay nilikha ng mga malicious cyber actor. Kasama sa mga video na ito ang mga tutorial kung paano gamitin ang mga application na binuo.

Natuklasan ng NCSC ang dalawang karagdagang channel sa YouTube na nauugnay sa mga operasyon ng mga threat actor. Ang YouTube channel na may URL handle na **'@josephjoey3499'** ay lumilitaw na nagpo-promote ng paggamit ng **'Maxgram'** at isang karagdagang channel na nakarehistro sa **'@uyghuraps3096'** ay nagpo-promote ng **'Uyghur APK Finder'**.

Bilang karagdagan, ang mga video sa YouTube na nagpo-promote ng **'Flygram'** at **'Signal Plus'**, ay nagpakita ng mga threat actor na gumagamit ng mga nakikitang numero ng telepono. Sa **'Flygram'** video, sa 0:36 na numero ng telepono na **'+1 (570) 378-7250'** ay makikita at sa panahon ng **'Signal Plus'** video, ang numero ng telepono na **'+1 (267)298 4259'** ay inihayag.

Iniulat ng Volexity ang isang pekeng news site na may temang Tibet na **'ignitetibet[.]net'**, na natuklasan nila sa mga Telegram channel na pinaniniwalaang pinapatakbo ng mga threat actor. Ang email address na **'choekyi.wangmo@ignitetibet[.]net'** ay naobserbahan na nag-iiwan ng mga komento sa mga post sa page na **'tibetone.org'** na pampublikong iniulat ng Lookout bilang isang C2 page na ginamit para sa iOS na variant ng BADBAZAAR.

Ang email address na ito ay pinaniniwalaang kontrolado ng actor, gamit ang persona ni **'Choekyi Wangmo'**.

Pagtatasa

Gumagamit ang BADBAZAAR at MOONSHINE ng ilang pamamaraan ng social engineering para partikular na i-target ang mga komunidad ng Uyghur, Tibetan at Taiwanese, katulad ng:

- trojanization ng mga app of interest sa mga komunidad na ito, tulad halimbawa ang Uyghur language Quran app, ay halos tiyak na iniangkop sa target victim base
- pagdaragdag ng mga trojanised app na ito sa mga official app store ay malamang na nagbibigay anyo ng pagiging lehitimo, at ang pagbabahagi sa mga panggrupong chat ay malamang na nilayon upang samantalahin ang mga pinagkakatiwalaang relasyon sa loob ng mga komunidad na ito

Ang BADBAZAAR at MOONSHINE ay nangongolekta ng datos na halos tiyak na may halaga sa estado ng China. Bagama't ang BADBAZAAR at MOONSHINE ay naobserbahan na nagta-target ng mga Uyghur, Tibetan at Taiwanese na mga indibidwal, mayroong iba pang mga malware na nagta-target ng iba pang mga grupo ng minorya sa China. Ang mga mamamayan mula sa mga co-sealing na bansa, sa China at sa ibang bansa, na itinuturing na sumusuporta sa mga naglalayon na pagbantaan ang katatagan ng rehimen, ay halos tiyak na pinagbabantaan ng mobile malware gaya ng BADBAZAAR at MOONSHINE. Ang capability na mag-capture ng datos ng lokasyon, audio at larawan ay halos tiyak na nagbibigay ng pagkakataong ipaalam sa hinaharap na pagsubaybay (surveillance) at mga operasyon ng panliligalig sa pamamagitan ng pagbibigay ng real-time na impormasyon sa aktibidad ng target.

MITER ATT&CK®

Ang ulat na ito ay pinagsama-sama tungkol sa balangkas ng MITER ATT&CK®, isang globally accessible na batayan ng kaalaman ng mga taktika at diskarte ng kalaban batay sa mga obserbasyon sa real-world.

Taktika	ID	Pamamaraan	Proseso
Pagmamanman	T1593.001	Mag-search sa mga Bukas na Website/Domain: Social Media	Ang mga actor ay nakahanap ng mga online na grupo at forum na tumutugma sa kanilang nilalayong biktima upang mag-share ng malware
Pabuo ng Kakailanganing Mapagkukunan	T1583.001	Kunin ang Imprastraktura: Mga domain	Nagrerehistro ang mga actor ng mga domain para sa kanilang mga command at control server
Pabuo ng Kakailanganing Mapagkukunan	T1587.001	Bumuo ng mga Kakayahan: Malware	Ang malicious code ay isinulat para sa pagpasok sa mga trojanised app
Pabuo ng Kakailanganing Mapagkukunan	T1608.001	Maghanda ng mga Kakayahan: Mag-upload ng Malware	Ang mga trojanised app ay ina-upload sa mga online na platform kabilang ang mga app store
Pabuo ng Kakailanganing Mapagkukunan	T1585.001	Magtatag ng mga Account: Mga Social Media Account	Ang mga actor ay lumilikha ng mga account sa mga website at social media upang i-share at i-advertise ang malware
Pabuo ng Kakailanganing Mapagkukunan	T1585.002	Magtatag ng mga Account: Mga Email Account	Gumagamit ang mga actor ng pribadong naka-host at komersyal na mga email account para sa pagho-host at pag-share ng malware
Paunang Pag-access	T1189	Drive-by na Pagkompromiso	Nakatago ang mga malicious script sa mga lehitimong app at ina-upload sa mga app store
Paunang Pag-access	T1566.003	Phishing: Spearphishing sa pamamagitan ng Serbisyo	Nagpapadala ang mga actor ng mga trojanised app sa mga target na grupo sa

			pamamagitan ng social media kabilang ang Telegram
Pagpapatupad	T1204.002	Pag-execute ng User: Malicious File	Kailangang i-install ng mga biktima ang mga trojanised app para maisagawa ang payload
Pag-iwas sa Pagtuklas	T1027.009	Naka-obfuscate na mga File o Impormasyon: Mga Naka-embed na Payload	Nakatago ang malicious payload sa loob ng mga lehitimong app
Pag-iwas sa Pagtuklas	T1036.005	Pagkukubli: Itugma ang Lehitimong Pangalan o Lokasyon	Ang mga trojanised na file ay tumutugma sa pangalan, hitsura at function ng mga lehitimong app.
Pag-iwas sa Pagtuklas	T1656	Pagpapanggap	Ang mga actor ay nagpapanggap bilang mga pinagkakatiwalaang indibidwal sa pamamagitan ng paggawa ng mga cover website at paggamit ng mga username na nauugnay sa mga target na grupo
Koleksyon	T1123	Audio Capture	Ang mga trojanised app ay maaaring humiling ng mga hindi kinakailangang permiso kabilang ang pag-access sa mikropono
Koleksyon	T1125	Pag-capture ng Video	Ang mga trojanised app ay maaaring humiling ng mga hindi kinakailangang permiso kabilang ang pag-access sa camera
Koleksyon	T1005	Datos mula sa Lokal na System	Ang mga trojanised app ay maaaring humiling ng mga hindi kinakailangang permiso kabilang ang mga lokal na file.
Command at Control	T1071.001	Application Layer Protocol: Mga Protocol sa Web	Kumokonekta ang malware sa C2 gamit ang HTTPS at WebSocket's.

Command and Control	T1509	Non-Standard Port	Ang mga non-standard port ay ginagamit tulad ng port 4432 at 2333
Exfiltration	T1041	Exfiltration sa C2 Channel	Ang malware ay nag-e-exfiltrate ng datos gamit ang mga koneksyong HTTPS at WebSocket.
Epekto	T1565.002	Pagmamanipula ng Datos: Nailipat na Pagmamanipula ng Datos	Ang mga actor ay kumukuha ng datos mula sa mga biktima sa pamamagitan ng enabling app web traffic na hindi kinakailangan para sa functionality ng app

Mga tagapagpahiwatig (Indicators)

MOONSHINE:

- Noong ika-1 ng Abril 2025, ang pag-search para sa mga panel ng VLiteUI ay nagbalik ng sumusunod:

IP Address	Port	Unang Nakita	Huling Nakita
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

- Noong ika-1 ng Abril 2025, isang pag-search para sa mga panel ng SCOTCH ADMIN ay nagbalik ng sumusunod:

IP Address	Port	Unang Nakita	Huling Nakita
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

- Noong ika-14 ng Marso 2024, isang pag-search para sa mga virtual na SCOTCH ADMIN panel ay nagbalik ng sumusunod:

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

BADBAZAAR:

Paglalarawan	Ang SSL certificate ay naobserbahan sa mga BADBAZAAR C2.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Noong ika-1 ng Abril 2025, ang pag-search para sa sertipiko ng BADBAZAAR sa itaas ay nagbalik ng sumusunod:

IP Address	Port	Unang Nakita	Huling Nakita
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

Paglalarawan	Ang sertipiko ng SSL ay naobserbahan sa mga BADBAZAAR C2
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- Noong ika-1 ng Abril 2025, ang pag-search para sa sertipiko ng BADBAZAAR sa itaas ay nagbalik ng sumusunod:

IP Address	Port	Unang Nakita	Huling Nakita
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

- Mga domain ng WHOIS

Nasa ibaba ang isang talahanayan ng mga domain na sa kasalukuyan o sa kasaysayan ay may mga tala ng WHOIS na may mga value na tumutugma sa mga naobserbahan sa mga domain ng BADBAZAAR C2.

WHOIS Value	Mga Domain
Naka-rehistrong Estado: UJYJYUJ **Naka-rehistrong Bansa: Bolivia** **Registrar: 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
Naka-rehistrong Estado: REWR **Naka-rehistrong Bansa: CF** **Registrar: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
Registrant na Estado: FSDF **Registrant na Bansa: AL** **Registrar: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

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

Ang mga sumusunod ay mga link sa iba pang mga indicator of compromise (IoCs) na nauugnay sa BADBAZAAR at MOONSHINE. Hindi makumpirma ng NCSC ang bisa ng lahat ng impormasyon sa mga link na ito at pinapayuhan ang mga mambabasa na independiyenteng alamin ang kanilang katumpakan at kaugnayan:

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

Pagpapagaan o mitigasyon

Hinihikayat ng NCSC ang pagpapatibay ng mga rekomendasyon sa ibaba upang labanan ang mga banta na inilarawan sa mga case study.

- **Dapat tiyakin ng mga operator ng app store, kabilang ang mga third party na app store, at mga developer na secure ang mga app sa kanilang platform at sumusunod sila sa Code of Practice ng pamahalaan.** Tingnan ang Gabay: 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

- **Suporta sa maraming wika:** Dapat mamuhunan ang mga developer ng app sa mga pagsisikap na gawing lokal ang mga popular na app para sa mga user na nagsasalita ng mga minoryang wika sa mga target na grupo kabilang ang Uyghur, Tibetic, Taiwanese Hokkien at Cantonese. Gabay ng Apple para gawing lokal (localising) ang mga app: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Gabay ng Google sa mga translation app: https://support.google.com/l10n/answer/6227218?hl=fil&ref_topic=6307483&sjid=5961568056509626593-EU

- **Pagpapanatiling secure ng iyong social media platform:** Maaaring gawing mas mahirap ng mga kumpanya ng social media para sa mga malicious cyber actor na lumikha ng mga pekeng account at mag-share ng mga malicious file o link sa kanilang mga platform sa talaga namang mga lehitimong online na komunidad. Kung saan posible, ang mga kumpanya ay dapat magbahagi ng mga malicious indicator sa mas malawak na industriya upang mapabuti ang kolektibong pag-unawa sa banta at upang makatulong sa mga hakbang para sa proteksyon.

- **Plano ng pagremedyo para sa mga kustomer:** Ang mga organisasyon ay dapat magkaroon ng mga pamamaraan upang maabisuhan ang mga kustomer na nag-install ng mga malicious app gamit ang kanilang mga

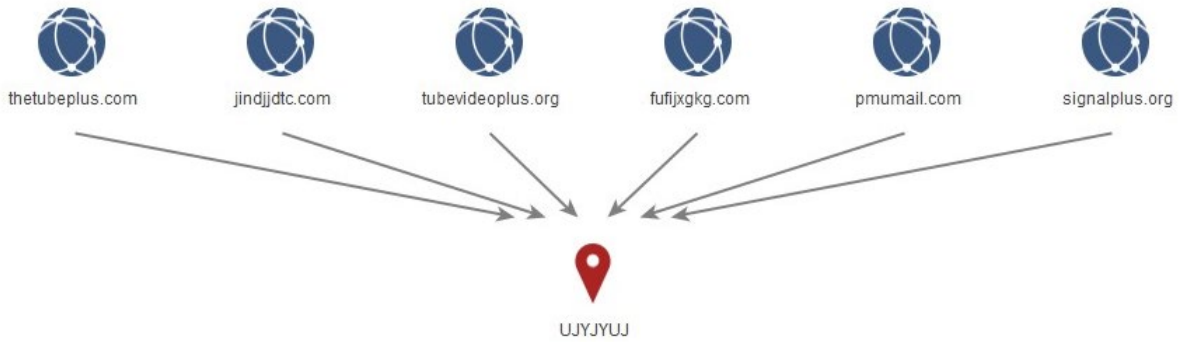
serbisyo. Ang mga alertong ito ay dapat nakakaakit ng pansin at nagbibigay-kaalaman. Kung naaangkop, dapat magbigay ang mga organisasyon ng gabay kung paano aalisin ang software at hikayatin ang mga biktima na mag-ulat sa kanilang mga awtoridad, gaya ng NCSC Sa UK.
Tingnan ang Code of Practice ng App Store para sa higit pang impormasyon: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Mga grupong nagtatrabaho para sa pakikipagtulungan:** Ang mga kumpanya ng social media ay maaaring bumuo ng mga working group, na nagbibigay-daan sa kani-kanilang mga security team na mag-share ng mga malicious indicator, TTP at mga obserbasyon, na ginagawang mas mahirap para sa mga actor na gamitin ang kanilang mga platform upang suportahan ang mga malicious na kampanya.

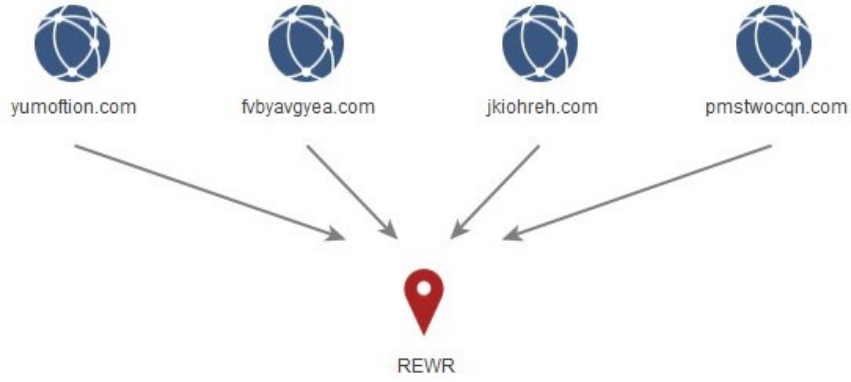
- **Pagtuklas ng mga binagong app:** Kung saan posible, ang mga app developer ay dapat magsama ng functionality na nagpapaalam sa user kung nag-download sila ng isang 'di-opisyal' na bersyon ng isang app, upang makatulong na maprotektahan laban sa mga malicious na kopya.

Appendix A: Mga graph ng BADBAZAAR WHOIS clustering / impormasyon ng broker ng domain

Larawan 1 - 'UKYJYUJ'

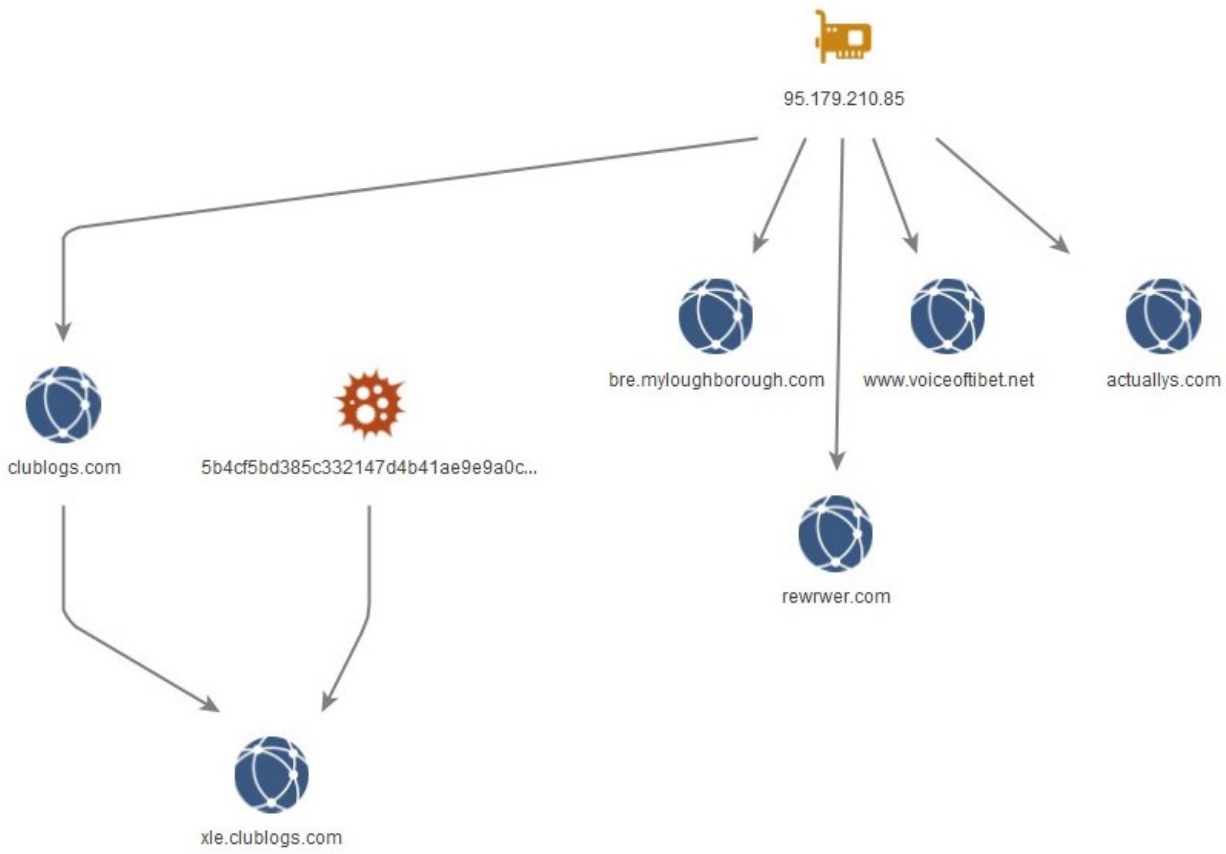


Larawan 2 – Mga keyboard walking value

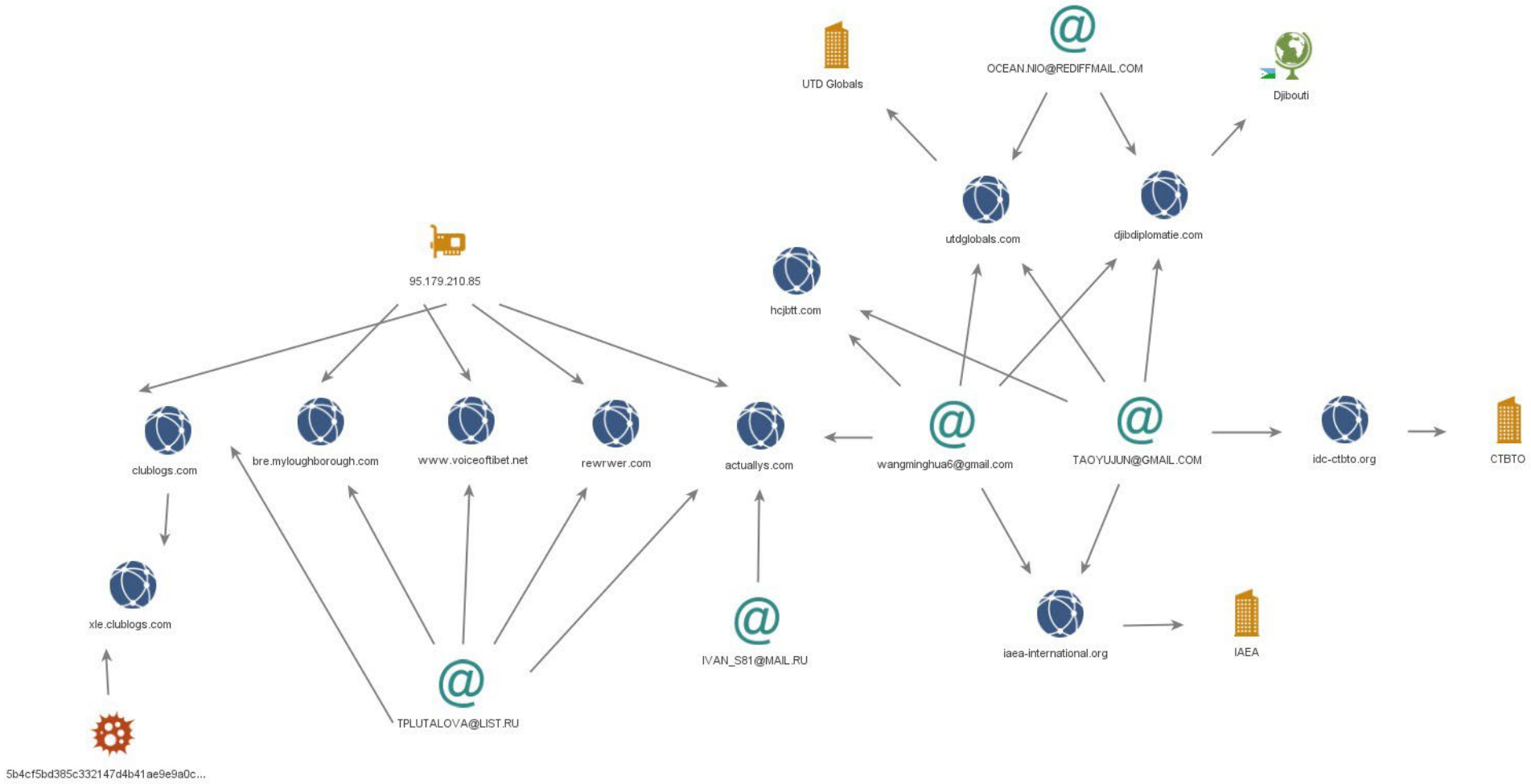


Larawan 3 – Mga karagdagang domain na may mga ‘FSDF’ state field value

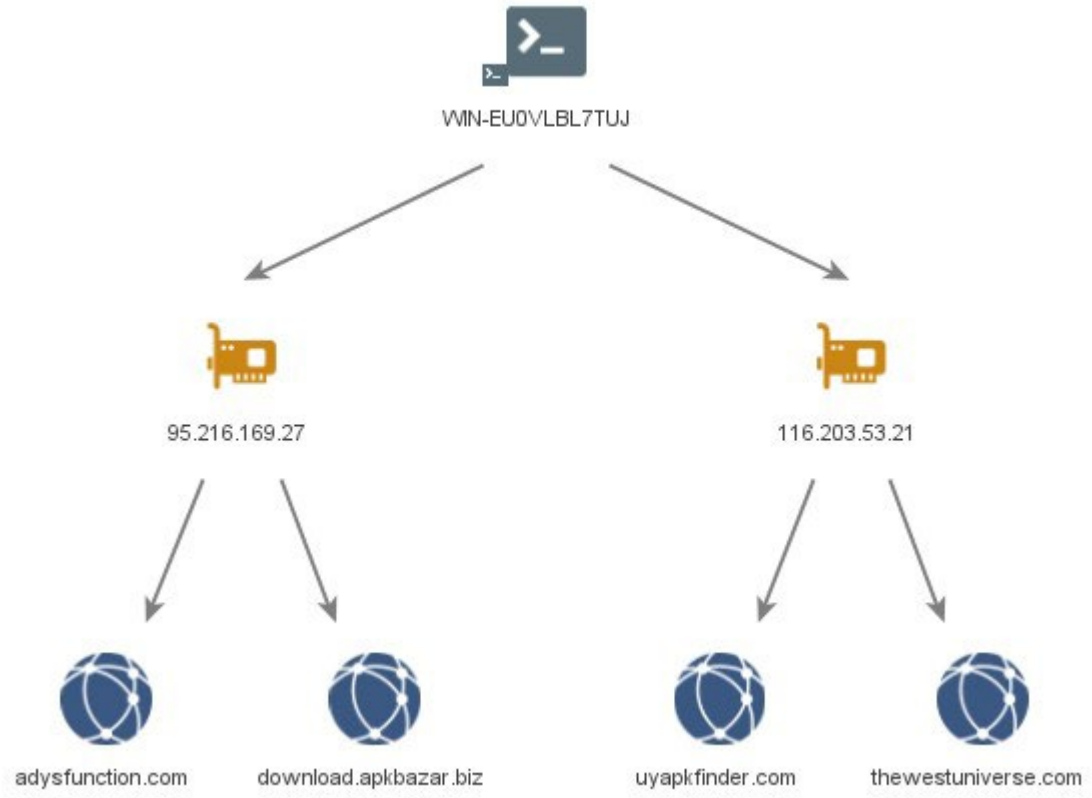
Larawan 4 – **95.179.210[.]85**



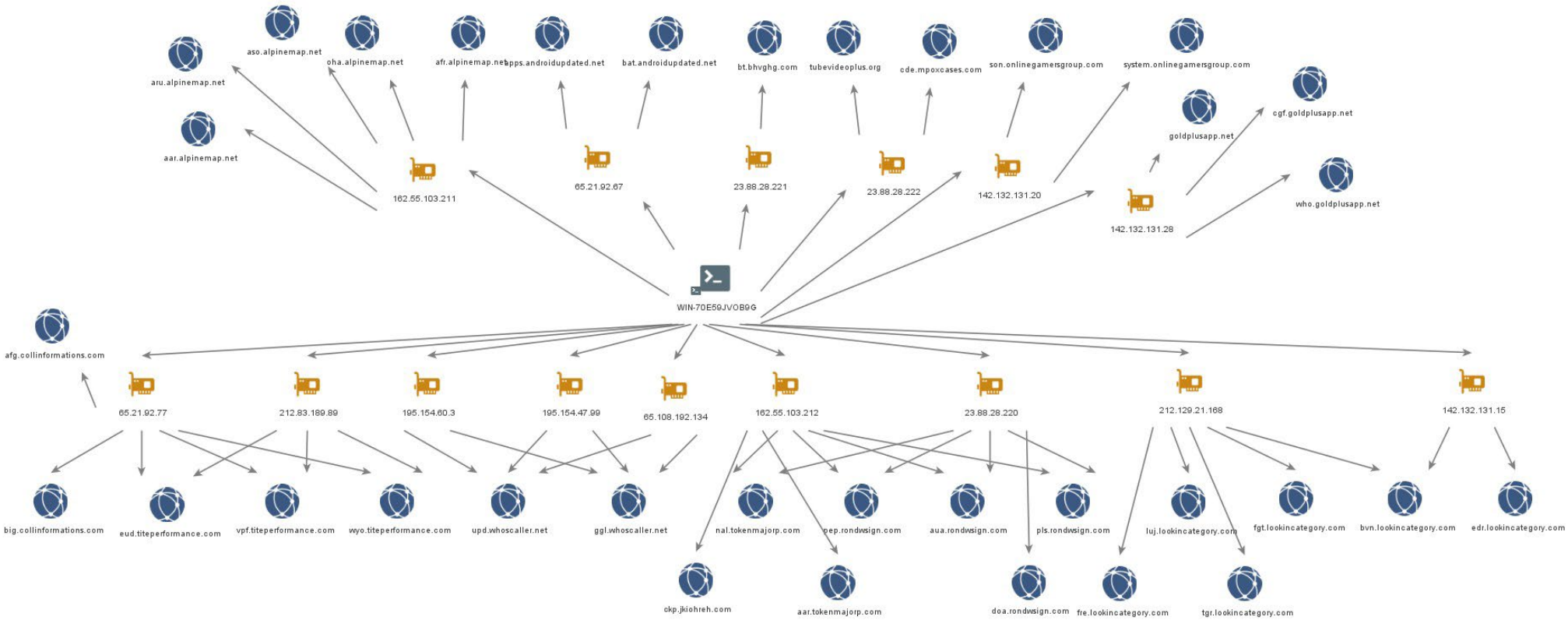
Larawan 5 – Mga link ng WHOIS



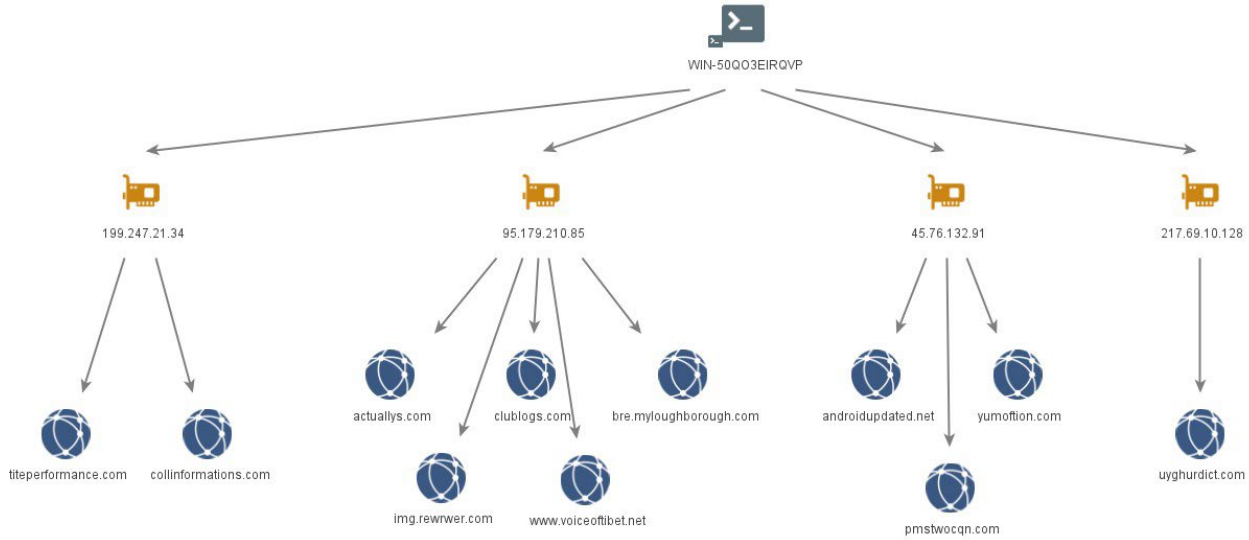
Larawan 6 – **WIN-EU0VLBL7TUJ**



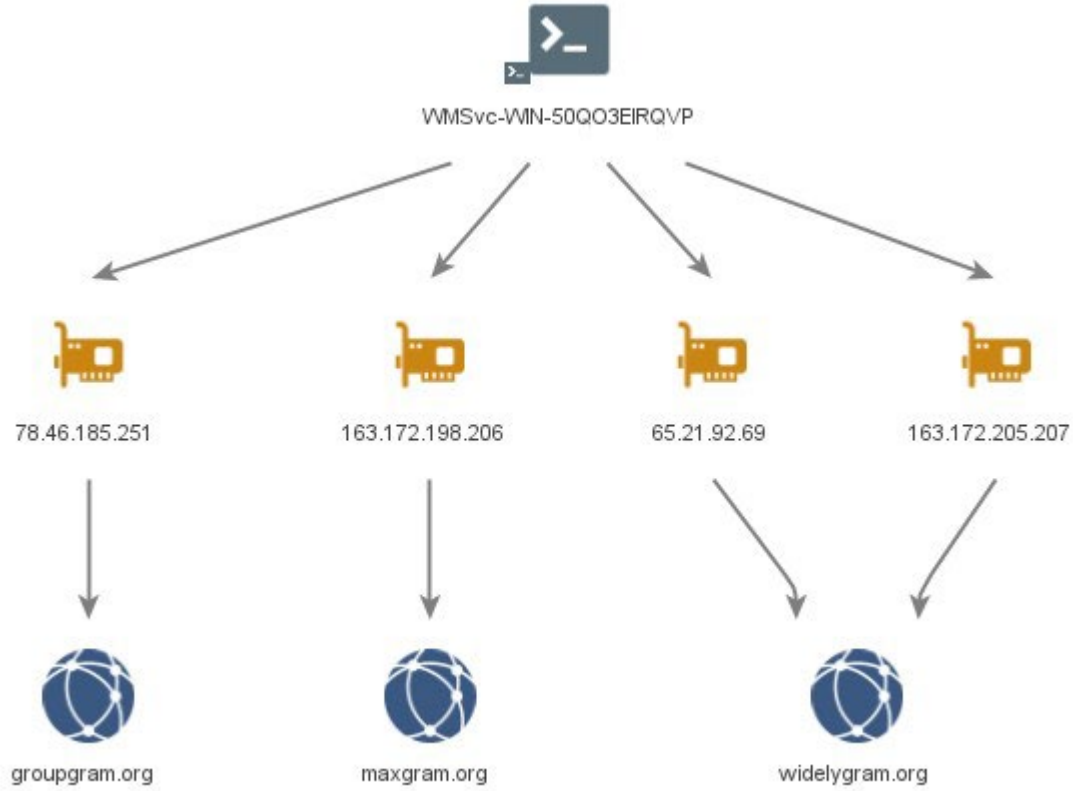
Larawan 7 – **WIN-70E59JVOB9G**



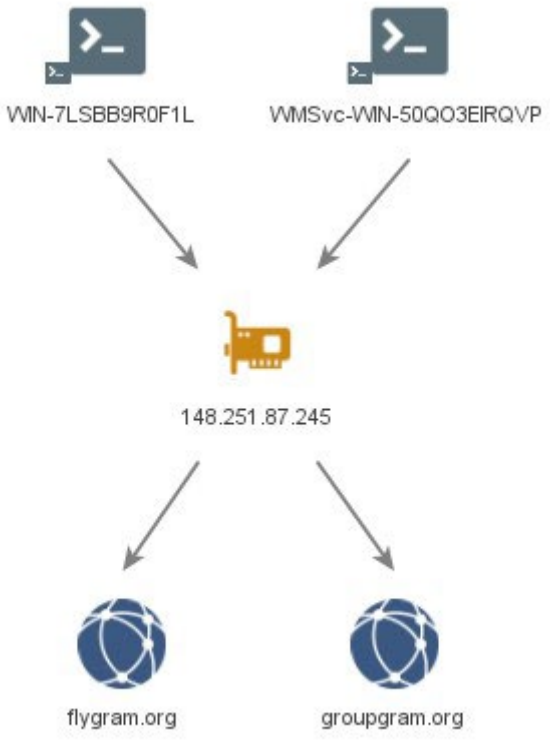
Larawan 8 - **WIN-50QO3EIRQVP**



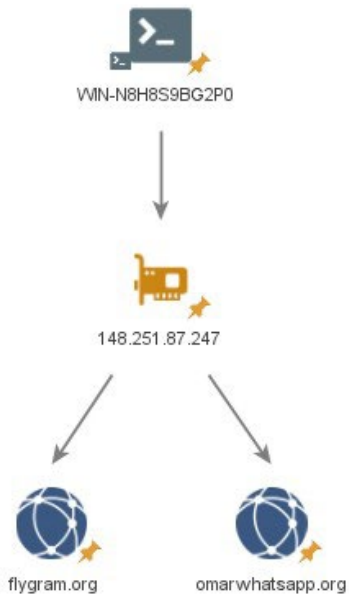
Larawan 9 - **VMSvc-WIN-50QO3EIRQVP**



Larawan 10 – **VMSvc-WIN-50QO3EIRQVP** at **WIN-7LSBB9R0F1L**



Larawan 11 - **WIN-N8H8S9BG2P0**



Larawan 12 – **WIN-I6VBN8MR92A**

Appendix B: Naobserbahang mga sample ng MOONSHINE at BADBAZAAR

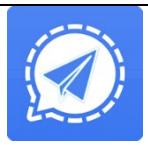
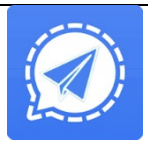
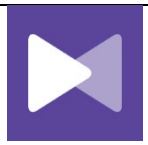
Inililista ng talahanayan sa ibaba ang mga app na ginamit sa MOONSHINE at BADBAZAAR campaign sa nakalipas na dalawang taon.

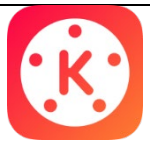
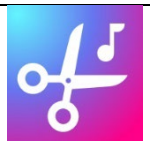
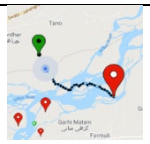
Marami sa mga app na ito ay nagpapakita ng malinaw na pagkakatulad sa mga naitatag na app. Ito ay malamang na isang sinadyang pamamaraan ng actor upang 'kopyahin' ang mga kilalang tatak.

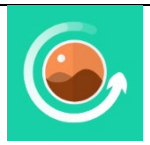
Mahalagang tandaan, ang title ng app, pangalan ng package, at icon ng app ay maaaring lahat gayahin o tumugma sa tunay na application at samakatuwid ay hindi dapat gamitin nang eksklusibo upang matukoy kung ang isang device ay nahawaan.

Title ng app	Pangalan ng package	Icon ng app
99 Pangalan ng 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	
Mga Kanta ng Budista (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
Libre ang Diksyunaryo ng EN-UG	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	

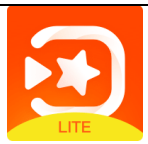
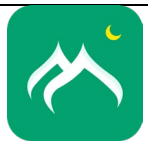
FMWhatsApp	com.fmwhatsapp	
Tagapamahala ng File +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Libreng WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Kalendaryo ng Hijri	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot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

KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter at Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distansya Calculator	com.routemap.mapdownload.gpsroute planner	
Pagbawi ng Media	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	

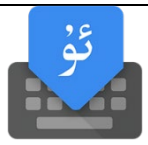
Editor ng Larawan	com.iudesk.android.photo.editor	
Pagbawi ng Larawan	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Aklat ng Panalangin	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Ibalik ang mga Natanggal na Larawan	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	

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

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

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

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

ئاۋازلىق ئەسەرلەر	com.ewlat.eserler	
ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
ئۇيغۇرچە قۇرئان	com.c9.uyghurquran	
القرآن الكريم	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	
نۇر كىرگۈزگۈچ	com.nur.ime	
《心灵法门》念佛机	com.guanyincitta.chant	

汉藏英辞典	com.dacd.dictionary	
藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate	

Karagdagang babasahin

Patnubay mula sa Australian Cyber Security

- Mag-ulat ng cybercrime, insidente o kahinaan
- Paano i-secure ang iyong mga device
- I-secure ang iyong mobile phone
- Phishing
- Mga Scam
- I-secure ang iyong social media
- Mga tip sa seguridad para sa social media at mga messaging app

Patnubay mula sa UK NCSC at NPSA

- Pagtatanggol sa Demokrasya
- Social Media: kung paano ito gamitin nang ligtas
- Gabay sa Seguridad ng Device para sa mga organisasyon kabilang ang mobile
- Ulat ng threat sa mga application store.
- Personal na kaligtasan at seguridad para sa mga indibidwal na may mataas na peligro

Patnubay mula sa US NSA

- Mga Pinakamahuhusay na Kagawian sa Mobile Device

Pagtatatwa

Pakitandaan na ang patnubay na ito ay nagbibigay ng impormasyon na napatunayan sa oras ng paglalathala.

Ang ulat na ito ay kumukuha ng impormasyong nakuha mula sa ahensya ng pag-akda at mga pinagkukunan ng industriya. Ang anumang mga natuklasan at rekomendasyong ginawa ay hindi ibinigay na may layuning iwasan ang lahat ng panganib at ang pagsunod sa mga rekomendasyon ay hindi mag-aalis ng lahat ng naturang panganib. Ang pagmamay-ari ng mga panganib sa impormasyon (information risks) ay nananatili sa may-kinalamang may-ari ng system sa lahat ng oras.

Sa UK, ang impormasyong ito ay hindi kasama sa ilalim ng Freedom of Information Act 2000 (FOIA) at maaaring maging exempt sa ilalim ng iba pang batas sa impormasyon sa UK.

Isangguni ang anumang mga pagtatanong sa FOIA sa ncscinfoleg@ncsc.gov.uk.