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

Advisory

BADBAZAAR and MOONSHINE: Technical analysis and mitigations

9 April 2025

BADBAZAAR and MOONSHINE: Technical analysis and mitigations

Summary

With support from the UK Cyber League, this advisory has been jointly produced by the National Cyber Security Centre (NCSC UK) and international partners:

- **The Australian Cyber Security Centre, part of the Australian Signals Directorate**
- **The Canadian Centre for Cyber Security, part of the 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, part of the Government Communications Security Bureau**
- **The United States Federal Bureau of Investigation**
- **The United States National Security Agency**

This advisory provides new and collated threat intelligence on two variants of spyware known as BADBAZAAR and MOONSHINE, and includes advice for app store operators, developers and social media companies to help keep their users safe.

This advisory is being published in parallel with an advisory for victims of these malware.

This document uses the NCSC glossary definition of spyware: "A type of malware that installs on a device without the user's consent, collecting data and then sending it to a third party."

Case study one: MOONSHINE

MOONSHINE is an Android spyware reported in 2019 by Citizen Lab as targeting Tibetan groups. MOONSHINE masquerades as a legitimate app to lure victims into installing it. It has been shared via Telegram channels and through links sent via WhatsApp.

The NCSC research into MOONSHINE indicates the following:

- MOONSHINE uses a management interface that has undergone changes since it was first reported.
- The management interface reveals extensive surveillance capabilities, including the ability to exfiltrate files from devices as well as capture live audio and screen recordings.
- A set of virtually hosted MOONSHINE management interfaces have been discovered. These interfaces have infrastructure overlap with login panels associated with UPSEC, which according to Intelligence Online refers to 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Management interface

Previous reporting of MOONSHINE management interfaces indicates that it has undergone changes, which suggests ongoing development.

The first example of the management interface is found in Citizen Lab's 2019 reporting.

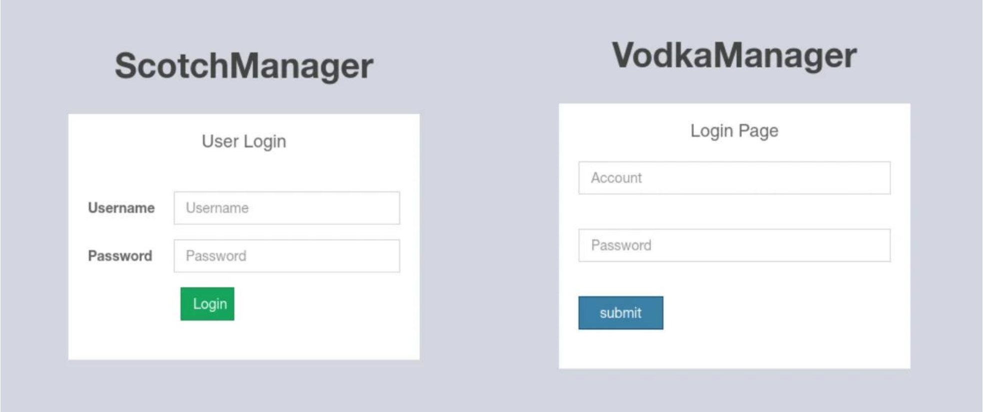


Figure 1: MOONSHINE management interfaces seen in Citizen Lab's 2019 report 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'.

In early 2022, Lookout reported a different management interface which had been redesigned to look as below (replacing the previous interfaces in figure 1):

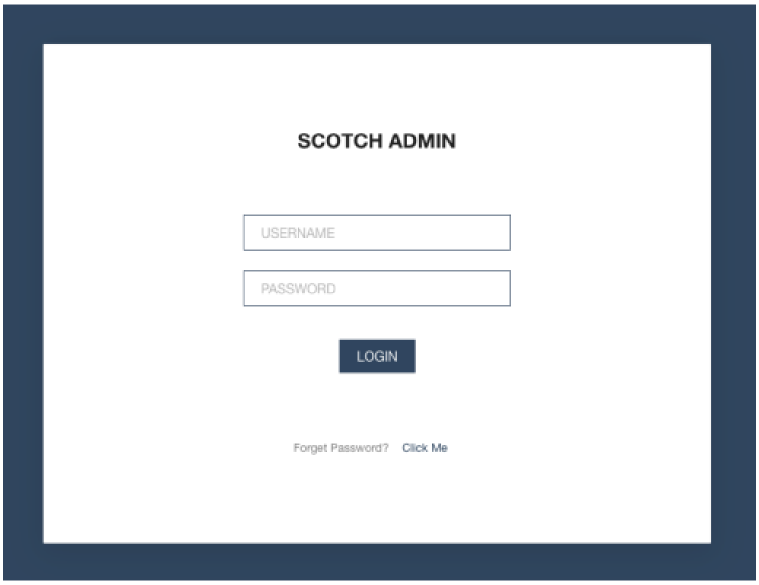


Figure 2: MOONSHINE management interface seen in Lookout's 2022 report 'MOONSHINE: Evolving Android Surveillanceware by Chinese APT POISON CARP To Target Tibetans and Uyghurs'.

In August 2023, a scan of MOONSHINE command and control (C2) revealed an interface similar to the 2022 interface with the '**Forget Password**' function no longer available as it is in figure 2:

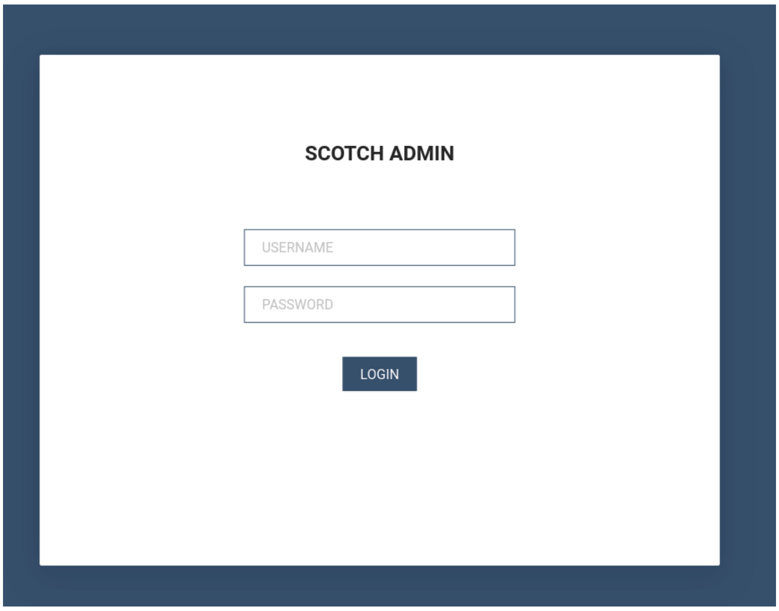


Figure 3: MOONSHINE management interface observed August 2023 which no longer has a 'Forget Password' prompt.

Further investigation of the management interface showed content within the panel which revealed how details of the compromised devices would be stored.

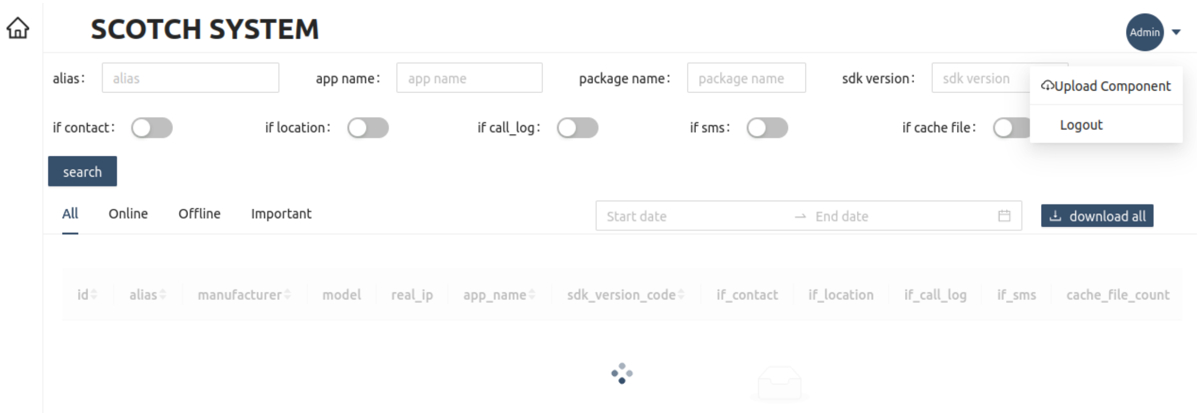


Figure 4: Webpage behind the login page of the MOONSHINE management interface.

Lookout research showed the passing of a '**score**' from the victim device to MOONSHINE C2 servers. The value of the 'score' is based on the permissions of the malicious sample on the victim device.

The columns 'if_contact', 'if_location', 'if_call_log' and 'if_sms' within the page suggest that not all MOONSHINE samples have full access to compromised devices. Knowledge of these columns and the 'score' passed from the device to the C2 suggests the threat actors are using the score to communicate the level of access the malware has to the compromised device to individuals who are accessing the management interface.

Generally, best-practice advice to prevent apps gathering information from devices is to inspect app permissions for anything unusual before downloading. However, MOONSHINE samples seek permissions which are relevant to the app's functionality, so may appear unsuspicious, but they also use these permissions to collect information from devices.

MOONSHINE also has an Application Programming Interface (API) revealing the breadth of its capabilities. Early versions of the API documentation contained API names in Mandarin.

Virtual hosts

In searches for MOONSHINE panels, virtually hosted instances were discovered. Virtual hosting is when one IP address can host multiple websites at once. The IP addresses of these virtually hosted instances and the domains hosted were not observed in any known malware samples.

These instances of the management interface differed, as the title of the pages were '**LOGIN**' instead of the previously seen '**SCOTCH ADMIN**'.

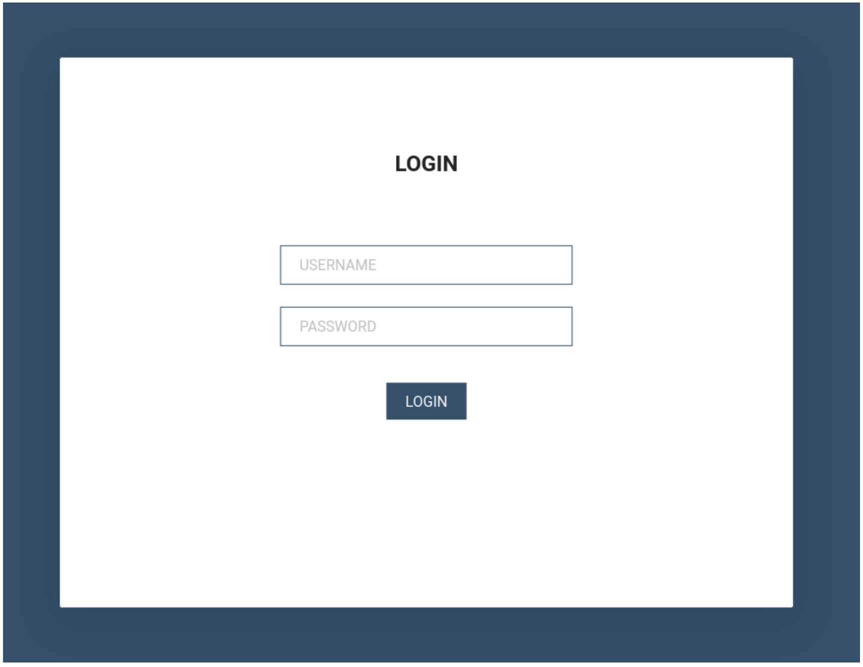


Figure 5: MOONSHINE management interface using LOGIN title instead of SCOTCH ADMIN.

In addition, the content on the panel also differs from figure 4, as seen in figure 6:

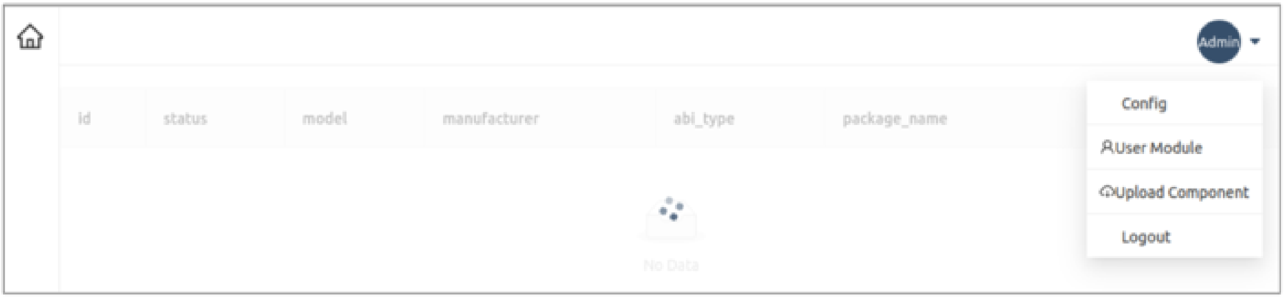


Figure 6: Webpage behind the login page of the virtually hosted MOONSHINE management interface.

The panel in figure 6 appears to be a stripped-down version of the panel in figure 4. The overlapping characteristics of the panels are the column names 'id', 'manufacturer' and 'model' in the table.

The virtually hosted MOONSHINE instances discovered were:

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

These domains are listed by Trend Micro as MOONSHINE exploit kits, responsible for exploiting browser vulnerabilities to install malware on mobile devices. Trend Micro name this malware 'Dark Nimbus'.

For clarification, MOONSHINE management interfaces are what MOONSHINE malware samples communicate with, and victim data is exfiltrated to. MOONSHINE exploit kits reported by Trend Micro, are a separate capability that exploits browser vulnerabilities to install a malware called Dark Nimbus on mobile devices. Furthermore, Dark Nimbus and MOONSHINE are different malware.

Both the MOONSHINE management interface and MOONSHINE exploit kit have code overlap hence the similar login prompts in figures 3 and 5 as well as the content of the page in figures 4 and 6. They also both contain the string 'webpackJsonpreact-scotchui' in the source code.

The threat actors generated URL links which connected to the MOONSHINE exploitation kit and then redirected to videos relevant to Tibetans and Uyghurs, which overlaps with the targeting of MOONSHINE.

Across many of the IP addresses hosting the MOONSHINE exploit kit domain, there is a login page titled 'VLiteUI' on port 444. This page is not widely observed and its presence on these IPs indicates a possible link to the actors' operations.

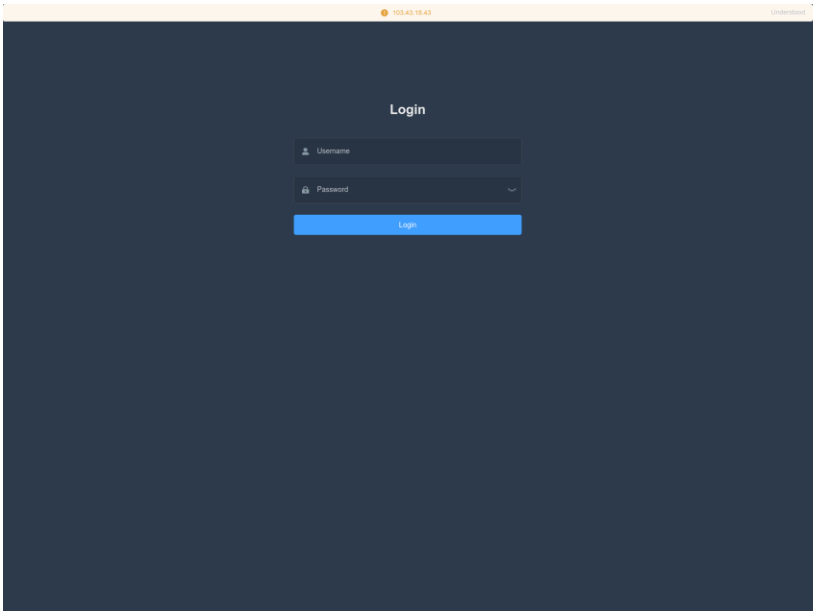


Figure 7: Login panel with HTML title 'VLiteUI' observed on IPs also hosting MOONSHINE exploit kits.

Trend Micro's analysis of Dark Nimbus revealed the malware can collect an exhaustive list of information on the device, and that it communicates with the C2 using the XMPP protocol.

Trend Micro also outlines that in some versions of Dark Nimbus, they identified the prevalence of the string 'DKNS'.

'**ansec[.]com**' (listed as a Dark Nimbus C2 by TrendMicro) was also observed in XMPP services for other IP addresses serving web pages with DKNS in the title:

- 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)

Another set of IP addresses with '**ansec[.]com**' in the XMPP service had web pages with the title:

- 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)

According to Intelligence Online, 'UPSEC' observed in the titles of the HTML pages, referred to 'Sichuan Dianke Network Security Technology Co., Ltd'.

Case study two: BADBAZAAR

BADBAZAAR is a mobile malware with iOS and Android variants that have targeted Uyghurs, Tibetans and Taiwanese individuals. This spyware is spread via social media platforms and official app stores. Recent reporting from Volexity shows different variants of BADBAZAAR, which are separated as BadSolar, BADBAZAAR and BadSignal. All three variants are linked together by overlapping functions used for collecting device and operator information.

The NCSC research into BADBAZAAR revealed the following:

- Clustering C2 domains reveal further links to domains reported in historical threat intelligence.
- C2 servers and malware samples reveal hostnames associated with actor infrastructure.
- Further profiles which the threat actors use for social engineering to spread their malware beyond official app stores.

WHOIS clustering / domain broker

'UJYJYUJ'

Analysis of the WHOIS records for the BADBAZAAR domain '**signalplus[.]org**' (reported by ESET) show the value '**UJYJYUJ**' in the '**State**' field.

A search for other domains with the same value reveals the following domains of interest:

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

(See Annex A, image 1)

The domains **signalplus[.]org**, **tubevideoplus[.]org** and **thetubeplus[.]com** are reported BADBAZAAR C2 domains, while ESET reports the sub domain **mail.pmumail[.]com** as a FlyGram proxy server. FlyGram is a BADBAZAAR app developed by the malicious cyber actors (see Appendix for a list of other BADBAZAAR apps).

Keyboard walking values

The NCSC has also seen similar keyboard walking patterns in other registered BADBAZAAR C2 domains.

For example, the following domains all have the value '**REWR**' observed in the '**State**' field (as used previously):

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

(See Annex A, image 2)

Domains with 'FSDF' state field values

Another set of BADBAZAAR C2 domains have '**State**' value '**FSDF**':

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

(See Annex A, image 3)

Historical reporting with keyboard walking values

The use of keyboard walking values in the WHOIS records of BADBAZAAR domains can also be seen in historically reported targeting of Tibetan organisations by TA413. Recorded Future has observed actor-controlled domains spoofing Tibetan organisations and the use of a registrant organisation value of "**asfasf**".

clublogs[.]com

BADBAZAAR samples obtained by Lookout contained '**xle.clublogs[.]com'** as the C2 domain. The root domain '**clublogs[.]com**' was hosted on IP address '**95.179.210[.]85**' and had an SSL certificate with the subject and issuer value of '**CN=WIN-50QO3EIRQVP**'. This value matched SSL certificates found in BADBAZAAR samples which used SSL pinning to avoid interception of communications.

The hosting history for IP address **95.179.210[.]85** returns the following domains of interest:

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

(See Annex A, image 4)

www.voiceoftibet[.]net

The domain '**www.voiceoftibet[.]net**' appears to be masquerading as the 'Voice of Tibet' radio station, similar to the TTP used by TA413.

The domain '**rewrwer[.]com**' is similar to the previously identified '**State**' value '**REWR**' found in the WHOIS records of the BADBAZAAR domains.

The domains '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' and '**myloughborough[.]com**' were all registered with email address '**tplutalova@list[.]ru**'.

actuallys[.]com

The WHOIS records for '**actuallys[.]com**' showed an instance where the tech and admin email addresses were '**tplutalova@list[.]ru**' but the registrant email was '**ivan_s81@mail[.]ru**'.

Historical WHOIS information for the domain '**actuallys[.]com**' revealed registration email '**wangminghua6@gmail[.]com**' listed on 24 February 2016. On 11 March 2016, the email was subsequently changed to '**ivan_s81@mail.ru**' although the registrar registration expiration date remained the same.

wangminghua6@gmail[.]com

The email address '**wangminghua6@gmail[.]com**' was used to register domains found in historical threat intelligence reporting. In 2015, Palo Alto identified the email used to register C2 domains for the malware, Cmstar. In 2014, it was also used to register domains identified by Mandiant in phishing campaigns conducted by APT3. In 2013, it was used to register domains found by CrowdStrike in a malware dropper with a Program Database (PDB) path containing Chinese characters. This suggests compilation on a Chinese system.

taoyujun@gmail[.]com

The domain '**hcjbtt[.]com**' is registered with email address '**taoyujun@gmail[.]com**' but its administrator email is registered with '**wangminghua6@gmail[.]com**'.

There is no malicious activity linked to domain '**hcjbtt[.]com**', however the email address '**taoyujun@gmail[.]com**' was found in historical threat intelligence reports. In 2014, it was used to register a domain found by Mandiant in '**Cueisfry Trojan**' samples used in targeting of Japanese organisations.

The email address also registered domains such as '**iaea-international[.]org**' which appeared to masquerade as the **International Atomic Energy Agency** and '**idc-ctbto[.]org**' masquerading as the **International Data Centre** at the **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

An earlier Whois record for the domain '**iaea-international[.]org**' showed the registrant email to be '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

The domain '**udtglobals[.]com**' was observed using '**wangminghua6@gmail[.]com**' as the administrator email and '**ocean.nio@rediffmail[.]com**' as the registrant email address. Other WHOIS records for this domain, showed the same registrant email but with the administrator email address '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' appeared to be masquerading as '**UDT Global**' which is a global event for undersea defence and security companies. The username '**ocean.nio**' within the email address could be imitating the **National Institute of Oceanography (NIO)** which exists in multiple countries. Although the use of the '**Rediff**' email service (which is India-based) could suggest imitation of the **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

The domain '**djibdiplomatie[.]com**' appeared to masquerade Djibouti diplomacy services, which had a similar WHOIS record to '**utdglobals[.]com**'**.** One record appeared to show the registrant '**ocean.nio@rediffmail[.]com**' and admin ‘**taoyujun@gmail[.]com**’ whereas other records showed ‘**wangminghua6@gmail[.]com**’ as the admin email address with ‘**ocean.nio@rediffmail[.]com**’ as the registrant email.

Both these domains also had keyboard walking type values in the WHOIS records. For example, ‘**udtglobals[.]com**’ has the value ‘**ASDF**’ as its registrant city and ‘**djibdiplomatie[.]com**’ has ‘**DAF DAGF**’ as its registrant name value. This is comparable to the values observed in other BADBAZAAR domains.

Although the email addresses ‘**wangminghua6@gmail[.]com**’ and ‘**taoyujun@gmail[.]com**’ are found in WHOIS records for domains masquerading as a **global undersea defence event**, **Djibouti diplomacy services** and the **International Atomic Energy Agency**, they are also in WHOIS records for numerous non-malicious domains.

The mix of masquerading domains and non-malicious domains could suggest the existence of an infrastructure-procuring entity used to support the malicious cyber actors' operations.

The email address ‘**ocean.nio@rediffmail[.]com**’ is only found in the masquerading domains described above. ‘**ivan_s81@mail[.]ru**’ and ‘**tplutalova@list[.]ru**’ have registered a very small number of domains respectively, and some of these domains have been hosted on BADBAZAAR infrastructure. These three email addresses are believed to be more closely linked to the malicious cyber actors' operations. This is because a higher number of domains they are associated with are linked to malicious activity, in comparison to emails ‘**wangminghua6@gmail[.]com**’ and ‘**taoyujun@gmail[.]com**’.

(See Annex A, image 5)

Links to other threat actors

Another common characteristic of the BADBAZAAR-linked domains ‘**actuallys[.]com**’, ‘**clublogs[.]com**’, ‘**myloughborough[.]com**’, ‘**rewrwer[.]com**’, and ‘**voiceoftibet[.]net**’ is that they were all registered with eNom and had been ‘parked’ at ‘**255.255.255[.]254**’.

Following previous NCSC investigations, other domains with these characteristics revealed activity linked to **APT5** in 2019, and **APT14** between 2009 and 2011.

The APT5-linked domains had historical WHOIS records which listed '**taoyujun@gmail[.]com**' as the registrant email address.

The APT14-linked domains had three-letter subdomains which appeared to represent the intended target of their malicious operations. An example of this is '**bae.cisconline[.]net**', which suggested intended targeting of BAE Systems and was found in a '**Poison Ivy**' sample.

A similar characteristic is observed in BADBAZAAR domains where the subdomains relate to the name of the 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

It is important to note that the activities related to APT5 and APT14 were historical and there were also other domains registered with eNom and resolved to '**255.255.255.254**' which cannot be linked to malicious activity. It is therefore not certain that the actors behind these campaigns are the same or related.

Machine Names

Analysis of BADBAZAAR C2s and samples revealed hostnames used as the 'Common Name' value in SSL certificates. NCSC investigations into hostnames observed in BADBAZAAR samples and infrastructure showed that these hostnames are used across multiple IP addresses. These IP addresses are hosting domains found in BADBAZAAR samples. There is more detail in the section below about the hostnames, and IP addresses with the hostname hosting BADBAZAAR C2 domains.

In almost all cases the presence of certificates with the hostname value overlaps with IP resolutions for the malicious domain names specified, the few instances where this was not the case have been outlined.

WIN-EU0VLBL7TUJ

Hostname ‘**WIN-EU0VLBL7TUJ**’ was observed on the following IP addresses of interest:

- ‘**116.203.53[.]21**’ hosted BADBAZAAR C2 domains ‘**uyapkfinder[.]com**’ and ‘**thewestuniverse[.]com**’.

- ‘**95.216.169[.]27**’ hosted BADBAZAAR C2 domains ‘**adysfunction[.]com’** and sub-domain ‘**download.apkbazar[.]biz**’ observed as a download link for a BADBAZAAR sample.

(See Annex A, image 6)

WIN-70E59JVOB9G

Hostname ‘**WIN-70E59JVOB9G**’ was observed on the following IP addresses of interest:

- ‘**23.88.28[.]220**’ hosted BADBAZAAR C2 sub-domains, **‘aua.rondwsign[.]com’**, **‘nal.tokenmajorp[.]com’**, **‘pep.rondwsign[.]com’** ‘**doa.rondwsign[.]com**’, and **‘pls.rondwsign[.]com’.** There was a period of two days between when the certificate with the machine was last seen, and when the malicious domains were first seen resolving to the IP.

- ‘**23.88.28[.]221**’ hosted BADBAZAAR linked sub-domain ‘**bt.bhvghg[.]com**’.

- **‘23.88.28[.]222**’ hosted BADBAZAAR C2 domains ‘**tubevideoplus[.]org**’ and ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67**’ hosted BADBAZAAR C2 sub-domain ‘**bat.androidupdated[.]net**’. It also hosted sub-domain ‘**apps.androidupdated[.]net**’ which is a DoubleAgent malware C2.

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

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

- '**142.132.131[.]15**' hosted BADBAZAAR C2 sub-domains '**bvn.lookincategory[.]com'** and '**edr.lookincategory[.]com'.** There was a period of eleven days between when the certificate with the machine name was last seen, and when the malicious domains were first seen resolving to the IP.

- **'142.132.131[.]20'** hosted sub-domains '**son.onlinegamersgroup[.]com'** and '**system.onlinegamersgroup[.]com'**, believed to be BADBAZAAR C2s as they were hosted whilst BADBAZAAR associated SSL certificates were observed on the IP.

- '**142.132.131[.]28'** hosted BADBAZAAR C2 domain '**goldplusapp[.]net**' and sub-domains '**who.goldplusapp[.]net**' and '**cgf.goldplusapp[.]net**'.

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

- '**162.55.103[.]212**' hosted BADBAZAAR C2 sub-domains **'pep.rondwsign[.]com', 'ckp.jkiohreh[.]com', 'aar.tokenmajorp[.]com', 'nal.tokenmajorp[.]com', 'pls.rondwsign[.]com'** and **'aua.rondwsign[.]com'.**

- '**195.154.47[.]99**' hosted BADBAZAAR C2 sub-domains '**ggl.whoscaller[.]net**' and '**upd.whoscaller.net**'. There was a period of three days between when the certificate with the machine name was first seen and when the malicious domains were last seen resolving to the IP.

- '**195.154.60[.]3**' hosted BADBAZAAR C2 sub-domains '**upd.whoscaller[.]net**' '**ggl.whoscaller[.]net**'.

- '**212.83.189[.]89**' hosted BADBAZAAR C2 sub-domains '**wyo.titeperformance[.]com**', '**eud.titeperformance[.]com**', '**vpf.titeperformance[.]com**' and '**afg.collinformations[.]com**'.

- '**212.129.21[.]168**' hosted BADBAZAAR C2 domains, '**fre.lookincategory[.]com**', '**tgr.lookincategory[.]com**', '**fgt.lookincategory[.]com**' '**luj.lookincategory[.]com**' and '**bvn.lookincategory[.]com**'.

(See Annex A, image 7)

WIN-50QO3EIRQVP

Hostname '**WIN-50QO3EIRQVP**' was observed on the following IP addresses of interest:

- '**45.76.132[.]91**' hosted domains, '**yumoftion[.]com**', '**androidupdated[.]net**'. Both domains are linked to BADBAZAAR as subdomains '**fow.yumoftion[.]com**' and '**bat.androidupdated[.]net**' are BADBAZAAR C2 domains. Additionally sub-domain '**apps.androidupdated[.]net**' is a DoubleAgent C2 domain. It also hosts domain '**pmstwocqn[.]com**', linked to BADBAZAAR through WHOIS records.

- '**95.179.210[.]85**' hosted '**clublogs[.]com**', of which '**xle.clublogs[.]com**' is a BADBAZAAR C2 domain and also hosted BADBAZAAR linked domains '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**'www.voiceoftibet[.]net**' and '**actuallys[.]com**'.

- '**199.247.21[.]34**' hosted '**titeperformance[.]com**', and '**collinformations[.]com'** of which subdomains are BADBAZAAR C2 domains.

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

(See Annex A, image 8)

WMSvc-WIN-50QO3EIRQVP

Hostname ‘**WMSvc-WIN-50QO3EIRQVP**’ was observed on the following IP addresses of interest:

- **’78.46.185[.]251’** hosted BADBAZAAR C2 domain **‘groupgram[.]org’**, reported by Volexity to be using port 4432 for malicious connections.
- **‘65.21.92[.]69’** and **‘163.172.205[.]207’** hosted domain **‘widelygram[.]org’** which is believed to be a BADBAZAAR C2 domain, as whilst being hosted on both IPs, port 4432 was open.
- **‘163.172.198[.]206’** hosted domain **‘maxgram[.]org’** which is believed to be a BADBAZAAR C2 domain, as whilst it was being hosted port 4432 was open.

(See Annex A, image 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Hostnames ‘**WMSvc-WIN-50QO3EIRQVP**’ and ‘**WIN-7LSBB9R0F1L**’ were observed on the following IP address simultaneously:

- ‘**148.251.87[.]245**’ hosted BADBAZAAR C2 domains ‘**flygram[.]org**’ and ‘**groupgram[.]org**’.

(See Annex A, image 10)

WIN-N8H8S9BG2P0

Hostnames ‘**WIN-N8H8S9BG2P0**’ was observed on the following IP address:

- ‘**148.251.87[.]247**’ hosted BADBAZAAR C2 domains ‘**omarwhatsapp[.]org**’ and ‘**flygram[.]org**’.

(See Annex A, image 11)

WIN-I6VBN8MR92A

Hostnames '**WIN-I6VBN8MR92A**' was observed on the following IP address:

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

(See Annex A, image 12)

Based on available commercial data the prevalence of these machine names across the internet varies. Some of them are observed simultaneously across multiple IP addresses which indicates VMs being created from the same template. It's important to note that for some of the hostnames, not all of the IPs on which they were observed can be linked to malicious activity. This could mean that use of the hostnames is not exclusive to these threat actors.

However, the prevalence of some of these machine names across IPs which have hosted BADBAZAAR C2 domains, could suggest that an infrastructure-procuring entity is being used to configure machines to support the malicious actors' cyber operations.

Social media presence

Previous reporting by Volexity showed that YouTube videos (promoting the use of the malicious applications) were created by the malicious cyber actors. These videos included tutorials on how to use the applications developed.

The NCSC has discovered two additional YouTube channels associated with the threat actors' operations. The YouTube channel with URL handle '**@josephjoey3499**' appeared to be promoting the use of '**Maxgram**' and an additional channel registered with '**@uyghurapks3096**' promotes '**Uyghur APK Finder**'.

Additionally, YouTube videos promoting '**Flygram**' and '**Signal Plus**', showed the threat actors using visible phone numbers. In the '**Flygram**' video, at 0:36 phone number '**+1 (570) 378-7250**' is visible and during the '**Signal Plus**' video, the phone number '**+1 (267) 298 4259**' is revealed.

Volexity reported a fake Tibet-themed news site '**ignitetibet[.]net**', which they discover in Telegram channels believed to be operated by the threat actors. Email address '**choekyi.wangmo@ignitetibet[.]net**' is observed leaving comments on posts on the page '**tibetone.org**' which has been publicly reported by Lookout as a C2 page used for the iOS variant of BADBAZAAR.

This email address is believed to be actor-controlled, using the persona of '**Choekyi Wangmo**'.

Assessment

BADBAZAAR and MOONSHINE use several social engineering methods to specifically target Uyghur, Tibetan and Taiwanese communities, namely:

- the trojanisation of apps of interest to these communities, such as a Uyghur language Quran app, is almost certainly tailored to the target victim base
- the adding of these trojanised apps to official app stores highly likely lends a sense of legitimacy, and the sharing in group chats is highly likely intended to exploit trusted relationships within these communities

BADBAZAAR and MOONSHINE collect data which would almost certainly be of value to the Chinese state. Although BADBAZAAR and MOONSHINE have been observed targeting Uyghur, Tibetan and Taiwanese individuals, there are other malwares that target other minority groups in China. Citizens from the co-sealing nations, in China and abroad, who are perceived to be supporting causes that threaten regime stability, are almost certainly under threat from mobile malware such as BADBAZAAR and MOONSHINE. The capability to capture location, audio and photo data almost certainly provides the opportunity to inform future surveillance and harassment operations by providing real-time information on the target's activity.

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Reconnaissance	T1593.001	Search Open Websites/Domains: Social Media	Actors find online groups and forums matching their intended victims to share the malware
Resource Development	T1583.001	Acquire Infrastructure: Domains	Actors register domains for their command and control servers
Resource Development	T1587.001	Develop Capabilities: Malware	Malicious code is written for insertion into trojanised apps
Resource Development	T1608.001	Stage Capabilities: Upload Malware	Trojanised apps are uploaded to online platforms including app stores
Resource Development	T1585.001	Establish Accounts: Social Media Accounts	Actors create accounts on websites and social media to share and advertise the malware
Resource Development	T1585.002	Establish Accounts: Email Accounts	Actors use privately hosted and commercial email accounts for hosting and sharing of malware
Initial Access	T1189	Drive-by Compromise	Malicious scripts are hidden in otherwise legitimate apps and uploaded to app stores
Initial Access	T1566.003	Phishing: Spearphishing via Service	Actors send trojanised apps to targeted groups via social media including Telegram
Execution	T1204.002	User Execution: Malicious File	Victims have to install the trojanised apps to execute the payload
Defense Evasion	T1027.009	Obfuscated Files or Information: Embedded Payloads	The malicious payload is hidden within otherwise legitimate apps

Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	Trojanised files match the name, appearance and function of legitimate apps.
Defense Evasion	T1656	Impersonation	Actors impersonate trusted individuals by creating cover websites and using usernames associated with target groups
Collection	T1123	Audio Capture	The trojanised apps may request unnecessary permissions including microphone access
Collection	T1125	Video Capture	The trojanised apps may request unnecessary permissions including camera access
Collection	T1005	Data from Local System	The trojanised apps may request unnecessary permissions including local files.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	Malware connects to C2 using HTTPS and WebSocket's.
Command and Control	T1509	Non-Standard Port	Nonstandard ports are used such as port 4432 and 2333
Exfiltration	T1041	Exfiltration Over C2 Channel	Malware exfiltrates data using HTTPS and WebSocket connections.

Indicators

MOONSHINE:

- On 1st April 2025, a search for VLiteUI panels returned the following:

IP Address	Port	First Seen	Last Seen
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

- On 1st April 2025, a search for SCOTCH ADMIN panels returned the following:

IP Address	Port	First Seen	Last Seen
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

- On 14th March 2024, a search for virtual SCOTCH ADMIN panels returned the following:

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:

Description	SSL certificate observed on BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85 b4a6a0b9f7

- On 1st April 2025, a search for the above BADBAZAAR certificate returned the following:

IP Address	Port	First Seen	Last Seen
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

Description	SSL certificate observed on BADBAZAAR C2s
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- On 1st April 2025, a search for the above BADBAZAAR certificate returned the following:

IP Address	Port	First Seen	Last Seen
162.55.103[.]211	20122	2023-01-12	2025-03-28
162.55.103[.]212	20121	2022-06-30	2025-03-28
162.55.103[.]212	20122	2023-07-14	2025-03-28
162.55.103[.]211	20121	2022-06-03	2025-03-28
162.55.103[.]211	20123	2023-07-22	2025-03-27
162.55.103[.]212	20123	2023-07-22	2025-03-27
212.83.162[.]152	9090	2022-10-13	2025-03-27
23.88.28[.]221	20422	2023-07-28	2023-09-30
23.88.28[.]221	20421	2023-05-18	2023-09-28
23.88.28[.]221	20423	2023-07-28	2023-09-28

162.55.103[.]210	20121	2022-09-30	2023-02-23
65.21.92[.]67	20121	2021-11-02	2022-10-13
65.21.92[.]67	20122	2022-08-10	2022-10-13
23.88.28[.]220	20121	2021-12-08	2022-05-13
94.130.92[.]230	20121	2021-01-04	2021-10-05
88.99.150[.]246	20121	2021-04-06	2021-09-08
45.76.132[.]91	20121	2021-02-02	2021-03-01

- WHOIS domains

Below is a table of domains which currently or historically have WHOIS records with values that match those observed in BADBAZAAR C2 domains.

WHOIS Value	Domains
Registrant State: UJYJYUJ **Registrant Country: BO** **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
Registrant State: REWR **Registrant Country: CF** **Registrar: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

Registrant State: FSDF **Registrant Country: 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

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

The following are links to other indicators of compromise (IoCs) associated with BADBAZAAR and MOONSHINE. The NCSC cannot confirm the validity of all the information in these links and readers are advised to independently verify their accuracy and relevance:

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

Mitigation

The NCSC encourages adoption of the recommendations below to defend against the threats described in the case studies.

- **App store operators, including third party app stores, and developers should ensure that the apps on their platform are secure and that they comply with the governmental Code of Practice.** See Guidance: 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

- **Multi-language support**: App developers should invest in efforts to localise popular apps for users who speak minority languages among targeted groups including Uyghur, Tibetic, Taiwanese Hokkien and Cantonese. Apple guidance for localising in apps: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Google guidance on translating apps: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Keeping your social media platform secure:** Social media companies can make it more difficult for malicious cyber actors to create bogus accounts and share malicious files or links on their platforms in otherwise legitimate online communities. Where possible, companies should share malicious indicators with wider industry to improve collective understanding of the threat and to help protection measures.

- **Remediation plan for customers:** Organisations should have procedures in place to notify customers who have installed malicious apps using their services. These alerts should be attention grabbing and informative. Where appropriate, organisations should provide guidance on how to remove the software and encourage victims to report to their authorities, such as the NCSC In the UK.

See the App Store Code of Practice for more information: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Working groups for collaboration:** Social media companies can form working groups, allowing their respective security teams to share malicious indicators, TTPs and observations, making it more difficult for actors to use their platforms to support malicious campaigns.

- **Detecting altered apps:** Where possible, app developers should include functionality that informs the user if they have downloaded an 'unofficial' version of an app, to help protect against malicious copies.

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

Image 1 - ‘UKYJYUJ’

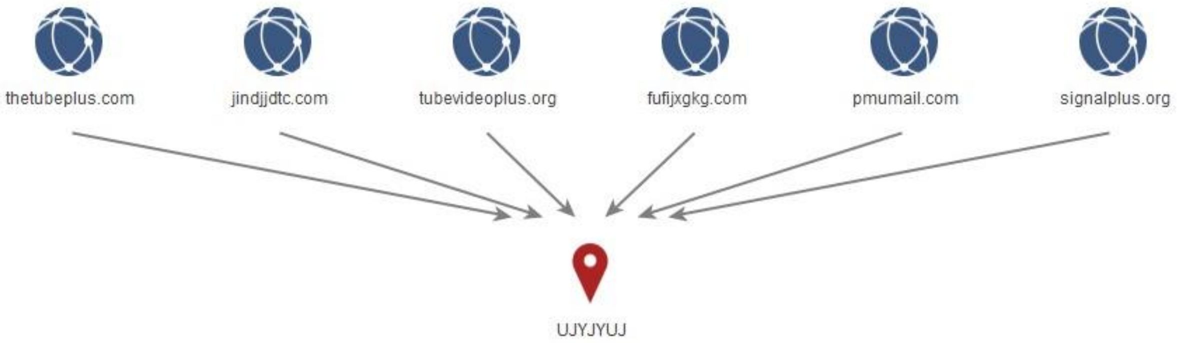


Image 2 – Keyboard walking values

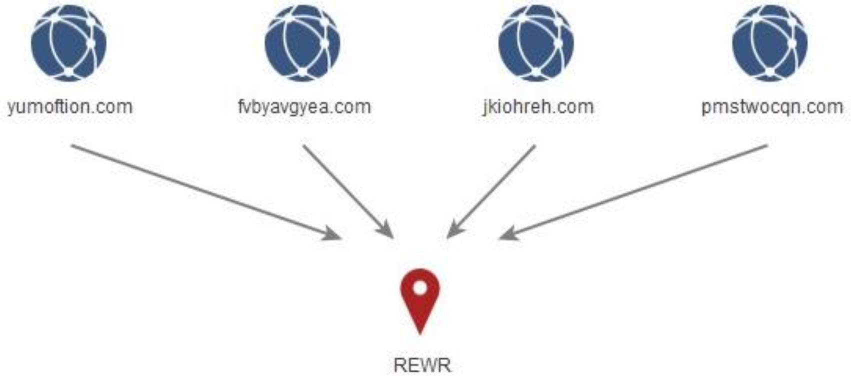


Image 3 – Additional domains with ‘FSDF’ state field values

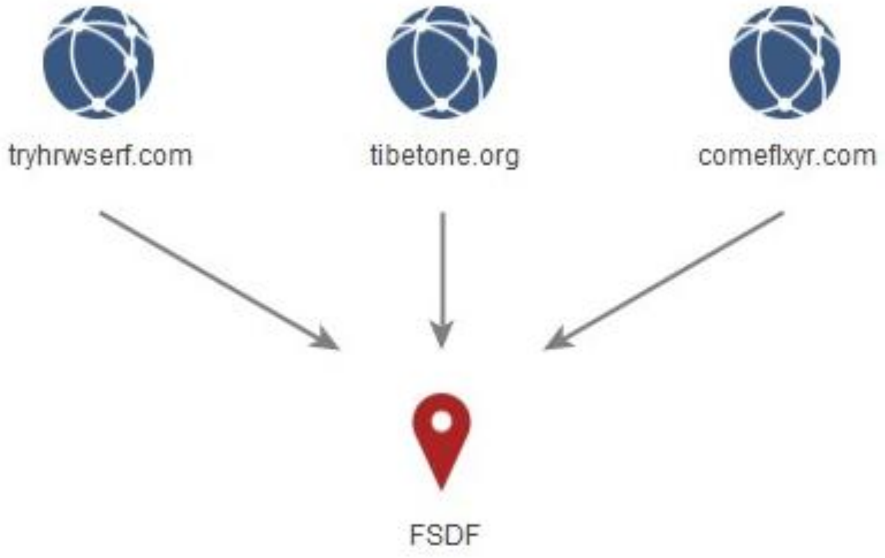


Image 4 – **95.179.210[.]85**

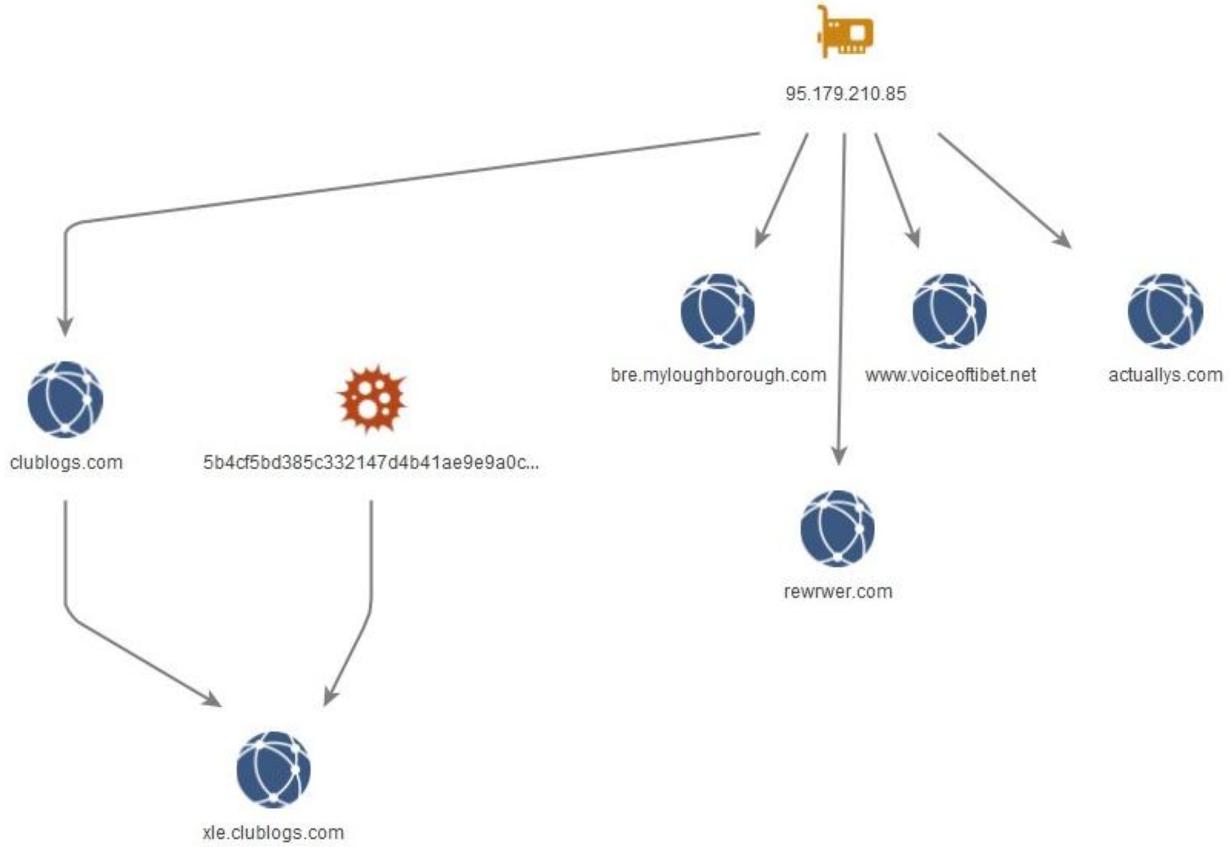


Image 5 – WHOIS links

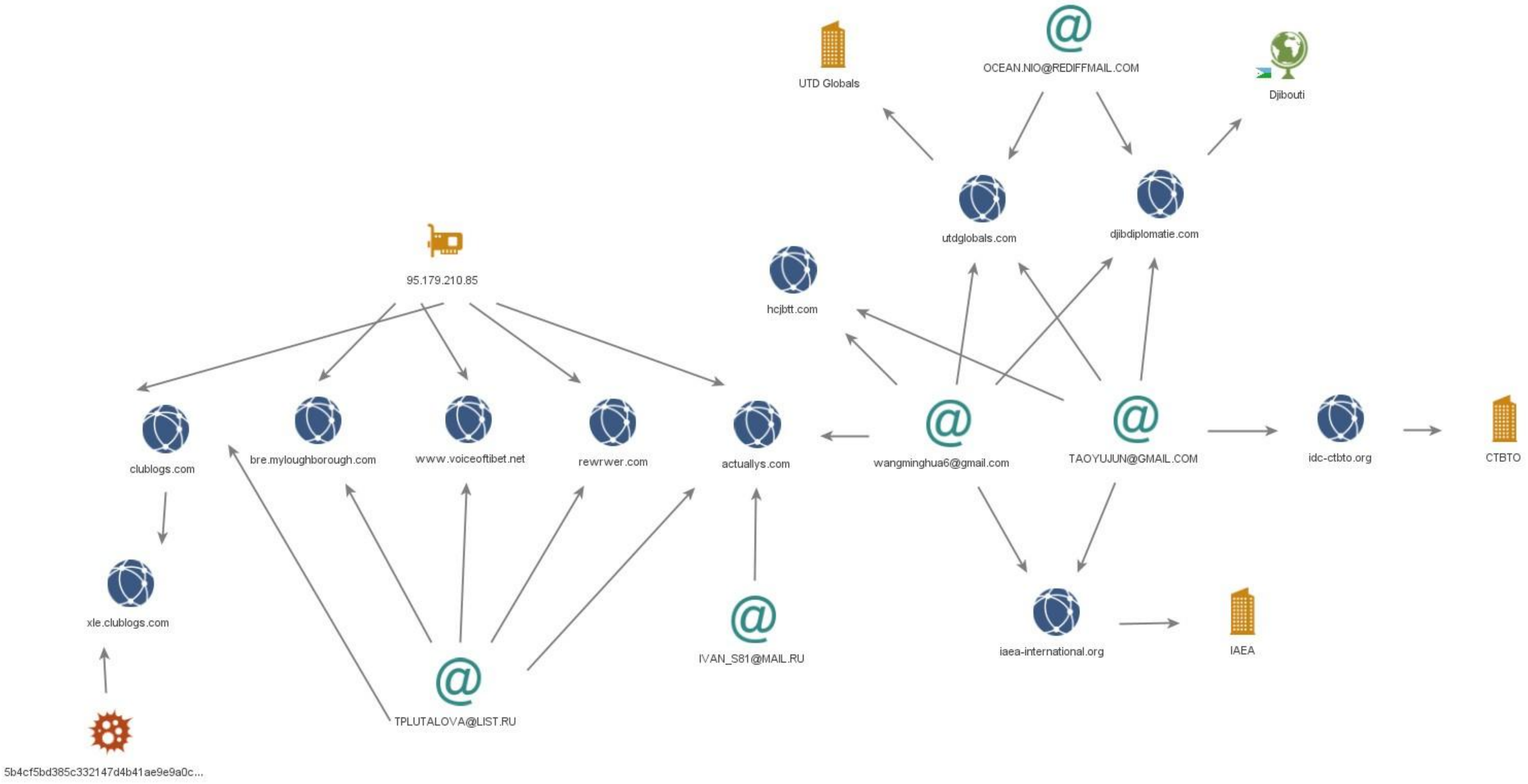


Image 6 – **WIN-EU0VLBL7TUJ**

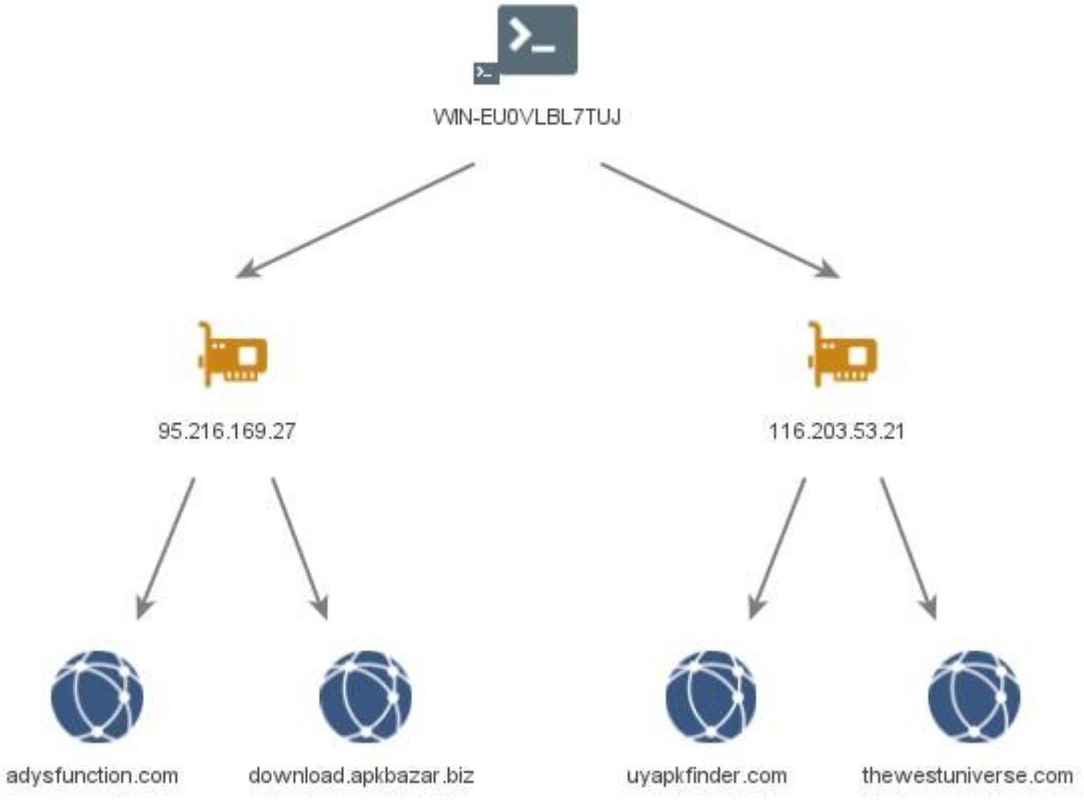


Image 7 – **WIN-70E59JVOB9G**

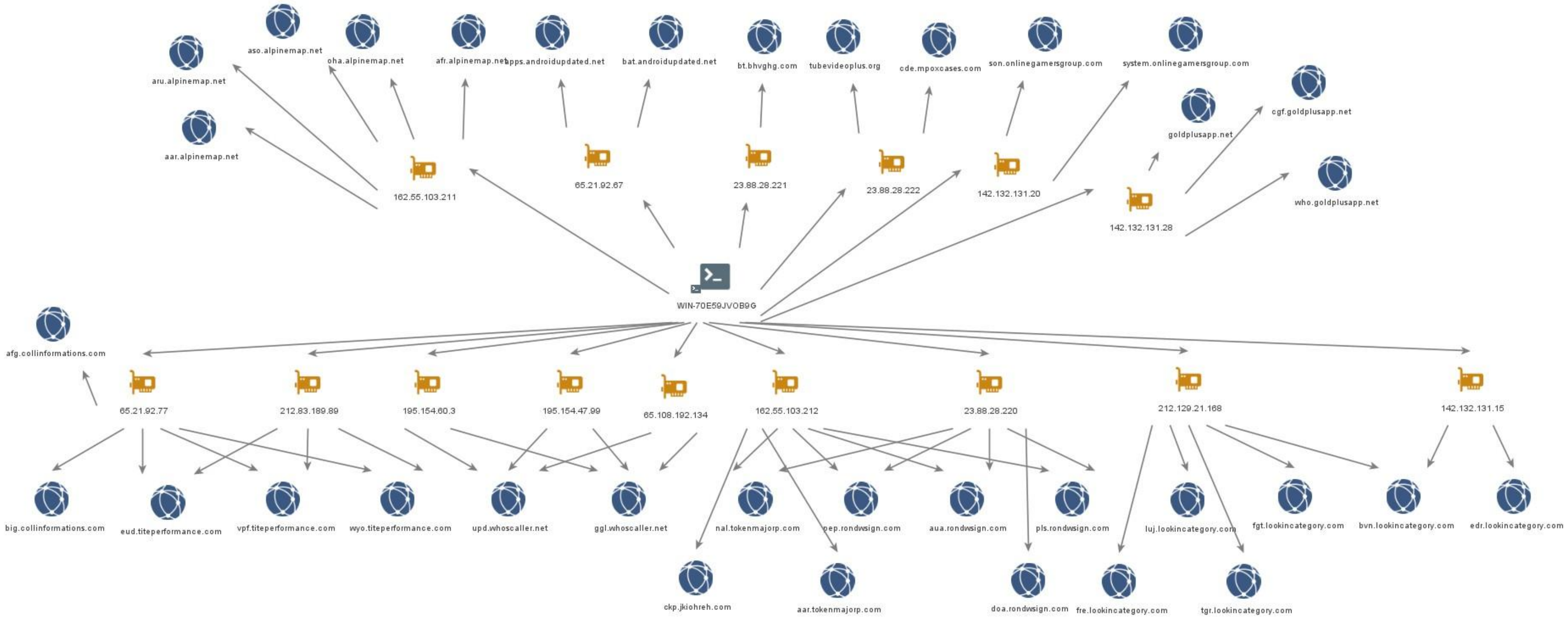


Image 8 - **WIN-50QO3EIRQVP**

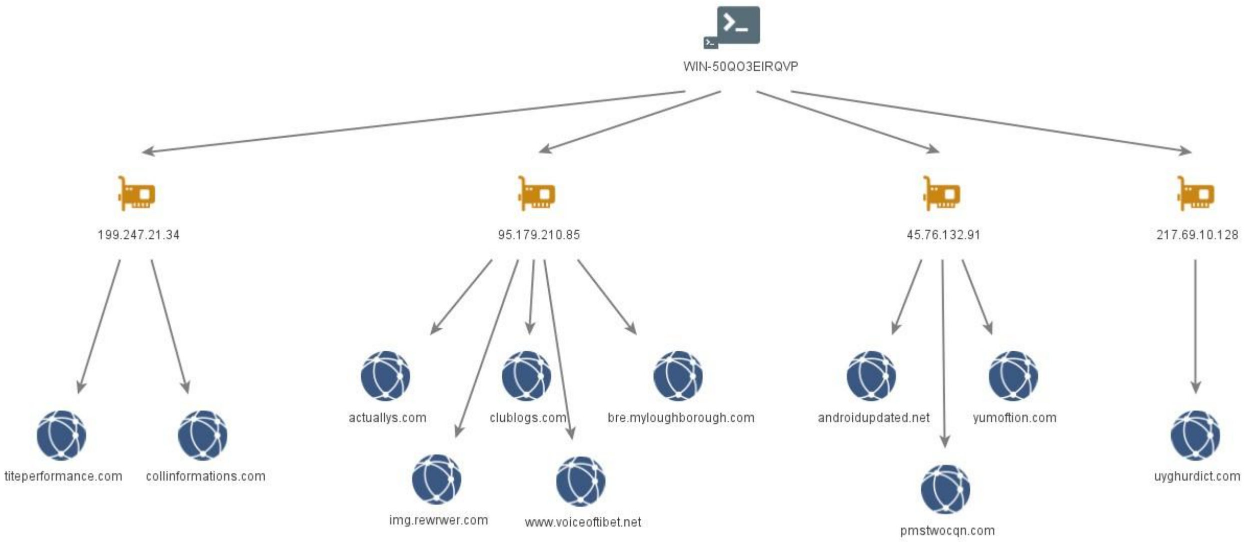


Image 9 - **VMSvc-WIN-50QO3EIRQVP**

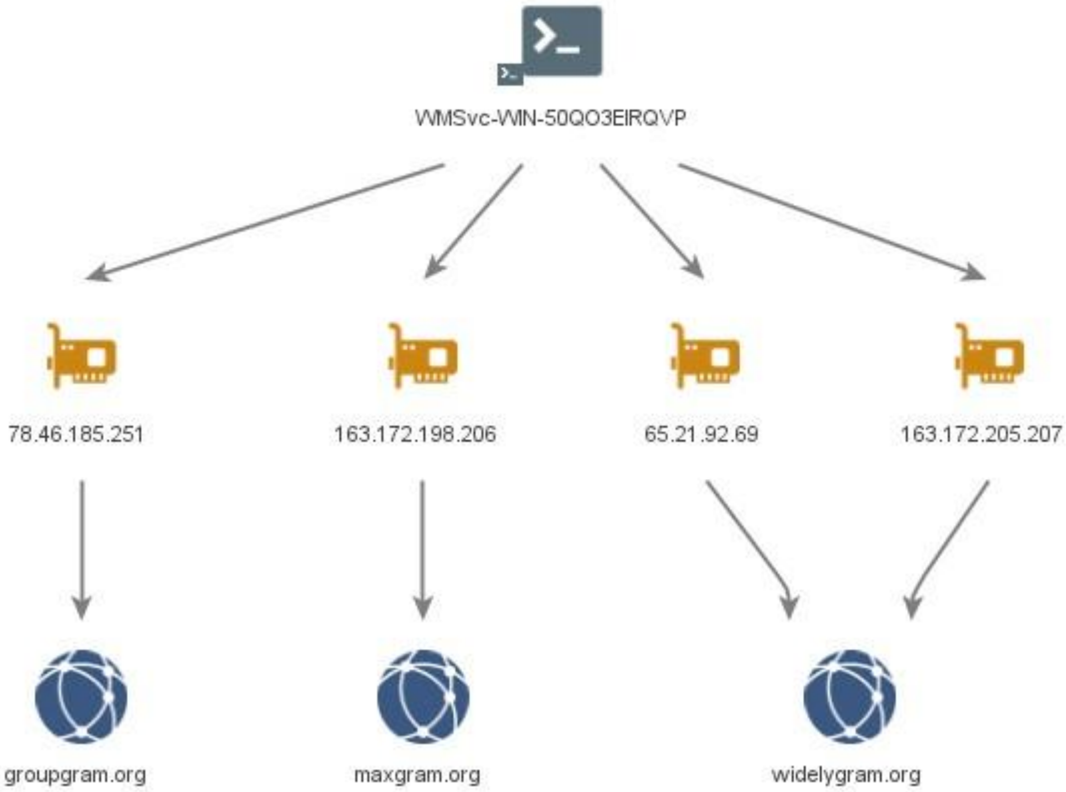


Image 10 – **VMSvc-WIN-50QO3EIRQVP** and **WIN-7LSBB9R0F1L**

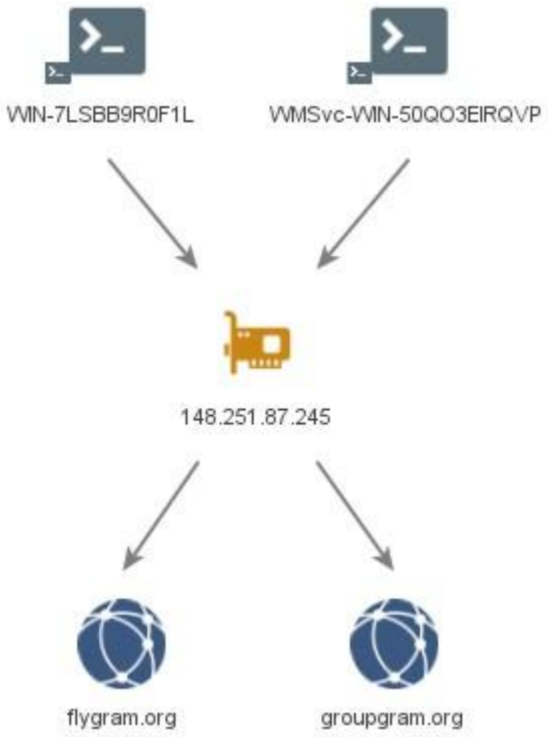


Image 11 - **WIN-N8H8S9BG2P0**

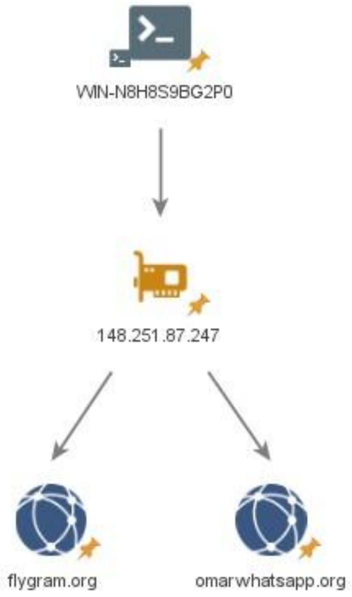
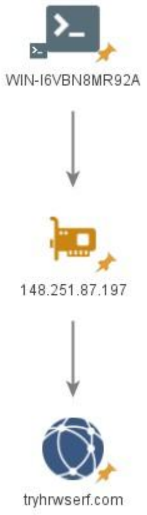


Image 12 – **WIN-I6VBN8MR92A**

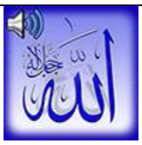
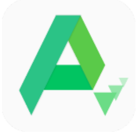
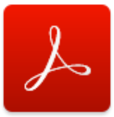
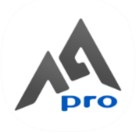
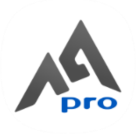
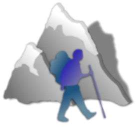


Appendix B: MOONSHINE & BADBAZAAR samples observed

The table below lists the apps used in MOONSHINE and BADBAZAAR campaigns in the past two years.

Many of these apps show a clear similarity to established apps. This is likely to be a deliberate actor technique to 'spoof' well-known brands.

It's important to note, the app title, package name, and app icon can all imitate or match the real application and should therefore not be used exclusively to identify if a device is infected.

App title	Package name	App icon
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	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	

FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	F
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	هجري
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

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

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	VPN 2023
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	UYGHUR KEYBOARD
Uyghurche Kirguzguch	com.ziipin.softkeyboard	ئۇ Tr
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	LITE
VivaVideo PRO	com.quvideo.xiaoying.pro	PRO
Vmuslim	com.alhiwar	
Voice Recorder	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast	com.graph.weather.forecast.channel	Paris 15:30 Feels:37° 35° 39° 28° Cloudy TUE WED THU FRI 36° 30° 33° 32°
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	

WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	whos call
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	Awazliq Eserler
ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	ع ئۇ
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	APK
ئۇيغۇرچە قۇرئان	com.c9.uyghurquran	قۇرئان
القرآن الكريم	com.maher4web.quran	القرآن الكريم
زىكىرلەر	com.my.newproject5	حصن المسلم
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	ك K
نۇر كىرگۈزگۈچ	com.nur.ime	ئۇ
《心灵法门》念佛机	com.guanyincitta.chant	卍

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

Further reading

Guidance from the Australian Cyber Security Centre

- Report a cybercrime, incident or vulnerability
- How to secure your devices
- Secure your mobile phone
- Phishing
- Scams
- Secure your social media
- Security tips for social media and messaging apps

Guidance from the UK NCSC and NPSA

- Defending Democracy
- Social Media: how to use it safely
- Device Security Guidance for organisations including mobile
- Threat report on application stores.
- Personal safety and security for high-risk individuals

Guidance from the US NSA

- Mobile Device Best Practices

Disclaimer

Please note that this advisory provides information that is validated at the time of publication.

This report draws on information derived from authoring agency and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

In the UK, this information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©