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

Avis

BADBAZAAR et MOONSHINE : Analyse technique et mesures d'atténuation

9 avril 2025

BADBAZAAR et MOONSHINE : Analyse technique et mesures d'atténuation

Résumé

Avec le soutien de la Cyber League britannique, cet avis a été rédigé conjointement par le Centre national de cybersécurité (NCSC UK) et des partenaires internationaux :

- **Le Centre Australien de Cybersécurité, qui fait partie de la Direction Australienne des Signaux**
- **Le Centre Canadien pour la Cybersécurité, qui fait partie du Centre de la Sécurité des Télécommunications**
- **Le Service Fédéral Allemand du Renseignement**
- **L'Office Fédéral Allemand pour la Protection de la Constitution**
- **Le Centre National de Cybersécurité de Nouvelle-Zélande, qui fait partie du Bureau de la Sécurité des Télécommunications du Gouvernement**
- **Le Bureau Fédéral d'enquête des États-Unis**
- **L'Agence Nationale de Sécurité des États-Unis**

Cet avis fournit des informations récentes et compilées sur les menaces concernant deux variantes de logiciels espions, BADBAZAAR et MOONSHINE, et propose des conseils aux opérateurs de boutiques d'applications, aux développeurs et aux réseaux sociaux pour assurer la sécurité de leurs utilisateurs.

Cet avis est publié parallèlement à un avis destiné aux victimes de ces logiciels malveillants.

Ce document utilise la définition du glossaire du NCSC pour les logiciels espions: 'Un type de logiciel malveillant qui s'installe sur un appareil sans le consentement de l'utilisateur, collecte des données et les transmet à un tiers.'

Étude de cas n° 1 : MOONSHINE

MOONSHINE est un logiciel espion Android signalé en 2019 par Citizen Lab comme ciblant des groupes tibétains. MOONSHINE se fait passer pour une application légitime afin d'inciter ses victimes à l'installer. Il a été partagé sur des chaînes Telegram et via des liens envoyés via WhatsApp.

Les recherches du NCSC sur MOONSHINE indiquent ce qui suit :

- MOONSHINE utilise une interface de gestion qui a subi des modifications depuis son premier signalement.
- Cette interface de gestion révèle des capacités de surveillance étendues, notamment la possibilité d'exfiltrer des fichiers des appareils, ainsi que de capturer des enregistrements audio et d'écran en direct.
- Un ensemble d'interfaces de gestion MOONSHINE hébergées virtuellement a été découvert. Ces interfaces présentent un chevauchement d'infrastructure avec les panneaux de connexion associés à UPSEC, qui, selon Intelligence Online, désigne 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Interface de gestion

De précédents rapports sur les interfaces de gestion de MOONSHINE indiquent que le système a subi des modifications, ce qui suggère un développement continu.

Le premier exemple d'interface de gestion figure dans le rapport de Citizen Lab de 2019.

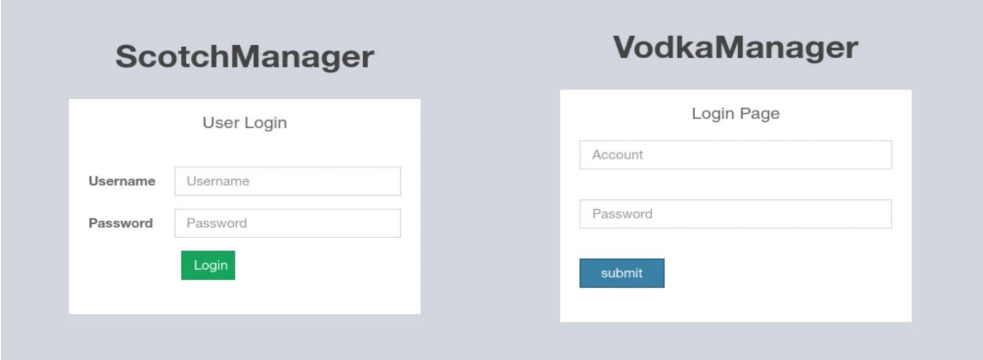


Figure 1 : Interfaces de gestion de MOONSHINE présentées dans le rapport de Citizen Lab de 2019 intitulé 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'.

Au début 2022, Lookout a signalé une interface de gestion différente, repensée pour ressembler à celle présentée ci-dessous (remplaçant les interfaces précédentes de la figure 1) :

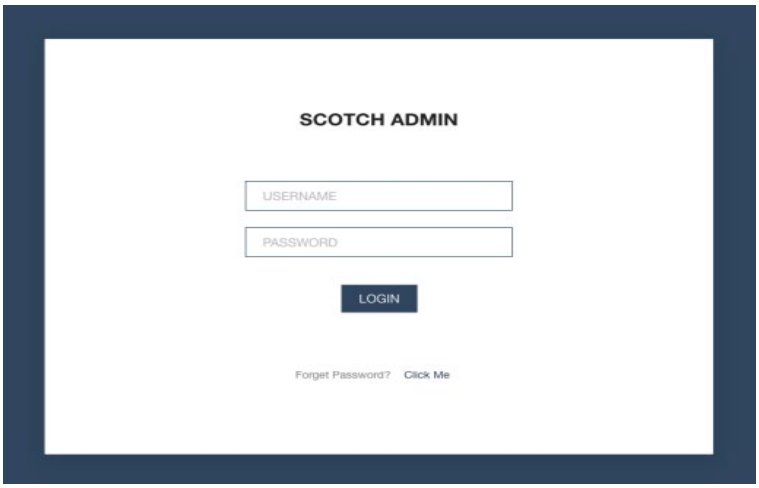


Figure 2 : L'interface de gestion de MOONSHINE présentée dans le rapport de Lookout de 2022 () 'MOONSHINE : Évolution du logiciel de surveillance Android par le système d'alerte avancé chinois POISON CARP visant les Tibétains et les Ouïghours'.

En août 2023, un scan du commandement et du contrôle (C2) de MOONSHINE a révélé une interface similaire à l'interface de 2022 avec la fonction '**Mot de passe oublié**' qui n'est plus disponible comme dans la figure 2 :

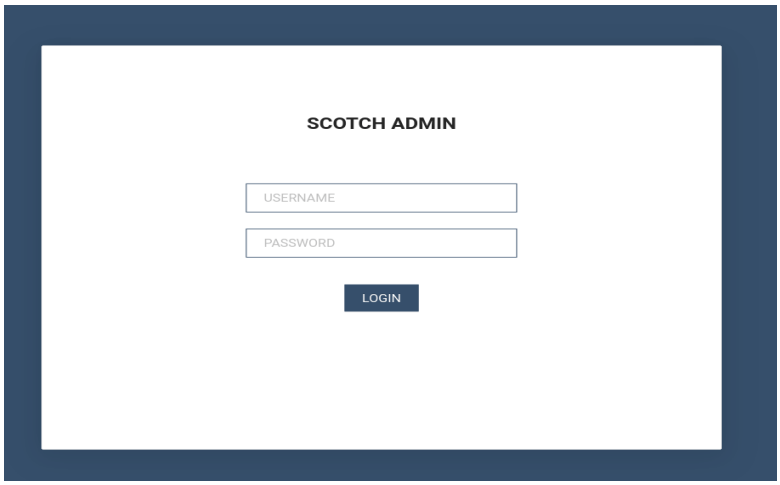


Figure 3 : L'interface de gestion de MOONSHINE a été observée en août 2023 et ne comporte plus d'invite ' Mot de passe oublié '.

Une analyse plus approfondie de l'interface de gestion a révélé le contenu du panneau révélant comment les informations des appareils compromis étaient stockées.

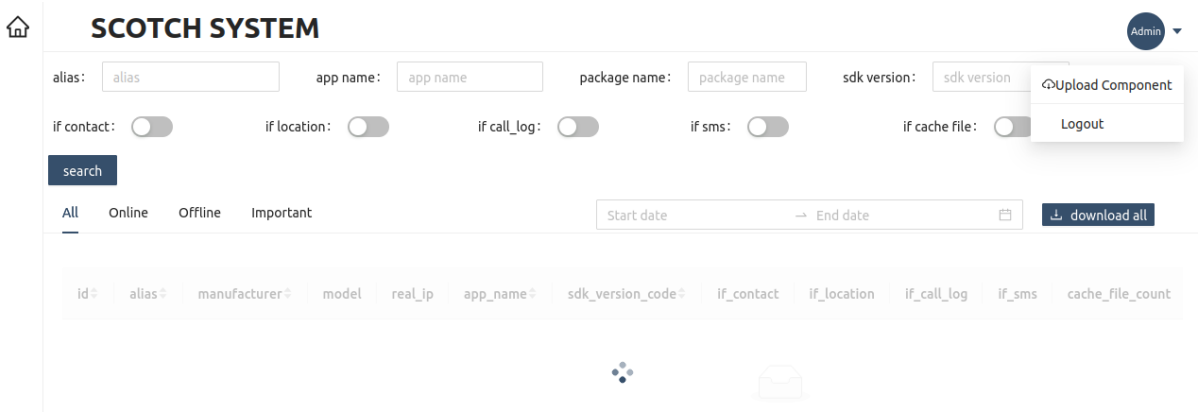


Figure 4 : Page web derrière la page de connexion de l'interface de gestion de MOONSHINE.

Une étude de Lookout a montré la transmission d'un **'score'** de l'appareil victime aux serveurs C2 de MOONSHINE. La valeur du 'score' est basée sur les autorisations de l'échantillon malveillant sur l'appareil victime.

Les colonnes 'if_contact', 'if_location , 'if_call_log' et 'if_sms' de la page suggèrent que tous les échantillons MOONSHINE n'ont pas un accès complet aux appareils compromis. La connaissance de ces colonnes et du score transmis de l'appareil au C2 suggère que les acteurs malveillants utilisent ce score pour communiquer le niveau d'accès du logiciel malveillant à l'appareil compromis aux personnes accédant à l'interface de gestion.

En général, pour empêcher les applications de collecter des informations sur les appareils, il est conseillé d'inspecter les autorisations des applications avant de les télécharger. Cependant, les échantillons MOONSHINE recherchent des autorisations pertinentes pour le fonctionnement de l'application et peuvent donc paraître anodins, mais ils les utilisent également pour collecter des informations sur les appareils.

MOONSHINE dispose également d'une interface de programmation d'applications (API) révélant l'étendue de ses capacités. Les premières versions de la documentation de l'API contenaient des noms d'API en mandarin.

Hôtes virtuels

Lors de la recherche de panneaux MOONSHINE, des instances hébergées virtuellement ont été découvertes. L'hébergement virtuel est une solution permettant d'héberger simultanément plusieurs sites web à partir d'une seule adresse IP. Les adresses IP de ces instances virtuelles et domaines hébergés n'ont été observés dans aucun échantillon de logiciels malveillants connus.

L'interface de gestion de ces instances différait, car le titre des pages était '**LOGIN**' au lieu de '**SCOTCH ADMIN**' précédemment utilisé.

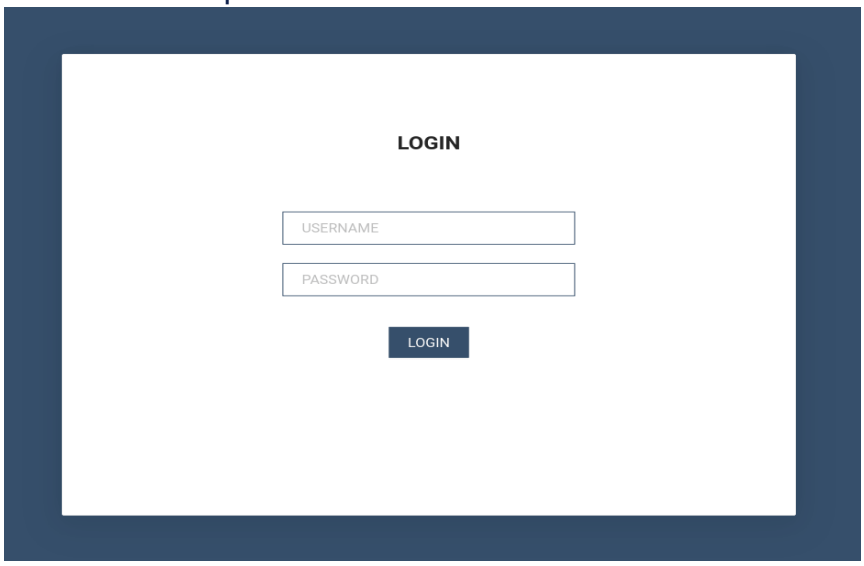


Figure 3 : Interface de gestion de MOONSHINE utilisant le titre ' LOGIN ' au lieu de ' SCOTCH ADMIN '.

De plus, le contenu du panneau diffère également de la figure 4, comme illustré à la figure 6 :

Figure 6 : Page web derrière la page de connexion de l'interface de gestion MOONSHINE hébergée virtuellement.

Le panneau de la figure 6 semble être une version simplifiée de celui de la figure 4. Les caractéristiques communes des panneaux sont les noms de colonnes 'id', 'manufacturer' et 'model' dans le tableau.

Les instances MOONSHINE hébergées virtuellement découvertes étaient :

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

Ces domaines sont répertoriés par Trend Micro comme des kits d'exploitation MOONSHINE, responsables de l'exploitation des vulnérabilités des navigateurs pour installer des logiciels malveillants sur les appareils mobiles. Trend Micro nomme ce logiciel malveillant 'Dark Nimbus'.

Pour plus de clarté, les échantillons de logiciels malveillants MOONSHINE communiquent avec les interfaces de gestion de MOONSHINE et vers lesquelles les données des victimes sont exfiltrées. Les kits d'exploitation MOONSHINE, signalés par Trend Micro, constituent une fonctionnalité distincte qui exploite les vulnérabilités des navigateurs pour installer un logiciel malveillant appelé Dark Nimbus sur les appareils mobiles. De plus, Dark Nimbus et MOONSHINE sont des logiciels malveillants totalement différents.

Les deux qui suivent, l'interface de gestion de MOONSHINE et le kit d'exploitation MOONSHINE présentent des chevauchements de code, d'où les invites de connexion similaires des figures 3 et 5, ainsi que le contenu de la page des figures 4 et 6. Le code source de ces deux éléments contient également la chaîne 'webpackJsonpreact-scocthui'.

Les auteurs de la menace ont généré des liens URL pointant vers le kit d'exploitation MOONSHINE, puis redirigeant vers des vidéos concernant les Tibétains et les Ouïghours, ce qui coïncide avec le ciblage de MOONSHINE.

Sur de nombreuses adresses IP hébergeant le domaine du kit d'exploitation MOONSHINE, il existe une page de connexion intitulée 'VLiteUI' sur le port 444. Cette page n'est pas largement observée et sa présence sur ces IP indique un lien possible avec les opérations des acteurs.

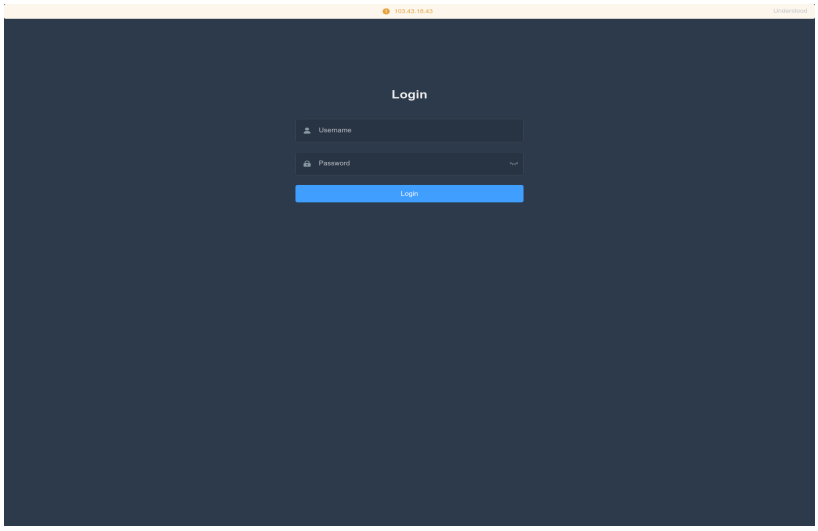


Figure 4 : Panneau de connexion avec le titre HTML 'VLiteUI' observé sur des adresses IP hébergeant également des kits d'exploitation MOONSHINE.

L'analyse de Dark Nimbus par Trend Micro a révélé que le logiciel malveillant peut collecter une liste exhaustive d'informations sur l'appareil et qu'il communique avec le C2 via le protocole XMPP.

Trend Micro souligne également que dans certaines versions de Dark Nimbus, la chaîne 'DKNS' a été identifiée comme prédominante.

'**ansec[.]com**' (répertorié comme C2 Dark Nimbus par Trend Micro) a également été observé dans les services XMPP d'autres adresses IP diffusant des pages web dont le titre contient DKNS :

- DKNS Android远程取证系统 (Système d'investigation à distance Android DKNS)
- DKNS云网侦控平台 (Plateforme d'investigation et de contrôle du réseau cloud DKNS)
- DKNS 云网侦控平台 (Plateforme d'investigation et de contrôle du réseau cloud DKNS)
- DKNS远程控制侦查系统 (Système d'enquête à distance DKNS)

Un autre ensemble d'adresses IP avec **'ansec[.]com'** dans le service XMPP avait des pages web avec le titre:

- UPSEC互联网控制指挥系统 (Système de contrôle et de commande Internet UPSEC)
- UPSEC无线侦控系统 (Système de surveillance et de contrôle sans fil UPSEC)
- UPSEC重点人数据还原系统 (Système de restauration des données des personnes clés UPSEC)

Selon Intelligence Online, 'UPSEC' observé dans les titres des pages HTML faisait référence à 'Sichuan Dianke Network Security Technology Co., Ltd'.

Étude de cas 2 : BADBAZAAR

BADBAZAAR est un logiciel malveillant mobile, décliné sur iOS et Android, qui cible les Ouïghours, les Tibétains et les Taïwanais. Ce logiciel espion se propage via les réseaux sociaux et les boutiques d'applications officielles. Un récent rapport de Volexity montre différentes variantes de BADBAZAAR, appelées BadSolar, BADBAZAAR et BadSignal. Les trois variantes sont liées entre elles par des fonctions qui se chevauchent et qui collectent des informations sur l'appareil et l'opérateur.

L'étude du NCSC sur BADBAZAAR a révélé les éléments suivants :

- Le regroupement des domaines C2 révèle d'autres liens avec des domaines signalés dans les rapports de veille sur les menaces historiques.
- Les serveurs C2 et les échantillons de logiciels malveillants révèlent des noms d'hôtes associés à l'infrastructure des acteurs.
- D'autres profils sont utilisés par les acteurs malveillants pour l'ingénierie sociale afin de diffuser leurs logiciels malveillants au-delà des plateformes d'applications officielles.

Clustering WHOIS / courtier de domaines

'UJYJYUJ'

L'analyse des enregistrements WHOIS pour le domaine BADBAZAAR '**signalplus[.]org**' (signalé par ESET) montre la valeur ' **UJYJYUJ** ' dans le champ '**État**'.

Une recherche d'autres domaines portant la même valeur révèle les domaines d'intérêt suivants :

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

(Voir Annexe A, image 1)

Les domaines **signalplus[.]org, tubevideoplus[.]org** et **thetubeplus[.]com** sont signalés comme des domaines C2 BADBAZAAR, tandis que ESET signale le sous-domaine **mail.pmumail[.]com** comme serveur proxy FlyGram. FlyGram est une application BADBAZAAR développée par des cybercriminels (voir l'annexe pour une liste des autres applications BADBAZAAR).

Valeurs de déplacement au clavier

Le NCSC a également observé des schémas de déplacement au clavier similaires dans d'autres domaines C2 BADBAZAAR enregistrés.

Par exemple, les domaines suivants ont tous la valeur '**REWR**' observée dans le champ '**État**' (comme précédemment) :

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

(Voir Annexe A, image 2)

Domaines avec des valeurs de champ d'état 'FSDF'

Un autre ensemble de domaines BADBAZAAR C2 a pour valeur '**État**' '**FSDF**' :

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

(Voir Annexe A, image 3)

Rapports historiques avec valeurs de reconnaissance vocale

L'utilisation de valeurs de reconnaissance vocale dans les enregistrements WHOIS des domaines BADBAZAAR est également observée dans le ciblage historique d'organisations tibétaines par TA413. Recorded Future a observé des domaines contrôlés par des acteurs usurpant l'identité d'organisations tibétaines et l'utilisation de la valeur d'organisation enregistrée '**asfasf**'.

clublogs[.]com

Les échantillons BADBAZAAR obtenus par Lookout contenaient '**xle.clublogs[.]com**' comme domaine C2. Le domaine racine '**clublogs[.]com**' était hébergé sur l'adresse IP '**95.179.210[.]85** ' et possédait un certificat SSL dont l'objet et l'émetteur étaient '**CN=WIN-50QO3EIRQVP**'. Cette valeur correspondait

aux certificats SSL trouvés dans les échantillons BADBAZAAR qui utilisaient l'épinglage SSL pour éviter l'interception des communications.
L'historique d'hébergement de l'adresse IP **95.179.210[.]85** renvoie les domaines d'intérêt suivants:

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

(Voir Annexe A, image 4)

www.voiceoftibet[.]net

Le domaine '**www.voiceoftibet[.]net**' semble se faire passer pour la station de radio 'Voice of Tibet', similaire au TTP utilisé par TA413.

Le domaine '**rewrwer[.]com**' est similaire à la valeur '**État**' '**REWR'** précédemment identifiée dans les enregistrements WHOIS des domaines BADBAZAAR.

Les domaines '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' et '**myloughborough[.]com**' ont tous été enregistrés avec le courriel '**tplutalova@list[.]ru**'.

actuallys[.]com

Les enregistrements WHOIS de '**actuallys[.]com**' ont montré un cas où les adresses e-mail techniques et administratives étaient '**tplutalova@list[.]ru**', mais le courriel du titulaire était '**ivan_s81@mail[.]ru**'.

Les informations WHOIS historiques du domaine '**actuallys[.]com**' ont révélé le courriel d'enregistrement '**wangminghua6@gmail[.]com**' enregistrée le 24 février 2016. Le 11 mars 2016, le courriel a été modifié en '**ivan_s81@mail.ru**', bien que la date d'expiration de l'enregistrement auprès du bureau d'enregistrement soit restée la même.

wangminghua6@gmail[.]com

Le courriel '**wangminghua6@gmail[.]com**' a été utilisé pour enregistrer des domaines identifiés dans les rapports historiques de renseignements sur les menaces. En 2015, Palo Alto a identifié l'adresse de courriel utilisée pour enregistrer des domaines C2 pour le malware Cmstar. En 2014, elle a également été utilisée pour enregistrer des domaines identifiés par Mandiant lors de campagnes

d'hameçonnage menées par APT3. En 2013, elle a été utilisée pour enregistrer des domaines trouvés par CrowdStrike dans un injecteur de malware dont le chemin d'accès à la base de données de programmes (PDB) contenait des caractères chinois. Cela suggère une compilation sur un système chinois.

taoyujun@gmail[.]com

Le domaine '**hcjbtt[.]com**' est enregistré avec le courriel '**taoyujun@gmail[.]com**', mais son courriel d'administrateur est '**wangminghua6@gmail[.]com**'.

Aucune activité malveillante n'est liée au domaine '**hcjbtt[.]com**', mais le courriel '**taoyujun@gmail[.]com**' a été identifié dans d'anciens rapports de renseignements sur les menaces. En 2014, ce domaine a été utilisé pour enregistrer un domaine identifié par Mandiant dans des échantillons du '**Cueisfry Trojan'** utilisés pour cibler des organisations japonaises.

L'adresse de courriel enregistrait également des domaines tels que '**iaea-international[.]org**', qui semblait se faire passer pour **l'Agence internationale de l'énergie atomique (AIEA**) ou **International Atomic Energy Agency** et '**idc-ctbto[.]org**', qui se faisait passer pour le **Centre international de données (CIDCT)** ou **International Data Centre** de **l'Organisation du Traité d'interdiction complète des essais nucléaires (OTICE).**

Un enregistrement Whois antérieur pour le domaine '**iaea-international[.]org**' indiquait que le courriel du titulaire était '**wangminghua6@gmail[.]com'**.

udtglobals[.]com

Le domaine '**udtglobals[.]com**' a été observé avec '**wangminghua6@gmail[.]com**' comme courriel d'administrateur et '**ocean.nio@rediffmail[.]com**' comme le courriel du titulaire. D'autres enregistrements WHOIS pour ce domaine indiquaient le même courriel du titulaire, mais avec le courriel d'administrateur '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' semblait se faire passer pour '**UDT Global**', un événement mondial pour les entreprises de défense et de sécurité sous-marines. Le nom d'utilisateur '**ocean.nio**' dans le courriel pourrait imiter **l'Institut national d'océanographie (NIO),** présent dans plusieurs pays L'utilisation du service de messagerie '**Rediff**' (basé en Inde) pourrait toutefois suggérer une imitation de **l'Institut national indien d'océanographie**

Djibdiplomatie[.]com

Le domaine '**djibdiplomatie[.]com**' semblait se faire passer pour les services diplomatiques de Djibouti, dont l'enregistrement WHOIS était similaire à celui de '**utdglobals[.]com**'. Un enregistrement semblait indiquer le titulaire '**ocean.nio@rediffmail[.]com**' et l'administrateur '**taoyujun@gmail[.]com**', tandis que d'autres indiquaient '**wangminghua6@gmail[.]com**' comme courriel de l'administrateur et '**ocean.nio@rediffmail[.]com**' comme courriel du titulaire.

Ces deux domaines présentaient également des valeurs de type balayage de clavier dans leurs enregistrements WHOIS. Par exemple, '**udtglobals[.]com**' a la valeur '**ASDF**' comme ville de dépôt et '**djibdiplomatie[.]com**' a '**DAF DAGF**' comme valeur du nom du titulaire. Ces valeurs sont comparables aux valeurs observées pour d'autres domaines BADBAZAAR.

Bien que les adresses de courriel '**wangminghua6@gmail[.]com**' et '**taoyujun@gmail[.]com**' figurent dans les enregistrements WHOIS de domaines se faisant passer pour un **événement mondial de défense sous-marine, les services diplomatiques de Djibouti** et **l'Agence internationale de l'énergie atomique**, elles sont également dans les enregistrements WHOIS de nombreux domaines non malveillants.

La combinaison de domaines se faisant passer pour des domaines et les domaines malveillants pourrait suggérer l'existence d'une entité acquéreuse d'infrastructures utilisées pour soutenir les opérations des cyberacteurs malveillants.

Le courriel '**ocean.nio@rediffmail[.]com**' n'apparaît que dans les domaines d'usurpation d'identité décrits ci-dessus. '**ivan_s81@mail[.]ru**' et '**tplutalova@list[.]ru**' ont enregistré un nombre très limité de domaines, dont certains sont hébergés sur l'infrastructure BADBAZAAR. Ces trois courriels sont considérés comme étroitement liées aux activités des cybercriminels. Cela s'explique par le fait qu'un plus grand nombre de domaines auxquels ils sont associés sont liés à des activités malveillantes, par rapport aux courriels '**wangminghua6@gmail[.]com**' et **taoyujun@gmail[.]com**.

(Voir Annexe A, image 5)

Liens vers d'autres acteurs malveillants

Une autre caractéristique commune des domaines liés à BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**' et '**voiceoftibet[.]net**' est qu'ils étaient tous enregistrés auprès d'eNom et étaient 'parqués' à '**255.255.255[.]254**'.

Suite à des enquêtes antérieures du NCSC, d'autres domaines présentant ces caractéristiques ont révélé une activité liée à **APT5** en 2019 et à **APT14** entre 2009 et 2011.

Les domaines liés à APT5- disposaient d'enregistrements WHOIS historiques indiquant '**taoyujun@gmail[.]com**' comme courriel du titulaire.

Les domaines liés à APT14 comportaient des sous-domaines de trois lettres qui semblaient représenter la cible visée par leurs opérations malveillantes. Par exemple, '**bae.cisconline[.]net**' suggérait une cible ciblée contre BAE Systems et a été trouvé dans un échantillon '**Poison Ivy**'.

Une caractéristique similaire est observée dans les domaines BADBAZAAR, où les sous-domaines sont liés au nom de l'application infectée par le cheval de Troie :

Titre de l'application	URL C2
Muslim Pro	**mpp.**pmstwocqn[.]com
Lecteur vidéo pour Android	**vpf.**titeperformance[.]com
Batter Master	**bat.**androidupdated[.]net
Radio Afghanistan	**afg.**collinformations[.]com
Dictionnaire EN-UG gratuit	**eud.**titeperformance[.]com
Récupération de vidéos sur disque	**dvr.**collinformations[.]com
TextNow	**ttn.**titeperformance[.]com

Il est important de noter que les activités liées à APT5 et APT14 étaient historiques et que d'autres domaines enregistrés auprès d'eNom, résolus en **' 255.255.255.254 '**, ne peuvent être liés à une activité malveillante. Il n'est donc pas certain que les acteurs à l'origine de ces campagnes soient les mêmes ou liés.

Noms de machines

L'analyse des C2 et des échantillons BADBAZAAR a révélé que des noms d'hôtes étaient utilisés comme valeur ' Nom commun ' dans les certificats SSL. Les enquêtes du NCSC sur les noms d'hôtes observés dans les échantillons et l'infrastructure BADBAZAAR ont montré que ces noms d'hôtes sont utilisés sur plusieurs adresses IP. Ces adresses IP hébergent des domaines trouvés dans les échantillons BADBAZAAR. Vous trouverez plus de détails dans la section ci-dessous sur les noms d'hôtes et les adresses IP hébergeant les domaines C2 BADBAZAAR.

Dans la quasi-totalité des cas, la présence de certificats dont la valeur du nom d'hôte chevauche les résolutions IP des noms de domaine malveillants spécifiés, les rares cas où ce n'était pas le cas ont été signalés.

WIN-EU0VLBL7TUJ

Le nom d'hôte '**WIN-EU0VLBL7TUJ**' a été observé sur les adresses IP suivantes:

- '**116.203.53[.]21**' hébergeait les domaines BADBAZAAR C2 '**uyapkfinder[.]com**' et '**thewestuniverse[.]com**'.

- '**95.216.169[.]27**' hébergeait les domaines BADBAZAAR C2 '**adysfunction[.]com**' et le sous-domaine '**download.apkbazar[.]biz**' observé comme lien de téléchargement pour un échantillon de BADBAZAAR. (Voir Annexe A, image 6)

WIN-70E59JVOB9G

Le nom d'hôte '**WIN-70E59JVOB9G**' a été observé sur les adresses IP suivantes :

- **'23.88.28[.]220'** hébergeait les sous-domaines C2 de BADBAZAAR, '**aua.rondwsign[.]com**', '**nal.tokenmajorp[.]com**', '**pep.rondwsign[.]com**', '**doa.rondwsign[.]com**' et '**pls.rondwsign[.]com**'. Un délai de deux jours s'est écoulé entre la dernière détection du certificat sur la machine et la première détection des domaines malveillants se résolvant vers l'adresse IP.

- **'23.88.28[.]221**' hébergeait le sous-domaine lié à BADBAZAAR '**bt.bhvghg[.]com**'.

- ‘**23.88.28[.]222’** hébergeait les domaines C2 BADBAZAAR ‘**tubevideoplus[.]org’** et ‘**cde.mpoxcases[.]com’**.

- ‘**65.21.92[.]67’** hébergeait le sous-domaine C2 BADBAZAAR ‘**bat.androidupdated[.]net’**. Il hébergeait également le sous-domaine ‘**apps.androidupdated[.]net’**, un malware C2 DoubleAgent.

- ‘**65.21.92[.]77’** hébergeait les sous-domaines BADBAZAAR C2 ‘**wyo.titeperformance[.]com’**, ‘**big.collinformations[.]com’**, ‘**vpf.titeperformance[.]com’**, ‘**eud.titeperformance[.]com’** et ‘**afg.collinformations[.]com’**.

- ‘**65.108.192[.]134’** hébergeait les sous-domaines BADBAZAAR C2 ‘**upd.whoscaller.net’** et ‘**ggl.whoscaller[.]net’**.

- ‘**142.132.131[.]15’** hébergeait les sous-domaines BADBAZAAR C2 ‘**bvn.lookincategory[.]com’** et ‘**edr.lookincategory[.]com’**. Il y a eu une période de onze jours entre le moment où le certificat avec le nom de la machine a été vu pour la dernière fois et le moment où les domaines malveillants ont été vus pour la première fois en train de se résoudre à l'adresse IP.

- Le domaine ‘**142.132.131[.]20**’ hébergeait les sous-domaines ‘**son.onlinegamersgroup[.]com**’ et ‘**system.onlinegamersgroup[.]com**’, suspectés d'être des C2 BADBAZAAR, car ils étaient hébergés alors que des certificats SSL associés à BADBAZAAR étaient détectés sur l'adresse IP.

- Le domaine ‘**142.132.131[.]28**’ hébergeait le domaine C2 BADBAZAAR ‘**goldplusapp[.]net**’ et les sous-domaines ‘**who.goldplusapp[.]net**’ et ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211’** hébergeait les sous-domaines C2 BADBAZAAR ‘**oha.alpinemap[.]net’**, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net’**, ‘**afr.alpinemap[.]net’** et ‘**aar.alpinemap[.]net’**.

- ‘**162.55.103[.]212’** hébergeait les sous-domaines C2 BADBAZAAR ‘**pep.rondwsign[.]com’**, ‘**ckp.jkiohreh[.]com**’, ‘**aar.tokenmajorp[.]com’**,

‘**nal.tokenmajorp[.]com**’, ‘**pls.rondwsign[.]com’** et ‘**aua.rondwsign[.]com’**.

- ‘**195.154.47[.]99**’ hébergeait les sous-domaines C2 BADBAZAAR ‘**ggl.whoscaller[.]net**’ et ‘**upd.whoscaller.net**’. Un délai de trois jours s'est écoulé entre la première détection du certificat portant le nom de la machine et la dernière détection des domaines malveillants se résolvant vers l'adresse IP.

- ‘**195.154.60[.]3**’ hébergeait les sous-domaines C2 BADBAZAAR ‘**upd.whoscaller[.]net**’ ‘ **ggl.whoscaller[.]net** ’.

- ‘**212.83.189[.]89**’ hébergeait les sous-domaines C2 BADBAZAAR ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ et ‘**afg.collinformations[.]com**’.

- **‘212.129.21[.]168’** hébergeait les domaines BADBAZAAR C2, **‘fre.lookincategory[.]com’, ‘tgr.lookincategory[.]com’, ‘fgt.lookincategory[.]com’, ‘luj.lookincategory[.]com’ et ‘bvn.lookincategory[.]com’.**

(Voir Annexe A, image 7)

WIN-50QO3EIRQVP

Le nom d'hôte ‘**WIN-50QO3EIRQVP**’ a été observé sur les adresses IP suivantes :

- ‘**45.76.132[.]91**’ hébergeait les domaines, ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. Les deux domaines sont liés à BADBAZAAR, car les sous-domaines ‘**fow.yumoftion[.]com**’ et ‘**bat.androidupdated[.]net**’ sont des domaines C2 BADBAZAAR. Le sous-domaine ‘**apps.androidupdated[.]net**’ est également un domaine C2 DoubleAgent. Il héberge également le domaine ‘**pmstwocqn[.]com**’, lié à BADBAZAAR via les enregistrements WHOIS.

- ‘**95.179.210[.]85** ’ hébergeait ‘**clublogs[.]com**’, dont ‘ **xle.clublogs[.]com**’ est un domaine C2 BADBAZAAR, et hébergeait également les domaines liés à BADBAZAAR ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, ‘ **www.voiceoftibet[.]net**’ et ‘**actuallys[.]com**’.

- '**199.247.21[.]34**' hébergeait '**titeperformance[.]com**' et '**collinformations[.]com**', dont les sous-domaines sont des domaines C2 BADBAZAAR.

- '**217.69.10[.]128**' hébergeait le domaine C2 BADBAZAAR '**uyghurdict[.]com**'.

(Voir Annexe A, image 8)

WMSvc-WIN-50QO3EIRQVP

Le nom d'hôte '**WMSvc-WIN-50QO3EIRQVP**' a été observé sur les adresses IP suivantes :

- '**78.46.185[.]251**' hébergeait le domaine C2 BADBAZAAR '**groupgram[.]org**', signalé par Volexity comme utilisant le port 4432 pour des connexions malveillantes.

- Les domaines '**65.21.92[.]69**' et '**163.172.205[.]207** hébergés par '**widelygram[.]org**' sont considérés comme des domaines C2 BADBAZAAR, car le port 4432 était ouvert pendant leur hébergement sur les deux adresses IP.

- Le domaine ' **163.172.198[.]206** ' hébergeait le domaine '**maxgram[.]org** ', qui semble être un domaine C2 BADBAZAAR, car le port 4432 était ouvert pendant son hébergement.

(Voir Annexe A, image 9)

WMSvc-WIN-50QO3EIRQVP et WIN-7LSBB9R0F1L

Les noms d'hôtes '**WMSvc-WIN-50QO3EIRQVP**' et '**WIN-7LSBB9R0F1L**' ont été observés simultanément sur l'adresse IP suivante :

- '**148.251.87[.]245**' hébergeait les domaines C2 BADBAZAAR '**flygram[.]org**' et '**groupgram[.]org**'.

(Voir Annexe A, image 10)

WIN-N8H8S9BG2P0

Les noms d'hôtes '**WIN-N8H8S9BG2P0**' ont été observés à l'adresse IP suivante :

- '**148.251.87[.]247**' hébergeait les domaines C2 BADBAZAAR '**omarwhatsapp[.]org**' et '**flygram[.]org**'.

(Voir Annexe A, image 11)

WIN-I6VBN8MR92A

Les noms d'hôtes '**WIN-I6VBN8MR92A**' ont été observés à l'adresse IP suivante :

- '**148.251.87[.]197**' hébergeait le domaine C2 BADBAZAAR '**tryhrwserf[.]com**'.

(Voir Annexe A, image 12)

D'après les données commerciales disponibles, la prévalence de ces noms de machines sur Internet varie. Certains d'entre eux sont observés simultanément sur plusieurs adresses IP, ce qui indique que des machines virtuelles sont créées à partir du même modèle. Il est important de noter que pour certains noms d'hôtes, les adresses IP observées ne sont pas toutes liées à une activité malveillante. Cela pourrait signifier que l'utilisation de ces noms d'hôtes n'est pas exclusive à ces acteurs malveillants.

Cependant, la prévalence de certains de ces noms de machines sur les adresses IP ayant hébergé des domaines C2 BADBAZAAR pourrait suggérer qu'une entité d'acquisition d'infrastructures est utilisée pour configurer des machines afin de soutenir les cyberopérations des acteurs malveillants.

Présence sur les réseaux sociaux

Un précédent rapport de Volexity a montré que des vidéos YouTube (promouvant l'utilisation des applications malveillantes) ont été créées par les acteurs malveillants. Ces vidéos comprenaient des tutoriels expliquant l'utilisation des applications développées.

Le NCSC a découvert deux chaînes YouTube supplémentaires associées aux opérations des pirates. La chaîne YouTube channel dont l'URL est '**@josephjoey3499**' semble promouvoir l'utilisation de '**Maxgram**', tandis qu'une autre chaîne channel enregistrée sous '**@uyghurapks3096**' fait la promotion de '**Uyghur APK Finder**'.

De plus, des vidéos YouTube faisant la promotion de '**Flygram**' et de '**Signal Plus**' ont montré que les pirates utilisaient des numéros de téléphone visibles. Dans la vidéo '**Flygram**' video, à 0:36, le numéro de téléphone '**+1 (570) 378-7250**' est visible, et dans la vidéo '**Signal Plus**' video, le numéro de téléphone '**+1 (267) 298 4259**' est révélé.

Volexity a signalé l'existence d'un faux site d'information sur le Tibet, '**ignitetibet[.]net**', découvert sur des chaînes Telegram soupçonnées d'être gérées par les pirates. Le courriel '**choekyi.wangmo@ignitetibet[.]net**' est observé en train de commenter des publications sur la page '**tibetone.org**', signalée publiquement par Lookout comme une page C2 utilisée pour la variante iOS de BADBAZAAR.

Ce courriel serait contrôlé par un individu utilisant l'identité de '**Choekyi Wangmo**'.

Évaluation

BADBAZAAR et MOONSHINE utilisent plusieurs méthodes d'ingénierie sociale pour cibler spécifiquement les communautés ouïghoure, tibétaine et taïwanaise, notamment :

- La conversion de chevaux de Troie d'applications susceptibles d'intéresser ces communautés, comme une application du Coran en langue ouïghour, est très probablement adaptée à la cible.
- L'ajout de ces applications trojanisées aux boutiques d'applications officielles confère très probablement un sentiment de légitimité, et le partage dans les discussions de groupe vise très probablement à exploiter les relations de confiance au sein de ces communautés.

BADBAZAAR et MOONSHINE collectent des données qui seraient très certainement utiles à l'État chinois. Bien que BADBAZAAR et MOONSHINE aient été observés ciblant des Ouïghours, des Tibétains et des Taïwanais, d'autres logiciels malveillants ciblent d'autres groupes minoritaires en Chine. Les citoyens des pays co-scellés, en Chine et à l'étranger, perçus comme soutenant des causes menaçant la stabilité du régime, sont très probablement menacés par des logiciels malveillants mobiles tels que BADBAZAAR et MOONSHINE. La capacité de capturer des données de localisation, audio et photo offre très certainement la possibilité d'éclairer les futures opérations de surveillance et de harcèlement en fournissant des informations en temps réel sur l'activité de la cible.

MITRE ATT&CK®

Ce rapport a été compilé dans le respect du cadre MITRE ATT&CK®, une base de connaissances accessible à l'échelle mondiale sur les tactiques et techniques adverses basées sur des observations du monde réel.

Tactique	ID	Technique	Procédure
Reconnaissance	T1593.001	Recherche de sites web/domaines ouverts : Réseaux sociaux	Les acteurs trouvent des groupes et des forums en ligne correspondant à leurs victimes cibles pour partager le logiciel malveillant.
Développement des ressources	T1583.001	Acquisition d'infrastructures : Dom aines	Les acteurs enregistrent des domaines pour leurs serveurs de commande et de contrôle.
Développement des ressources	T1587.001	Développer les capacités : Logiciel malveillant	Un code malveillant est écrit pour être inséré dans des applications infectées par des chevaux de Troie.
Développement des ressources	T1608.001	Fonctionnalités de l'étape : Téléchargement de logiciels malveillants	Les applications infectées par des chevaux de Troie sont téléchargées sur des plateformes en ligne, notamment des boutiques d'applications.
Développement des ressources	T1585.001	Création de comptes : Comptes sur les réseaux sociaux	Les acteurs créent des comptes sur des sites web et des réseaux sociaux pour partager et promouvoir le logiciel malveillant.
Développement des ressources	T1585.002	Création de comptes : Comptes de messagerie	Les acteurs utilisent des comptes de messagerie privés et commerciaux pour héberger et partager des logiciels malveillants.
Accès initial	T1189	Compromission par téléchargement furtif	Des scripts malveillants sont dissimulés dans des applications légitimes et téléchargés sur les plateformes de téléchargement d'applications.

Accès initial	T1566.003	Hameçonnage : Hameçonnage ciblé via le service	Les acteurs envoient des applications infectées par un cheval de Troie à des groupes ciblés via les réseaux sociaux, y compris Telegram.
Exécution	T1204.002	Exécution par l'utilisateur : Fichier malveillant	Les victimes doivent installer les applications infectées par un cheval de Troie pour exécuter la charge utile.
Évasion de la défense	T1027.009	Fichiers ou informations obscurcis : Charges utiles intégrées	La charge utile malveillante est dissimulée dans des applications par ailleurs légitimes.
Évasion de la défense	T1036.005	Masquage : Correspondance avec un nom ou un emplacement légitime	Les fichiers infectés par un cheval de Troie correspondent au nom, à l'apparence et à la fonction d'applications légitimes.
Évasion de la défense	T1656	Usurpation d'identité	Les acteurs se font passer pour des personnes de confiance en créant des sites web de couverture et en utilisant des noms d'utilisateur associés à des groupes cibles.
Collection	T1123	Audio capture	Les applications infectées peuvent demander des autorisations inutiles, notamment l'accès au microphone.
Collection	T1125	Capture vidéo	Les applications infectées peuvent demander des autorisations inutiles, notamment l'accès à la caméra.
Collection	T1005	Données du système local	Les applications infectées par un cheval de Troie peuvent demander des autorisations inutiles, y compris des fichiers locaux.
Commande et contrôle	T1071.001	Protocole de couche applicative : Protocoles Web	Les logiciels malveillants se connectent au C2 via HTTPS et WebSocket.

Commande et contrôle	T1509	Port non standard	Des ports non standard sont utilisés, tels que les ports 4432 et 2333.
Exfiltration	T1041	Exfiltration via le canal C2	Les logiciels malveillants exfiltrent des données via des connexions HTTPS et WebSocket.
Impact	T1565.002	Manipulation des données : Manipulation des données transmises	Les pirates obtiennent des données auprès des victimes en autorisant le trafic web de l'application, ce qui n'est pas nécessaire à son fonctionnement.

Indicateurs

MOONSHINE :

- Le 1er avril 2025, une recherche sur les panneaux VLiteUI a généré les résultats suivants :

Adresses IP	Port	Première connexion	Dernière connexion
103.254.108[.]87	888	17-10-2024	14-02-2025
43.159.192[.]7	444	21-11-2024	13-02-2025
103.27.109[.]109	444	11-07-2024	07-02-2025
45.119.99[.]83	444	26-12-2024	24-01-2025
103.254.108[.]76	444	12-09-2024	05-12-2024
194.71.107[.]160	444	10-12-2023	01-11-2024
103.254.108[.]108	444	12-11-2023	25-09-2024
103.56.17[.]194	444	03-04-2024	23-08-2024
103.254.108[.]87	444	14-11-2023	15-08-2024
62.72.58[.]168	444	29-01-2024	07-08-2024
103.43.18[.]43	444	12-02-2024	19-07-2024
77.91.123[.]208	444	04-02-2024	09-04-2024
46.246.98[.]229	444	07-03-2024	26-03-2024
2.58.15[.]101	444	23-02-2024	27-02-2024
46.246.98[.]209	444	08-01-2024	14-02-2024
103.254.108[.]87	8000	17-10-2023	17-10-2023
103.254.108[.]87	8080	15-04-2023	16-10-2023
103.254.108[.]108	9090	13-04-2023	16-10-2023
103.45.66[.]123	9090	02-03-2023	08-04-2023
103.45.66[.]32	8080	29-07-2022	04-04-2023
27.124.20[.]23	9090	28-05-2022	24-03-2023
27.124.20[.]22	9090	28-05-2022	23-03-2023
27.124.20[.]24	9090	27-05-2022	17-03-2023
69.176.94[.]148	9090	04-03-2023	10-03-2023
69.176.94[.]228	9090	14-12-2022	25-02-2023
103.253.40[.]137	8000	24-06-2022	02-09-2022
27.124.4[.]80	8080	25-02-2022	23-06-2022
27.124.4[.]81	8080	25-02-2022	23-06-2022
47.242.46[.]79	8080	03-05-2021	17-06-2022
27.124.4[.]82	8080	24-02-2022	15-06-2022
27.124.4[.]165	9090	14-05-2022	28-05-2022

27.124.4[.]184	9090	14-05-2022	27-05-2022
27.124.4[.]178	9090	13-05-2022	26-05-2022
103.15.28[.]165	8080	05-03-2022	25-05-2022
69.176.94[.]226	8080	05-03-2022	22-04-2022
27.124.4[.]3	8080	11-03-2022	02-04-2022
103.140.238[.]235	8080	04-03-2022	01-04-2022
27.124.4[.]2	8080	12-03-2022	01-04-2022
165.84.180[.]107	8000	25-02-2022	19-03-2022
69.176.94[.]156	8000	25-02-2022	05-03-2022
141.98.212[.]70	9090	05-10-2021	04-03-2022
5.188.33[.]50	8000	15-02-2022	04-03-2022
5.188.70[.]193	8000	15-02-2022	04-03-2022
69.176.94[.]140	8080	24-02-2022	24-02-2022
27.124.20[.]83	8000	14-02-2022	18-02-2022
208.87.200[.]106	8000	02-01-2022	02-01-2022
121.127.241[.]37	8000	08-12-2021	08-12-2021
156.255.2[.]211	443	05-10-2021	05-10-2021
156.255.2[.]211	8000	04-10-2021	04-10-2021
156.255.2[.]203	8000	03-10-2021	03-10-2021
47.243.43[.]248	8000	05-07-2021	05-07-2021
45.115.236[.]6	8080	03-05-2021	01-06-2021
43.251.118[.]97	8000	03-01-2021	01-03-2021
185.243.43[.]138	8000	04-01-2021	02-02-2021
47.245.59[.]33	8000	05-01-2021	05-01-2021

- Le 1er avril 2025, une recherche sur les panneaux SCOTCH ADMIN a donné les résultats suivants :

Adresses IP	Port	Première connexion	Dernière connexion
104.194.152[.]24	2333	06-02-2025	27-02-2025
172.86.80[.]126	2333	07-02-2025	27-02-2025
154.90.59[.]62	2333	20-06-2024	20-09-2024
154.90.59[.]88	2333	21-06-2024	20-09-2024
154.90.58[.]210	2333	16-05-2024	14-06-2024
154.90.59[.]225	2333	17-05-2024	13-06-2024
38.60.199[.]208	2333	26-11-2023	09-01-2024
38.60.199[.]254	2333	28-11-2023	09-01-2024

38.60.199[.]99	2333	26-08-2023	21-11-2023
38.60.199[.]44	2333	20-07-2023	11-09-2023
194.163.34[.]23	443	30-09-2022	14-04-2023
45.32.125[.]112	10443	01-10-2022	17-03-2023

- Le 14 mars 2024, une recherche de panneaux virtuels SCOTCH ADMIN a donné les résultats suivants :

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

BADBAZAAR :

Description	Certificat SSL observé sur les C2 BADBAZAAR. MD5
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Le 1er avril 2025, une recherche du certificat BADBAZAAR ci-dessus a généré les résultats suivants :

Adresses IP	Ports	Première connexion	Dernière connexion
65.108.192[.]173	31237	14-03-2025	28-03-2025
65.108.192[.]173	31236	14-03-2025	28-03-2025
65.108.192[.]173	31235	14-03-2025	28-03-2025
157.90.129[.]73	31236	27-03-2025	27-03-2025

142.132.131\ [.]15	31236	24-07-2024	27-03-2025
142.132.131[.]15	31235	26-07-2024	27-03-2025
142.132.131[.]20	31237	11-08-2023	27-03-2025
142.132.131[.]15	31237	24-07-2024	27-03-2025
142.132.131[.]20	31236	27-09-2023	26-03-2025
142.132.131[.]20	31235	18-10-2023	26-03-2025
65.108.192[.]155	31236	05-12-2024	20-02-2025
65.108.192[.]155	31237	05-12-2024	20-02-2025
65.108.192[.]155	31235	05-12-2024	19-02-2025
23.88.28[.]222	31237	25-04-2024	29-11-2024
23.88.28[.]222	31235	02-05-2024	28-11-2024
23.88.28[.]222	31236	01-05-2024	28-11-2024
212.129.21[.]168	31235	16-10-2023	17-03-2024
212.129.21[.]168	31237	28-04-2023	17-03-2024
212.129.21[.]168	31236	26-09-2023	14-03-2024

Description	Certificat SSL observé sur les C2 BADBAZAAR
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- Le 1er avril 2025, une recherche du certificat BADBAZAAR ci-dessus a généré les résultats suivants
-

Adresses IP	Ports	Première connexion	Dernière connexion
162.55.103[.]211	20122	12-01-2023	28-03-2025
162.55.103[.]212	20121	30-06-2022	28-03-2025
162.55.103[.]212	20122	14-07-2023	28-03-2025
162.55.103[.]211	20121	03-06-2022	28-03-2025
162.55.103[.]211	20123	22-07-2023	27-03-2025
162.55.103[.]212	20123	22-07-2023	27-03-2025
212.83.162[.]152	9090	13-10-2022	27-10-2025

2 3.88.28[.]221	20422	28-07-2023	30-09-2023
23.88.28[.]221	20421	18-05-2023	28-09-2023
23.88.28[.]221	20423	28-07-2023	28-09-2023
162.55.103[.]210	20121	30-09-2022	23-02-2023
65.21.92[.]67	20121	02-11-2021	13-10-2022
65.21.92[.]67	20122	10-08-2022	13-10-2022
23.88.28[.]220	20121	08-12-2021	13-05-2022
94.130.92[.]230	20121	04-01-2021	05-10-2021
88.99.150[.]246	20121	06-04-2021	08-09-2021
45.76.132[.]91	20121	02-02-2021	01-03-2021

- Domaines WHOIS

Vous trouverez ci-dessous un tableau des domaines qui possèdent actuellement ou historiquement des enregistrements WHOIS dont les valeurs correspondent à celles observées dans les domaines C2 BADBAZAAR.

Valeur WHOIS	Domaines
État du titulaire : UJYJYUJ **Pays du titulaire : Bolivie** **Bureau d'enregistrement : 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
État du titulaire : REWR **Pays du titulaire : CF** **Bureau d'enregistrement : eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com

	• verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
État d'enregistrement : FSDF **Pays du déclarant : AL** **Bureau d'enregistrement : eNom**	• tryhrwserf[.]com • tibetone[.]org • venirflxyr[.]com • adopteur[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

Adresses de courriel
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

Voici des liens vers d'autres indicateurs de compromission (IoC) associés à BADBAZAAR et MOONSHINE. Le NCSC ne peut pas confirmer la validité de toutes les informations contenues dans ces liens ; il est donc conseillé aux lecteurs de vérifier indépendamment leur exactitude et leur pertinence :

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

Atténuation

Le NCSC encourage l'adoption des recommandations ci-dessous pour se protéger contre les menaces décrites dans les études de cas.

- **Les opérateurs de plateformes d'applications, y compris les plateformes tierces, et les développeurs doivent s'assurer que les applications sur leur plateforme sont sécurisées et conformes au Code de bonnes pratiques gouvernemental.** Voir les directives sur le site : 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

- **Prise en charge multilingue :** Les développeurs d'applications doivent s'efforcer de localiser les applications populaires pour les utilisateurs parlant des langues minoritaires parmi les groupes ciblés, notamment l'ouïghour, le tibétain, le hokkien taïwanais et le cantonais. Conseils d'Apple pour la localisation dans les applications : https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Conseils de Google pour la traduction des applications : https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Sécuriser votre plateforme de médias sociaux :** Les entreprises de médias sociaux peuvent compliquer la tâche des cybercriminels qui souhaitent créer de faux comptes et partager des fichiers ou des liens malveillants sur leurs plateformes au sein de communautés en ligne légitimes. Dans la mesure du possible, les entreprises devraient partager les indicateurs de malveillance avec l'ensemble du secteur afin d'améliorer la compréhension collective de la menace et de contribuer aux mesures de protection.

- **Plan de remédiation pour les clients :** Les organisations doivent mettre en place des procédures pour informer les clients qui ont installé des applications malveillantes via leurs services. Ces alertes doivent attirer

l'attention et être informatives. Le cas échéant, les organisations doivent fournir des conseils sur la suppression des logiciels et encourager les victimes à signaler les incidents aux autorités compétentes, comme le NCSC au Royaume-Uni.
Pour en savoir plus, consultez le Code de bonnes pratiques de l'App Store : https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Groupes de travail pour la collaboration :** Les entreprises de médias sociaux peuvent former des groupes de travail permettant à leurs équipes de sécurité respectives de partager des indicateurs malveillants, des TTP et des observations, ce qui complique l'utilisation de leurs plateformes par les acteurs malveillants pour soutenir des campagnes malveillantes.

- **Détection des applications altérées :** Dans la mesure du possible, les développeurs d'applications devraient inclure une fonctionnalité informant l'utilisateur du téléchargement d'une version ' non officielle ' d'une application, afin de se protéger contre les copies malveillantes.

Annexe A : Graphiques des informations de clustering WHOIS / de courtier des domaines de BADBAZAAR

Image 1 - 'UKYJYUJ'

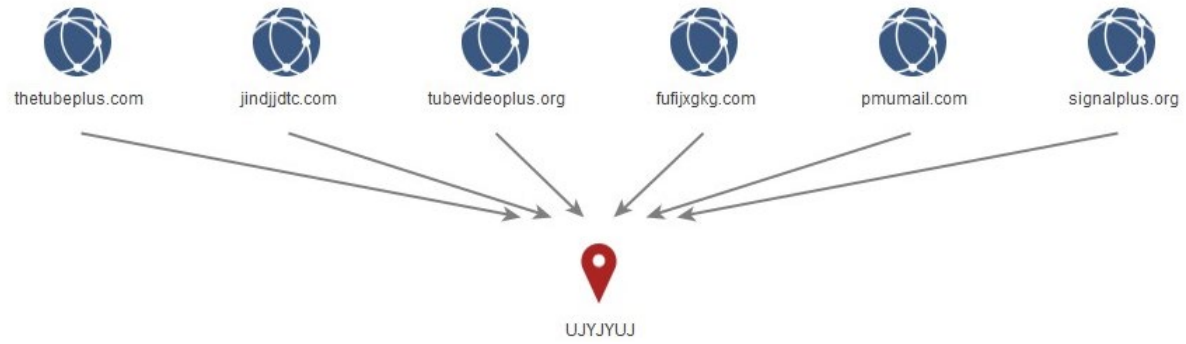


Image 2 – Valeurs de déplacement du clavier

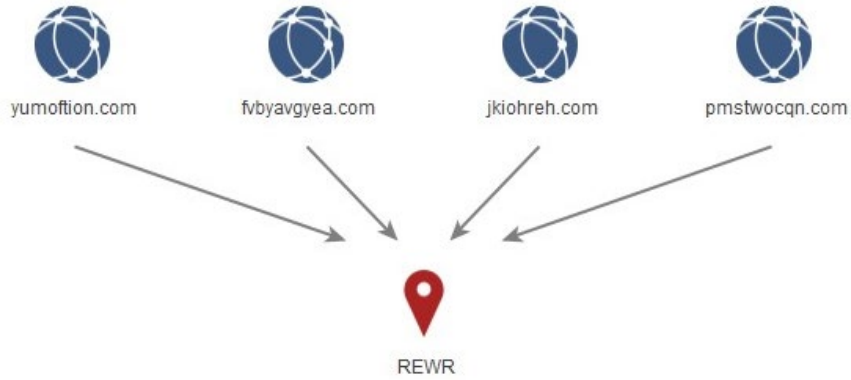


Image 3 – Domaines supplémentaires avec valeurs de champ d'état ' FSDF '

Image 4 – 95.179.210[.]85

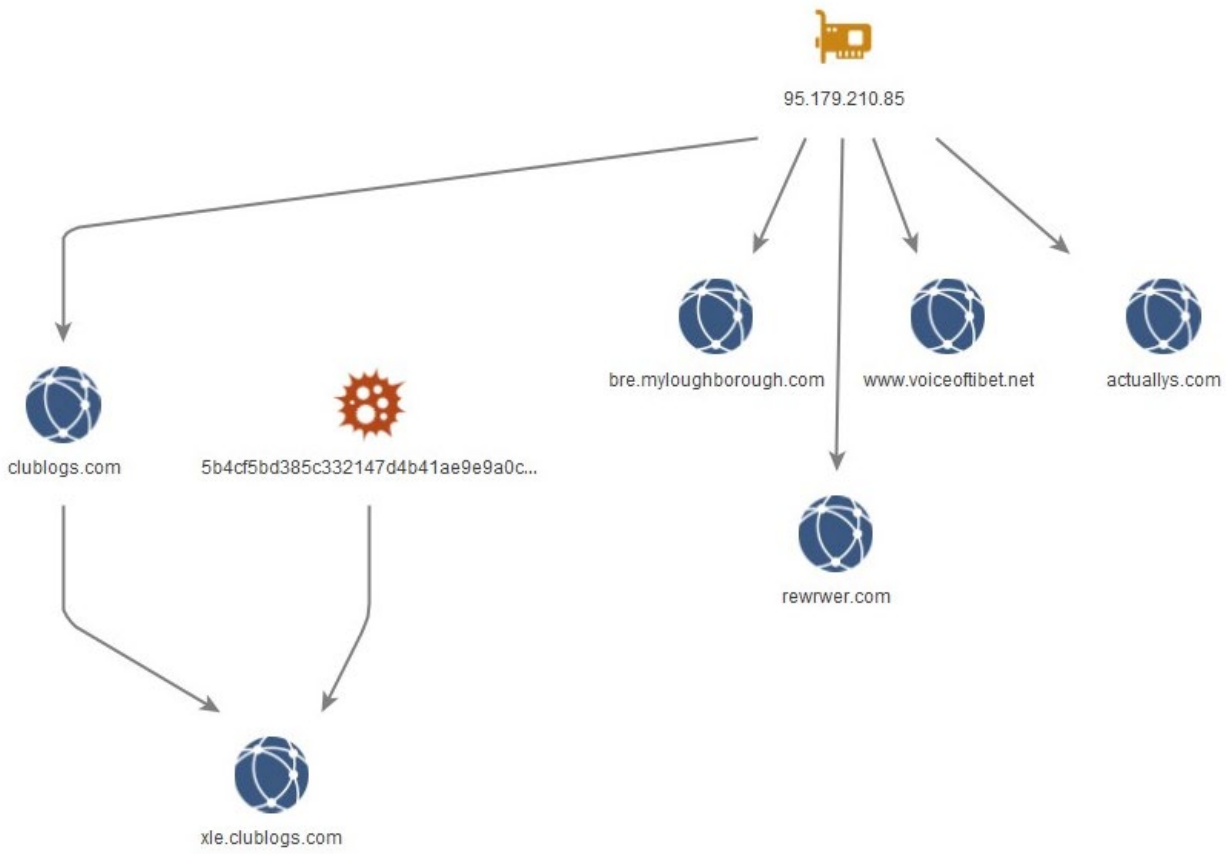


Image 5 – Liens WHOIS

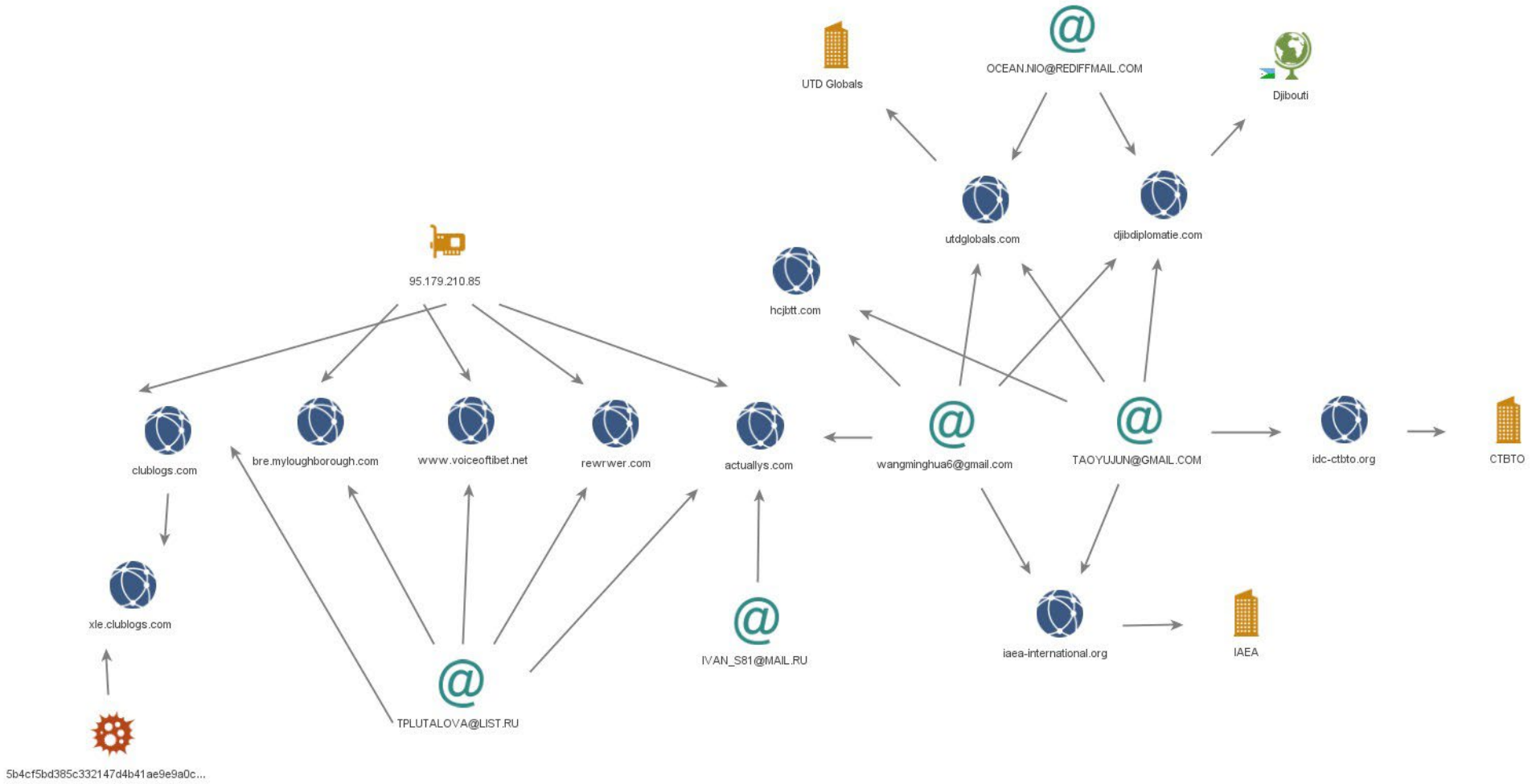


Image 6 – WIN-EU0VLBL7TUJ

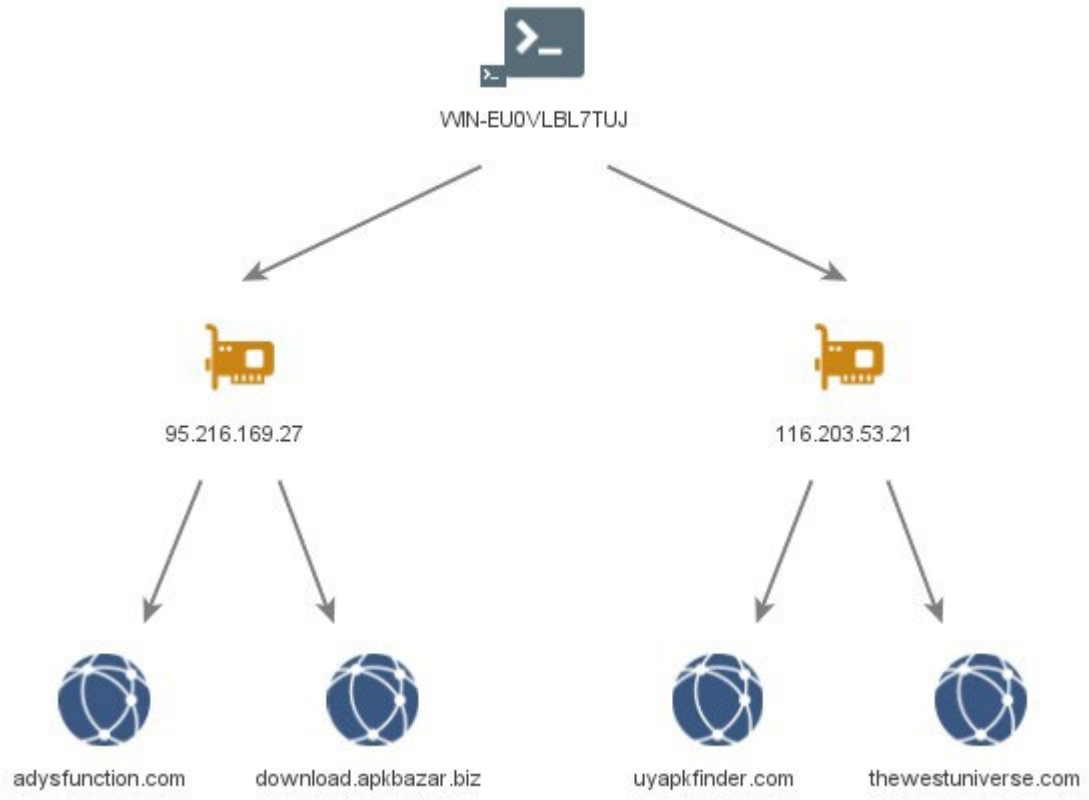


Image 7 – WIN-70E59JVOB9G

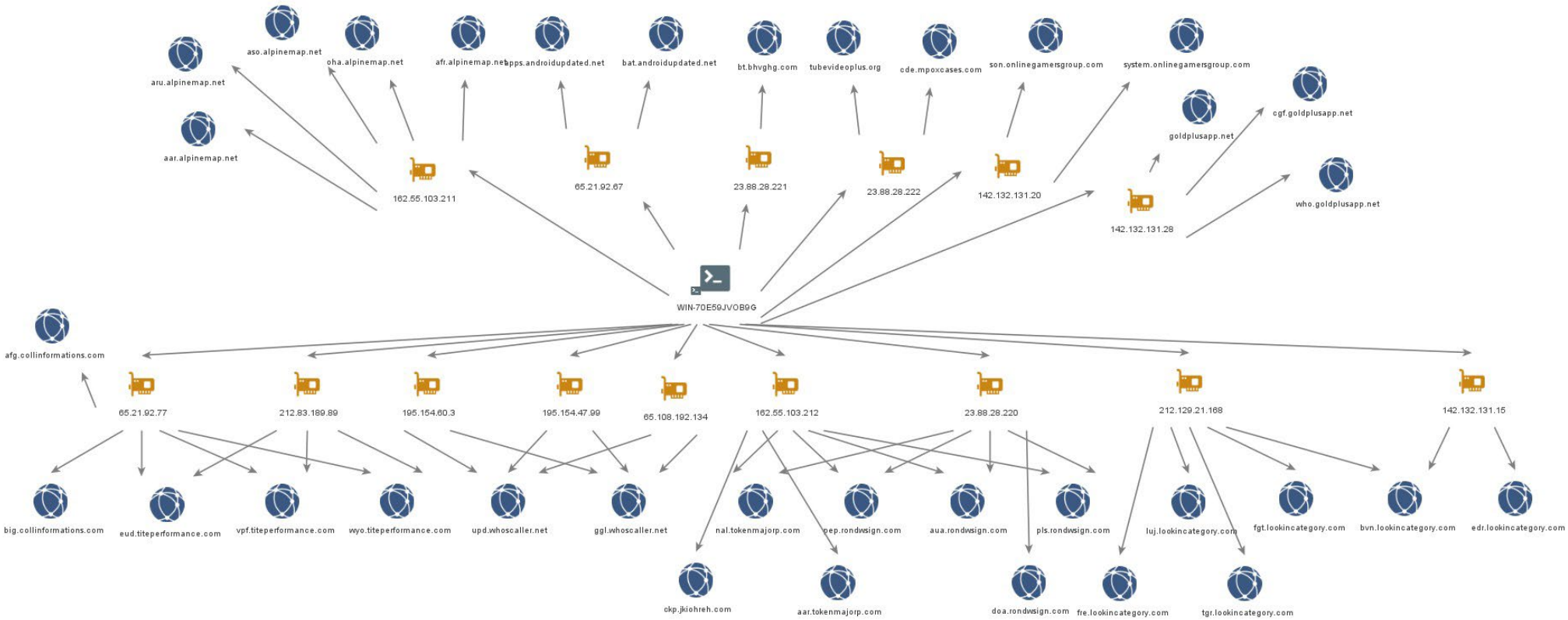


Image 8 - WIN-50QO3EIRQVP

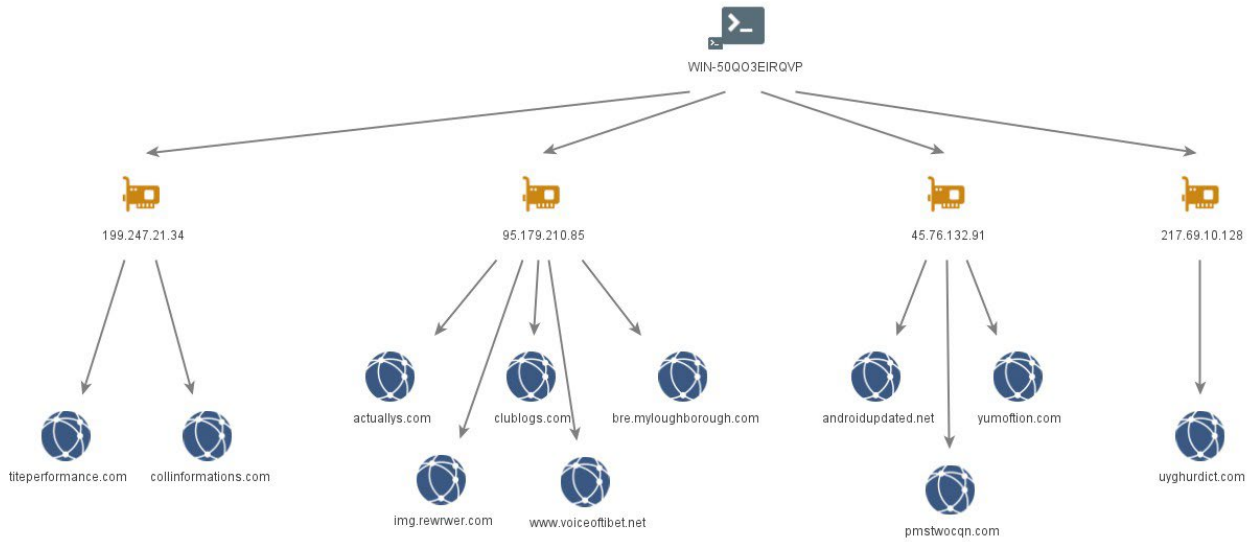


Image 9 - VMSvc-WIN-50QO3EIRQVP

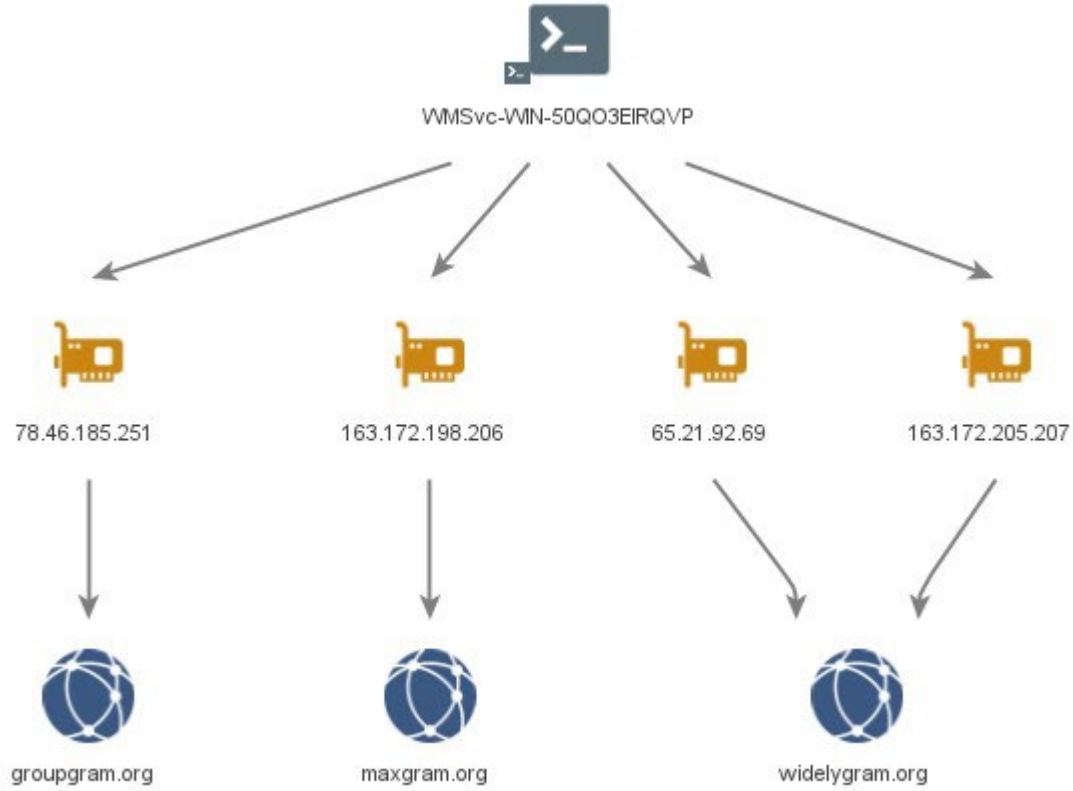


Image 10 – VMSvc-WIN-50QO3EIRQVP et WIN-7LSBB9R0F1L

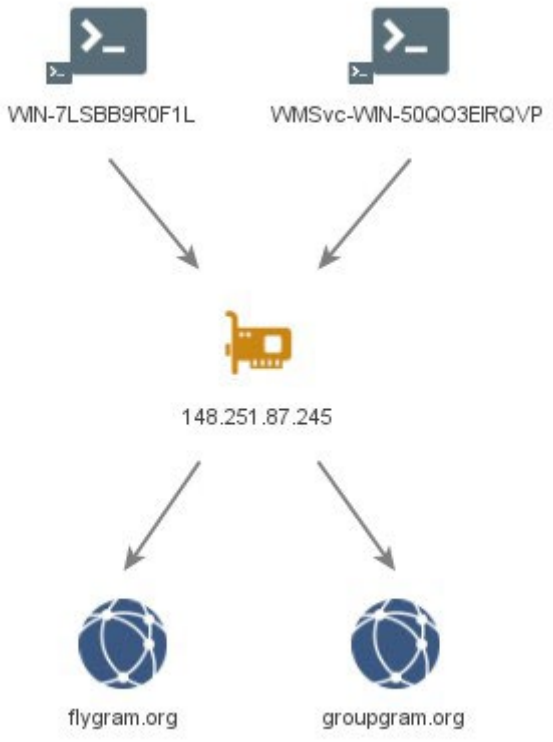


Image 11 - WIN-N8H8S9BG2P0

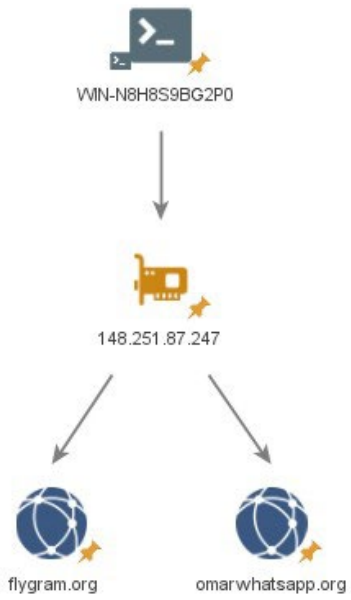


Image 12 – WIN-I6VBN8MR92A

Annexe B : Échantillons MOONSHINE et BADBAZAAR observés

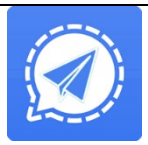
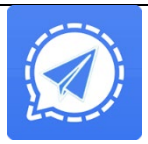
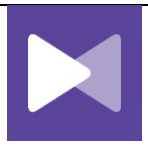
Le tableau répertorie les applications utilisées dans les campagnes MOONSHINE et BADBAZAAR au cours des deux dernières années.

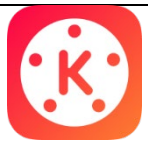
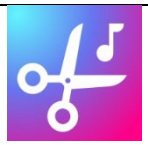
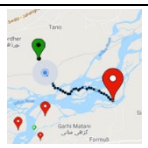
Nombre de ces applications présentent une nette similitude avec des applications établies. Il s'agit probablement d'une technique délibérée visant à usurper l'identité de marques connues.

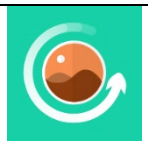
Il est important de noter que le nom de l'application, le nom du package et l'icône peuvent tous imiter ou correspondre à l'application réelle et ne doivent donc pas être utilisés exclusivement pour identifier si un appareil est infecté.

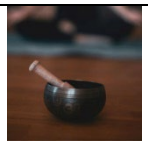
Titre de l'application	Noms du progiciel	Icône de l'application
99 Noms d'Allah	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Clavier arabe	com.arabic.keyboard.arabic.language.keyboard.app	
Cutteur audio et vidéo	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Chansons bouddhistes (1)	com.bigkidsapps.buddhistsongs1	
Calculatrice	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
Dictionnaire EN-UG gratuit	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
RAPIDE	com.netflix.Speedtest	

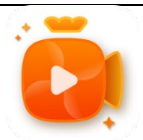
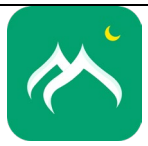
FMWhatsApp	com.fmwhatsapp	
Gestionnaire de fichiers +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Pass Wi-Fi gratuit	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Coran Hefz	com.golap.hefzquran	
Hégire Calendrier	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

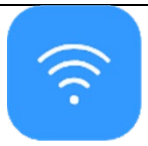
KineMaster	com.nexstreaming.app.kinemasterfree	
Créateur de sonneries et de MP3	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Calculateur de distance cartographique	com.routemap.mapdownload.gpsroute planner	
Récupération de médias	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
Lecteur PDF	pdf.pdfreader.pdfviewer.pdfeditor	

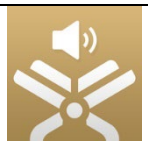
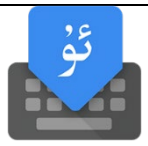
Lecteur PDF	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Éditeur	com.iudesk.android.photo.editor	
Récupération de photos	recover.restore.undelete.photo.video.file	
Studio photo	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Livre de prières	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Coran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restaurer les photos supprimées	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	

Signal Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Sons de bols chantants HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
Clavier SwiftKey	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	

Système de divination tibétain MO	net.rhombapp.mo	
Prière tibétaine	com.chorig.tibetanprayer	
Traducteur AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Clavier ouïghour	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Ouïghour Kirguzguch	com.ziipin.softkeyboard	
Convertisseur vidéo	com.inverseai.video_converter	
Découpeur vidéo	com.naing.cutter	
Téléchargeur vidéo	downloader.video.download.free	

Créateur vidéo	com.bstech.slideshow.videomaker	
Lecteur vidéo pour 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 Enregistreur	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Météo	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	

WhatsApp	com.WhatsApp3Plus	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
Wi-Fi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
Téléchargeur YouTube	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	

Lectures complémentaires

Conseils du Centre australien de cybersécurité

- Signaler un cybercrime, un incident ou une vulnérabilité
- Comment sécuriser vos appareils
- Sécuriser votre téléphone portable
- Hameçonnage
- Escroqueries
- Sécurisez vos réseaux sociaux
- Conseils de sécurité pour les réseaux sociaux et les applications de messagerie

Conseils du NCSC et de la NPSA du Royaume-Uni

- Défendre la démocratie
- Médias sociaux : comment les utiliser en toute sécurité
- Conseils de sécurité des appareils pour les organisations, y compris les appareils mobiles
- Rapport sur les menaces pesant sur les boutiques d'applications.
- Sécurité personnelle des personnes à haut risque

Conseils de la NSA américaine

- Bonnes pratiques pour les appareils mobiles

Clause de non-responsabilité

Veuillez noter que cet avis fournit des informations validées au moment de sa publication.

Ce rapport s'appuie sur des informations provenant d'agences rédactrices et de sources industrielles. Les conclusions et recommandations fournies n'ont pas été formulées dans le but d'éviter tous les risques, et le respect de ces recommandations ne les éliminera pas tous. La propriété des risques liés aux informations reste la propriété du propriétaire du système concerné.

Au Royaume-Uni, ces informations sont exemptées de la loi sur la liberté d'information (Freedom of Information Act-FOIA) de 2000 et peuvent l'être en vertu d'autres lois britanniques sur l'information.

Pour toute question relative à la FOIA, veuillez contacter ncscinfoleg@ncsc.gov.uk.