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

Зөвлөмж

BADBAZAAR ба MOONSHINE: Техникийн шинжилгээ ба эрсдэлийг бууруулах арга хэмжээ

2025 оны **4** сарын **9**

BADBAZAAR болон MOONSHINE: Техникийн шинжилгээ ба эрсдэлийг бууруулах арга хэмжээ

Хураангуй

Их Британий Цахим Холбоо дэмжлэгтэйгээр энэхүү зөвлөгөөг Үндэсний Цахим Аюулгүй Байдлын Төв (NCSC UK) болон олон улсын түншлэл эрхлэн гаргасан болно:

- **Австралийн Радиотехникийн Газрын харьяа Цахим Аюулгүй Байдлын Төв**
- **Харилцаа Холбооны Аюулгүй Байдлын Газрын харьяа Канадын Кибер Аюулгүй Байдлын Төв**
- **Германы Холбооны Тагнуулын Алба**
- **Германы Үндсэн Хуулийг Хамгаалах Холбооны Алба**
- **Засгийн Газрын Харилцаа Холбооны Аюулгүй Байдлын Газрын харьяа Шинэ Зеландын Үндэсний Цахим Аюулгүй Байдлын Төв**
- **АНУ-ын Холбооны Мөрдөх Товчоо**
- **АНУ-ын Үндэсний Аюулгүй Байдлын Агентлаг**

Энэхүү зөвлөмж нь BADBAZAAR болон MOONSHINE гэх хоёр төрлийн тагнуулын программтай холбоотой шинэ болон нэгтгэсэн тагнуулын мэдээллийг хүргэж байгаа бөгөөд хэрэглэгчдээ хамгаалахад дэмжлэг үзүүлэх зорилгоор апп дэлгүүрийн үйл ажиллагаа эрхлэгчид, хөгжүүлэгчид болон олон нийтийн сүлжээний компаниудад зориулсан зөвлөмжүүдийг мөн багтаасан болно.

Энэхүү зөвлөмж нь эдгээр хортой программд өртсөн хохирогчдод зориулсан тусгай зөвлөмжийн хамт нийтлэгдэж байна.

Энэхүү баримт бичигт Үндэсний Цахим Аюулгүй Байдлын Төв (NCSC)-ийн нэр томьёоны тайлбарт өгсөн тагнуулын программ:-ын тодорхойлолтыг ашигласан болно. "Хэрэглэгчийн зөвшөөрөлгүйгээр төхөөрөмжид сууж, мэдээлэл цуглуулж, дараа нь гуравдагч этгээдэд илгээдэг хортой төрлийн программ юм."

Кейс судалгаа нэг: MOONSHINE

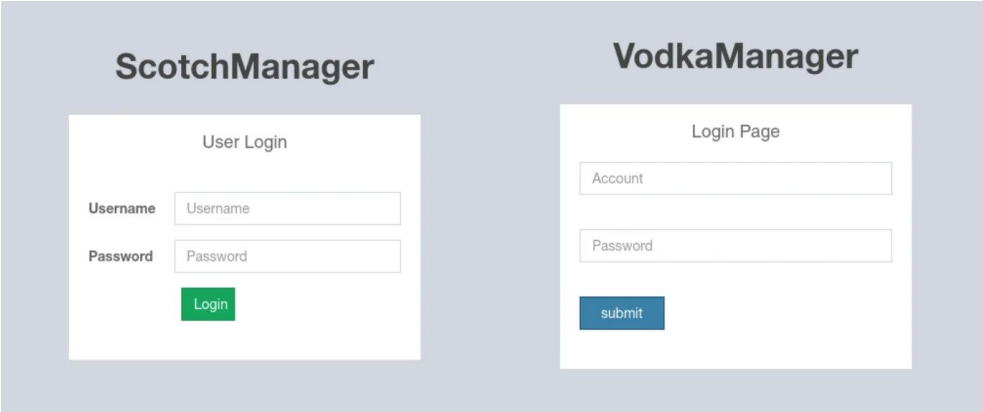
MOONSHINE нь 2019 онд Citizen Lab -н мэдээлснээр Төвдийн бүлэг хүмүүсийг онилсон Android үйлдлийн системд зориулсан тагнуулын программ юм. MOONSHINE нь хохирогчдыг анхаарлыг татаж, төхөөрөмж дээр нь суулгуулах зорилготой жинхэнэ апп шиг харагддаг хортой программ юм. Энэ нь Telegram сувгууд болон WhatsApp-аар дамжуулан холбоос хэлбэрээр тараагдсан байна.
NCSC-ийн MOONSHINE-ийн талаарх судалгаагаар дараах зүйлсийг тогтоожээ:

- MOONSHINE нь анх илэрч мэдээлэгдсэн цагаас хойш өөрчлөгдсөн удирдлагын интерфейс ашиглаж байна.
- Тус удирдлагын интерфэйс нь өргөн хүрээтэй тагнан турших чадвартай болохыг илтгэж байгаа бөгөөд үүнд төхөөрөмжөөс файлуудыг хуулж авах, шууд байдлаар дуу болон дэлгэцийн бичлэг хийх зэрэг боломжууд багтдаг.
- Цахим орчинд байрлах MOONSHINE-ийн удирдлагын интерфейсийн хэд хэдэн багцыг илрүүлсэн байна. Эдгээр удирдлагын интерфейсүүд нь “UPSEC” нэртэй нэвтрэх хуудаснуудад ашиглагддаг дэд бүтэцтэй таарч байгаа бөгөөд Intelligence Online -ийн мэдээлснээр “UPSEC” нь “Sichuan Dianke Network Security Technology Co., Ltd.” компанитай холбоотой гэж үздэг.

Удирдлагын интерфейс

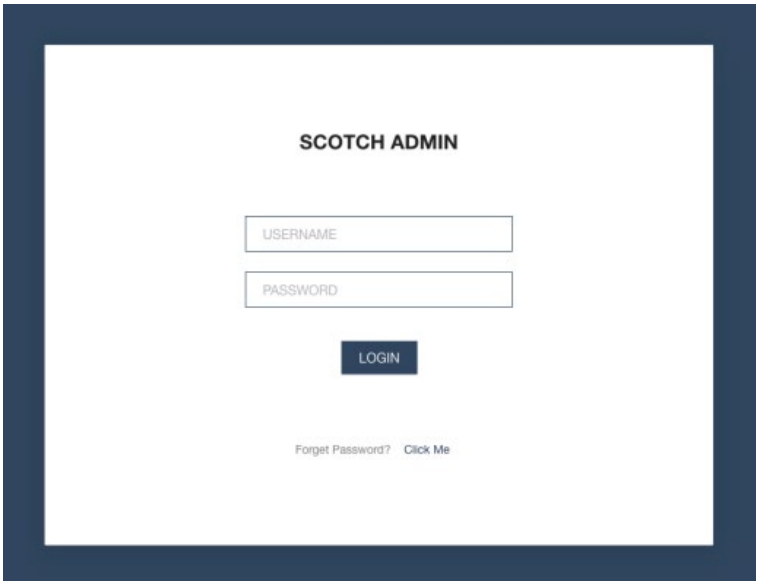
MOONSHINE-ийн удирдлагын интерфейсүүдийн өмнөх тайлангууд түүний хөгжүүлэлт тасралтгүй явагдаж байгааг харуулж байна.

Удирдлагын интерфейсийн анхны жишээ нь Citizen Lab-ийн 2019 оны тайланд гарсан байна.



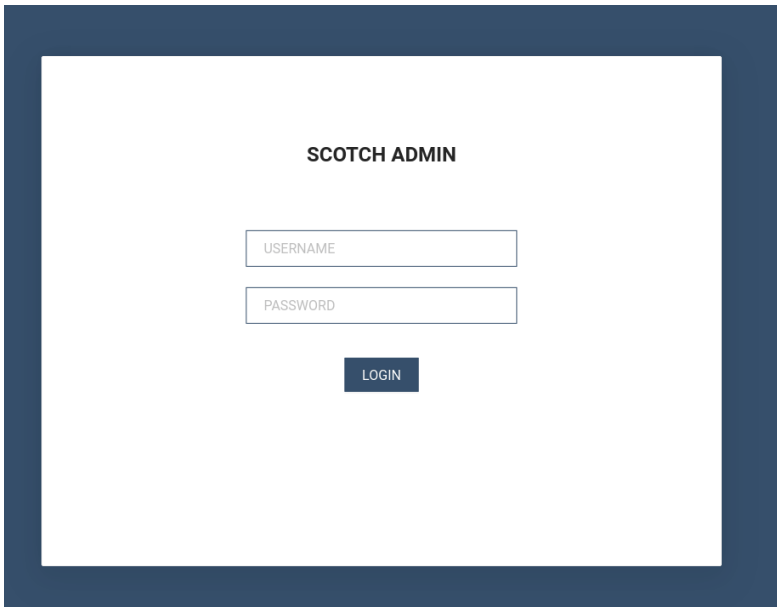
Зураг 1: MOONSHINE-ийн удирдлагын интерфейсүүд нь Citizen Lab-ийн 2019 оны "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits" тайланд гарсан байна.

2022 оны эхээр Lookout нь MOONSHINE-ийн удирдлагын интерфейсийг дахин загварчилсан шинэ хувилбарыг тайлагнасан байна (энэ нь 1-р зураг дахь өмнөх интерфейсүүдийг орложээ):



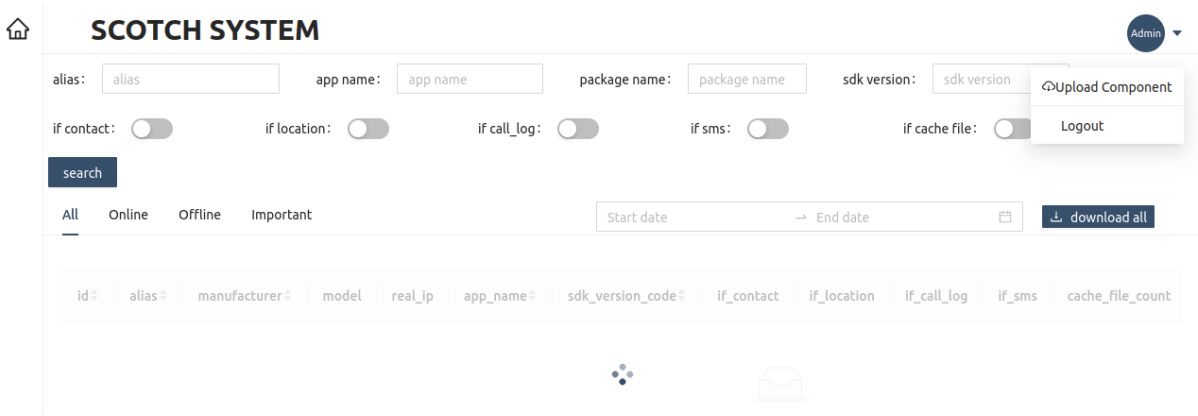
Зураг 2: Lookout компаний 2022 тайланд MOONSHINE удирдлагын интерфейс 'MOONSHINE: Хятадын APT POISON CARP-ийн хөгжүүлсэн Android хяналтын программыг Төвдүүд болон Уйгуруудыг байгаа болгохын тулд хөгжүүлж байна.

2023 оны 8 дугаар сард MOONSHINE команд болон хяналтын (C2) системийн хайлт хийсэн дүн шинжилгээ нь 2022 оны интерфэйстэй төстэй байгааг харуулж байгаа бөгөөд **"Нууц үгээ мартсан"** функц нь одоо байхгүй болсон ба зураг 2-д үзүүлсэн байна:



Зураг 3: 2023 оны 8-р сард MOONSHINE удирдлагын интерфейс нь "Нууц үгээ мартсан" гэсэн сануулгагүй болсон.

Удирдлагын интерфейсийг илүү гүнзгий судлахад уг самбар дотор халдлагад өртсөн төхөөрөмжүүдийн мэдээллийг хэрхэн хадгалахыг харуулсан агуулга илэрсэн байна.



Зураг 4: MOONSHINE удирдлагын интерфейсийн нэвтрэх хуудсын ард байгаа веб хуудас.

Lookout-ийн судалгаа нь хохирогчийн төхөөрөмжөөс MOONSHINE-ийн C2 серверүүд рүү **‘оноо’** дамжуулж байгааг харуулсан байна. ‘Онооны’ үнэлэмж нь хохирогчийн төхөөрөмж дээрх хортой програмын зөвшөөрлүүд дээр үндэслэсэн байна.

Хуудасны “if_contact”, “if_location”, “if_call_log” ба “if_sms” гэсэн баганууд нь MOONSHINE-ний загвар нь халдлагад өртсөн төхөөрөмжүүдэд бүрэн хандаж чадаагүй болохыг харуулж байна. Эдгээр баганууд болон төхөөрөмжөөс C2 сервер рүү дамжуулж буй ‘оноо’ нь цахим халдлага үйлдэгч этгээдүүд тухайн оноог ашиглан хяналтын интерфейсээр дамжуулан халдлагад өртсөн төхөөрөмж дээрх хандалтын түвшнийг харуулж, мэдээлэл авч буй этгээдүүдэд дамжуулж байгааг харуулж байна.

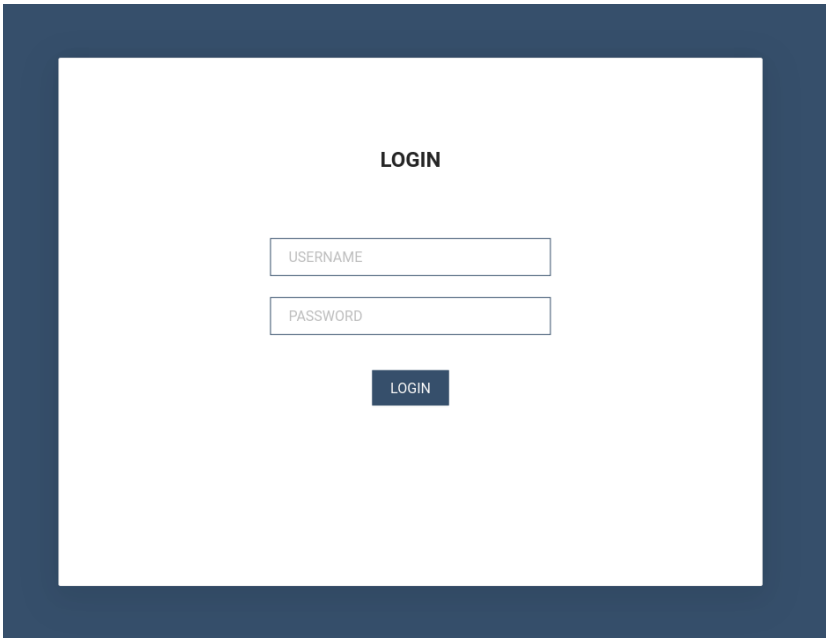
Ерөнхийдөө, аппликейшнүүд төхөөрөмжийн мэдээллийг авахаас урьдчилан сэргийлэхэд туслах хамгийн сайн зөвлөгөө бол татаж авахын өмнө апп-ийн зөвшөөрлүүдийг шалгаж, сэжигтэй зүйл байгаа эсэхийг нягтлах явдал юм. Гэсэн хэдий ч MOONSHINE-ийн хувилбарууд нь аппликейшний хэвийн үйл ажиллагаанд шаардлагатай мэт харагдах зөвшөөрлүүдийг асуудаг тул хэрэглэгчийн сэжиг төрүүлэхгүй байж болох бөгөөд уг зөвшөөрлүүдийг ашиглан төхөөрөмжөөс мэдээлэл хулгайлах боломжтой болгодог.

MOONSHINE нь мөн түүний цар хүрээг илтгэдэг Программ хангамжийн интерфейс (API)-тэй. API-ийн анхны хувилбарууд дээр API нэрс нь Хятад хэл дээр бичигдсэн байжээ.

Виртуал хостууд

MOONSHINE удирдлагын самбаруудыг хайх явцад виртуал сервер дээр байрлуулсан хэд хэдэн тохиолдлууд илэрсэн. Виртуал хостинг гэдэг нь нэг IP хаяг дээр нэгэн зэрэг олон вебсайт байрлуулахыг хэлдэг. Эдгээр виртуал хостинг хийсэн IP хаягууд болон домэйнүүд нь одоогоор танигдсан байгаа хортой программын загварууд дээр илрээгүй байна.

Эдгээр удирдлагын интерфейсийн хувилбарууд нь өмнө нь байсан '**SCOTCH ADMIN**' гэсэн нэрийн оронд '**LOGIN**' гэсэн гарчигтай байв.



Зураг 5: MOONSHINE-ийн удирдлагын интерфейс нь 'SCOTCH ADMIN' биш, 'LOGIN' гарчгийг ашигласан байна.

Түүнчлэн, удирдлагын самбар дээрх агуулга нь 4-р зургаас ялгаатай бөгөөд үүнийг 6-р зурагт харуулжээ:

Зураг 6: Виртуал хостинг ашигласан MOONSHINE удирдлагын интерфейсийн нэвтрэх хуудасны ард байгаа вэб хуудсаны дүрслэл.

6-р зурган дээрх хянах самбар нь 4-р зурган дээрх хянах самбарын багасгасан хувилбар мэт харагдаж байна. Хянах самбарын давхцаж буй хэсэг нь хүснэгтэд байгаа 'id' (таних дугаар), 'manufacturer' (үйлдвэрлэгч) болон 'model' (загвар) гэсэн баганууд юм.

Одоогоор илэрсэн виртуал хостинг хийсэн MOONSHINE-ийн тохиолдлууд нь дараах байна:

Домэйн	IP хаяг
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

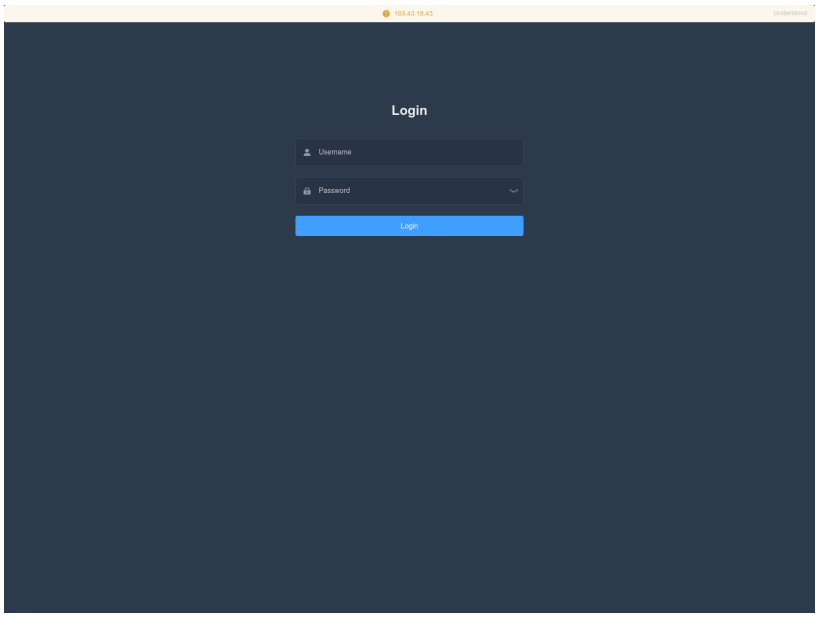
Эдгээр домэйнуудыг Trend Micro компани MOONSHINE ашиглагдахуун гэж тодорхойлсон бөгөөд эдгээр нь гар утасны төхөөрөмжүүдэд хортой программ суулгахын тулд веб хөтөчийн аюулгүй байдлын сул талыг ашигладаг. Trend Micro энэ хортой программыг 'Dark Nimbus' гэж нэрлэсэн.

Тодруулбал, MOONSHINE-ийн удирдлагын интерфейс гэдэг нь MOONSHINE хортой программын загварууд холбогдож хохирогчийн мэдээллийг авдаг хэсэг юм. Trend Micro байгууллагын тайлагнасан MOONSHINE ашиглагдахуун гэдэг нь гар утасны төхөөрөмжүүд дээр Dark Nimbus хэмээх хортой программыг суулгахад веб хөтөчийн сул талыг ашигладаг тусдаа чадвар юм. Мөн Dark Nimbus ба MOONSHINE нь өөр өөр төрлийн, тусдаа хортой программууд юм.

MOONSHINE-ийн удирдлагын интерфейс болон MOONSHINE ашиглагдахууны код нь хоорондоо давхцдаг тул 3 болон 5-р зургууд дахь ижил төстэй нэвтрэх хүсэлтүүд болон 4 болон 6-р зургууд дахь хуудсны агуулга нь төстэй байна. Мөн хоёулангийнх нь эх кодонд 'webpackJsonpreact-scotchui' гэсэн мөр байдаг.

Цахим халдагчид MOONSHINE ашиглагдахуунтай холбогддог URL холбоосуудыг үүсгэж, дараа нь Төвд болон Уйгур хүмүүстэй холбоотой видеог үзүүлдэг бөгөөд энэ нь MOONSHINE-ийн зорилтот бүлэгтэй давхцаж байна.

MOONSHINE ашиглагдахууны домэйнүүдийг байршуулж буй олон IP хаяг дээр 444 порт дээр ‘VLiteUI’ нэртэй нэвтрэх хуудасны хэсэг байдаг. Энэхүү хуудас нь өргөн хүрээнд ажиглагддаггүй бөгөөд эдгээр IP хаягууд дээр байгаа нь цахим халдагчдын үйл ажиллагаатай холбоотой байж болзошгүй гэж үзэж байна.



Зураг 7: MOONSHINE ашиглагдахууныг хостолдог IP хаягууд дээр 'VLiteUI' гэсэн HTML гарчигтай нэвтрэх хяналтын самбар ажиглагдсан байна.

Trend Micro-ийн Dark Nimbus хортой программыг судлах дүн шинжилгээгээр уг программ нь төхөөрөмжийн мэдээллийн бүрэн жагсаалтыг цуглуулж, XMPP протокол ашиглан C2-той холбогддог болохыг тогтоожээ.

Trend Micro мөн Dark Nimbus-ийн зарим хувилбаруудад ‘DKNS’ гэсэн тэмдэгт олныг илэрсэн гэж тэмдэглэсэн байна.

‘ansec[.]com’ (TrendMicro-аас Dark Nimbus C2 гэж бүртгэсэн) нь DKNS гэсэн гарчигтай веб хуудсуудыг ажиллуулдаг бусад IP хаягуудын XMPP үйлчилгээнд мөн ажиглагдсан.

- DKNS Android远程取证系统 (DKNS Android Алсын Шүүх Шинжилгээний Систем)
- DKNS云网侦控平台 (DKNS Үүлэн Сүлжээний Судалгаа ба Хяналтын Платформ)
- DKNS云网侦控平台 (DKNS Үүлэн Сүлжээний Судалгаа ба Хяналтын Платформ)
- DKNS远程控制侦查系统 (DKNS Алсын Удирдлагатай Мөрдөн Шалгах Систем)

XMPP үйлчилгээний ' **ansec[.]com**' бүхий өөр нэг IP хаяг нь дараах гарчигтай веб хуудастай байсан:

- UPSEC互联网控制指挥系统 (UPSEC Интернэт Хяналтын Командын Систем)
- UPSEC无线侦控系统 (UPSEC Утасгүй Тандалт ба Хяналтын Систем)
- UPSEC重点人数据还原系统(UPSEC Гол Хүний Мэдээллийг Сэргээх Систем)

Intelligence Online-н дагуу "UPSEC" 'Sichuan Dianke Network Security Technology Co., Ltd'-д] хамааралтай нь HTML хуудасны гарчигт илэрсэн байна.

Кейс судалгаа хоёр: BADBAZAAR

BADBAZAAR нь iOS ба Android хувилбартай гар утасны хортой программ бөгөөд Уйгур, Төвд болон Тайваний иргэдийн эсрэг чиглэн халддаг байна. Энэхүү хортой программ нь олон нийтийн мэдээллийн сүлжээний платформ болон албан ёсны апп дэлгүүрээр тархсан. Сүүлийн үеийн Volexity-ийн мэдээллээр BADBAZAAR-ийн хэд хэдэн төрөл байдгийг тогтоосон бөгөөд тэдгээрийг BadSolar, BADBAZAAR болон BadSignal гэж ялгадаг. Эдгээр гурван хувилбарууд нь төхөөрөмж болон операторын мэдээлэл цуглуулахад ашиглагддаг давхцсан үйлдлүүдээр хоорондоо холбогддог.

NCSC-ийн BADBAZAAR-д хийсэн судалгаагаар дараах зүйлийг илрүүлсэн:

- C2 домэйнүүдийг бүлэглэхэд өмнө хадгалагдсан эрсдлийн тагнуулын тайланд дурдсан бусад домэйнүүдтэй холбоо илэрдэг.
- C2 серверүүд болон хортой программын загварууд нь цахим халдагчдын дэд бүтцэд холбоотой хост нэрсийг харуулж байна.
- Халдагчид албан ёсны апп дэлгүүрүүдээс гадуур хортой программ тараахдаа ашигладаг нэмэлт сошиал инженерчлэлийн профайлүүд.

WHOIS кластер / домэйн брокер

'UJYJYUJ'

BADBAZAAR домэйн **‘signalplus[.]org’**-ын WHOIS бүртгэлийн шинжилгээнээс (ESET-ээр мэдээлсэн) **‘State’** талбарт **‘UJYJYUJ’** утга байгааг харуулж байна.

Ижил утгатай бусад домэйнуудыг хайхад дараах чухал домэйнууд илэрсэн байна:

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

(Хавсралт A, 1-р зургийг үзнэ үү)

Signplus[.]org , **tubevideoplus[.]org** болон **thetubeplus[.]com** домайнуудыг BADBAZAAR C2 домэйн гэж мэдээлдэг бол ESET нь **mail.pmumail[.]com дэд домайныг** FlyGram прокси сервер гэж мэдээлдэг. FlyGram нь цахим гэмт этгээдүүдийн боловсруулсан BADBAZAAR төрлийн аппликейшн юм (бусад BADBAZAAR аппуудын жагсаалтыг хавсралтаас үзнэ үү).

Компьютерын гар дээр дараалсан үсэг, тоо, тэмдэгтэн утгууд

NCSC нь бүртгэлтэй бусад BADBAZAAR C2 домэйнуудад ижил төрлийн “keyboard walking” (компьютерын гарын товчлууруудыг дарааллуулан дарсан мэт санамсаргүй тэмдэгтүүд) хэв маягийг ажигласан байна.

Жишээ нь, доорх домэйнууд бүгд **‘REWR’** утгыг ‘**State’** талбарт агуулж байгааг ажигласан (өмнө нь ашиглаж байсан):

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

(Хавсралт А, 2-р зургийг үзнэ үү)

‘FSDF’ гэсэн утгатай State талбартай домэйнууд:

BADBAZAAR-ийн өөр нэг C2 домэйнуудын **‘State’** талбарт **‘FSDF’** утга байна:

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

(Хавсралт А, 3-р зургийг үзнэ үү)

“Keyboard walking” утгууд бүхий хадгалагдсан тайлан

BADBAZAAR домэйнуудын WHOIS бүртгэлд ашиглагдсан “keyboard walking” утгуудыг өмнө нь TA413 байгууллагын Төвдийн байгууллагууд руу чиглэсэн довтолгоонд хэрэглэсэнтэй холбон харж болно. Recorded Future байгууллагаас халдагчдын хяналтад байдаг зарим домэйнууд Төвдийн байгууллагуудыг хуурч дуурайсан бөгөөд бүртгүүлэгч байгууллагын утгыг “asfasf” гэж тохируулсан тохиолдлуудыг ажигласан байна.

clublogs[.]com

Lookout-аас олж авсан BADBAZAAR загварт C2 домэйнтэй ижлээр '**xle.clublogs[.]com**' орсон байна. **‘clublogs[.]com**' үндсэн домэйн нь '**95.179.210[.]85**' IP хаяг дээр байрладаг бөгөөд '**CN=WIN-50QO3EIRQVP**' субъект болон олгогчийн утгатай SSL сертификаттай байсан. Энэ утга нь BADBAZAAR загварууд дээр олдсон SSL гэрчилгээнүүдтэй таарч, холбоог тасалдуулахаас сэргийлэх үүднээс SSL хадах замаар ашигласан байна.

95.179.210[.]85 IP хаягийн хостинг түүх нь дараах чухал домэйнүүдийг харуулсан байна:

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

(Хавсралт А, 4-р зургийг үзнэ үү)

www.voiceoftibet[.]net

'www.voiceoftibet[.]net' домэйн нь TA413-ын ашигладаг TTP-тэй адил 'Төвдийн дуу хоолой' радио станцын дүр эсгэж байж болзошгүй юм.

'rewrwer[.]com' домэйн нь BADBAZAAR домайнуудын WHOIS бүртгэлээс олдсон өмнө нь тодорхойлсон '**State**' утгатай '**REWR**' -тэй төстэй юм.

'clublogs[.]com', '**rewrwer[.]com**', '**voiceoftibet[.]net**' болон ' **myloughborough[.]com** ' домэйнууд бүгд '**tplutalova@list[.]ru**' и-мэйл хаягаар бүртгэгдсэн .

actuallys[.]com

'facts[.]com' -ын WHOIS бүртгэлд технологийн болон админ имэйл хаягууд нь '**tplutalova@list[.]ru**' байсан ч бүртгүүлэгчийн имэйл нь '**ivan_s81@mail[.]ru' байсан** жишээг харуулсан.

'actuallys[.]com' домэйнд холбогдох түүхэн WHOIS бүртгэлд 2016 оны 2-р сарын 24-нд бүртгэгдсэн имэйл хаяг нь '**wangminghua6@gmail[.]com'** байсан нь илэрсэн байна 2016 оны 3-р сарын 11-нд уг имэйл хаяг **'ivan_s81@mail.ru'** болгон өөрчлөгдсөн боловч бүртгүүлэгчийн бүртгэл дуусах огноо нь хэвээр үлдсэн байна.

wangminghua6@gmail[.]com

Имэйл хаяг '**wangminghua6@gmail[.]com**' бүртгэгдсэн цахим тагнуулын тайланд олдсон домайнуудыг бүртгэхэд ашиглагдсан. 2015 онд Palo Alto компани Cmstar хортой программын C2 домэйнуудыг бүртгүүлэхэд ашиглагдсан имэйл хаягийг илрүүлсэн байна. 2014 онд мөн энэ имэйл хаягийг Mandiant байгууллагын илрүүлсэн APT3 бүлгийн явуулсан фишинг халдлагын домэйнуудыг бүртгүүлэхэд ашигласан байна. 2013 онд уг имэйл хаягийг CrowdStrike байгууллагын илрүүлсэн, Хятад үсэг бүхий Program Database (PDB) хортой программ тараагчийн (malware dropper)

домэйнуудыг бүртгүүлэхэд ашигласан байна. Энэ нь хортой программыг Хятадын систем дээр боловсруулсан болохыг илтгэж байна.

taoyujun@gmail[.]com

‘hcjbtt[.]com’ домэйн нь ‘**taoyujun@gmail[.]com’** и-мэйл хаягаар бүртгэгдсэн боловч администраторын имэйл нь ‘**wangminghua6@gmail[.]com’** хаягаар бүртгэгдсэн байна.

‘hcjbtt[.]com’ домэйнтэй холбоотой ямар ч хортой үйл ажиллагаа байхгүй ч ‘**taoyujun@gmail[.]com’** имэйл хаяг аюулын талаарх тагнуулын түүхэн тайланд олдсон байна. 2014 онд уг имэйл хаягийг Mandiant-ын илрүүлсэн, Японы байгууллагуудыг чиглэсэн халдлагад ашиглагдсан **‘Cueisfry Trojan’** загвар бүхий домэйнийг бүртгүүлэхэд ашигласан байна.

Уг имэйл хаяг нь мөн **‘iaea-international[.]org’** домэйнийг бүртгүүлсэн бөгөөд энэ нь **Олон Улсын Цөмийн Эрчим Хүчний Агентлаг** (International Atomic Energy Agency)-ын нэрийг дуурайлган ашигласан бол **‘idc-ctbto[.]org’** домэйн нь **Цөмийн Туршилтыг Бүрэн Хориглох Гэрээний Байгууллага (CTBTO)-**ын **Олон Улсын Мэдээллийн Төвийн** нэрийг дуурайлган ашигласан байна.

‘iaea-international[.]org’ домэйний өмнөх Whois бүртгэлд бүртгүүлэгчийн имэйл хаяг нь **‘wangminghua6@gmail[.]com’** гэж бүртгэгдсэн байсан байна.

udtglobals[.]com

‘udtglobals[.]com’ домэйнд администратор имэйл хаяг болгон **‘wangminghua6@gmail[.]com’**, бүртгүүлэгчийн имэйл хаяг болгон **‘ocean.nio@rediffmail[.]com’** ашигласныг ажигласан байна. Энэхүү домэйнд холбогдох бусад WHOIS бүртгэлүүдэд бүртгүүлэгчийн имэйл хаяг ижил байсан бөгөөд администраторын имэйл хаяг нь **‘taoyujun@gmail[.]com’** байжээ.

‘udtglobals[.]com’ нь далайн доорх хамгаалалтын болон аюулгүй байдлын салбарын дэлхийн арга хэмжээ болох ‘**UDT Global**’ -ыг дуурайлган ашигласан болохыг илтгэж байна. Имэйл хаяг дахь " **ocean.nio** " хэрэглэгчийн нэр нь олон улсын **Далай судлалын үндэсний хүрээлэнг (NIO)** дуурайсан байж магадгүй юм. Энэтхэгт байрладаг **‘Rediff’** имэйл үйлчилгээний ашиглалт нь **Энэтхэгийн Үндэсний Далайн Судалгааны Институтыг** дуурайлгасан байж болзошгүйг харуулж байна.

Djibdiplomatie[.]com

‘djibdiplomatie[.]com’ домэйн нь Жибути улсын гадаад харилцааны байгууллагыг дуурайлган ашигласан байх магадлалтай бөгөөд түүний WHOIS бүртгэл нь

‘udtglobals[.]com’ домэйнтэй төстэй байсан байна. Нэгэн бүртгэлд бүртгүүлэгчийн имэйл хаяг нь **‘ocean.nio@rediffmail[.]com’**, администраторынх нь **‘taoyujun@gmail[.]com’** гэж тэмдэглэгдсэн бол, бусад бүртгэлүүдэд администраторын имэйл хаяг нь ‘**wangminghua6@gmail[.]com’**, харин бүртгүүлэгчийнх нь ‘**ocean.nio@rediffmail[.]com’** гэж тус тус бүртгэгдсэн байна.

Эдгээр хоёр домэйнд мөн WHOIS бүртгэлд "keyboard walking" төрлийн утгууд (гарын товчлууруудыг дараалуулан дарсан мэт санамсаргүй тэмдэгтүүд) илэрсэн байна. Жишээлбэл, **‘udtglobals[.]com’** домэйний бүртгүүлэгчийн хотын талбарт **‘ASDF’** гэж, харин **‘djibdiplomatie[.]com’** домэйний бүртгүүлэгчийн нэрийн талбарт **‘DAF DAGF’** гэж бичигдсэн байсан нь "keyboard walking" буюу гарын дараалалтай товчлол ашигласан шинжтэй байна. Энэ нь бусад BADBAZAAR домайнуудад ажиглагдсан утгуудтай харьцуулах боломжтой юм.

‘wangminghua6@gmail[.]com’ болон **‘taoyujun@gmail[.]com’** имэйл хаягууд нь **дэлхийн далайн доорх батлан хамгаалахын арга хэмжээ**, **Жибути улсын гадаад харилцааны байгууллага**, мөн **Олон Улсын Цөмийн Эрчим Хүчний Агентлагийг** дуурайлган бүртгүүлсэн домэйнуудын WHOIS бүртгэлд илэрсэн хэдий ч, эдгээр хаягууд нь хортой шинжгүй олон домэйний WHOIS бүртгэлд ч мөн илэрч байна.

Дуурайлгасан домэйнууд болон хортой бус домэйнуудыг хослуулан ашигласан байдал нь хортой цахим халдлага үйлдэгчдийг дэмжих зорилготой, дэд бүтцийг бүрдүүлж хангадаг тусгай байгууллага эсвэл оролцогч байж болзошгүйг харуулж байна.

‘ocean.nio@rediffmail[.]com’ имэйл хаяг нь зөвхөн дээр дурдсан дуурайлгасан домэйнуудад л илэрсэн байна. Харин **‘ivan_s81@mail[.]ru’** болон **‘tplutalova@list[.]ru’** хаягууд нь тус бүр цөөн тооны домэйн бүртгүүлсэн бөгөөд зарим нь BADBAZAAR хортой программын дэд бүтцэд байршуулсан байжээ. Эдгээр гурван цахим шуудангийн хаяг нь цахим гэмт этгээдүүдийн үйл ажиллагаатай илүү нягт холбоотой гэж үздэг. Учир нь тус имэйл хаягуудтай холбогдсон домэйнуудын тоо цөөн боловч хортой үйл ажиллагаатай холбоотой байдал нь харьцангуй өндөр бөгөөд энэ нь **‘wangminghua6@gmail[.]com’** болон **‘taoyujun@gmail[.]com’**. хаягуудтай харьцуулахад илүү ноцтой холбоог харуулж байна.

(Хавсралт А, 5-р зургийг үзнэ үү)

Бусад цахим халдагчийн холбоосууд

BADBAZAAR-тэй холбоотой **‘actuallys[.]com’**, **‘clublogs[.]com’**, **‘myloughborough[.]com’**, **‘rewrwer[.]com’** болон **‘voiceoftibet[.]net’** зэрэг

домэйнуудын нийтлэг нэг онцлог нь бүгд **eNom** бүртгүүлэгчээр дамжуулан бүртгэгдсэн бөгөөд бүгдийг нь **‘255.255.255[.]254’** IP хаягт байршуулсан байсан явдал юм.

Өмнөх NCSC-ийн мөрдөн шалгалтуудын үр дүнд эдгээр ижил шинж чанартай бусад домэйнууд нь 2019 онд **APT5**, мөн 2009–2011 оны хооронд **APT14** бүлэглэлтэй холбоотой үйл ажиллагаанд ашиглагдаж байсан нь илэрсэн байна.

APT5-тэй холбоотой домэйнуудын түүхэн WHOIS бүртгэлүүдэд бүртгүүлэгчийн имэйл хаяг болгон **‘taoyujun@gmail[.]com’** хаяг бичигдсэн байдаг байна.

APT14-тэй холбоотой домэйнууд нь гурван үсэгтэй дэд домэйнүүдийг ашигладаг байсан бөгөөд эдгээр нь тэдний халдлагын байг илтгэдэг байжээ. Үүний жишээ нь ‘**bae.cisconline[.]net’** бөгөөд энэ нь BAE Systems компанийг чиглэсэн байж болохыг харуулж, ‘**Poison Ivy**’ гэдэг хортой программын загвараас илэрсэн байна.

BADBAZAAR домэйнуудад мөн ижил төстэй шинж тэмдэг ажиглагддаг бөгөөд дэд домэйнүүд нь халдлагад өртсөн аппликейшний нэртэй холбоотой байдаг.

Аппликейшны нэр	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

APT5 болон APT14-тэй холбоотой үйл ажиллагаа нь өмнө бүртгэгдсэн бөгөөд эдгээрээс гадна eNom-д бүртгэгдсэн, **‘255.255.255.254’** IP хаягт холбогдсон ч хортой үйл ажиллагаатай холбоогүй бусад домэйнууд ч мөн байдаг болохыг онцлох нь чухал юм. Тиймээс эдгээр кампанит ажлын ард буй этгээдүүд ижил эсвэл хоорондоо холбоотой эсэх нь тодорхойгүй байна.

Системийн нэрс

BADBAZAAR-ын C2 серверүүд болон дээжүүдийн шинжилгээ нь SSL гэрчилгээнд ‘Common Name’ утгаар ашиглагдсан хост нэрсийг илрүүлсэн байна. NCSC-ын BADBAZAAR загваруудад болон дэд бүтцэд илэрсэн хост нэрсийг судлахад эдгээр хост

нэрс нь олон IP хаяг дээр ашиглагдаж байгааг тогтоожээ. Эдгээр IP хаягууд нь BADBAZAAR загваруудаас олдсон домэйнуудыг байршуулж байна. Доорх хэсэгт BADBAZAAR C2 домэйныг байршуулсан хостын нэр болон IP хаягуудын талаар дэлгэрэнгүй мэдээлэл байна.

Олон тохиолдолд, SSL гэрчилгээний хост нэрсийн утга нь тухайн хортой домэйн нэрсийн IP хаягуудтай давхцдаг ба гэрчилгээ болон IP хаяг давхцахгүй тохиолдлуудыг тусгайлан тэмдэглэсэн болно.

WIN-EU0VLBL7TUJ

‘WIN-EU0VLBL7TUJ’ хост нэрийг дараах IP хаягууд дээр илрүүлсэн байна:

- **‘116.203.53[.]21’** IP хаяг нь BADBAZAAR C2 домэйнууд болох **‘uyapkfinder[.]com’** болон **‘thewestuniverse[.]com’**-ыг байршуулсан байна.
- **‘95.216.169[.]27’** IP хаяг нь BADBAZAAR C2 домэйн болох ‘**adysfunction[.]com’**-ыг болон BADBAZAAR загварын татаж авах холбоосоор ашиглагдсан **‘download.apkbazar[.]biz’** дэд домэйнийг байршуулсан байна.

(Хавсралт А, зураг 6-г үзнэ үү)

WIN-70E59JVOB9G

‘WIN-70E59JVOB9G’ хост нэрийг дараах IP хаягууд дээр илрүүлсэн байна:

- **‘23.88.28[.]220’** IP хаяг нь BADBAZAAR C2-ийн дараах дэд домэйнүүд болох **‘aua.rondwsign[.]com’**, **‘nal.tokenmajorp[.]com’**, **‘pep.rondwsign[.]com’**, **‘doa.rondwsign[.]com’**, болон **‘pls.rondwsign[.]com’**-ыг байршуулсан байна. Тухайн систем дээрх гэрчилгээг хамгийн сүүлд харсан хугацаа болон хортой домэйнууд анх тус IP хаяг руу холбогдож эхэлсэн хугацааны хооронд хоёр хоногийн зөрүү байсан байна.

- **‘23.88.28[.]221’** IP хаяг нь BADBAZAAR-тэй холбоотой **‘bt.bhvghg[.]com’** дэд домэйнийг байршуулсан байна.

- **‘23.88.28[.]222’** IP хаяг нь BADBAZAAR C2 домэйн болох **‘tubevideoplus[.]org’** болон **‘cde.mpoxcases[.]com’**-ыг байршуулсан байна.

- **‘65.21.92[.]67’** IP хаяг нь BADBAZAAR C2 дэд домэйн **‘bat.androidupdated[.]net’**-ийг байршуулсан байна. Мөн энэ нь **‘apps.androidupdated[.]net’** дэд домэйнийг байршуулсан бөгөөд энэ нь DoubleAgent хортой программын C2 сервер юм.

- **‘65.21.92[.]77’** IP хаяг нь BADBAZAAR C2-ийн дэд домэйнүүд болох **‘wyo.titeperformance[.]com’, ‘big.collinformations[.]com’, ‘vpf.titeperformance[.]com’, ‘eud.titeperformance[.]com’** болон **‘afg.collinformations[.]com’**-ыг байршуулсан байна.

- **‘65.108.192[.]134’** IP хаяг нь BADBAZAAR C2-ийн дэд домэйнүүд болох **‘upd.whoscaller.net’** болон **‘ggl.whoscaller[.]net’**-ийг байршуулсан байна.

- **‘142.132.131[.]15’** IP хаяг нь BADBAZAAR C2-ийн дэд домэйнүүд болох **‘bvn.lookincategory[.]com’** болон **‘edr.lookincategory[.]com’**-ыг байршуулсан байна. Системийн нэр бүхий гэрчилгээ сүүлд ажиглагдсан өдрөөс эхлээд, хортой домэйнууд анх тухайн IP хаяг руу холбогдож эхэлсэн өдрийг хүртэл 11 хоногийн завсар хугацаа байсан.

- **‘142.132.131[.]20’** IP хаяг нь **‘son.onlinegamersgroup[.]com’** болон **‘system.onlinegamersgroup[.]com’** дэд домэйнүүдийг байршуулсан бөгөөд эдгээр нь BADBAZAAR-ийн C2 серверүүд байж болзошгүй юм, учир нь энэ IP дээр BADBAZAAR-тай холбогдсон SSL гэрчилгээнүүд ажиглагдсан байна.

- **‘142.132.131[.]28’** IP хаяг нь BADBAZAAR-ийн C2 домэйн **‘goldplusapp[.]net’** болон түүний дэд домэйн **‘who.goldplusapp[.]net’** ба **‘cgf.goldplusapp[.]net’**-г байршуулсан байна.

- **‘162.55.103[.]211’** IP хаяг нь BADBAZAAR-ийн C2 дэд домэйнүүд болох **‘oha.alpinemap[.]net’, ‘aru.alpinemap[.]net’, ‘aso.alpinemap[.]net’, ‘afr.alpinemap[.]net’,** болон **‘aar.alpinemap[.]net’**-г байршуулсан байна.

- **‘162.55.103[.]212’** IP хаяг нь BADBAZAAR C2 дэд домэйнууд болох **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** болон **‘aua.rondwsign[.]com’**-ыг байршуулжээ.

- **‘195.154.47[.]99’** IP хаяг нь BADBAZAAR C2 дэд домэйнууд болох **‘ggl.whoscaller[.]net’** болон **‘upd.whoscaller.net’**-ыг байршуулсан байна. Системийн нэртэй гэрчилгээг анх ажиглагдсан өдрөөс эхлэн, хортой домэйнууд сүүлд уг IP хаяг руу заагдсан өдрийг хүртэл гурван өдрийн хугацаа өнгөрсөн байна.

- ‘**195.154.60[.]3’** IP хаяг нь BADBAZAAR-ийн C2 дэд домэйнүүд **болох ‘upd.whoscaller[.]net’** ‘**ggl.whoscaller[.]net**’ байршуулсан.

- **‘212.83.189[.]89’** IP хаяг нь BADBAZAAR-ийн C2 дэд домэйнүүд болох **‘wyo.titeperformance[.]com’, ‘eud.titeperformance[.]com’, ‘vpf.titeperformance[.]com’** болон **‘afg.collinformations[.]com’**-ыг байршуулсан.

- ‘**212.129.21[.]168’** IP хаяг нь BADBAZAAR-ийн C2 домэйнүүд болох **‘fre.lookincategory[.]com’, ‘tgr.lookincategory[.]com’, ‘fgt.lookincategory[.]com’, ‘luj.lookincategory[.]com’** болон **‘bvn.lookincategory[.]com’**-ыг байршуулсан.

(Хавсралт А, зураг 7-г үзнэ үү)

WIN-50QO3EIRQVP

Дараах IP хаягууд дээр ‘**WIN-50QO3EIRQVP**’ хостын нэр ажиглагдсан**:**

- **’45.76.132[.]91’** IP хаяг нь **‘yumoftion[.]com’** болон **‘androidupdated[.]net’** домэйныг байршуулсан байна. Эдгээр хоёр домэйн BADBAZAAR-тай холбоотой бөгөөд ‘**fow.yumoftion[.]com’** болон **‘bat.androidupdated[.]net’** гэсэн дэд домэйнүүд нь BADBAZAAR C2 серверүүд юм. Нэмж хэлэхэд, ‘**apps.androidupdated[.]net’** дэд домэйн нь DoubleAgent хортой

программын C2 сервер юм. Мөн **‘pmstwocqn[.]com’** домэйн хаягийг хост хийдэг бөгөөд энэ нь WHOIS бүртгэлээр BADBAZAAR-тай холбогдсон байна.

- **‘95.179.210[.]85’** IP хаяг нь **‘clublogs[.]com’** домэйнийг хостолдог ба үүн дотроос **‘xle.clublogs[.]com’** нь BADBAZAAR C2 домэйн юм. Мөн энэ IP дээр BADBAZAAR-тай холбогдсон ‘**bre.myloughborough[.]com’, ‘img.rewrwer[.]com’, ‘www.voiceoftibet[.]net**’ болон ‘**actuallys[.]com’** зэрэг домэйнуудыг байршуулсан байна.

- **‘199.247.21[.]34’** IP хаяг нь **‘titeperformance[.]com’** болон **‘collinformations[.]com’** домэйнийг хостолдог бөгөөд эдгээр домэйний дэд домайн-ууд нь BADBAZAAR C2 домэйнууд юм.

- **‘217.69.10[.]128’** IP хаяг нь BADBAZAAR C2 домэйн **‘uyghurdict[.]com’**-ыг хостолдог.

(Хавсралт A, 8-р зургийг үзнэ үү)

WMSvc-WIN-50QO3EIRQVP

‘WMSvc-WIN-50QO3EIRQVP’ хост нэр нь дараах анхаарал татах IP хаягууд дээр ажиглагдсан:

- **’78.46.185[.]251’** IP хаяг нь Volexity-аас мэдээлсэнээр порт 4432-оор халдлагын холболт хийдэг BADBAZAAR C2 домэйн **‘groupgram[.]org’**-ыг байршуулсан байна.

- **‘65.21.92[.]69’** ба **‘163.172.205[.]207’** IP хаягууд нь **‘widelygram[.]org’** домэйнийг байршуулсан бөгөөд энэ нь BADBAZAAR C2 домэйн байж болзошгүй гэж үзэж байна. Учир нь эдгээр IP дээр байрлаж байх үед 4432 порт нээлттэй байжээ.

- **‘163.172.198[.]206’** IP хаяг нь **‘maxgram[.]org’** домэйнийг байршуулсан бөгөөд энэ нь BADBAZAAR C2 домэйн байж болзошгүй юм. Учир нь байршуулж байх үед 4432 порт нээлттэй байсан байна.

(Хавсралт A, 9-р зургийг үзнэ үү)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

‘WMSvc-WIN-50QO3EIRQVP’ ба ‘**WIN-7LSBB9R0F1L’** нэртэй хост нэрүүд дараах IP хаяг дээр зэрэгцэн ажиглагдсан байна:

- ‘**148.251.87[.]245’** IP хаяг нь BADBAZAAR-ын C2 домэйн болох **‘flygram[.]org’** болон **‘groupgram[.]org’**-ыг хостолдог байна.

(Хавсралт A, 10-р зургийг үзнэ үү)

WIN-N8H8S9BG2P0

‘WIN-N8H8S9BG2P0’ хост нэр дараах IP хаяг дээр ажиглагдсан:

- **‘148.251.87[.]247’** IP хаяг нь BADBAZAAR C2 домэйнүүд болох **‘omarwhatsapp[.]org’** ба **‘flygram[.]org’**-ийг байрлуулсан байна.

(Хавсралт A, 11-р зургийг үзнэ үү)

WIN-I6VBN8MR92A

‘WIN-I6VBN8MR92A’ хост нэр дараах IP хаяг дээр ажиглагдсан:

- **‘148.251.87[.]197’** IP хаяг нь BADBAZAAR C2 домэйн **‘tryhrwserf[.]com’**-ийг байршуулсан байна.

(Хавсралт A, 12-р зургийг үзнэ үү)

Ил байгаа худалдааны мэдээллээр энэхүү системийн нэрсийн интернет дэх тархалт харилцан адилгүй байна. Тэдгээрийн заримыг нэгэн зэрэг олон IP хаягууд дээр ажигласнаас үүсэл нь нэг загвараас гарсан виртуал систем болохыг илтгэж байна. Ажиглалтанд орсон зарим хост нэрүүдийн хувьд бүх IP хаяг нь заавал муу үйл ажиллагаатай холбоотой байдаггүй гэдгийг тэмдэглэх нь чухал юм. Энэ нь дээрх хост нэрсийг зөвхөн эдгээр хортой цахим ажиллагаа явуулдаг этгээдүүд ашигладаггүй байж болохыг илтгэж байна.

Гэсэн хэдий ч эдгээр машины нэрсийн зарим нь BADBAZAAR C2 домэйнуудыг хостлосон IP хаягууд дээр давтамжтайгаар илэрч байгаа нь сэжигтэй байж болох ба энэ нь хортой цахим ажиллагаа явуулдаг этгээдүүдийн цахим ажиллагааг дэмжих зорилгоор дэд бүтэц бүрдүүлдэг тусгайлсан нэгж эсвэл байгууллага байгаа байж болзошгүйг харуулж байна.

Нийгмийн сүлжээний оролцоо

Өмнөх мэдээгээр Volexity YouTube-ийн видеонуудыг (хортой программуудын хэрэглээг сурталчилсан) цахим гэмт этгээдүүд бүтээсэн болохыг харуулсан. Эдгээр видео бичлэгүүд нь боловсруулсан программуудыг хэрхэн ашиглах тухай зааварчилгааг агуулсан болно.

NCSC нь уг заналхийлэгч этгээдүүдийн ажиллагаатай холбоотой хоёр шинэ YouTube сувгийг илрүүлсэн байна. YouTube-ийн суваг болох '**@josephjoey3499**' хаягтай сувгаар '**Maxgram**' аппликейшныг сурталчилж байсан ба мөн суваг болох **'@uyghurapks3096'** хаягтай суваг нь '**Uyghur APK Finder'** аппликейшныг сурталчилж байсан.

Нэмж дурдахад, **'Flygram'** болон **'Signal Plus'** аппликейшнуудыг сурталчилсан YouTube видеонууд дээр кибер халдлага үйлдэгч этгээдүүдийн хэрэглэж буй утасны дугаарууд ил тод харагдаж байсан. **'Flygram'** video-д 0:36 секундэд утасны дугаар **'+1 (570) 378-7250'** харагдаж байна, мөн **'Signal Plus'** video-д утасны дугаар **'+1 (267) 298 4259'** ил болж байна.

Volexity нь цахим халдлага үйлдэгч этгээдүүдийн явуулдаг гэж үзэж буй Telegram сувгууд дээр хуурамч Төвдийн талаарх сэдэвтэй мэдээний сайт **'ignitetibet[.]net'**-ийг мэдүүлсэн байна. И-мэйл хаяг **'choekyi.wangmo@ignitetibet[.]net'** нь **'tibetone.org'** хуудсан дээрх нийтлэлүүд дээр сэтгэгдэл үлдээж байгаа нь ажиглагдсан бөгөөд уг хуудас нь Lookout компанийн олон нийтэд мэдээлснээр BADBAZAAR-ийн iOS variant -ын хувилбарын C2 хуудсаар ашиглагддаг гэж үздэг.

Энэ и-мэйл хаягийг '**Choekyi Wangmo'** гэх нэрийг ашигласан этгээд ажиллуулж байгаа гэж үзэж байна.

Үнэлгээ

BADBAZAAR ба MOONSHINE нь Уйгур, Төвд, Тайванийн иргэдийг онцлон онилохын тулд хэд хэдэн нийгмийн инженерчлэлийн аргуудыг ашигладаг бөгөөд үүнд:

- Эдгээр бүлгийн сонирхлыг татахуйц аппликейшнүүдийг, жишээлбэл, Уйгур хэл дээрх Кораны апп-ыг троян хэлбэрт оруулах нь зориуд тухайн зорилтот хохирогчдын бүлэгт тохируулан бэлдсэн байгааг харж болно.
- Эдгээр троян вирус агуулсан апп-уудыг албан ёсны апп дэлгүүрүүдэд оруулснаар илүү хууль ёсны мэт харагддаг ба түүнийг групп чатад хуваалцах нь олон нийтийн бүлгийн итгэлцэлийг ашиглах зорилготой байдаг гэж үзэж болно.

BADBAZAAR ба MOONSHINE нь Хятадын төрд үнэ цэнэ бүхий мэдээллийг цуглуулдаг. BADBAZAAR болон MOONSHINE нь Уйгур, Төвд, Тайваний иргэдийг чиглэдэг нь ажиглагдсан хэдий ч, Хятад доторх бусад үндэстний цөөнх бүлгүүдэд чиглэсэн бусад хортой программууд ч мөн байдаг. Улс төрийн дэглэмийн тогтвортой байдалд заналхийлж болзошгүй үйл явдлыг дэмжиж байгаа гэж үзэгддэг Хятадад болон гадаадад амьдарч буй иргэд нь BADBAZAAR болон MOONSHINE зэрэг хортой программын халдлагад өртөх өндөр эрсдэлтэй байна. Байршил, дуу болон зураг зэрэг мэдээллийг хураан авах чадвар нь халдлагад өртсөн хохирогчдын юу хийж байгаа мэдээллийг шууд олж авах боломжтой болгож, үүнийг дараагийн тагнан турших болон дарамт шахалт үзүүлэх ажиллагааг төлөвлөхөд ашиглагддаг.

MITER ATT&CK®

Энэхүү тайлан нь цахим аюултай холбоотой үйл ажиллагааны тактик, аргачлалыг тодорхойлон харуулдаг MITRE ATT&CK® хүрээний дагуу, бодит ажиглалт, нотолгоонд үндэслэн боловсруулагдсан.

Тактик	ID	Техник	Ажиллагаа
Тандалт	T1593.001	Нээлттэй вебсайт/домэйн хайх: Нийгмийн сүлжээ	Цахим халдлага үйлдэгчид хохирогчдод тохируулан онлайнаар групп болон форумуудыг олж, тэнд хортой программ (malware) тараадаг.
Нөөцийн хөгжүүлэлт	T1583.001	Дэд бүтцийг олж авах: Домэйн	Цахим халдлага үйлдэгчид удирдлага ба хяналтын серверүүддээ зориулж домэйн бүртгэдэг.
Нөөцийн хөгжүүлэлт	T1587.001	Чадварыг хөгжүүлэх: Хортой программ	Троянжуулсан апп руу оруулах зорилгоор хортой код бичдэг
Нөөцийн хөгжүүлэлт	T1608.001	Шаталсан үйлдлийн боломжууд: Хортой программыг байршуулах	Троянжуулсан аппуудыг апп дэлгүүр зэрэг онлайн платформд байршуулдаг
Нөөцийн хөгжүүлэлт	T1585.001	Аккаунт үүсгэх: Нийгмийн сүлжээний аккаунт	Цахим халдлага үйлдэгчид вебсайт болон нийгмийн сүлжээнд хувийн бүртгэл үүсгэн хортой программыг хуваалцаж, сурталчилдаг.
Нөөцийн хөгжүүлэлт	T1585.002	Аккаунт үүсгэх: Имэйл бүртгэл	Цахим халдлага үйлдэгчид онлайн орчинд хорт программ байрлууж, хуваалцахад хувийн болон байгууллагын имэйл хаягийг ашигладаг.
Анхны хандалт	T1189	Шууд халдлага	Хортой кодыг бусад хууль ёсны аппууд дотор нууж, апп дэлгүүрүүдэд байршуулдаг.
Анхны хандалт	T1566.003	Фишинг: Үйлчилгээгээр дамжуулан спирфишинг хийх	Цахим халдлага үйлдэгчид Telegram зэрэг нийгмийн сүлжээгээр дамжуулан зорилтот бүлэг рүү троянчилсан аппуудыг илгээдэг.
Гүйцэтгэл	T1204.002	Хэрэглэгчийн гүйцэтгэл: Хортой файл	Хортой кодыг ачаалахын тулд эхлээд хохирогчид трояндсан аппликейшнийг суулгах шаардлага гардаг.
Хамгаалалтаас зайлсхийх	T1027.009	Нууцлагдсан файлууд эсвэл мэдээлэл: Нуусан хортой программ (Payloads)	Хортой кодыг (payload) хууль ёсны программууд дотор нуудаг
Хамгаалалтаас зайлсхийх	T1036.005	Хуулбарлан дуурайх: Хууль ёсны нэр эсвэл	Троянжуулсан файлууд нь хууль ёсны программуудын нэр,

		байршилтай тааруулан дуурайх	хэлбэр дүрс, функцтэй адилхан байдаг.
Хамгаалалтаас зайлсхийх	T1656	Дүр эсгэх	Цахим халдлага үйлдэгчид зорилтот бүлгийн нэрийг ашиглан хуурамч вебсайт болон хэрэглэгчийн нэр үүсгэж, итгэл бүхий хүмүүсийн дүрд тоглодог.
Цуглуулга	T1123	Аудио зураг авалт	Троянжуулсан программууд нь микрофон руу нэвтрэх зэрэг шаардлагагүй зөвшөөрөл хүсч болно
Цуглуулга	T1125	Видео бичлэг хийх	Троянжуулсан программууд нь камерт нэвтрэх зэрэг шаардлагагүй зөвшөөрөл хүсч болно
Цуглуулга	T1005	Локал системийн өгөгдөл	Троянжуулсан программууд нь төхөөрөмж дээрх файл руу гэх мэт шаардлагагүй газар луу нэвтрэх зөвшөөрөл хүсч болно.
Комманд ба удирдлага	T1071.001	Аппликейшний үечлэлийн протокол: Веб протоколууд	Хортой программ HTTPS болон WebSocket ашиглан C2 руу холбогддог.
Удирдлага ба хяналт	T1509	Стандарт бус порт	4432, 2333 гэх мэт стандарт бус портуудыг ашигладаг
Өгөгдлийг зөвшөөрөлгүй дамжуулан авах	T1041	C2 сувгаар өгөгдлийг нууцаар дамжуулан авах	Хортой програм нь HTTPS болон WebSocket холболтуудыг ашиглан өгөгдлийг дамжуулан авдаг.
Нөлөөлөл	T1565.002	Өгөгдлийн боловсруулалт: Илгээгдсэн өгөгдлийг өөрчлөх	Цахим халдлага үйлдэгчид аппликейшний үндсэн үйл ажиллагаанд шаардлагагүй веб урсгалыг идэвхжүүлэн, хохирогчдоос өгөгдлийг олж авдаг.

Үзүүлэлтүүд

MOONSHINE:

- 2025 оны 4-р сарын 1-нд VLiteUI панелыг хайхад дараах илэрсэн байна:

IP хаяг	Порт	Анх харсан	Сүүлд харсан
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

- 2025 оны 4-р сарын 1-нд SCOTCH ADMIN самбаруудыг хайхад дараах зүйлс илэрсэн:

IP хаяг	Порт	Анх харсан	Сүүлд үзсэн
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

- 2024 оны 3-р сарын 14-нд виртуал SCOTCH ADMIN самбаруудыг хайхад дараахь зүйл гарч ирэв.

Домэйн	IP хаяг
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:

Тодорхойлолт	**BADBAZAAR C2 дээр SSL сертификат ажиглагдсан.**
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- 2025 оны 4-р сарын 1-нд дээрх BADBAZAAR гэрчилгээг хайхад дараах үр дүн гарсан байна:

IP хаяг	Порт	Анх харсан	Сүүлд харсан
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

Тодорхойлолт	**BADBAZAAR C2 дээр SSL сертификат ажиглагдсан**
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- 2025 оны 4 сарын 1-ний өдөр дээрх BADBAZAAR гэрчилгээг хайхад дараах илэрцүүд гарч ирэв.

IP хаяг	Порт	Анх харсан	Сүүлд харсан
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 домэйнууд

Доорх нь BADBAZAAR C2 домэйнд илэрсэнтэй таарч байгаа WHOIS бүртгэлтэй одоогийн болон бүртгэгдсэн домэйнуудын хүснэгт юм.

WHOIS Утга	**Домэйн**
Бүртгүүлсэн муж: UJYJYUJ **Бүртгүүлсэн улс: Боливи** **Бүртгүүлэгч: 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
Бүртгүүлсэн муж: REWR **Бүртгүүлсэн улс: CF** **Бүртгүүлэгч: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

Бүртгүүлсэн муж: FSDF **Бүртгүүлсэн улс: AL** **Бүртгүүлэгч: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

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

Дараах холбоосууд нь BADBAZAAR ба MOONSHINE-той холбогдсон бусад халдлагын илэрцүүд (IoC) юм. NCSC нь эдгээр холбоос дахь мэдээллийн үнэн зөв байдлыг бүгдийг баталгаажуулах боломжгүй бөгөөд уншигчдыг тухайн мэдээллийн үнэн зөв байдал болон хамаарал бүхий эсэхийг бие даан шалгахыг зөвлөж байна:

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

Эрсдэлийг бууруулах арга хэмжээ

NCSC нь кейс судалгаанд дурдсан эрсдлийн эсрэг хамгаалах зорилгоор доор дурдсан зөвлөмжүүдийг хэрэгжүүлэхийг уриалж байна.

- **Гуравдагч апп дэлгүүрүүдийг хамааруулан апп дэлгүүрийн операторууд, мөн хөгжүүлэгчид нь өөрсдийн платформ дээрх аппуудыг аюулгүй байлгах, мөн засгийн газрын стандартад нийцэж буй эсэхийг шалгах ёстой.** Удирдамжийг үзнэ үү: 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-version-version

- **Олон улсын хэл дээрх дэмжлэг** : Апп хөгжүүлэгчид нь Уйгур, Төвд, Тайваний Хоккиен, Кантон зэрэг зорилтот бүлгийн цөөнхийн хэлээр ярьдаг хэрэглэгчдэд зориулан алдартай аппуудыг орчуулах, барйшуулах ажилд хөрөнгө оруулах хэрэгтэй. Аппликешнүүдийг байршуулах Apple-н заавар: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Апп орчуулах Google-н заавар: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Нийгмийн сүлжээний платформоо аюулгүй байлгах нь:** Нийгмийн сүлжээний компаниуд цахим халдлага үйлдэгч этгээдүүдэд хуурамч аккаунт үүсгэх, хууль ёсны онлайн нийгэмлэгүүд дотор хортой файл, холбоос түгээхийг хэцүү болгох арга хэмжээ авч болно. Боломжтой тохиолдолд компаниуд цахим халдлагыг салбарын хэмжээнд ярилцаж, эрсдлийг хамтдаа илүү сайн ойлгож, хамгаалалах арга хэмжээг сайжруулахад хувь нэмэр оруулах хэрэгтэй.

- **Хэрэглэгчдэд зориулсан сэргээх төлөвлөгөө:** Байгууллагууд өөрсдийн үйлчилгээг ашиглан хортой аппликейшн суулгасан хэрэглэгчдэд мэдэгдэл хүргэх журамтай байх ёстой. Эдгээр анхааруулга нь хэрэглэгчийн анхаарлыг татахуйц, мөн мэдээлэл өгөхүйц байх ёстой. Зохих тохиолдолд байгууллагууд тус программыг хэрхэн устгах талаар зааварчилгаа өгч, хохирогчдод UK NCSC гэх мэт эрх бүхий байгууллагуудад мэдээлэхийг уриалж байх хэрэгтэй.

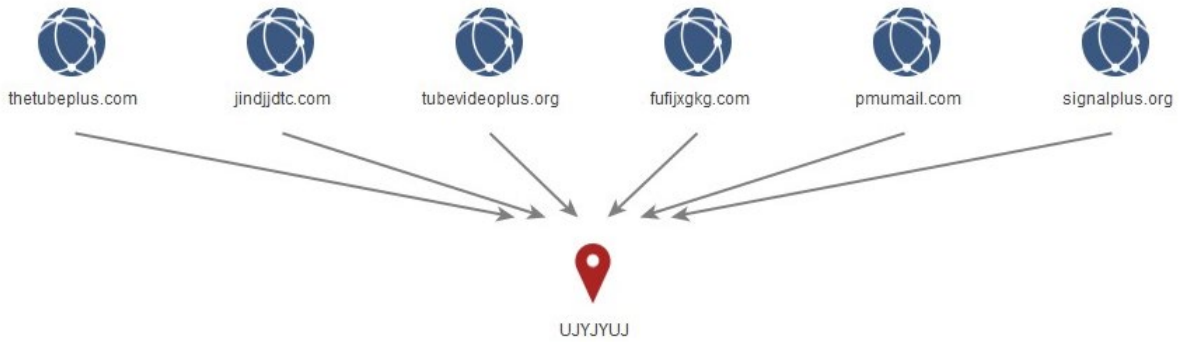
Дэлгэрэнгүй мэдээллийг App Store-н Практик Дүрмээс үзнэ үү: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Хамтран ажиллах ажлын хэсгүүд:** Нийгмийн сүлжээний компаниуд хамтарсан ажлын хэсэг байгуулж, өөрсдийн цахим аюулгүй байдлын багуудын хооронд хортой үйл ажиллагаа, тактик, техник, арга барил (TTPs), ажиглалтуудыг хоорондоо хуваалцах боломжийг бүрдүүлснээр цахим халдлага үйлдэгч этгээдүүд эдгээр платформыг ашиглан халдлага явуулахад илүү хүндрэл учруулах болно.

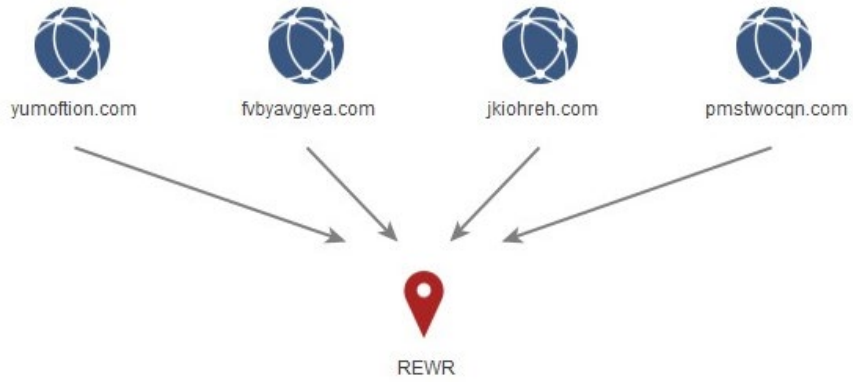
- **Өөрчлөгдсөн программуудыг илрүүлэх:** Боломжтой тохиолдолд, апп хөгжүүлэгчид хэрэглэгчийг “албан бус” хувилбарыг татаж авсан эсэхийг мэдээлэх функцтэй байхаар апп-аа зохион бүтээснээр хортой хуулбар татаж авахаас сэргийлэхэд тус болно.

Хавсралт A: BADBAZAAR WHOIS кластерчлал / домэйн брокерийн мэдээллийн графикууд

Зураг 1 – 'UKYJYUJ'

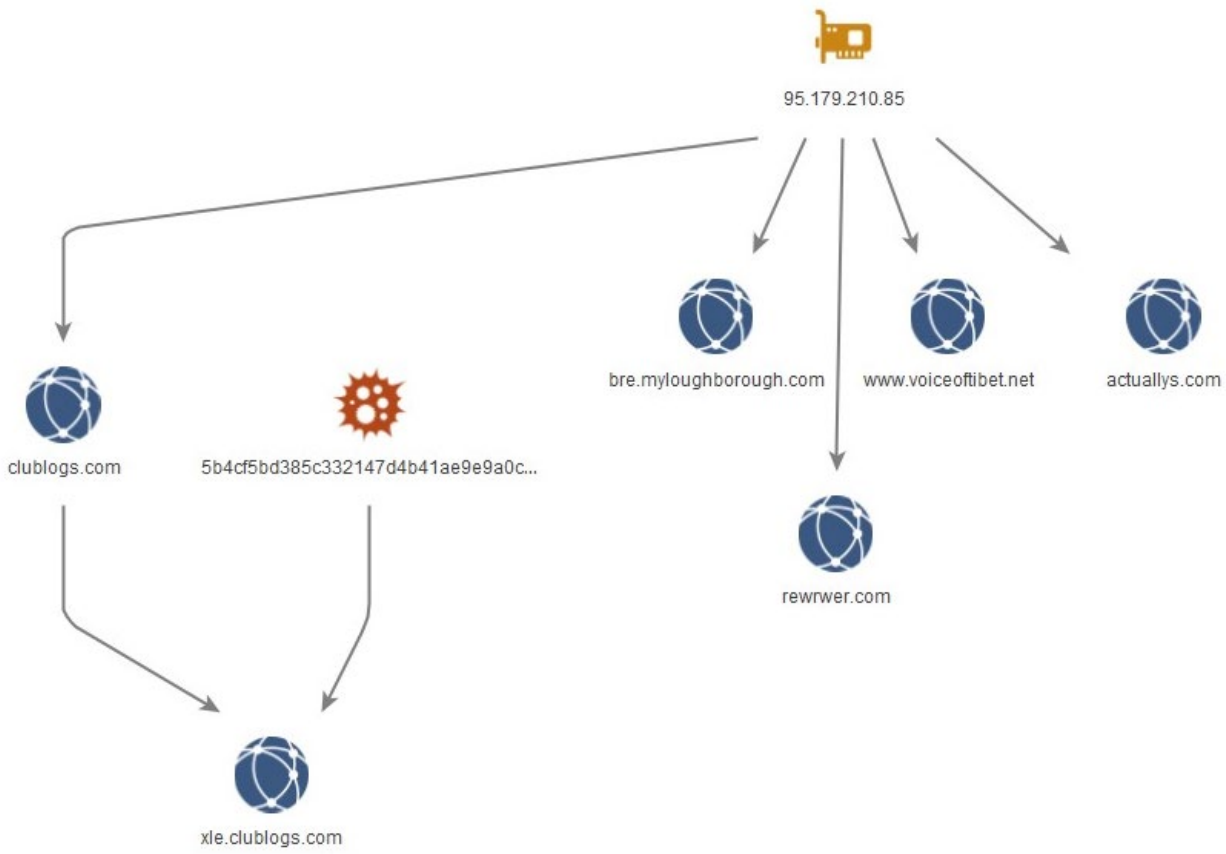


Зураг 2 – Компьютерын гар дээр дараалсан үсэг, тоо, тэмдэгт утга

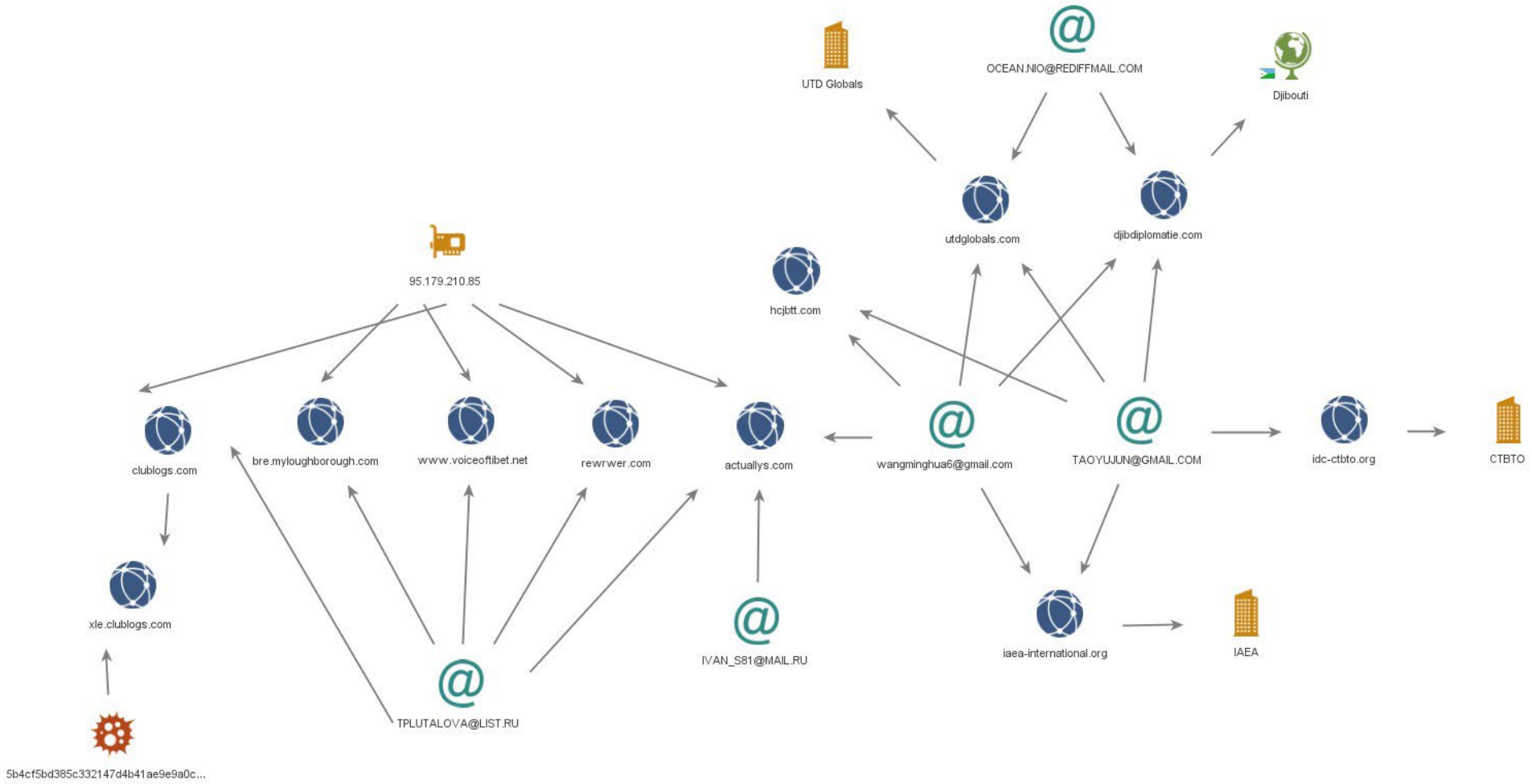


Зураг 3 – 'FSDF' төлөвийн талбарын утгууд бүхий нэмэлт домэйнүүд

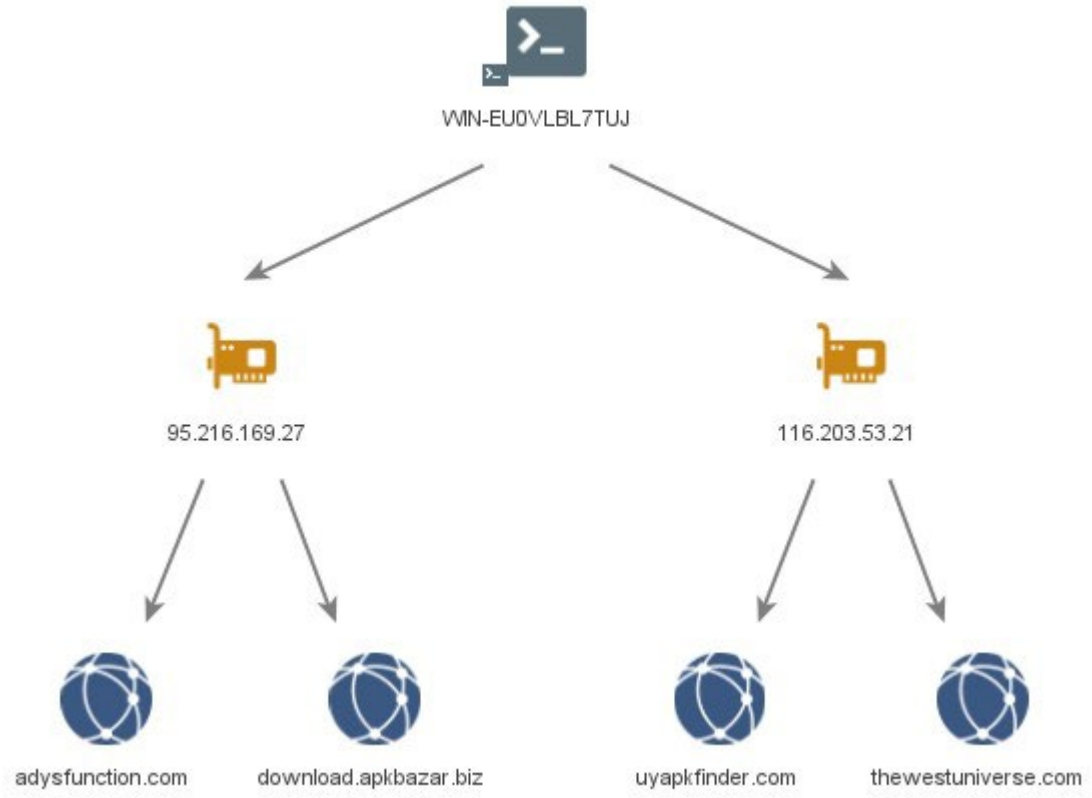
Зураг 4 – **95.179.210[.]85**



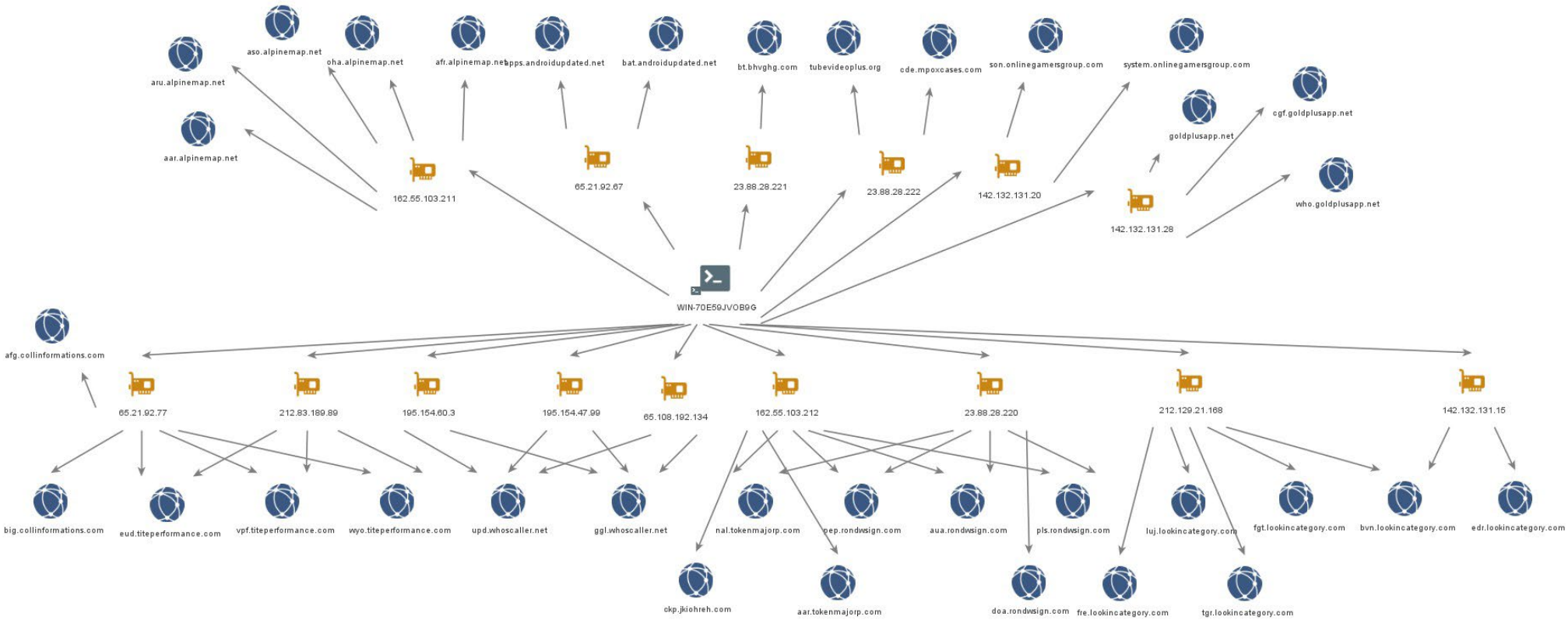
Зураг 5 – WHOIS холбоосууд



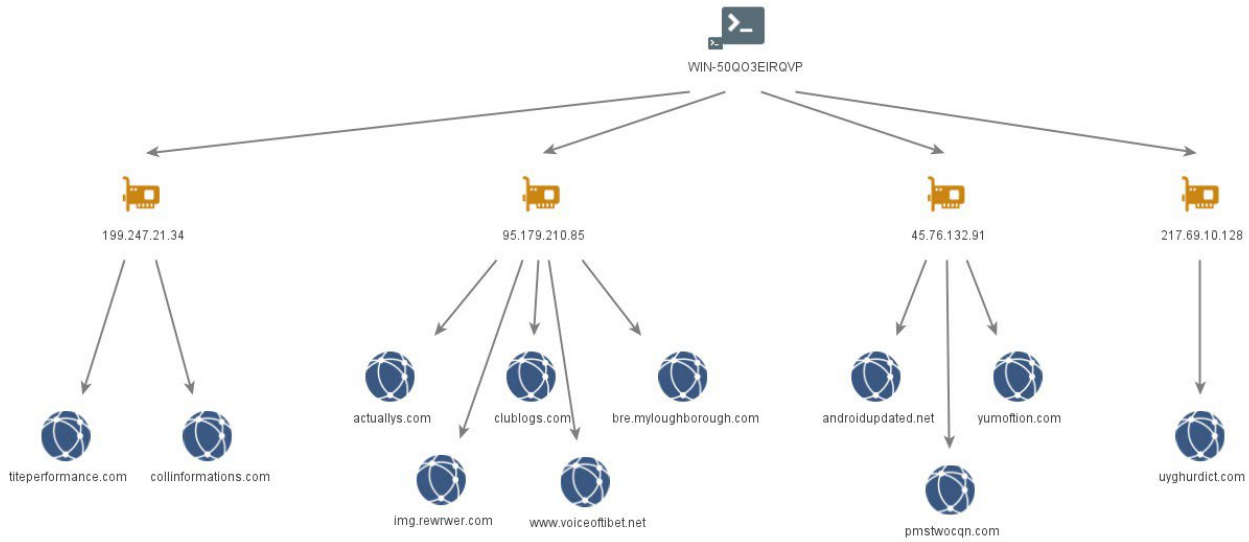
Зураг 6 – **WIN-EU0VLBL7TUJ**



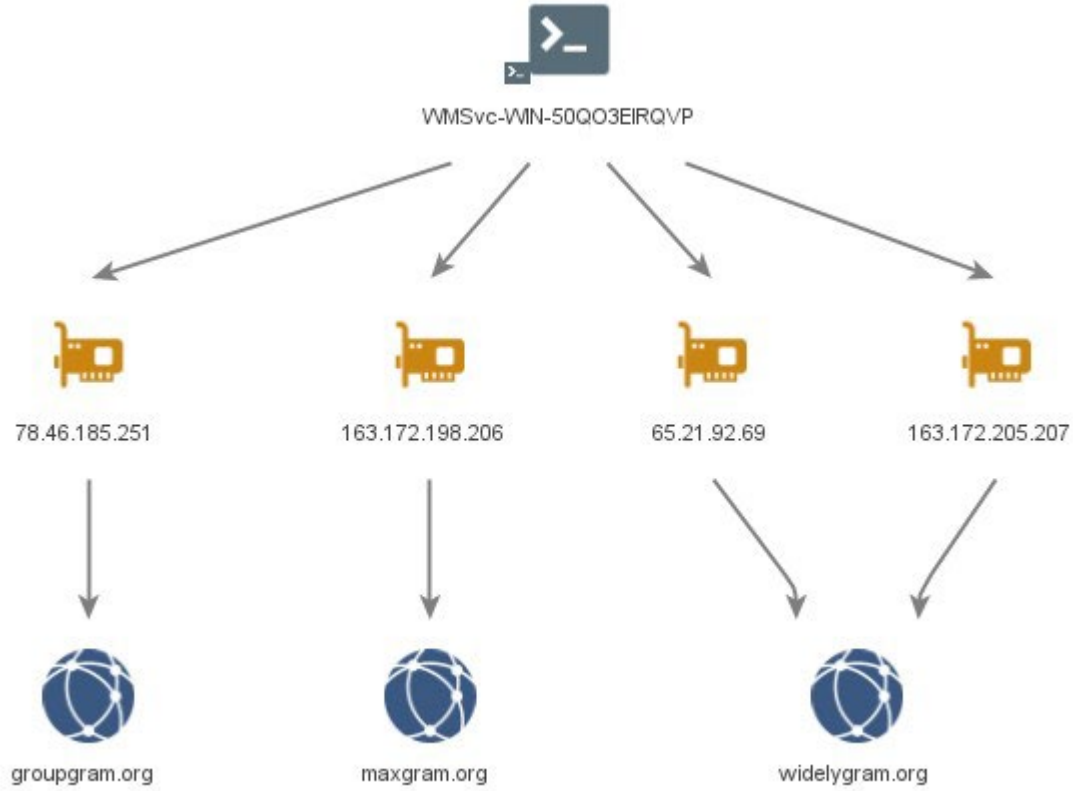
Зураг 7 – **WIN-70E59JVOB9G**



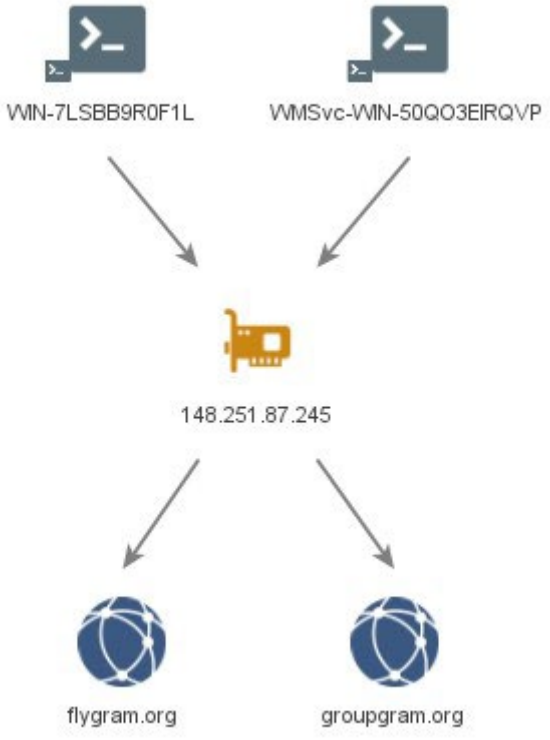
Зураг 8 - **WIN-50QO3EIRQVP**



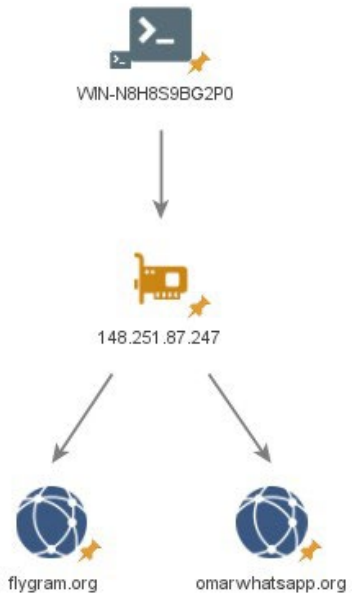
Зураг 9 - **VMSvc-WIN-50QO3EIRQVP**



Зураг 10 – **VMSvc-WIN-50QO3EIRQVP** ба **WIN-7LSBB9R0F1L**



Зураг 11 - **WIN-N8H8S9BG2P0**



Зураг 12 - **WIN-I6VBN8MR92A**

Хавсралт Б: MOONSHINE & BADBAZAAR загварыг ажиглав

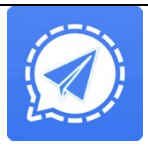
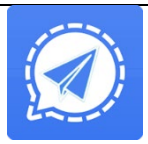
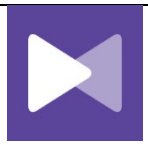
Энэхүү хүснэгт нь сүүлийн хоёр жилийн хугацаанд MOONSHINE болон BADBAZAAR-ийн ажиллагаанд ашиглагдсан аппликейшнуудыг жагсаан харуулж байна.

Эдгээр аппликешнүүдийн ихэнх нь тогтсон программуудтай ижил төстэй байгааг харуулж байна. Энэ нь алдартай брэндүүдийг "дуурайн мэхлэх" санаатай цахим халдлага үйлдэгч этгээдийн арга байх магадлалтай.

Аппийн нэр, багцын нэр, апп дүрс нь жинхэнэ аппликейшнийг дуурайж эсвэл тохируулж болдог тул төхөөрөмж халдлагад өртсөн эсэхийг тодорхойлоход хангалтгүй гэдгийг анхаарах нь чухал юм.

Апп нэр	Багцын нэр	Апп дүрс тэмдэг
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	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

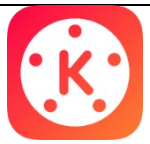
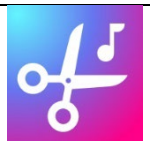
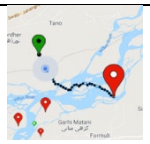
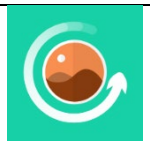
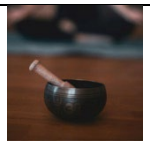
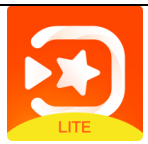
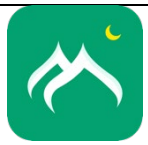
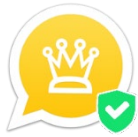
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

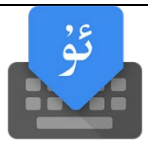
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

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

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

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

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

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

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

Цааш унших

Австралийн Цахим Аюулгүй Байдлын Төвийн удирдамж

- Цахим гэмт хэрэг, тохиолдол эсвэл сул талын талаар мэдээлэх
- Төхөөрөмжөө хэрхэн хамгаалах вэ?
- Гар утсаа хамгаална уу
- Фишинг
- Луйвар
- Сошиал медиагаа хамгаалаарай
- Сошиал медиа болон мессежийн аппуудын аюулгүй байдлын зөвлөмжүүд

Их Британийн NCSC болон NPSA-ийн удирдамж

- Ардчиллыг хамгаалах
- Сошиал медиа: үүнийг хэрхэн аюулгүй ашиглах вэ?
- Байгууллагуудад зориулсан төхөөрөмжийн аюулгүй байдлын зөвлөмж (гар утсыг багтаасан)
- Аппликейшн дэлгүүрүүдтэй холбоотой эрсдэлийн тайлан
- Цахим халдлагад өртөх өндөр эрсдэлтэй хүмүүсийн хувийн аюулгүй байдал, хамгаалалт

АНУ-ын NSA-аас өгсөн заавар

- Мобайл төхөөрөмжийн шилдэг туршлага

Хариуцлагаас татгалзах мэдэгдэл

Энэхүү зөвлөмж нь уг нийтлэл нийтлэгдсэн үед баталгаажсан мэдээллийг агуулж байгааг анхаарна уу.

Энэхүү тайлан нь зохиогч агентлаг болон салбарын эх сурвалжаас авсан мэдээлэлд үндэслэн гаргасан болно. Энэхүү дүгнэлт болон зөвлөмжүүд нь бүх эрсдлээс бүрэн хамгаалж чадахгүй бөгөөд зөвлөмжүүдийг дагаснаар эрсдлээс бүрэн хамгаалагдахгүй гэдгийг анхаарна уу. Мэдээллийн эрсдэлийн хариуцлагыг үргэлж тухайн системийн эзэмшигч хүлээнэ.

Их Британи улсад энэхүү мэдээлэл 2000 оны Мэдээллийн эрх чөлөөний тухай хуулиар (FOIA) мэдээллийн ил тод байдалд хамрагдахгүй бөгөөд бусад мэдээллийн хууль тогтоомжид харьяалагдаж болно.

Мэдээллийн Эрхийн тухай хууль (FOIA) холбоотой асуултыг ncscinfoleg@ncsc.gov.uk хаяг руу илгээнэ үү.

Бүх материал нь Их Британийн Хааны Эрхээр хамгаалагдсан болно. ©