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:**

Уйгур, Тайвань, Төвд гаралтай иргэд болон иргэний нийгмийн байгууллагуудыг чиглэсэн тагнуулын программын халдлагууд

2025 оны **4** сарын **9**

BADBAZAAR ба MOONSHINE: Уйгур, Тайвань, Төвд гаралтай иргэд болон иргэний нийгмийн байгууллагуудыг чиглэсэн тагнуулын программын халдлагууд

NCSC болон түнш байгууллагууд нь хоёр төрлийн тагнуулын програм халдлагад өртөх өндөр эрсдэлтэй бүлэгт зориулан шинэ мэдээлэл болон эрсдлийг бууруулах арга хэмжээг нийтэллээ.

Хураангуй

Их Британий Цахим Лигийн дэмжлэгтэйгээр энэхүү зөвлөмжийг Үндэсний Цахим Аюулгүй Байдлын Төв (NCSC UK) болон олон улсын түншүүд хамтран боловсруулсан болно.

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

Энэ мэдэгдлийн зорилго нь Тайвань, Төвд, Шинжаан Уйгурын өөртөө засах орон, ардчиллын хөдөлгөөнүүд болон Фалун Гун зэрэг сэдвүүдтэй хамаарал бүхий иргэдэд чиглэсэн хортой цахим ажиллагаа нэмэгдэж буй талаар олон нийтэд мэдээлэхэд оршино.

Энэхүү зөвлөмжид ухаалаг гар утас гэх мэт зөөврийн төхөөрөмж дээр Хятадын төрийн анхаарал татахуйц сэдэв бүхий өгөгдлийн халдлага ба цахим халдлага үйлдэгч этгээдүүдийн BADBAZAAR болон MOONSHINE гэх тагнуулын программыг хэрхэн ашигласан талаар тайлбарласан хоёр кейс судалгаа багтсан болно. Мөн хувь хүмүүс өөрсдийгөө, төхөөрөмжөө болон хувийн мэдээллээ хамгаалахад нь туслах зөвлөмжүүдийг чиглүүлэн заав.

Энэхүү зөвлөмжтэй хамт NCSC нь тусгай зөвлөмжийг багтаасан техникийн дэлгэрэнгүй мэдээлэллийг нийтлэв.

Ямар хүмүүс халдлагад өртөх магадлалтай вэ?

Оролцогч агентлагууд болон салбарын түншүүдийн ажигласнаар BADBAZAAR болон MOONSHINE хэмээх тагнуулын хортой программ нь Хятадын төрийн дотоод засаглал, улс төрийн зорилго болон олон улсын нэр хүндэд нь заналхийлж болзошгүй гэж үзсэн агуулгатай холбоотой хувь хүмүүсийг онилж байна. Халдлагад өртөх эрсдэлтэй зүйлсэд дараах орно. Гэхдээ үүгээр хязгаарлагдахгүйг анхаарна уу.

- **Тайванийн тусгаар тогтнол**
- **Төвдийн эрх**
- **Хятадын Шинжааны Уйгурын өөртөө засах оронд амьдардаг эсвэл тэндээс гаралтай Уйгур мусульманчууд болон бусад үндэстний цөөнхүүд**
- **ардчиллыг дэмжих үйл ажиллагаа (Хонконг бас хамаарна)**
- **Фалун Гонг шашны хөдөлгөөн**

Үүнд төрийн бус байгууллагууд (ТББ), сэтгүүлчид, бизнесийн байгууллагууд болон эдгээр бүлгүүдийг дэмждэг, өөрсдийгөө холбож ойлгодог, эсвэл тэднийг төлөөлдөг хувь хүмүүс багтана. Энэхүү тагнуулын программ нь цахим орчинд шууд тархдаг тул тооцоолсон хохирогчдоос гадна бусад хүмүүс бас халдлагад өртөх эрсдэлтэй.

Энэхүү зөвлөмж нь BADBAZAAR болон MOONSHINE тагнуулын программын тодорхой халдлагад өртөх эрсдэлтэй хүмүүсийг хамгаалах, хариу арга хэмжээ авахад нь дэмжлэг үзүүлэх зорилготой болно. Уг урьдчилсан арга хэмжээнүүд нь ерөнхий цахим аюулгүй байдлын зөвлөмжид тулгуурлан нэмэлт зөвлөгөө өгч байгаа бөгөөд дангаар нь зөвлөмж болгон авч үзэж болохгүй.

Хэрэглэгчид энэхүү зөвлөмжид дурдсан зааврыг дагаж мөрдсөнөөр зөөврийн төхөөрөмж болон мэдээллийн халдлагад өртөх эрсдлийг бууруулах боломжтой болно.

Аюул

MOONSHINE ба BADBAZAAR нь троян гэх хортой программын нэг жишээ бөгөөд эдгээр нь хэвийн ажиллаж байгаа аппликейшн дотор далд хэлбэрийн хортой үйлдлүүдийг агуулсан байдаг. Эдгээр аппуудыг аппликейшн дэлгүүрүүд эсвэл онлайн файл хуваалцах үйлчилгээнээс татаж авч болдог.

Эдгээр аппликейшнүүдийг хэрэглэгчийн төхөөрөмж дээр суулгуулахын тулд хэрэглэгчдийг хуурах байдлаар бүтээгдсэн. Аппликейшн суулгагдсаны дараа төхөөрөмжийн сул талыг ашиглан зөвшөөрөлгүй үйлдэл гүйцэтгэх боломжтой бөгөөд эсвэл хэрэглэгчээс зөвшөөрөл авах замаар дараах мэдээлэлд хандан, татаж авч болдог:

- **шууд хяналтыг оролцуулан бүх байршлын мэдээлэл**
- **микрофон болон камерт нэвтрэх эрх**
- **төхөөрөмжид хадгалагдсан зурвас, зураг болон бусад файлуудыг авах эрх**
- **төхөөрөмжийн мэдээлэл болон бусад**

Үүний дараа цахим этгээдүүд нь халдлагад өртөх өндөр эрсдэлтэй бүлгүүдийн эрх ашиг, сонирхлыг ашиглан аль болох олон хохирогчийг байгаа болгож, тэдний мэдээлэлд нэвтрэхийг оролддог. Хохирогчдын сонирхлыг татах зорилгоор тэдний эх хэл, соёл, эсвэл тодорхой газар нутагтай холбоотой контентыг агуулсан (жишээ нь, Хятадын Төвдийн бүс, Шинжаан зэрэг) аппликейшнуудыг зориудаар бүтээдэг.

Энэхүү зөвлөмжид TibetOne болон Uyghur Quran аппликейшнүүд жишээ болж орсон болно.

Эдгээр цахим этгээдүүд өөрсдийн тооцоолсон хохирогчдын хэрэглэдэг онлайн форумууд дээр идэвхтэй оролцдог бөгөөд ингэснээр халдлага хийх боломжоо нэмэгдүүлдэг. Тэд санаатайгаар Төвдтэй холбоотой Telegram сувгууд болон Reddit форумууд дээр тагнуулын програм хуваалцаж байгаа нь ажиглагдсан байна. Энэхүү зөвлөмжид орсон кэйсүүд нь эдгээр аргуудыг жишээ болгон харуулдаг.

Хортой аппликейшнүүдийг ихэвчлэн Android дээрх APK файлууд гэх мэт бие даасан файл хэлбэрээр хуваалцдаг бөгөөд үүнийг хэрэглэгчид татаж авах, суулгах шаардлагатай байдаг. Тухайн этгээдүүд нь тагнуулын программыг илүү хууль ёсны мэт харагдуулахын тулд Google Play Store, Apple App Store зэрэг албан ёсны аппликейшн дэлгүүрт байрлуулдаг ба эсвэл өмнө нь хоргүй байсан апп-д хортой код нэмж тараадаг. Гэсэн хэдий ч эдгээр албан ёсны апп дэлгүүрүүд нь аюулгүй байдлын хамгаалалт, шалгах ажиллагаатай тул энэ төрлийн арга барилын үр дүн харьцангуй бага байдаг. Ингэснээр албан ёсны апп дэлгүүрүүдээс татаж авсан аппликейшнуудыг аюул багатай болгож байгаа ч, кейс судалгаа болон NCSC-ийн Апп дэлгүүр Эрсдлийн Тайлан-д тусгагдсанаар, эдгээр шалгуурын процессууд бүрэн баталгаатай биш юм.

Дараах 4 зөвлөгөөг дагаснаар энэхүү зөвлөмжид дурдагдсан эрсдлээс өөрийгөө хамгаалахад тусална.

Дэлгэрэнгүй зөвлөгөөг эрсдэл бууруулах арга хэмжээ хэсгээс үзнэ үү.

Кейс судалгаа

Эдгээр хоёр кейс судалгаа нь MOONSHINE ба BADBAZAAR хэрхэн ажилладаг, мөн хортой кибер этгээдүүд халдлагын эрсдэлд байгаа хүмүүст хэрхэн халдаж байгааг тодорхой харуулах болно.

Кейс судалгаа нэг: MOONSHINE

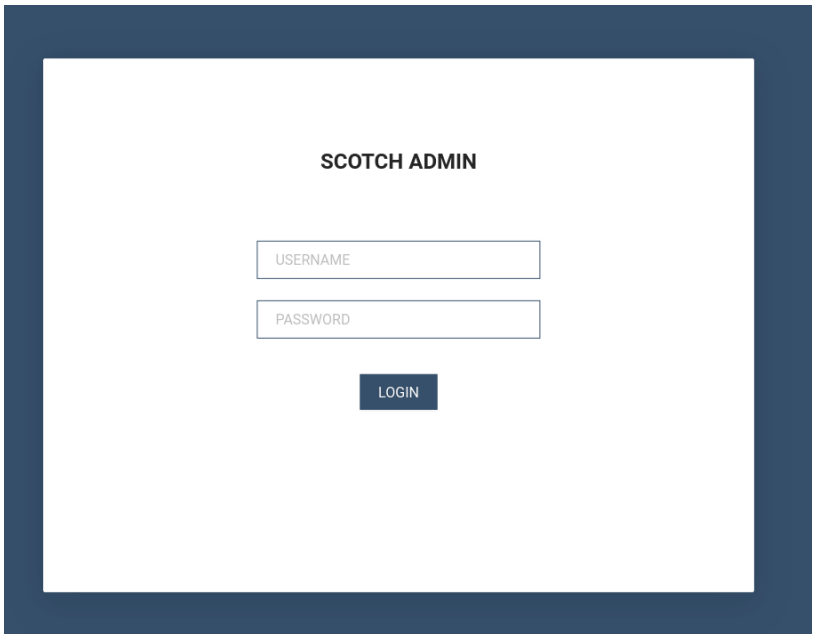
MOONSHINE нь 2019 онд Citizen Lab -н мэдээлснээр Төвдийн бүлэг хүмүүсийг онилсон Android үйлдлийн системд зориулсан тагнуулын программ юм. MOONSHINE нь хохирогчдыг анхаарлыг татаж, төхөөрөмж дээр нь суулгуулах зорилготой жинхэнэ апп шиг харагддаг хортой програм юм. Энэ нь Telegram сувгууд болон WhatsApp-аар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

MOONSHINE нь өргөн хүрээний тагнах чадвартай бөгөөд үүнд:

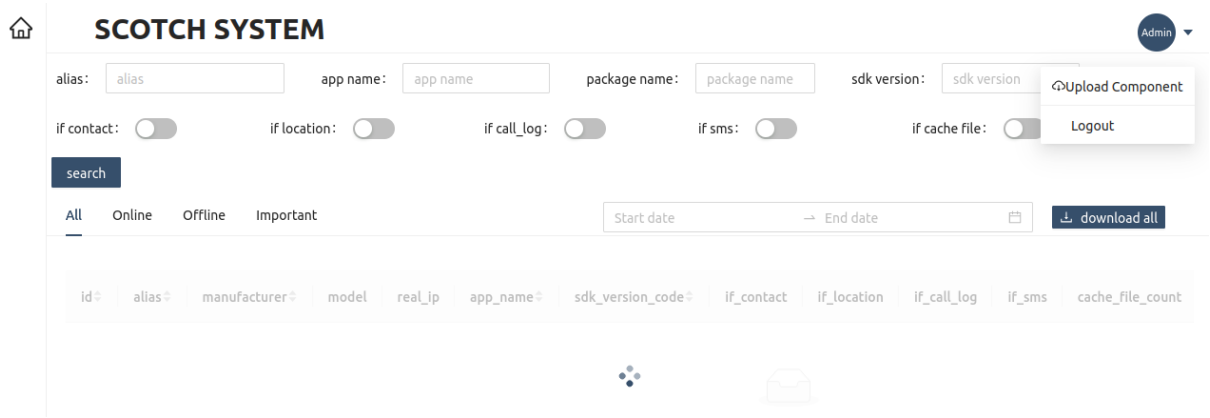
- **шууд хяналт зэрэг байршлын мэдээлэл**
- **шууд аудио болон зураг авах**
- **төхөөрөмжөөс файл татаж авах**
- **төхөөрөмжийн мэдээллийг олж авах**
- **төхөөрөмж дээр аудио тоглуулах**

ئاۋازلىق قۇرئان.apk буюу **‘Audio Quran.apk’** аппликейшн нь MOONSHINE хорт программ Уйгурчуудыг онилоход хэрхэн ашиглагдаж байгааг харуулсан жишээ юм. Файлын нэрэнд уйгур хэл ашигласан нь, тухайн аппликейшн нь Коран болохыг илтгэж, уйгур мусульманчуудыг татах зорилготой бүтээсэн байж магадгүй юм.

Аппликейшн суулгагдсаны дараа цахим гэмт этгээдүүд хохирогчдын төхөөрөмжөөс мэдээлэл цуглуулах боломжтой болдог. Мэдээллийг 'SCOTCH ADMIN' хяналтын самбарын (панелийн) тусламжтайгаар олж авдаг



Нэвтэрсний дараа, цахим этгээдүүд доорх скриншот-д харуулсан хуудсанд нэвтрэх боломжтой болно. Энэ хуудас халдлагад өртсөн төхөөрөмжийн мэдээлэл болон цахим этгээдүүд тухайн төхөөрөмжинд ямар түвшний нэвтрэх эрхтэй байгааг харуулна:



Хортой программын удирдлагын самбар дээр цуглуулсан мэдээлэл дараах зүйлсийг агуулна:

- **Төхөөрөмжид нэвтрэх түвшин**
- **SMS мессежүүд**
- **дуудлагын бүртгэл**
- **байршлын өгөгдөл**
- **төхөөрөмжийн мэдээлэл**

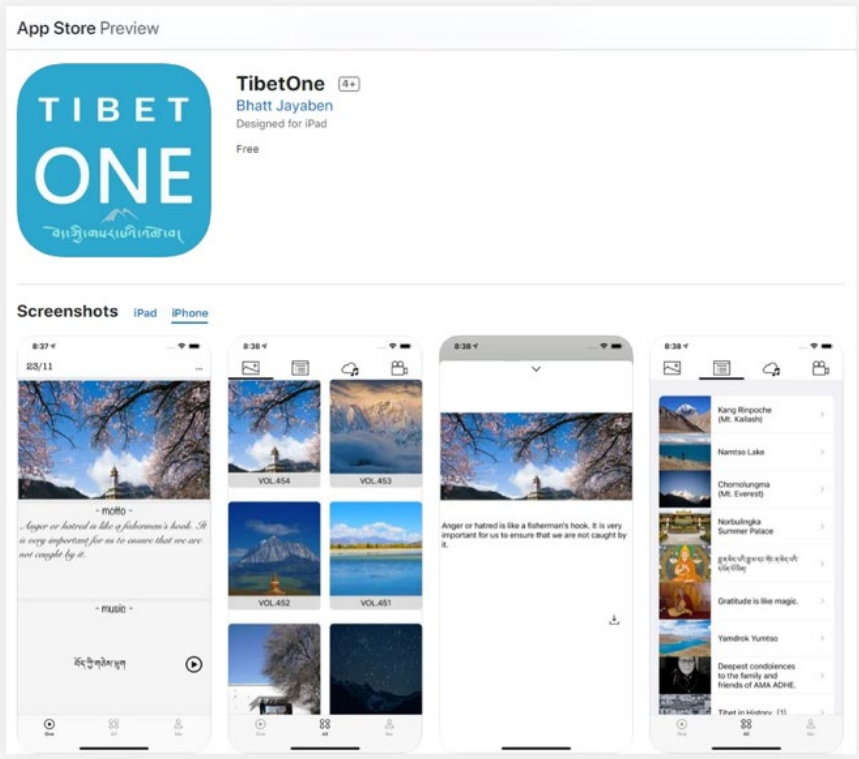
Cyber League-тэй хамтран ажилласны үр дүнд Үндэсний кибер аюулгүй байдлын төв (NCSC) нь Trend Micro тайлан дээр үндэслэн MOONSHINE хэрэглэгдэхүүн болон нэвтрэх хуудаснуудын HTML гарчигт “UPSEC” гэсэн нэр давхцаж байгааг илрүүлжээ. Дэлгэрэнгүй мэдээлэл нь хавсаргасан техникийн зөвлөмжид багтсан байна.

Intelligence Online мэдээлснээр UPSEC гэдэг нь ‘Sichuan Dianke Network Security Technology Co. Ltd’ хэмээх компанитай холбоотой нэр томьёо юм. Оролцогч агентлагууд энэ мэдэгдлийг баталгаажуулаагүй байна.

Кейс судалгаа хоёр: BADBAZAAR

BADBAZAAR нь iOS ба Android хувилбартай гар утасны хортой програм бөгөөд Уйгурууд, Төвдүүд болон Тайваний иргэдийг чиглэн халддаг байна. Энэхүү хортой программ нь олон нийтийн мэдээллийн хэрэгслийн платформ болон албан ёсны апп дэлгүүрээр тархсан.

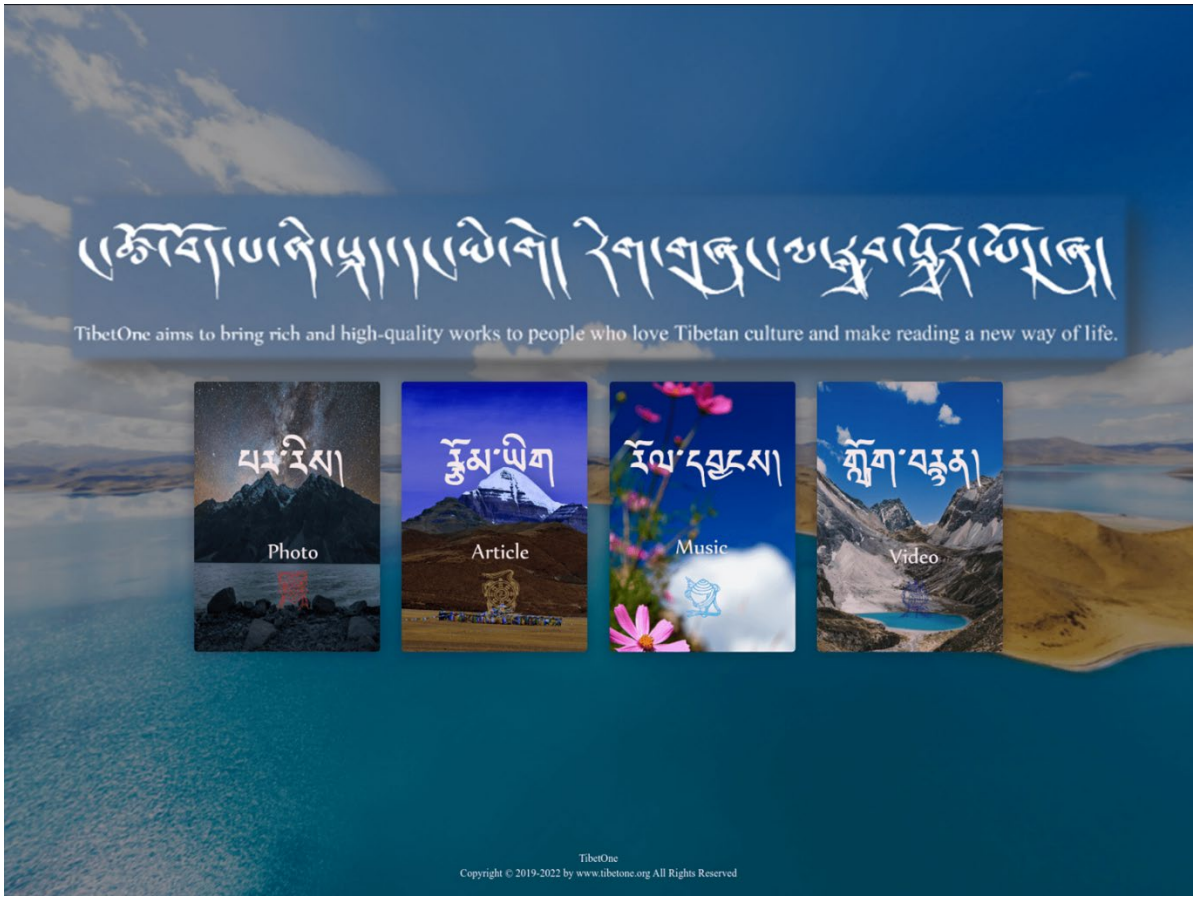
Lookout болон Volexity -ын мэдээлснээр BADBAZAAR-ыг ' **TibetOne'** аппликейшнээр дамжуулан Төвдүүдийг онилоход ашигласан. **TibetOne** нь төхөөрөмжийн мэдээлэл болон байршлын өгөгдөлд хандах чадвартай, цахим этгээдүүдийн бүтээсэн iOS программ юм. Үүнийг 2021 оны 12-р сард Apple App Store-д байршуулсан боловч ашиглах боломжгүй болсон. Тагнуулын программыг цаашид түгээхийн тулд цахим этгээдүүд ‘**tibetanphone**’ нэртэй Telegram сувагт уг программыг сурталчилжээ.



Зураг 1: Apple App Store дээрх TibetOne программын хуудас. Үүнээс хойш уг программыг устгасан.

Зураг 2: TibetOne-г Телеграм сувгуудаар хуваалцсан.

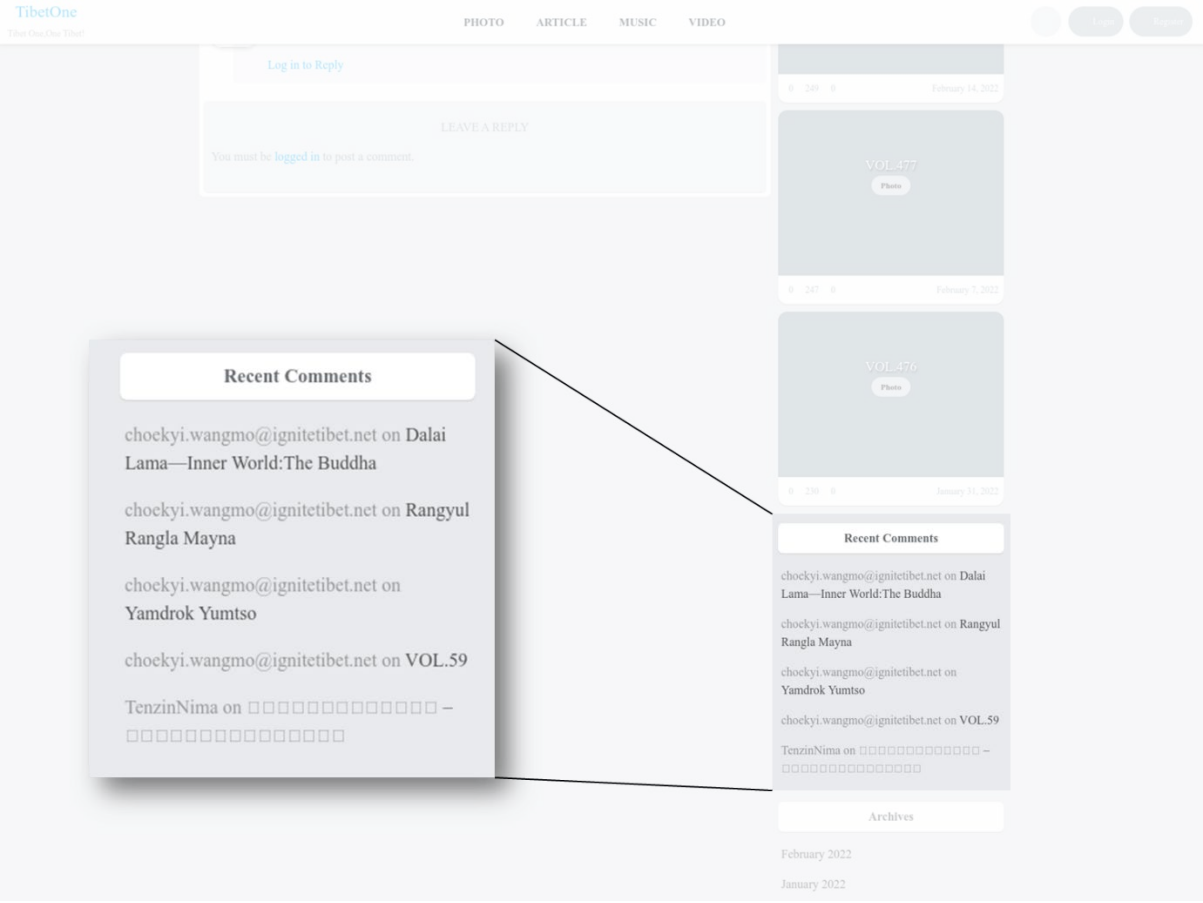
Уг аппликейшныг хууль ёсны мэт харагдуулахын тулд зохион байгуулагчид ‘**tibetone[.]org**’ нэртэй веб сайтыг бүтээсэн бөгөөд энэ сайт *‘Төвдийн соёлд дурлагчдад баялаг, чанартай бүтээлүүдийг хүргэж, уншлагыг амьдралын шинэ хэв маяг болгоно’* гэж тодорхойлсон байна.



Зураг 3: 'tibetone[.]org'-ын нүүр хуудас.

Холбогдох хэсгүүдийг илүү ойлгомжтой болгох үүднээс энэ зургийг зассан.

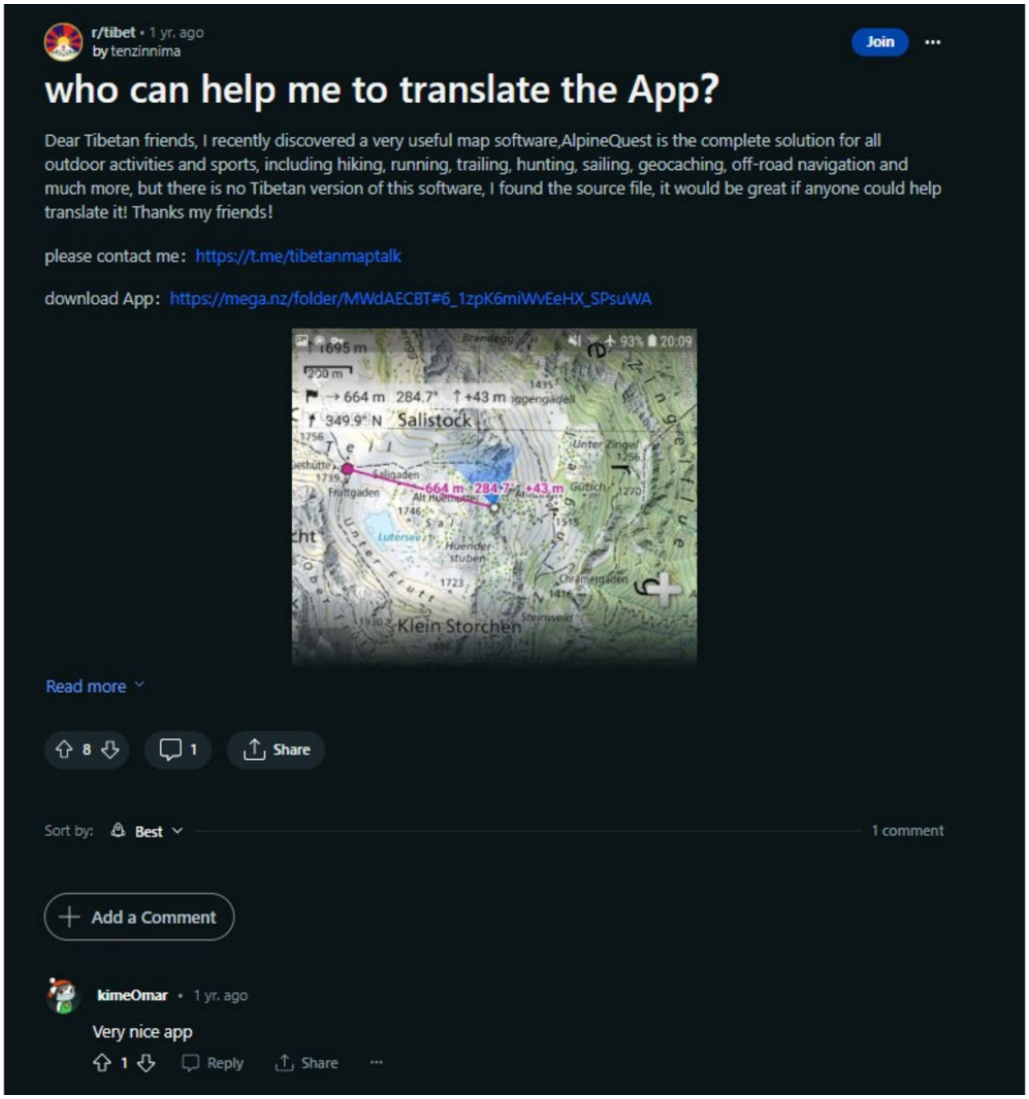
Энэ вебсайт нь хэрэглэгчдэд сэтгэгдэл үлдээх боломжийг олгодог нийтлэлийн хуудастай байсан. '**choekyi.wangmo@ignitetibet.net**' имэйл хаягаар үлдээсэн сэтгэгдэл нь халдлагад оролцогч этгээдээр удирдуулж байгаа гэж үзэж байгаа. Мөн уг хаяг Төвдийн Хүний Эрхийн ба Ардчиллын Төвд Төвдийн талын эсэргүүцэгч гэж бүртгэгдсэн ‘**Choekyi Wangmo**’ хэмээх хүний дүр эсгэж байж магадгүй байна. Үүний цаад зорилго нь тус аппликейшн үнэхээр Төвдийн тусгаар тогтнолыг дэмжиж байгаа мэт төсөөллийг бий болгох нэг төрлийн оролдлого байж магадгүй юм.



Зураг 4: 'tibetone[.]org' хуудсан дээр цахим гэмт этгээдийн удирдсан гэж үзэж буй хэрэглэгчдийн сэтгэгдлийг харуулсан.

Холбогдох хэсгүүдийг илүү ойлгомжтой болгох үүднээс энэ зургийг зассан.

"**TenzinNima**" гэдэг нь энэ сайтад сэтгэгдэл үлдээсэн өөр нэг хэрэглэгчийн нэр юм. Volexity мэдээлснээр энэ хэрэглэгчийн нэрийг Reddit дээр '**Tibetanmaptalk**' Telegram сувгийг сурталчлахад ашигласан байна. Үүнд Android төхөөрөмж дээр ашиглагддаг '**AlpineQuest**' навигацийн аппын хортой загварыг татаж авах холбоос орсон байна. Өгөгдсөн татаж авах холбоос нь Mega нэртэй гуравдагч талын файл хуваалцах үйлчилгээнд зориулагдсан болно.



Зураг 5: Цахим халдлага үйлдэгч этгээдийн хяналтад байгаа гэж үзсэн хуурамч акаунтаас хортой аппликейшныг сурталчилсан Reddit нийтлэл оруулсан байна.

Volexity мөн **‘KimeOmar’** нэртэй хэрэглэгч нь тухайн бичлэг дээр сэтгэгдэл үлдээсэн төдийгүй өөр нэгэн Reddit-ийн салбар форумд ч хортой аппликейшнүүдийг тарааж байгааг ажигласан байна. Энэ үйлдэл нь цахим халдлага үйлдэгч этгээд олон нийтийн сүлжээнд олон профайл ашиглаж, өөрсдийн нийтлэлүүдийг итгэхүйц, үнэн мэт харагдуулахыг оролдож байж болохыг харуулж байна.

Дүгнэлт

BADBAZAAR ба MOONSHINE нь Уйгур, Төвд, Тайваний иргэдийг онцлон байгаа болгохын 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 хохирогчдын бүлэгт тохируулан бэлдсэн байна.
- 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 итгэлцлийг ашиглах зорилготой байдаг гэж үзэж болно.

BADBAZAAR ба MOONSHINE нь Хятадын төрд үнэ цэнэтэй 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.

Гар утасны апп хэрэглэгчдэд зориулсан эрсдэл бууруулах арга хэмжээ

Тухайн тохиолдлуудад дурдсан эрсдэлээс хамгаалахад дараах аюулгүй байдлын дадал зуршлыг хэрэгжүүлэхийг зохиогч байгууллагууд зөвлөж байна. Эдгээр зөвлөмж нь Үндэсний Цахим Аюулгүй Байдлын Төвийн (NCSC) шилдэг аргачлалд суурилсан зааварчилгаанд үндэслэсэн болно. Австрали болон АНУ-ын уншигчдад зориулсан шилдэг аргачлалын удирдамжуудын холбоосыг “Нэмэлт мэдээлэл” хэсгээс үзнэ үү.

Төхөөрөмжөө аюулгүй байлгаарай

- **Апп-уудыг зөвхөн Google Play Store, Apple App Store зэрэг албан ёсны апп дэлгүүрүүдээс татаж аваарай.** Google-н Play Store болон Apple-ийн App Store дэлгүүрүүд нь программыг нийтлэхээс өмнө вирусийн шалгалт хийдэг тул татаж авч буй зүйл тань аюулгүй байх магадлал өндөр байдаг.. Найдвартай апп дэлгүүрээс татсан апп ч тодорхой хэмжээний эрсдэл дагуулж байж болох ч, бусад эх сурвалжаас татсан апп ямар ч хамгаалалтгүй байх аюултай. NCSC нь апп дэлгүүрүүдтэй холбоотой эрсдлийн тайлан гаргасан: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **Төхөөрөмж болон аппуудаа үргэлж шинэчилж байгаарай.** Апп болон төхөөрөмжийн програм хангамж дээр шинэчлэлт гармагц суулгаж байгаарай. Хэрэв боломжтой бол төхөөрөмжийнхөө тохиргоонд 'автомат шинэчлэлт' функцийг идэвхжүүлээрэй, ингэснээр та шинэчлэлт шууд хийгдэж байх болно. Одоогоор танигдсан байгаа вирус болон бусад төрлийн хортой программуудаас сэргийлэхийн тулд NCSC-ийн “Интернэт орчинд аюулгүй байх зөвлөмж”-ийг үзнэ үү. Шинэчлэлтүүд ихэвчлэн сайжруулалт болон шинэ хувилбаруудыг агуулдаг: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **Төхөөрөмжөө ‘jailbreak’ эсвэл ‘root’ хийж болохгүй**, учир нь энэ нь аюулгүй байдлын хяналтыг тойрон гарахын тулд төхөөрөмжийн сул талыг ашигладаг. Ингэснээр төхөөрөмж халдлагад илүү өртөмтгий болдог. NCSC-ийн удирдамжийг үзнэ үү: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Аппуудаа удирдах

- **Аппуудаа болон тэдгээрийн зөвшөөрлийг шалгаж үзээрэй.** Хэрэв танд тус апп хэрэггүй бол устгана уу. Хортой програм нь ихэвчлэн камер, микрофон зэрэг хамгаалагдсан файлууд эсвэл дагалдах хэрэгсэлд халдах зориулалттай байдаг тул та боломжтой бол программын зөвшөөрлийг хязгаарлаж, мэдээлэлд халдах эрсдэлийг багасгана уу.
  - Apple хэрэглэгчдэд зориулсан апп зөвшөөрлийг шалгах арга: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Андройд хэрэглэгчдийн апп зөвшөөрлийг шалгах арга: https://support.google.com/android/answer/9431959?hl=en-GB

- **Мэдэхгүй аппуудыг автоматаар Google руу илгээх.** Хэрэв та Android хэрэглэгч бөгөөд Google Play Store-оос бусад эх сурвалжаас апп татаж авсан бол тухайн апп-ыг Google руу илгээж болох бөгөөд үүний тулд Play Store аппын тохиргоон дунд 'Play Protect' хэсгээс 'Хортой апп илрүүлэлтийг сайжруулах' тохиргоог идэвхжүүлэх шаардлагатай. Энэ нь хэрэглэгчдийг хамгаалахад тусалж хортой программ илрүүлэх програмыг уншуулах болно. Үүнийг хэрхэн тохируулах тухай мэдээлэл: https://support.google.com/android/answer/2812853?hl=en-GB

Кибер аюулгүй байдлын үйлчилгээг ашиглах

- **Холбоос дээр дарахаасаа өмнө URL-ийн найдвартай байдлыг шалгах үйлчилгээ ашиглаарай.** Google Transparency Report or Virus Total. үйлчилгээ ашиглан имэйл, мессеж эсвэл бусад эх сурвалжаас ирсэн холбоос аюулгүй эсэхийг шалгахын тулд эхлээд уншуулж болно. Мөн сэжигтэй файлууд болон аппликейшнүүдийг VirusTotal зэрэг хортой программ анализ хийгч платформд байршуулах боломжтой бөгөөд ингэснээр тухайн файл хортой эсэхийг илрүүлэхэд тусална. Хайлтын (Scan) программууд зарим тохиолдолд буруу үр дүн (false negative) гаргаж болзошгүйг анхаарна уу

- **Google-ийн “Advanced Protection” хөтөлбөрт бүртгүүлэх.** Энэ нь Gmail, Play Store зэрэг Google-ийн үйлчилгээг ашигладаг, халдлагад өртөх эрсдэлтэй хүмүүст зориулсан үнэгүй хамгаалалтын үйлчилгээ юм. Энэ үйлчилгээ нь Google-н үйлчилгээг ашиглах үед аюулгүй байдлыг дээшлүүлдэг: https://landing.google.com/advancedprotection/

- **Боломжтой тохиолдолд нэмэлт хамгаалалтын үйлчилгээнд бүртгүүлнэ үү.** Жишээлбэл, Их Британид цахим халдлагын эрсдэл өндөртэй хүмүүс цахим аюулгүй байдлын нэмэлт хамгаалалтын үйлчилгээ авах эрхтэй байж болно. Тавигдах шаардлага болон, дэлгэрэнгүй мэдээлэлийг дараах холбоосоос үзнэ үү: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

Эрсдлийг мэдээлэх

- **Хуурамч аккаунтыг илрүүлэх ба мэдээлэх.** Цахим халдлага үйлдэгч этгээдүүд өөрсдийн зорилгод хүрэхийн тулд хуурамч аккаунт үүсгэх эсвэл бодит аккаунтыг хакердах тохиолдол бий. Хэрэв та аккаунтыг хуурамч эсвэл халдлагад өртсөн гэж сэжиглэж байгаа бол платформд мэдэгдээд блоклоно уу. Олон төрлийн үйлчилгээ аккаунтыг баталгаажуулах үйл явцтай байдаг бөгөөд үүнд Instagram, Facebook-ийн ‘баталгаажсан тэмдэг’ зэрэг орно. Энэ нь тухайн аккаунт жинхэнэ эсэхийг тодорхойлоход тусална. NCSC нь нийгмийн сүлжээг аюулгүй ашиглах талаар зөвлөмж гаргасан бөгөөд үүнд хакердуулсан аккаунтыг хэрхэн баталгаажуулах, мэдээлэх тухай дэлгэрэнгүй мэдээлэл багтсан болно : https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **Залилангийн имэйл, мессеж, холбоос ашиглан хийдэг фишинг халдлага.** NCSC нь сэжигтэй имэйл хаяг болон вебсайтуудыг шалгаж, мөрдлөг явуулах боломжтой. Хэрэв та ямар нэгэн вебсайт, имэйл эсвэл зурвасыг сэжигтэй гэж үзвэл дараах хаягаар мэдээлэх боломжтой: https://www.ncsc.gov.uk/collection/phishing-scams

NCSC толь бичиг

- **Android**

Олон төрлийн ухаалаг гар утас, таблет үйлдвэрлэгчид ашигладаг Google-ийн гар утасны үйлдлийн систем.

- **Апп**

Аппликейшн буюу апп нь хэрэглэгч төхөөрөмждөө нэмэлт үйлдэл эсвэл агуулга ашиглах боломжийг олгодог, суулгаж болох эсвэл урьдчилан суулгагдсан программ хангамжийн багц юм.

- **Кибер аюулгүй байдал**

Төхөөрөмж, үйлчилгээ, сүлжээ болон тэдгээр дээрх мэдээллийг зөвшөөрөлгүй нэвтрэх, хулгайлах эсвэл гэмтээхээс хамгаалах үйл ажиллагаа.

- **Төхөөрөмж**

Суурин компьютер, ухаалаг гар утас, таблет зэрэг биет байдлаар оршин байдаг компьютер дээр суурилсан техник хангамж.

- **iOS**

Apple компанийн гар утас, таблет зэрэг төхөөрөмжүүдэд ашиглагддаг гар утасны үйлдлийн систем.

- **Хортой программ**

‘Хортой программ хангамж’ гэсэн үгнээс гаралтай Malware нь компьютерийн систем, сүлжээ болон төхөөрөмжид хохирол учруулж болзошгүй бүх төрлийн программ хангамжийг хэлнэ. Вирус, барьцаалагч программ, троян зэрэг төрлүүдийг багтаана.

- **Үйлдлийн систем**

Компьютер, таблет болон ухаалаг гар утас дээр ажилладаг, нэмэлт аппликейшн болон тоног төхөөрөмжийг ажиллуулахад шаардлагатай үндсэн программ хангамж.

- **Фишинг**

Хортой програм агуулсан байж болзошгүй вебсайтын холбоостой залилангийн имэйл эсвэл зурвас бөгөөд эдгээр нь хувийн мэдээлэл (жишээ нь хэрэглэгчийг нууц үг) эсвэл мөнгө шилжүүлэхэд төөрөгдүүлэх зорилготой байж болно.

- **Тагнуулын программ**

Хэрэглэгчийн зөвшөөрөлгүйгээр төхөөрөмж дээр суух бөгөөд мэдээлэл цуглуулан гуравдагч этгээд рүү илгээдэг хортой программын нэг төрөл юм.

- **Нийгмийн сүлжээ**

Facebook, X, Instagram зэрэг вебсайт болон аппликейшнүүд нь хэрэглэгчдийн нийтэлсэн агуулгыг (текст нийтлэл, зураг, видео гэх мэт) хуваалцах болон хариу өгөх боломжийг олгодог.

- **Ухаалаг утас**

Android болон iOS үйлдлийн системтэй, нарийн үйлдэл гүйцэтгэх чадвартай орчин үеийн ухаалаг гар утаснууд

- **Троян**

Энэ нь хууль ёсны программ мэт харагддаг боловч хэрэглэгчийн төхөөрөмжид зөвшөөрөлгүй нэвтрэх зорилготой хортой программын нэг төрөл юм.

- **URL**

Uniform Resource Locator. www буюу world wide web-д хандах хаяг бөгөөд жишээлбэл домэйн нэр (жишээ нь: www.bbc.co.uk) хэлбэрээр илэрхийлэгдэнэ.

- **Вирус**

Энэ нь хууль ёсны программ хангамжийг халдварлуулах зориулалттай хортой программын нэг төрөл бөгөөд тухайн программ ажиллах үед сүлжээгээр дамжин өөрийгөө хуулбарлан тархдаг.

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 халдлагын 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 үеийн байдлаар баталгаажсан байсан мэдээллийг агуулж байгааг анхаарна уу.

Энэхүү тайлан нь оролцогч агентлаг болон салбарын эх сурвалжаас авсан мэдээлэлд үндэслэн гаргасан болно. Энэхүү дүгнэлт болон зөвлөмжүүд нь бүх эрсдэлээс бүрэн хамгаалж чадахгүй бөгөөд зөвлөмжүүдийг дагаснаар эрсдэлээс 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.

Хавсралт: MOONSHINE & BADBAZAAR жишээг ажиглав

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

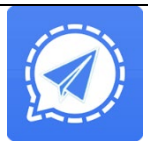
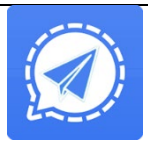
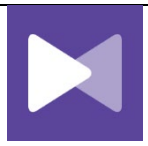
Эдгээр аппликешнүүдийн ихэнх нь тогтсон программуудтай ижил төстэй байгааг харуулж байна. Энэ нь алдартай брэндүүдийг "дуурайн мэхлэх" санаатай цахим халдлага үйлдэгч этгээдийн арга байх магадлалтай.

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.

Сэрэмжлүүлэх арга хэмжээний хэсэгт дурдсаны дагуу, та Android төхөөрөмж дээрээ ‘Хортой программ илрүүлэлтийг сайжруулах’ тохиргоог идэвхжүүлснээр Play Store-оос бусад эх сурвалжаас суулгасан программуудыг Google-д илгээж, аюулгүй эсэхийг шалгуулах боломжтой.

Программын нэр	Багцын нэр	Аппликейшны 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	

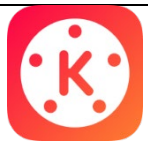
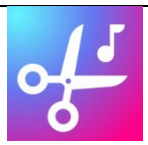
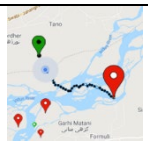
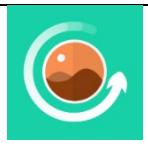
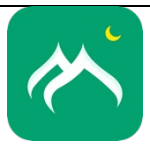
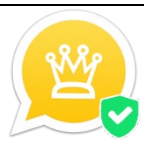
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

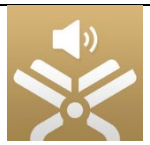
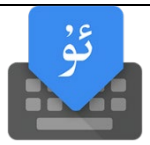
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore 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	
زىكرلەر	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