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

مەسلىھەت

«ئەسكى بازار» ۋە «ئاي نۇرى»: ئۇيغۇر، تەيۋەن ۋە تىبەت گۇرۇپپىلىرى ۋە پۇقراۋي جەمىيەت ئىشتىراكچىلىرىغا قارىتىلغان جاسۇسلۇق يۇمتاللىرى

2025-يىلى 9-ئاپرېل

«ئەسكى بازار» ۋە «ئاي نۇرى»: ئۇيغۇر، تەيۋەن ۋە تىبەت گۇرۇپپىلىرى ۋە پۇقراۋىي جەمىيەت ئىشتىراكچىلىرىغا قارىتىلغان جاسۇسلۇق يۇمتاللىرى

دۆلەتلىك تور بىخەتەرلىك مەركىزى ۋە ئۇنىڭ ھەمكارلاشقۇچىلىرى ئىككى خىل جاسۇسلۇق يۇمتالىنىڭ يۈكسەك خەتىرگە دۇچ كېلىۋاتقانلار ئۈچۈن يېڭى مەلۇماتلار ۋە بۇ خەتەرلەرنى ئازايتىش چارىلىرىنى ئېلان قىلدى.

خۇلاسە

ئەنگلىيە تور بىرلەشمىسى نىڭ ياردىمى ھەمدە دۆلەتلىك تور بىخەتەرلىك مەركىزى (NCSC UK) ۋە ئۇنىڭ خەلقئارالىق ھەمكارلاشقۇچىلىرىنىڭ ئورتاق كۈچ چىقىرىشى بىلەن مەزكۇر كۆرسەتكۈچ تەييارلاندى.

- **ئاۋسترالىيە سىگناللار ئىدارىسى قارمىقىدىكى ئاۋسترالىيە تور بىخەتەرلىك مەركىزى**
- **ئالاقە-ئۇچۇر بىخەتەرلىك ئورگىنى قارمىقىدىكى كانادا تور بىخەتەرلىك مەركىزى**
- **گېرمانىيە فېدېراتسىپ ئىستىخبارات ئىدارىسى**
- **گېرمانىيە فېدېراتسىپ ئاساسىي قانۇنىنى قوغداش ئىدارىسى**
- **ھۆكۈمەت ئۇچۇر-ئالاقە بىخەتەرلىك ئىدارىسى قارمىقىدىكى يېڭى زېللاندىيە دۆلەتلىك تور بىخەتەرلىكى مەركىزى**
- **ئامېرىكا قوشما شىتاتلىرى فېدېراتسىيە تەكشۈرۈش ئىدارىسى**
- **ئامېرىكا قوشما شىتاتلىرى دۆلەت بىخەتەرلىك ئىدارىسى**

بۇنىڭدا كىشىلەرنىڭ تەيۋەن، تىبەت، شىنجاڭ ئۇيغۇر ئاپتونوم رايونى قاتارلىق جايلار بىلەن، شۇنىڭدەك دېموكراتىيە ھەرىكەتلىرى ۋە فالۇنگۇڭ ھەركىتى بىلەن مۇناسىۋەتلىك شەخسلەر دۇچ كېلىۋاتقان ھەمدە كۈنسېرى ئېغىرلاۋاتقان قەبىھ تەھدىتلەر ھەققىدىكى

ئۇشبۇ قوللانما ئىككى تۈرلۈك دېلو ھەققىدىكى تەتقىقاتنى ئۆز ئىچىگە ئالىدىغان بولۇپ، قەبىھ تور مەشغۇلاتچىلىرىنىڭ «ئەسكى بازار» ۋە «ئاي نۇرى» نامىدىكى جاسۇسلۇق يۇمتالى ئارقىلىق قوللانغان تېخنىكا تەپسىلاتلىرى، جۈملىدىن ئەقلىي تېلېفونلاردىكى خىتاي دۆلىتى ئۈچۈن مەنپەئەتلىك، دەپ ھېسابلىنىدىغان ئۇچۇرلارنى قارىغا ئېلىش قىلمىشلىرىنى ئۆز ئىچىگە ئالىدۇ. ئۇ يەنە كىشىلەرنىڭ ئۆزلىرىنى، ئېلېكترونلۇق ئۇسكۇنىلىرىنى ۋە ئۇلاردا ساقلىنىۋاتقان ئۇچۇرلارنى قانداق قوغدىشىغا يېتەكچىلىك قىلىدۇ.

مەزكۇر كۆرسەتمە بىلەن بىرلىكتە دۆلەتلىك تور بىخەتەرلىك مەركىزى يەنە تولۇق تېخنىكىلىق تەپسىلاتلارنى ئۆز ئىچىگە ئالغان ئايرىم بىر كۆرسەتمىنىمۇ ئېلان قىلدى.

كىم خەۋپتە؟

مەزكۇر كۆرسەتمىنى تەييارلىغان ئورگانلار ۋە ئۇلارنىڭ ھەمكارلاشقۇچىلىرى شۇنى بايقىغانكى، «ئەسكى بازار» ۋە «ئاي نۇرى» مەخسۇس خىتاي دۆلىتى ئۆزلىرىنىڭ ئىچكى نوپۇزى، نىشانلىرى ۋە دۇنياۋى ئوبرازى ئۈچۈن تەھدىت، دەپ ھېسابلىغان شەخسلەرنى نىشان قىلغان. بۇنىڭ ئەڭ زور خەۋپىگە دۇچ كېلىدىغانلار تۆۋەندىكىلەرگە چېتىشلىق بولغانلىكى كىشىلەر بولۇپ، بۇنىڭ بىلەنلا چەكلىنىپ قالمايدۇ:

- **تەيۋەن مۇستەقىللىقى**
- **تىبەت ھەقلەر كۈرىشى**
- **ئۇيغۇر مۇسۇلمانلىرى ۋە شىنجاڭ ئۇيغۇر ئاپتونوم رايونىنىڭ ئىچى ياكى تېشىدىكى باشقا مىللىي تۈركۈمگە مەنسۇپ كىشىلەر**
- **دېموكراتىيە ھېمايىچىلىرى (خۇكۇكىنى ئۆز ئىچىگە ئالىدۇ)**
- **فالۇنگونىڭ مەنىۋى ھەرىكىتى**

بۇ يەنە غەيرى ھۆكۈمەت تەشكىلاتلىرى (NGO)، مۇخبىرلار، كارخانىلار ھەمدە ئۇشبۇ گۇرۇھلارنى ھېمايە قىلىدىغان، ئۇلار بىلەن تونۇشىدىغان ياكى باشقا تەرزدە ئۇلارغا ۋەكىللىك قىلىدىغان شەخسلەرنىمۇ ئۆز ئىچىگە ئالىدۇ. بۇ جاسۇسلۇق يۇمتالىنىڭ تورلاردا پەرقسىز شەكىلدە تارقىلىشى بۇ خىل يۇقۇملىنىشنىڭ خەۋپى ئۆز نۆۋىتىدە نىشاندىكى زىيانكەشلىككە ئۇچرىغۇچىلاردىنمۇ ھالقىپ چۈشىدىغانلىقىنى كۆرسىتىدۇ.

مەزكۇر كۆرسەتمە ئاشۇ خىل خەۋپلەرگە دۇچ كېلىۋاتقانلارنىڭ «ئەسكى بازار» ۋە «ئاي نۇرى» جاسۇسلۇق يۇمتاللىرىنىڭ تەھدىتلىرىگە ئۇنۇملۇك تاقابىل تۇرۇشىغا ياردەم بېرىشنى نىشان قىلىدۇ. تەۋسىيە قىلىنغان ئېھتىيات چارىلىرى تېخنىكا مەنىلەردىكى تور بىخەتەرلىكىگە دائىر مەسىلىھەتلەرنىڭ قوشۇمچىسى بولۇپ، ئۇلارنى ئايرىم تەدبىر دەپ چۈشىنىۋالماسلىق لازىم.

ئۇشبۇ قوللانمىدا كۆرسىتىلگەن كۆرسەتمىلەر بويىچە ئىش كۆرۈش ئارقىلىق پايدىلانغۇچىلار ئۆزلىرىنىڭ كۆچمە ئېلېكترونلۇق ئۇسكۇنىلىرى ۋە ئۇلاردىكى مەلۇماتلار دۇچ كېلىش ئېھتىمالى بولغان خەۋپلەرنى ئازايتالىشى مۇمكىن.

«ئاي نۇرى» ۋە «ئەسكى بازار» دېگەنلەر تروياn ئېتى ۋىرۇسلىرىنىڭ مىساللىرىدۇر؛ ئۇلارنىڭ يامان غەرەزلىك ئىقتىدارى ئەپلەر دۇكىنى ياكى باشقا خىل ھۆججەت ھەمبەھىرلەش مۇلازىمەتلىرىدىن چۈشۈرگىلى بولىدىغان نورمال ئەپلەرنىڭ ئىچكى قىسمىغا يوشۇرۇنغان بولىدۇ.

بۇ ئەپلەر پايدىلانغۇچىلارنى ئاشۇ ئەپلەرنى چۈشۈرۈش ۋە ئېلىكترونلۇق ئۇسكۇنىلەرگە ئورنىتىشقا قىزىقتۇرۇش ئۈچۈن لايىھىلەنگەن. بۇ ئەپلەر ئورنىتىلغاندىن كېيىن ئاشۇ ئۇسكۇنىدىكى ئاجىز نۇقتىلاردىن پايدىلىنىپ ئىجازەت بېرىلمىگەن مەشغۇلاتلار بىلەن شۇغۇللىنىدۇ، ياكى بولمىسا پايدىلانغۇچى ئاشۇ ئەپكە بەرگەن ئىجازەت ئارقىلىق تۆۋەندىكى ئۇچۇرلارنى كۆرىدۇ ۋە چۈشۈرۈۋالىدۇ:

- **ئورۇن ھەققىدىكى سانلىق مەلۇماتلار، جۈملىدىن دەرقەدەم بولۇپ ئىز قوغلاش**
- **مىكروفون ۋە كامېراغا كىرىش**
- **شۇ ئۇسكۇنىدە ساقلانغان ئۇچۇرلار، سۈرەتلەر ۋە باشقا ھۆججەتلەرگە كىرىش**
- **ئۇسكۇنە ئۇچۇرلىرى ۋە باشقىلار**

كېيىن بۇ تور ئارتىستلىرى ئاشۇ خەۋپ ئاستىدىكى گۇرۇپپىلارنىڭ يوللۇق قىزىقىشلىرىدىن پايدىلىنىش ئارقىلىق تېخىمۇ كۆپ زىيانكەشلىك ئوبيېكتلىرىنى بايقاش ۋە ئۇلارنىڭ ئۇسكۇنىلىرىنى يۇقۇملاندۇرۇش، شۇنىڭدەك ئۇلارنىڭ ئۇچۇرلىرىنى قولغا كەلتۈرۈش بىلەن شۇغۇللىنىدۇ. ئۇلارنىڭ بۇنداق قىلىشتىكى ئۇسۇللىرىنىڭ بىرى زىيانكەشلىككە ئۇچرىغۇچىلارنى جەلپ قىلىشى مۇمكىن، دەپ قارىلىدىغان ئەپلەرنى لايىھىلەش بولۇپ، بۇئەپلەر ئانا تىلىنى ھېمايە قىلىدىغان، خىتاينىڭ تىبەت ياكى شىنجاڭ رايونىغا خاس مەزمۇنلارنى ئۆز ئىچىگە ئالىدىغان شەكىلدە بولىدۇ.

بۇ كۆرسەتمىدىكى ئەملىي تەتقىقاتلار بۇ ھەقتىكى بەزى مىساللارنى كۆرسىتىپ بېرىدىغان بولۇپ، «تىبەت بىرىنچى» ۋە «ئۇيغۇر قۇرئان» قاتارلىق ئەپلەرنى ئۆز ئىچىگە ئالىدۇ.

تور ھۇجۇمچىلىرى نىشانىدىكى زىيانكەشلىك ئوبيېكتلىرى پائالىيەت قىلىدىغان تور مۇنبەرلىرىدە ئاكتىپ پائالىيەتتە بولۇش ئارقىلىق زىيانكەشلىك ئوبيېكتلىرىنى يۇقۇملاندۇرۇش دەرىجىسىنى ئەڭ زور دەرىجىدە ئاشۇرىدۇ. كۆزىتىشلەر نەتىجىسىدە ئۇلارنىڭ تىبەت بىلەن ئالاقىدار بولغان Telegram قانالىلىرىدا ۋە Reddit مۇنبەرلىرىدە قەستەن جاسۇسلۇق يۈمتاللىرىنى ھەمبەھىرلەۋاتقانلىقى مەلۇم بولدى. مەزكۇر كۆرسەتمىدىكى ئەملىي تەتقىقاتلارمۇ مۇشۇ خىل ئۇسۇللارنىڭ قوللىنىلغانلىقى ھەققىدىكى مىساللارنى نامايەن قىلىدۇ.

زىيانلىق ئەپلەر ھەرقاچان مۇستەقىل ھۆججەت شەكلىدە ھەمبەھىرلىنىدۇ. مەسىلەن، Android ئۇسكۇنىلىرىدىكى APK ھۆججەتلىرى دائىم قوللانغۇچىلارنىڭ چۈشۈرۈشى ۋە ئورنىتىشىنى تەلەپ قىلىدۇ. تور ھۇجۇمچىلىرى ئۆزلىرىنىڭ جاسۇسلۇق يۈمتاللىرىنى رەسمىي ئەپ دۇكانلىرى بولغان گۇگۇل ئويۇن دۇكىنى (Google Play Store) ۋە ئالما ئەپ دۇكىنى (Apple App Store)غا يۈكلەپ قويۇش، ياكى بولمىسا ئىلگىرىكى زەرەرسىز ئەپلەرگە زەرەرلىك كودلارنى قوشۇپ قويۇش ئارقىلىق راستتەك كۆرسىتىشكە ئۇرۇندۇ. ھالبۇكى رەسمىي ئەپ دۇكانلىرىنىڭ بىخەتەرلىك تەدبىرلىرى ۋە تەكشۈرۈش ھالقىلىرى مەۋجۇت بولغاندا بۇ تور ھۇجۇمچىلىرىنىڭ بۇ چارىلىرىمۇ ئانچە بەك ئىشلەپ كەتمەيدۇ. بۇ ھال رەسمىي ئەپ دۇكانلىرىدىن چۈشۈرۈلگەن ئەپلەرنى بىخەتەرمۇ قىلالىسىمۇ ئەملىي تەتقىقاتلار ۋە دۆلەتلىك تور بىخەتەرلىكى مەركىزى (NCSC) ئىشلىگەن «ئەپ دۇكانلىرىدىكى خەۋپلىك ھەققىدە دوكلات» تا كۆرسىتىلگەندەك بۇ جەريانىنمۇ مۇكەممەل دەپ كەتكىلى بولمايدۇ.

تۆۋەندىكى تۆت خىل كۆرسەتمىگە رىئايە قىلىش سىزنى ئۇشبۇ كۆرسەتمىدە كۆرسىتىلگەن خېپىم-خەتەرلەردىن ساقلاپ قالىدۇ.

تېخنىكا تەپسىلى مەسلىھەتلەر ئۈچۈن «خېپىم-خەتەرنى ئازايتىش» ھەققىدىكى بۆلەككە قارالسۇن.

National Cyber Security Centre
a part of GCHQ

Four tips to stay safe when using your smartphone

Reduce the risk from malicious apps with good cyber hygiene, then follow these four principles:

Stay Mainstream

Don't root or jailbreak devices, only use trusted app stores.

Stay Organised

Review installed apps and permissions regularly.

Stay in Touch

Report suspicious messages and files to online services.

Stay Alert

Stay vigilant on social media and check shared files and links.

تەتقىقات دېلولىرى

بۇ ئىككى تەتقىقات دېلوسى «ئاي نۇرى» ۋە «ئەسكى بازار» نىڭ قانداق ئىشلەيدىغانلىقى، شۇنىڭدەك زەھەرلىك تور ھۇجۇمچىلىرىنىڭ ئەڭ زور خەۋپىنىكى كىشىلەرنى قانداق قارىغا ئالىدىغانلىقىنى نامايەن قىلىپ بېرىدۇ.

بىرىنچى تەتقىقات دېلوسى: ئاي نۇرى

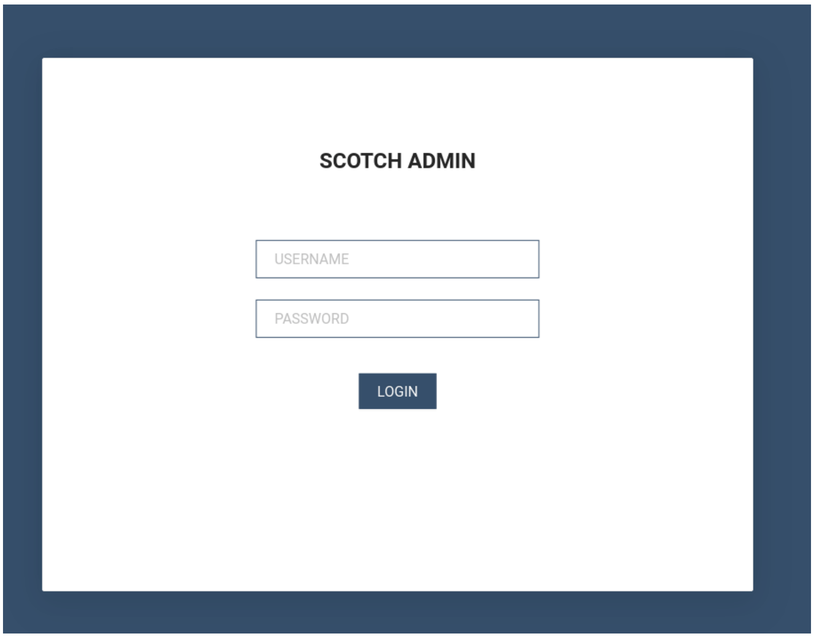
«ئاي نۇرى» بولسا ئاندرويد (Android) سىستېمىسىدا ئىشلەيدىغان جاسۇسلۇق يۇمتالى بولۇپ، 2019-يىلى «يۇقرالار تەجرىبىخانىسى» ئۇلارنىڭ تىبەت پائالىيەتچىلىرىنى نىشان قىلىدىغانلىقىنى مەلۇم قىلغانىدى. «ئاي نۇرى» زىيانكەشلىك ئوبېكتلىرىنى جەلپ قىلىش ئۈچۈن راست ئەپ سىياقىدا نامايەن بولغان. ئۇ ئادەتتە «تېلېگرام» (Telegram) قاناللىرى ئارقىلىق ھەمبەھىرلەنگەن ھەمدە ئۇنىڭ ئۇلانمىلىرى «ۋاتسئەپ» WhatsApp ئارقىلىق ئەۋەتىلگەن.

«ئاي نۇرى»نىڭ كەڭ كۆلەملىك نازارەت ئىقتىدارى بولۇپ، تۆۋەندىكىلەرنى ئۆز ئىچىگە ئالىدۇ:

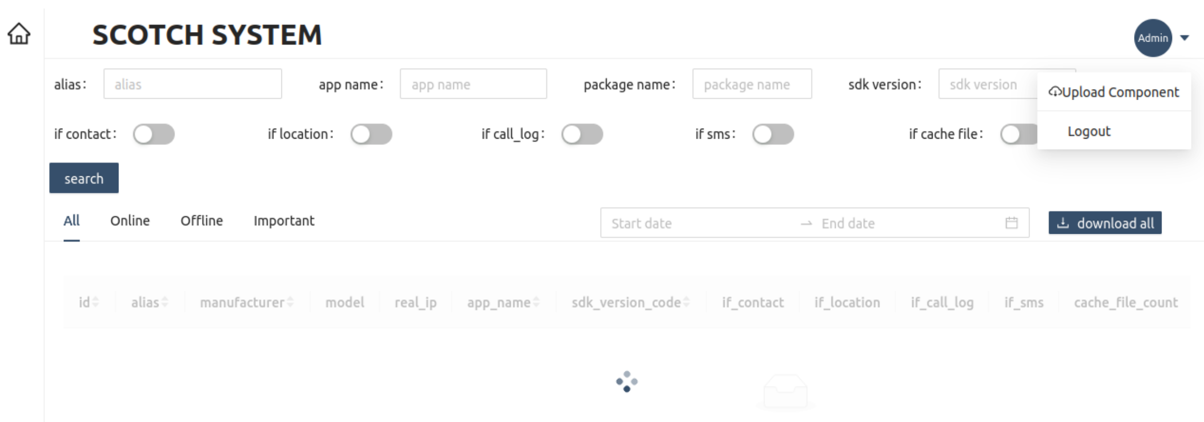
- **ئورۇن ھەققىدىكى سانلىق مەلۇماتلار، جۈملىدىن دەرقەدەم بولۇپ ئىز قوغلاش**
- **جانلىق ئاۋاز ۋە سۈرەتكە ئېلىش**
- **ھۆججەتلەرنى ئۈسكۈنىدىن چۈشۈرۈۋېلىش**
- **ئۈسكۈنە ئۇچۇرلىرىنى تارتىپ چىقىش**
- **ئۈسكۈنىدە ئاۋاز ھۆججىتىنى قويۇش**

«**ئاۋازلىق قۇرئان. apk**» بولسا «**ئاي نۇرى**»نىڭ ئۇيغۇرلارنى نىشان قىلىشتا قوللىنىلغانلىقىنىڭ بىر مىسالىدۇر. ھۆججەت نامى ئۈچۈن ئۇيغۇرچە سۆز قوللىنىش ۋە بۇنىڭ «قۇرئان» ھەققىدىكى ئەپ ئىكەنلىكىنى كۆرسىتىشتە بۇ ئەپنىڭ ئۇيغۇر مۇسۇلمانلىرىنىڭ دىققىتىنى ئۆزىگە جەلپ قىلىشى كۆزلەنگەن.

ئۇنى ئورناتقان ھامان زەھەرلىك تور ھۇجۇمچىلىرى زىيانكەشلىك ئوبېكتلىرىنىڭ ئۈسكۈنىلىرىدىن ئۇچۇر يىغالايدۇ. بۇ ئۇچۇرلارنى بولسا «باشقۇرغۇچى سكوچ» (SCOTCH ADMIN) كۆزنىكى ئارقىلىق كۆرۈشكە بولىدۇ.



تىزىم ئارقىلىق كىرگەندىن كېيىن تور ھۇجۇمچىلىرى تۆۋەندىكى ئېكران سۈرىتىدە كۆرسىتىلگەن تەرىزدە ئاشۇ بەتلەرنى كۆرەلەيدۇ. بۇ بەتتە زەرەرلەنگەن ئۈسكۈنىلەرنىڭ تەپسىلاتى ۋە تور ھۇجۇمچىلىرىنىڭ زەرەرلەنگەن ئۈسكۈنىگە كىرىش دەرىجىسى كۆرسىتىلگەن.



زىيانلىق يۇمتاللارنى باشقۇرۇش كۆزنىكى توپلانغان ئۇچۇرلارنى كۆرسىتىپ بېرىدۇ. ئۇلار:

- **ئۈسكۈنىگە كىرىش دەرىجىسى**
- **«قىسقا ئۇچۇر مۇلازىمىتى» (SMS) ئۇچۇرلىرى**
- **تېلېفون خاتىرىسى**
- **ئورۇن ئۇچۇرلىرى**
- **ئۈسكۈنە ئۇچۇرلىرى**

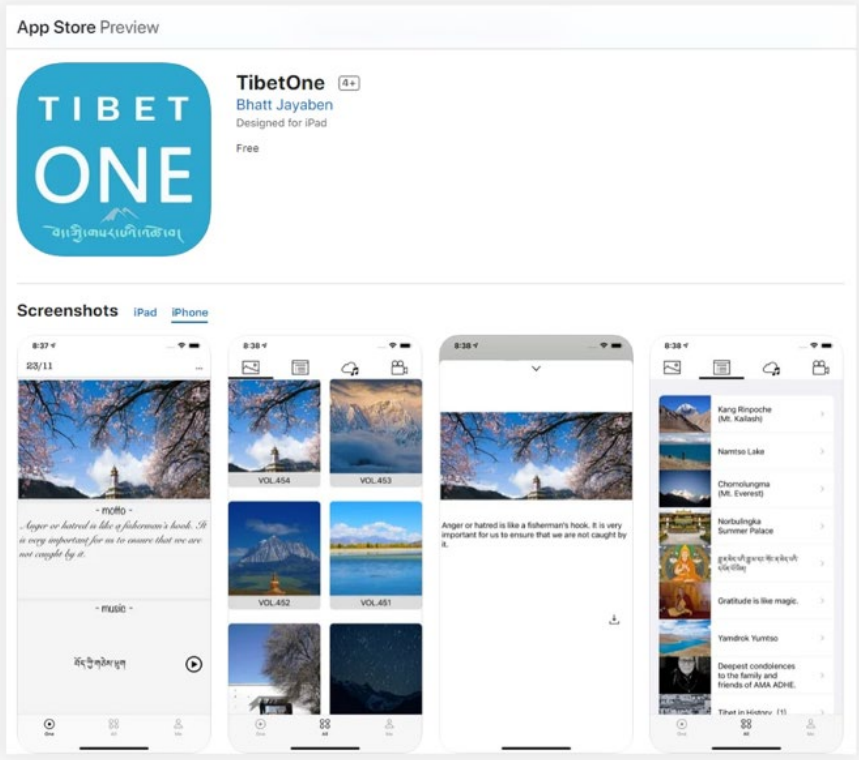
«تور بىرلەشمىسى» بىلەن ھەمكارلىشىپ «دۆلەتلىك تور بىخەتەرلىكى مەركىزى» مەخسۇس ئورگان تەسىس قىلىپ «مىكرو يۇزلىنىش» (Trend Micro) نى مەنبە قىلغان ھالدا «ئاي نۇرى»نىڭ قىدىرىش قوراللىرى ۋە تىزىم ئارقىلىق كىرىش تاختىسى ئوتتۇرىسىدىكى تەكرارلىقنى خەۋەر قىلغانىدى. ئۇنىڭ HTML ماۋزۇسىدا UPSEC دېگەن سۆز ئۇچرايدۇ. بۇنىڭ تولۇق تەپسىلاتى ئۇچۇن «قوشۇمچە تېخنىكىلىق مەسلىھەت» قىسمىغا قاراڭ.

«تور ئىستىخباراتى» (Intelligence Online) نىڭ مەلۇماتلىرىغا ئاساسلانغاندا UPSEC دېگىنى «سىچۇەن دېنكې تور بىخەتەرلىكى تېخنولوگىيە چەكلىك شىركىتى»نى كۆرسىتىدۇ.

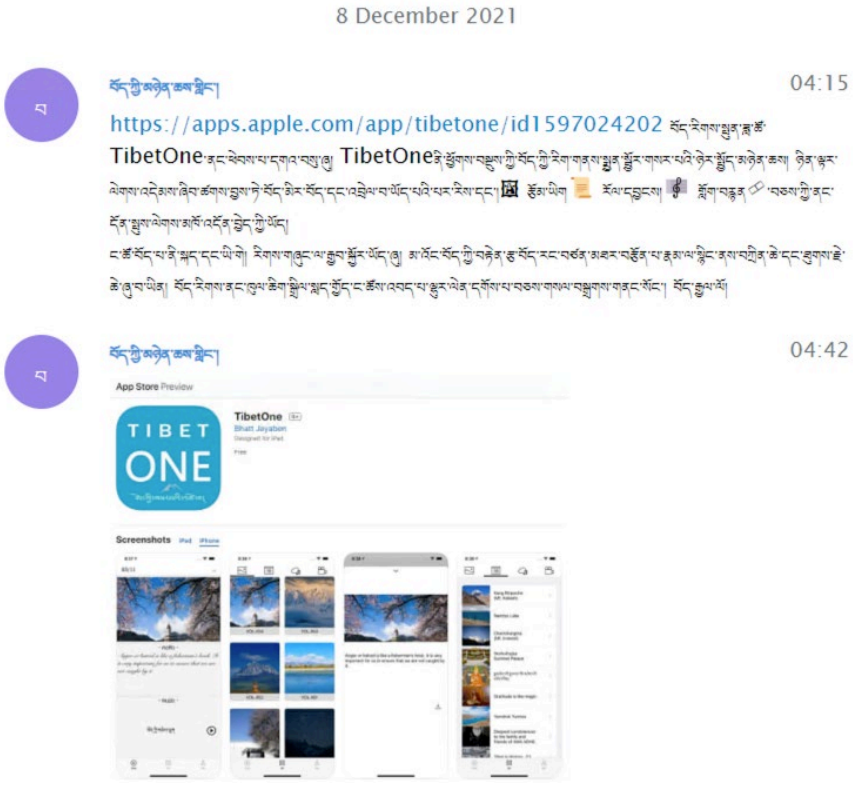
ئىككىنچى تەتقىقات دېلوسى: «ئەسكى بازار»

«ئەسكى بازار» بولسا iOS ۋە Android نۇسخىلىرىدىكى يان تېلېفونلىرىغا زەرەر يەتكۈزگۈچى يۇمتال بولۇپ ئۇيغۇرلار، تىبەتلەر ۋە تەيۋەنلىك شەخسلەرنى نىشان قىلغان. مەزكۇر يۇمتال ئىجتىمائىي تاراتقۇ سۇپىلىرى ۋە رەسمىي ئەپ دۇكانلىرى ئارقىلىق تارقىتىلغان .

Lookout ۋە Volexity قاتارلىقلارغا ئاساسلانغاندا «ئەسكى بازار» يۇمتالى تىبەتلەرنى نىشان قىلىشتا «تىبەت بىرىنچى» (**TibetOne**) ناملىق ئەپنى ۋاستە قىلغان. «تىبەت بىرىنچى» ناملىق ئەپ بولسا زەرەرلىك تور ھۇجۇمچىلىرى ياساپ چىققان iOS مۇھىتىدىكى ئەپ بولۇپ، ئۇسكۇنە ئۇچۇرلىرى ۋە ئورۇن مەلۇماتلىرىنى كۆرۈش ئىقتىدارىغا ئىگە. بۇ ئەپ 2021-يىلى دېكابىردا «ئالما» شىركىتىنىڭ ئەپ دۇكىنىغا يۈكلەنگەن بولۇپ، ھازىر مەۋجۇت ئەمەس. زەرەرلىك يۇمتالنى تېخىمۇ كۆپ كىشىلەرگە تارقىتىش ئۇچۇن تور ھۇجۇمچىلىرى «تېلېگرام» قانىلىدا «**تىبەت تېلېفونى**» ناملىق بىر ئەپنى كەڭ كۆلەمدە بازارغا سالغان.

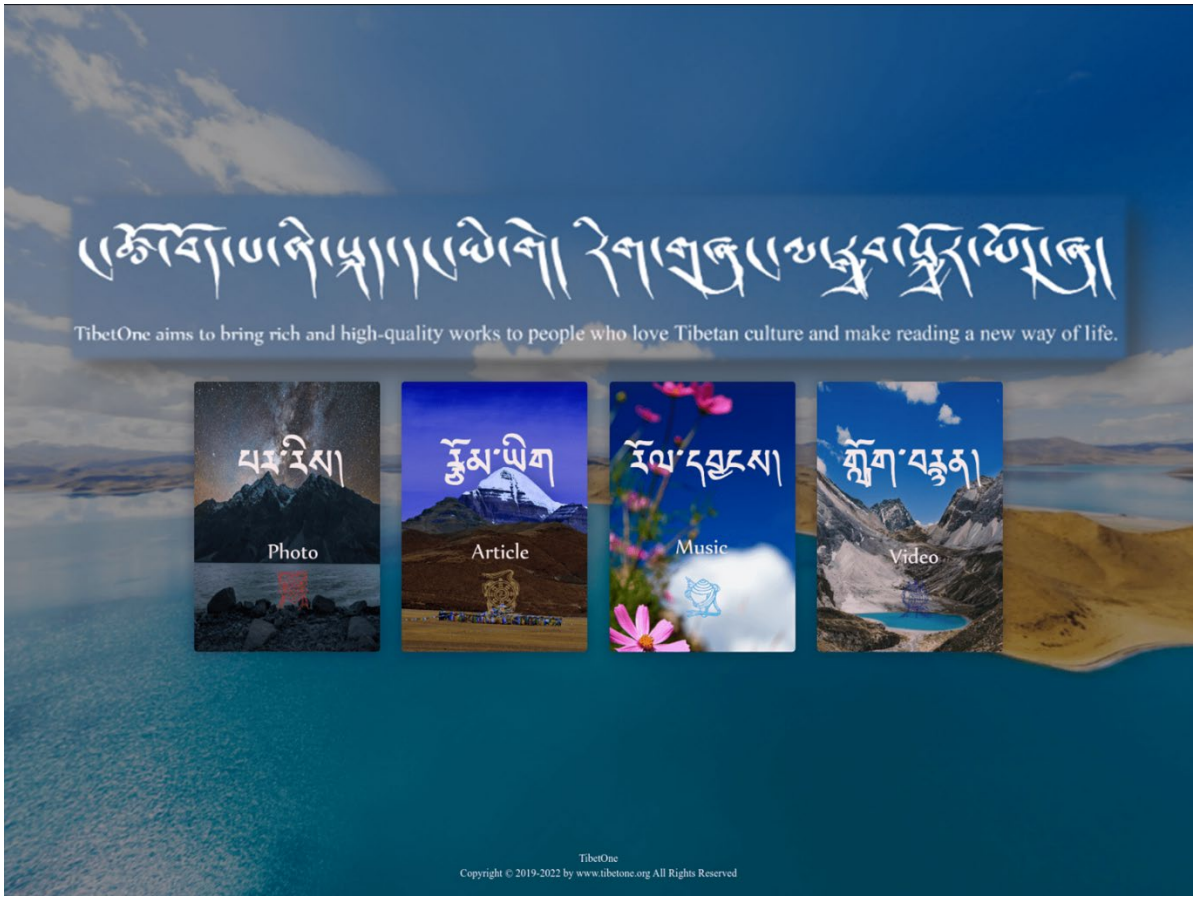


رەسىملەر: «تىبەت بىرىنچى» نامىلىق ئەپنىڭ «ئالما» ئەپ دۇكىنىدىكى كۆرۈنۈشى. بۇ ئەپ كىيىنچە دۇكاندىن چىقىرىۋېتىلگەن.



رەسىملەر: «تىبەت بىرىنچى» نامىلىق ئەپنىڭ «تېلېگرام» قانالىدىكى ھەمبەھىرلىنىشى

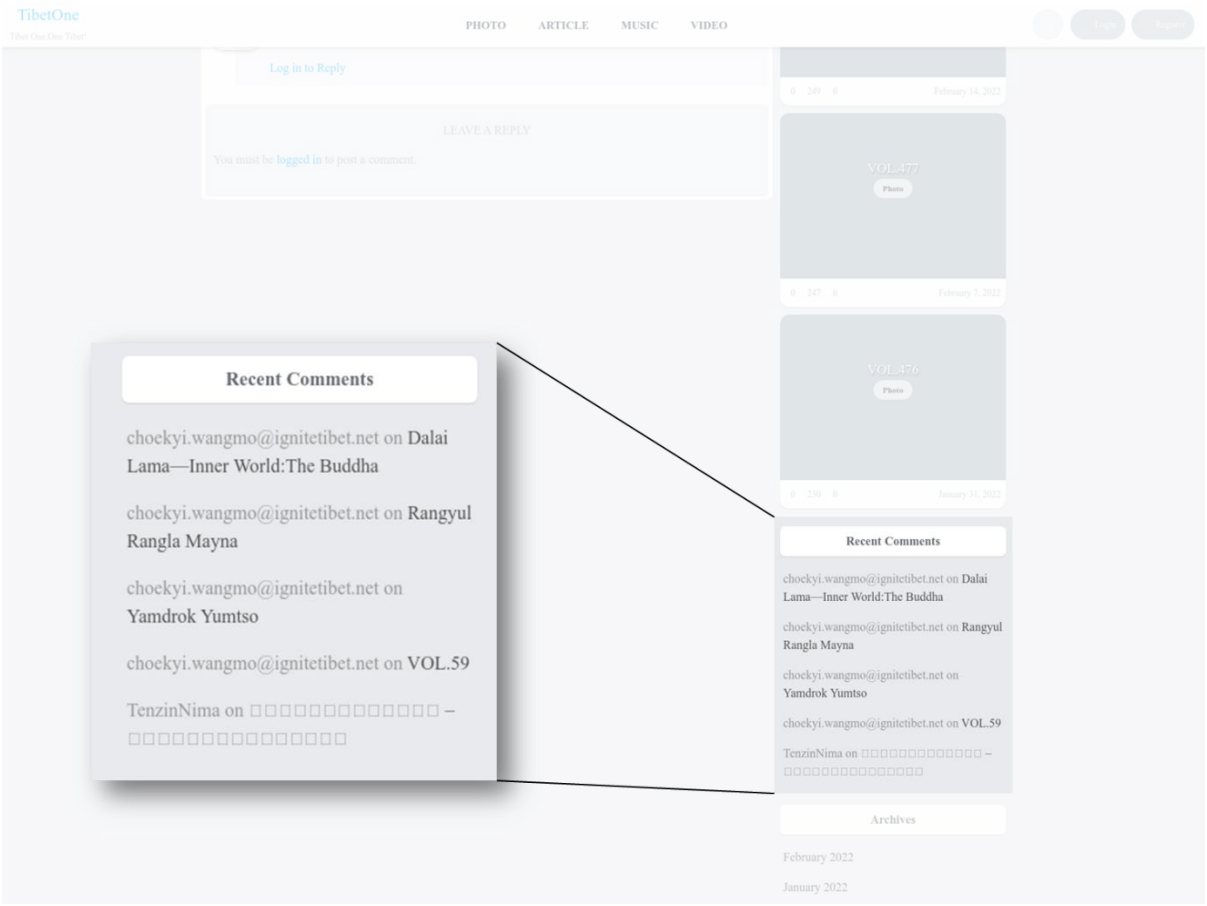
بۇ ئەپنى راستتەك قىلىپ كۆرسىتىش ئۈچۈن تور ھۇجۇمچىلىرى يەنە «**tibetone\[.]org**» ناملىق بىر تور بەت قۇرۇپ چىققان. بۇ تور بەتتە بۇ ھەقتە چۈشەنچە بېرىپ «بىز تىبەت مەدەنىيىتىنى سۆيىدىغان ھەمدە بۇ ھەقتىكى ئەسەرلەرنى ئوقۇشنى ھاياتىنىڭ بىرىگە مۇساپىسىگە ئايلاندۇرغان كىشىلەرگە مول مەزمۇنلۇق ۋە يۇقىرى سۈپەتلىك ئەسەرلەرنى تەقدىم ئېتىمىز» دېگەن.



رەسىملەر: «tibetone\[.]org» تور بېتىنىڭ ئانا سەھىپىسى

بۇ سۇرەت مۇناسىۋەتلىك قىسىملارنى ئېنىقراق كۆرسىتىش ئۈچۈن تەھرىرلەنگەن.

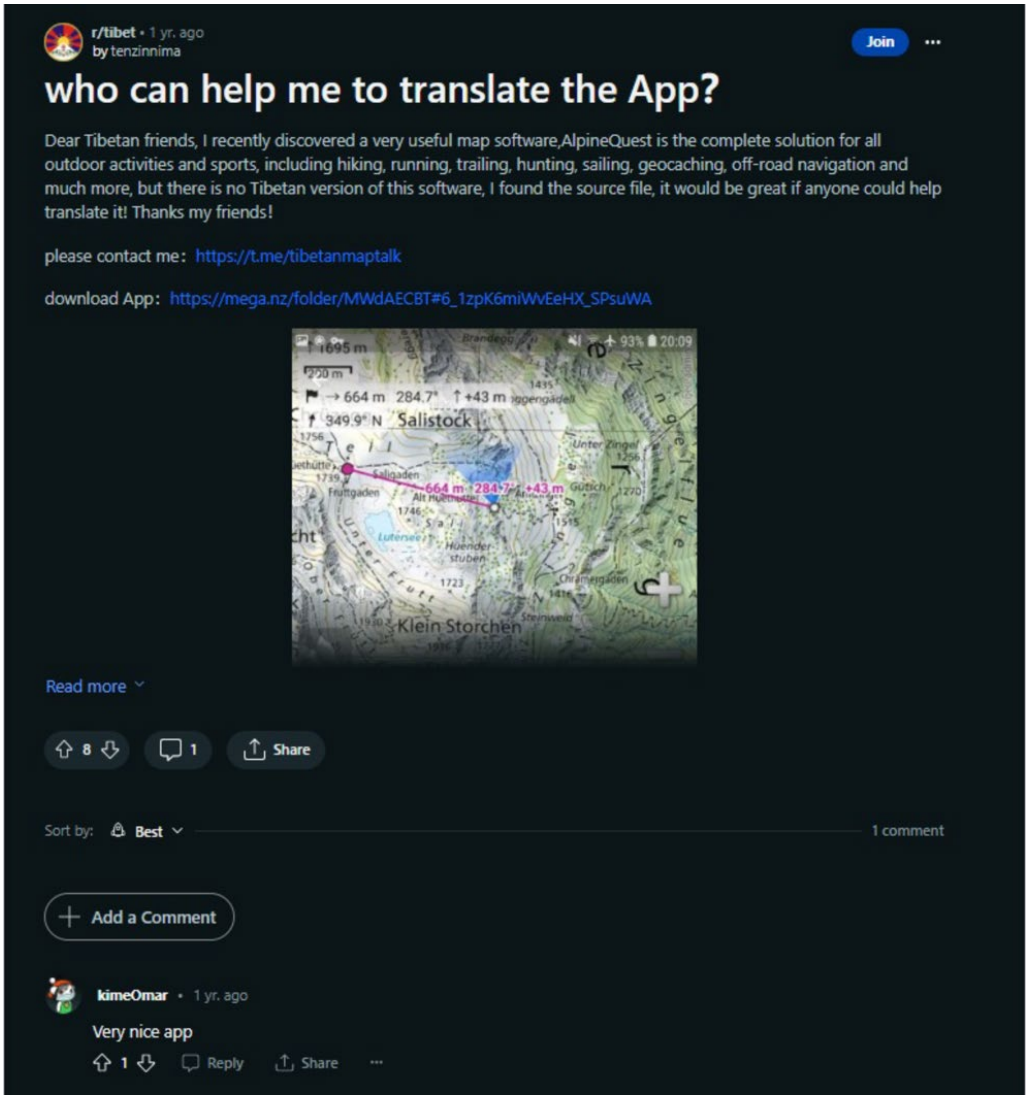
بۇ تور بەتنىڭ ماقالىلار سەھىپىسى بار بولۇپ، ئۇنىڭدا پايدىلانغۇچىلارغا پىكىر قالدۇرۇش ئىمكانىيىتى بېرىلگەن. پىكىرلەرنىڭ بىر قىسمىنى '**choekyi.wangmo@ignitetibet.net**' نامىدىكى ئېل خەت ئادرېسى قالدۇرغان بولۇپ، بۇ ئادرېسنىڭ زەھەرلىك تور ھۇجۇمچىلىرىنىڭ كونترول‌لۇقىدا ئىكەنلىكى تەخمىن قىلىنىدۇ. بۇ ئادرېس «**چوكيى ۋاڭمو**» نامىدا ئېچىلغان بولۇپ، بۇ كىشى «تىبەت كىشىلىك ھوقۇق ۋە دېموكراتىيە مەركىزى»دە تىبەت پەرۋەر شەخس سۈپىتىدە تىلغا ئېلىنىدۇ. بۇمۇ بەلكىم ئاشۇ ئەپنى راستىنلا تىبەت مۇستەقىللىقىنى تەشەببۇس قىلىدىغاندەك قىلىپ كۆرسىتىش ئۈچۈن ئوتتۇرىغا چىققان ئويۇنلارنىڭ بىرى بولۇشى مۇمكىن.



رەسىملەر tibetone\[.]org : تور بېتى زەرەرلىك تور ھۇجۇمچىلىرىنىڭ كونتروللۇقىدا بولۇشى مۇمكىن، دەپ قارىلىنىۋاتقان قوللانغۇچىلار قالدۇرغان پىكىرلەرنى نامايەن قىلماقتا.

بۇ سۇرەت مۇناسىۋەتلىك قىسىملارنى ئېنىقراق كۆرسىتىش ئۈچۈن تەھرىرلەنگەن.

Volexity بولسا بۇ نامىنىڭ Reddit [4][3] مۇنبىرىدە «**Tibetanmaptalk**» نامىدىكى Telegram قانىلىنى بازارغا سېلىۋاتقان يەنە بىر قوللانغۇچى نامى ئىكەنلىكىنى مەلۇم قىلدۇ. ئۇ يەنە «**AlpineQuest**» نامىدىكى زەرەرلىك ئەپنى چۈشۈرىدىغان بىر ئۇلانمىنى ئۆز ئىچىگە ئالىدىغان بولۇپ، بۇ ئەپ ئادەتتە Android ئۈسكۈنىلىرىدىكى يول باشلاش ئەپلىرىدىن بىرىدۇر. تەمىنلەنگەن چۈشۈرۈش ئۇلانمىسى «مېگا» نامىدىكى ئۇچىنچى تەرەپنىڭ ھۆججەت ھەمبەھىرلىگۈچى مۇلازىمىتى ھېسابلىنىدۇ.



رەسىملەر: Reddit مۇنبىرىدىكى يازمىلار ئاشۇ يامان غەرەزلىك تور ھۇجۇمچىلىرىنىڭ كونتروللۇقىدىكى ھېسابقا مەنسۇپ بولۇپ، ئۇلار يامان غەرەزلىك پروگراممىلارنى بازارغا سېلىپ كەلگەن.

تورى دىققەت قىلغان يەنە بىر نۇقتا شۇكى، بۇ يازمىلارغا پىكىر يازغان «**KimeOmar**» نامىدىكى يەنە بىرەيلەننىڭ Reddit مۇنبىرىدىكى قوشۇمچە سۇيىقەستچىلىرىنىڭ بىرىدە زەرەرلىك ئەپلەرنى ھەمبەھىرلەۋاتقانلىقى بايقالغان. بۇ ئاشۇ يامان غەرەزلىك تور ھۇجۇمچىلىرىنىڭ ئوخشىمىغان ئىجتىمائىي تاراتقۇ ماتېرىياللىرىدىن پايدىلىنىپ ئۆزلىرىنىڭ يازمىلىرىنى راستتەك قىلىپ كۆرسىتىش ئۇرۇنۇشىنىڭ ئىپادىسى بولۇشى مۇمكىن.

باھالاش

«ئەسكى بازار» ۋە «ئاي نۇرى» ئەپلىرى ئۇيغۇر، تىبەت ۋە تەيۋەن جامائىتىنى نىشانغا ئېلىش ئۈچۈن كۆپلىگەن ئىجتىمائىي ئىنتېرنېتلىق ئۇسۇللىرىدىن پايدىلانغان. خۇسۇسەن:

- ئۇيغۇر تىلىدىكى قۇرئان ئەپلىرىگە ئوخشاش بۇ خىلدىكى تېرورلاشتۇرۇلغان ئەپلەر ئاشۇ جامائەتلەرنى قىزىقتۇرۇش مەقسىتىدە نىشان قىلىنغان زىيانكەشلىك ئوبيېكتلىرىغا ماسلاشتۇرۇلغان.
- تېرورلاشتۇرۇلغان بۇ ئەپلەرنى رەسمىي ئەپ دۇكانلىرىغا قوشۇپ قويۇش بولسا ئۇلارنى ئاسانلا راست ئەپتەك قىلىپ كۆرسىتىش رولىنى ئوينىغان. يەنە بىر ياقتىن ھەرقايسى توپلاردا ھەمبەھىرلەش ئارقىلىق ئاشۇ جامائەت ئىچىدە ئىشەنچ قازىنىشنى مەقسەت قىلغان.

«ئەسكى بازار» ۋە «ئاي نۇرى» ئاساسەن خىتاي ھۆكۈمىتى ئۈچۈن پايدىلىنىش قىممىتى بولغانلىكى ئۈچۈرلارنى توپلاپ ماڭغان. گەرچە «ئەسكى بازار» «ئاي نۇرى»نىڭ ئۇيغۇر، تىبەت ۋە تەيۋەن پائالىيەتچىلىرىنى observed نىشان قىلغانلىقى بايقالغان بولسىمۇ، يەنە باشقا يامان غەرەزلىك پروگراممىلار خىتايدىكى باشقا ئاز سانلىق گۇرۇپپىلارنى نىشان قىلغان. خىتاي ئىچى ۋە سىرتىدا «خىتاي ھاكىمىيىتىنىڭ مۇقىملىقىغا تەھدىت سالىدىغان سەۋەبلەرنى قوللايدۇ» دەپ قارىلىدىغانلىكى پۇقرالار ئاساسەن «ئەسكى بازار» ۋە «ئاي نۇرى»غا ئوخشاش يانفون جاسۇسلۇق ئەپلىرىنىڭ خەۋپىگە دۇچ كەلمەكتە. ئورۇن، ئاۋاز ۋە سۈرەت ئۇچۇرلىرىنى قولغا چۈشۈرۈۋېلىش ئىقتىدارى شۇبھىسىزكى نىشان ئوبيېكتىنىڭ پائالىيەتلىرى ھەققىدە دەرھەدەم مەلۇماتلار بىلەن تەمىنلەش ئارقىلىق كەلگۈسىدىكى نازارەت ۋە تەقىب پائالىيەتلىرى ئۈچۈن پۈرسەت يارىتىپ بېرىدۇ.

يانفون ئەپلىرىنى قوللانغۇچىلار ئۇچۇن خەۋپىنى ئازايتىش چارىلىرى

كۆرسەتمىنى تەييارلىغۇچىلار ئەملي تەتقىقاتلاردا تەسۋىرلەنگەن تەھدىتلەرگە تاقابىل تۇرۇش ئۇچۇن تۆۋەندىكى خەۋپسىزلىك چارىلىرىنى قوللىنىشقا رىغبەتلەندۇرىدۇ. بۇ تەۋسىيەلەر NCSC نىڭ ئەڭ ياخشى ئەملي كۆرسەتمىلىرىنى ئاساس قىلىدۇ. ئاۋستىرالىيە ۋە ئامېرىكا تەۋسىيدىكى ئوقۇرمەنلەر ئەڭ ياخشى ئەملي كۆرسەتمىلەر ئۇلىنىشى ئۇچۇن «تېخمۇ كۆپ ئوقۇشلۇق» قىسمىغا قارا.

ئۇسكۇنىڭىزنى بىخەتەر ساقلاڭ

- **ئەپلەرنى پەقەت گۇگۇلنىڭ «ئويۇن دۇكىنى» ياكى «ئالما» شىركىتىنىڭ «ئەپ دۇكىنى»غا ئوخشاش رەسمىي ئەپ دۇكانلىرىدىن چۈشۈرۈڭ.** گۇگۇلنىڭ «ئويۇن دۇكىنى» ۋە ئالما شىركىتىنىڭ «ئەپ دۇكىنى» يۇمتاللارنى پايدىلىنىشقا تاپشۇرۇشتىن ئاۋۋال ۋىرۇسلارنى تەكشۈرىدۇ ھەمدە شۇ ئارقىلىق سىزنىڭ چۈشۈرگەن ئەپلىرىڭىزنىڭ بىخەتەر بولۇشىغا تېخمۇ زور ئىشەنچ ھاسىل قىلىدۇ. ئىشەنچلىك دۇكانلاردىن چۈشۈرگەن ئەپلەرمۇ قىسمەن خەۋپلەرنى پەيدا قىلىشى مۇمكىن، ئەمما ئەپلەرنى باشقا مەنبەلەردىن چۈشۈرۈش سىزنى ھېچقانداق دەرىجىدە قوغداپ قالالماسلىقى مۇمكىن. مەركىزى» (NCSC)نىڭ ئەپ دۇكانلىرىدىكى خەۋپلەر توغرىسىدا بىر مەلۇماتنامە تەييارلىغان: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **ئۇسكۇنىلىرىڭىزنى ۋە ئەپلەرنى يېڭىلاپ تۇرۇڭ** . ئەپلەر ۋە ئۇسكۇنىلىرىڭىزدىكى يۇمتاللارنىڭ يېڭى نەشرى بارلىققا كەلگەن ھامان ئۇلارنى قاچىلاڭ.Updates often include improvements and new . ئىمكانىيەت بولسا ئۇسكۇنىڭىزنىڭ تەڭشىكىدىكى «ئاپتوماتىك يېڭىلاش»نى قوزغىتىپ قويۇڭ. بۇنىڭدا ۋاقتىدا يېڭىلاشنى ئۇنتۇپ قېلىشتىن قۇتۇلسىز. مەلۇم ۋىرۇسلار ۋە باشقا تۇردىكى زىيانلىق يۇمتاللاردىن قوغدىنىش ئۇچۇن NCSC نىڭ توردا بىخەتەر بولۇش ھەققىدىكى كۆرسەتمىلىرىنى كۆرۈپ چىقىڭ.. يېڭىلىنىشلار كۆپىنچە ياخشىلىنىش ۋە يەنى يېڭى ئالاھىدىلىكلەرنى ئۆز ئىچىگە ئالىدۇ: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **ئۇسكۇنىلىرىڭىزنى «تۇرمىدىن قاچۇرماڭ» ياكى «يىلتىز»لىماڭ. چۈنكى بۇلار** ئۇسكۇنىلەرگە ئورنىتىلغان خەۋپسىزلىك كونتروللۇقىنى ھالقىپ ئۆتۈش ئۇچۇن يامالمىغان زەئىپلىكلەردىن پايدىلىنىدۇ. بۇ ھال ئۇسكۇنىلىرىڭىزنى تېخمۇ ئاسان ھۇجۇمغا ئۇچرايدىغان قىلىپ قويىدۇ. بۇ ھەقتە NCSC نىڭ كۆرسەتمىلىرىگە قارا: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

ئەپلىرىكىزنى ياخشى باشقۇرۇڭ

- **ئەپلىرىكىزنى ۋە ئۇلارنىڭ ئىجازەتلىرىنى تەكشۈرۈپ تۇرۇڭ.** ئەگەر مەلۇم ئەپكە ئۇزۇن مۇددەت ئىھتىياجىڭىز بولمىسا ئۇنى يۇيۇۋېتىڭ. ئۇچۇرلارنىڭ ئوغرىلىنىپ كېتىشىنى ئەڭ تۆۋەن چەككە چۈشۈرۈش ئۈچۈن ئىمكان بار ئەپ ئىجازەتلىرىنى چەكلەڭ. چۈنكى زىيانلىق ۋىرۇسلار ھەرقاچان كامېرا ياكى مىكروفونغا ئوخشاش قوغدىلىدىغان ھۆججەتلەر ياكى تاشقى قۇرۇلمىلارغا كىرىش ئۈچۈن لايىھىلىنىدۇ.
  - «ئالما» مەھسۇلاتلىرى ئۈچۈن ئەپ رۇخسىتىنى قانداق تەكشۈرۈش مۇمكىن؟ https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - «ئاندرويد» مەھسۇلاتلىرى ئۈچۈن ئەپ رۇخسىتىنى قانداق تەكشۈرۈش مۇمكىن؟ https://support.google.com/android/answer/9431959?hl=en-GB
- **ئاپتوماتىك ھالدا نامەلۇم ئەپلەرنى گۇگۇل (Google)غا يوللاڭ.** ئەگەر سىز ئاندرويد ئىشلەتكۈچى بولسىڭىز ھەمدە گۇگۇلنىڭ «ئويۇن دۇكىنى»دىن بولمىغان بىرەر ئەپنى چۈشۈرۈپ سالغان بولسىڭىز گۇگۇلنىڭ «ئويۇن دۇكىنى» ئەپ دېتالىدىكى «ئويۇننى قوغداش» تەڭشىكىدىكى «زىيانلىق ئەپنى بايقاشنى كۈچەيتىش» فۇنكتسىيەسىنى يانداۇرۇش ئارقىلىق ئۇنى گۇگۇلغا ئەۋەتەلەيسىز. بۇنىڭ پايدىلانغۇچىلارنى قوغداشقا ياردىمى تېگىدىغان بولۇپ، ئەپتىكى يامان غەرەزلىك يۇمتاللارنى سايىلەپ چىقىدۇ. بۇنى قانداق تەڭشەش توغرىسىدىكى ئۇچۇرلار: https://support.google.com/android/answer/2812853?hl=en-GB

تور مۇلازىمىتىدىن پايدىلىنىڭ

- **ئۇلىنىشنى چېكىشتىن ئاۋۋال URL نىڭ ئىناۋەت مۇلازىمىتىنى ئىشلىتىڭ.** ئېلىخەت، قىسقا ئۇچۇر ياكى باشقا مەنبەلەرگە خاس ئۇلانمىلارنىڭ بىخەتەر ياكى ئەمەسلىكىنى ئالدى بىلەن Google transparency Report Virus Total قاتارلىق مۇلازىمەتلەر ئارقىلىق تەكشۈرۈپ باقسىڭىز بولىدۇ. گۇمانلىق ھۆججەتلەر ۋە ئەپلەرنى زىيانلىق ۋىرۇسلارنى تەھلىل قىلىدىغان Virus Total قاتارلىقلارغا يۈكلەش ئارقىلىق ئاشۇ ھۆججەتنىڭ يامان غەرەزلىك ياكى ئەمەسلىكىنى بايقاشقا بولىدۇ. يادىڭىزدا بولسۇنكى، سايىلاش مۇلازىمىتى بەزىدە خاتا ھۆكۈم چىقىرىپ قويىدۇ.

- گۇگۇل يۇقىرى دەرىجىلىك مۇھاپىزەت (**Google Advanced Protection**) پروگراممىسىغا قېتىلىڭ. بۇ بىر تۈرلۈك ھەقسىز مۇلازىمەت بولۇپ، گۇگۇل مۇلازىمىتىنى ئىشلىتىدىغان شەخسلەر (Gmail ، ئويۇن دۇكىنى ۋە باشقىلار) نىشانغا ئېلىنىش خەۋپىگە دۇچ كەلگەندە شۇلارنى ھىمايە قىلىشقا لايىھىلەنگەن. بۇ مۇلازىمەت گۇگۇل مۇلازىمەتلىرىدىن پايدىلانغاندا يۇكسەك خەۋپسىزلىك بىلەن تەمىن ئېتىدۇ. https://landing.google.com/advancedprotection/

- ***ئەگەر قوشۇمچە ئەسلىگە كەلتۈرگۈچى مۇلازىمەتلەر مەۋجۇت بولسا ئۇلارغا تىزىملىتىڭ.*** مەسىلەن، ئەنگلىيەدە يۇقىرى دەرىجىلىك خەتەرگە دۇچ كېلىۋاتقان شەخسلەر تور بىخەتەرلىكىگە ياردەم بېرىدىغان قوشۇمچە مۇداپىئە مۇلازىمىتىدىن بەھرىمەن بولۇش ھوقۇقىغا ئىگە بولۇشى مۇمكىن. بۇنىڭغا لايىقىتلىك ياكى ئەمەسلىكىڭىزنى، شۇنداقلا تېخنىكا كۆپ مەزمۇنلار ئۈچۈن بۇنىڭغا قاراڭ:
https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

تەھدىتلەرنى مەلۇم قىلىش

- **ساختا ھېسابئاتلارنى پەرقلەندۈرۈش ۋە مەلۇم قىلىش.** ئۆز مەقسەدلىرىگە يېتىش ئۈچۈن يامان غەرەزلىك تور ھۇجۇمچىلىرى ساختا ھېسابئات ئېچىشى ياكى راست ھېسابئاتلارغا خاككېرلىق قىلىشى مۇمكىن. ئەگەر بىرەر ھېسابئاتنىڭ ساختا ئىكەنلىكى ياكى ئوغرىلانغان بولۇشى مۇمكىنلىكىدىن گۇمانلانسىڭىز ئۇنى سۈپىغا مەلۇم قىلىڭ ۋە توسۇۋېتىڭ. كۆپلىگەن مۇلازىمەتلەرنىڭ Instagram ۋە Facebook قا ئوخشاش «دەللالەنگەن بەلگە» دېگەندەك ھېسابئاتنى دەللالەش جەريانى مەۋجۇت. بۇلار ئاشۇ ھېسابئاتنىڭ راست ياكى ئەمەسلىكىنى پەرقلەندۈرەلەيدۇ. NCSC ئىجتىمائىي تاراتقۇلاردىن بىخەتەر پايدىلىنىش ھەققىدىكى كۆرسەتمىلەر بىلەن تەمىنلىگەن بولۇپ، ھۇجۇمغا ئۇچرىغان ھېسابئاتلارنى قانداق دەللالەش ۋە مەلۇم قىلىش ھەققىدىكى تەپسىلاتلارنى ئۆز ئىچىگە ئالىدۇ:
https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **ساختا ئېلخەت، ئۇچۇر ۋە ئۇلانما ئارقىلىق قارماقلا ئىلىندۇرۇش.** NCSC گۇمانلىق ئېلخەت ئادرېسلىرىنى ۋە تور بەتلىرىنى تەكشۈرىدۇ. ئاۋادا بىرەر تور بېتى، ئېلخەت ياكى ئۇچۇردىن گۇمانلىنىپ قالسىڭىز ئۇلارنى مەلۇم قىلسىڭىز بولىدۇ:
https://www.ncsc.gov.uk/collection/phishing-scams

ئاندرويد (Android)

گۇگۇلنىڭ كۆچمە مەشغۇلات سىستېمىسى بولۇپ، بىرنەچچە خىل ئەقلىي تېلېفون ۋە تاختا كومپيۇتېرلاردا ئىشلىتىلىدۇ.

ئەپ

بۇ ئادەتتە قوللىنىشچان پروگراممىنى كۆرسىتىدىغان بولۇپ، قىسقارتىلىپ «ئەپ» دېيىلىدۇ. بۇ خىلدىكى يۇمتال بولىقى قوشۇمچە ئىقتىدار ياكى مەزمۇن بىلەن تەمىنلەيدىغانلىقى ئۈچۈن قوللانغۇچىلار ئۆزى ئۈسكۈنىلىرىگە ئورنىتىدۇ ياكى ئالدىن ئورنىتىپ قويۇلىدۇ.

تور بېكەتلىكى

ئۈسكۈنىلەر، مۇلازىمەتلەر ۋە تورلارنى قوغداش، شۇنىڭدەك ئۇلاردىكى ئۇچۇرلارنى رۇخسەتسىز زىيارەت قىلىش، ئوغرىلاش ياكى بۇزۇلۇشتىن ساقلاشنى كۆرسىتىدۇ.

ئۈسكۈنە

ئۈستەل كومپيۇتېرى، ئەقلىي تېلېفون ياكى تاختا كومپيۇتېر قاتارلىق ماددىي شەكىلدە مەۋجۇت بولىدىغان كومپيۇتېر ئاساسىدىكى قاتتىق دېتال.

iOS

«ئالما» شىركىتىنىڭ كۆچمە مەشغۇلات سىستېمىسى بولۇپ، شۇلارنىڭ بىر يۈرۈش كۆچمە ئۈسكۈنىلىرىگە ئىشلىتىلىدۇ.

زىيانلىق يۇمتاللار

«يامان غەرەزلىك زىيانلىق يۇمشاق دېتال»دىن كەلگەن. بۇ خىلدىكى يۇمتاللار ئادەتتە كومپيۇتېر سىستېمىسى، تور ياكى ئۈسكۈنىلەرگە زەرەر يەتكۈزىدۇ. ۋىرۇس، تۆلەم يۇمتالى ۋە تروياندىن ئېتى قاتارلىقلارنى ئۆز ئىچىگە ئالىدۇ.

مەشغۇلات سىستېمىسى

كومپيۇتېر، تاختا كومپيۇتېر ۋە ئەقلىي تېلېفوندا ئىشلىتىلىدىغان ئاساسلىق يۇمتال بولۇپ، قوشۇمچە ئەپلەر ۋە قاتتىق دېتالنىڭ بولۇشىنى تەلەپ قىلىدۇ.

قارماق

بۇنداق ئالدامچىلىق خاراكتېرىدىكى ئېلخەتلەر ياكى تېكىستلىق ئۇچۇرلاردا مەلۇم تور بېكەتلەرگە ئۇلىنىدىغان ئۇلانمىلار بولىدۇ، بۇ تور بېكەتلەردە بولسا زەرەرلىك يۇمتاللار بولىدۇ. ياكى بولمىسا بۇ خىلدىكى ئۇچۇرلار قوللانغۇچىلارنى بەزى سەزگۈر ئۇچۇرلار (مەسىلەن، مەخپىي نومۇر)نى ئاشكارىلاشقا ياكى پۇل سېلىشقا دەۋەت قىلىدۇ.

جاسۇسلۇق يۇمتاللىرى

زەرەرلىك يۇمتاللارنىڭ بىر تۈرى بولۇپ، قوللانغۇچىلارنىڭ رۇخسىتىسىز ئۈسكۈنىلەرگە ئورنىتىلىدۇ ھەمدە ئۆزى توپلىغان سانلىق مەلۇماتلارنى ئۈچىنچى تەرەپكە يوللاپ بېرىدۇ.

ئىجتىمائىي تاراتقۇ

Facebook ، X ۋە Instagram قاتارلىق تور بەتلىرى ۋە ئەپلەرنى كۆرسىتىدىغان بولۇپ، كىشىلەرنى قوللانغۇچىلار پەيدا قىلغان مەزمۇنلار (تېكىست يازمىلىرى، سۈرەتلەر ۋە سىن ماتېرىياللىرى)نى ھەمبەھىرلەش ۋە ئۇلارغا ئىنكاس قايتۇرۇش ئىمكانىيىتىگە ئىگە قىلىدۇ.

ئەقلىي تېلېفون

مۇرەككەپ ئىقتىدارلارنى ھازىرلىغان زامانىۋى تېلېفونلار بولۇپ، ئاندرويد ۋە iOS مەشغۇلات سىستېمىلىرىنى ئۆز ئىچىگە ئالىدۇ.

تروياىن

ياماق غەرەزلىك يۇمتاللارنىڭ بىرى بولۇپ، ھەقىقى يۇمتال سىياقىدا زىيانكەشلىككە ئۇچرىغۇچىنىڭ ئۇسكۇنىسىگە رۇخسەتسىز كىرىۋالىدۇ.

URL

يىگانە مەنبە بېكىتكۈچى. تور بەتلىرىنىڭ ئادرېسى بولۇپ، ئادەتتە تەۋەلىك نامىنى كۆرسىتىدۇ (مەسىلەن: www.bbc.co.uk)

ۋىرۇس

قانۇنىي يۇمتاللارنى يۇقۇملاندۇرىدىغان ۋە بۇ پروگراممىلار ئاكتىپلانغاندىن كېيىن تور ئارقىلىق ئۇنىڭ ساختىسىنى ياساپ چىقىدىغان ياماق غەرەزلىك يۇمتال.

قوشۇمچە ئوقۇشلۇق

ئاۋسترالىيە تور بىخەتەرلىكى مەركىزىنىڭ كۆرسەتمىسى

- تور جىنايەتلىرى، ۋەقەلىرى ياكى يوچۇقلار
- ئۇسكۇنىلىرىڭىزنى قانداق قوغداش مۇمكىن
- كۆچمە تېلېفونىڭىزنى قوغداش
- قارماق
- ئالدامچىلىق
- ئىجتىمائىي تاراتقۇلىرىڭىزنى قوغداش
- ئىجتىمائىي تاراتقۇ ۋە ئۇچۇر ئەپلىرى ئۈچۈن بىخەتەرلىك مەسلىھەتلىرى

ئەنگلىيە NCSC ۋە NPSA نىڭ كۆرسەتمىلىرى

- دېموكراتىيەنى ھىمايە قىلىش
- ئىجتىمائىي تاراتقۇ: ئۇنى قانداق قىلىپ بىخەتەر قوللىنىش كېرەك؟
- تەشكىلاتلار، جۈملىدىن كۆچمە ئۇسكۇنىلەرنىڭ بىخەتەرلىكى ئۈچۈن خەۋپسىزلىكى ئۈچۈن كۆرسەتمىلەر
- ئەپ دۇكانلىرى ھەققىدىكى تەھدىت دوكلاتى
- زور خەتەرگە دۇچ كېلىۋاتقان شەخسلەرنىڭ بىخەتەرلىكى

ئامېرىكاNSA نىڭ كۆرسەتمىلىرى

- كۆچمە ئۇسكۇنىلەرنى ئىشلىتىشنىڭ ئەڭ ياخشى يوللىرى

باياناتنامە

يادىڭىزدا بولسۇنكى، مەزكۇر كۆرسەتمە تەمىن ئەتكەن ئۇچۇرلار كۆرسەتمە ئېلان قىلىنغان ۋاقىتتا دەلىللەشتىن ئۆتكەن.

مەزكۇر دوكلاتتا پايدىلىنىلغان ئۇچۇرلار دوكلاتنى تەييارلىغان ئورۇنلارنى مەنبە قىلىدۇ. بۇنىڭدىكى بايقاشلار ۋە تەۋسىيەلەر پۈتكۈل يوشۇرۇن خەۋپ-خەتەرلەردىن تولۇق ساقلايدۇ، دېگەن مەقسەتتە ئوتتۇرىغا قويۇلغىنى يوق. شۇنىڭدەك بۇلارغا تولۇق ئەمەل قىلىش پۈتكۈل خەۋپ-خەتەرنى تۈپ يىلتىزىدىنمۇ يوق قىلالمايدۇ. ئۇچۇر خېيىم-خەتىرىگە كىمنىڭ مەسئۇل بولۇشى ھەر دائىم مۇناسىۋەتلىك سىستېما ئىگىسىگە باغلىق بولىدۇ.

2000-يىلىدىكى «ئۇچۇر ئەركىنلىكى قانۇنى» (FOIA) بويىچە بىرىتانىيە تەۋەسىدە بۇ ئۇچۇرلار ئۇنىڭدىن مۇستەسنا قىلىنغان، شۇنىڭدەك بىرىتانىيەدىكى ئۇچۇرغا دائىر باشقا قانۇنلاردىنمۇ مۇستەسنا بولۇشى مۇمكىن.

FOIA ھەققىدىكى ھەرقانداق سوئالىڭىزنى بۇنىڭغا يوللاڭ: ncscinfoleg@ncsc.gov.uk.

ئىلاۋە: «ئاي نۇرى» ۋە «ئەسكى بازار» نىڭ كۆزگە چېلىققان مىسالىرى

بۇ جەدۋەلدە «ئاي نۇرى» ۋە «ئەسكى بازار»نىڭ ئۆتكەن ئىككى يىلدىكى پائالىيەتلىرىدە ئىشلەتكەن ئەپلىرى كۆرسىتىلگەن.

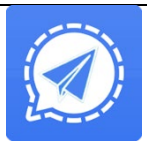
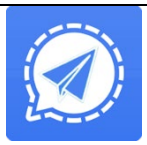
بۇ ئەپلەرنىڭ كۆپ قىسمى ھازىر قوللىنىلۋاتقان ئەپلەرگە بەكلا ئوخشاپ كېتىدۇ. بۇ بەلكىم ئاشۇ تور ھۇجۇمچىلىرىنىڭ داڭلىق ماركىلار نامىدا ئالدامچىلىق قىلىش ھۇنەرلىرىدىن بولۇشى مۇمكىن.

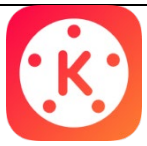
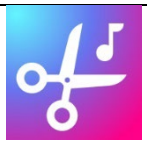
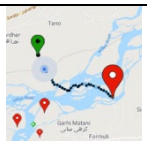
دىققەت قىلىشقا تېگىشلىك بولغان بىر نۇقتا شۇكى، بۇ ئەپلەرنىڭ نامى، ئۇرۇلما نامى ۋە سىمۋوللۇق بەلگىلىرى ھەققىي ئەپلەرگە تەقلىد قىلىنغان ياكى ئۇنىڭغا نەق ئوخشايدىغان بولسىمۇ، بۇ ھالنى ئاشۇ ئۇسكۇنىنىڭ يۇقۇملانغان ياكى يۇقۇملانمىغانلىقىنى ئايدىڭلاشتۇرۇشنىڭ خاس ئۇلچىمى قىلىۋېلىشقا بولمايدۇ.

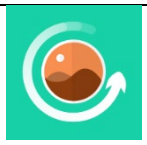
«خېيىم-خەتەرنى ئازايتىش» بۆلۈكىگە كىرگۈزۈلگەندەك ئاندرويىد ئۇسكۇنىلىرىدىكى ئەپلەرنى «زىيانلىق ئەپنى بايقاشنى كۈچەيتىش» قۇنكتىسىيەسىنى ياندۇرۇش ئارقىلىق گۇگۇلغا ئەۋەتىلەيسىز. چۈنكى بۇ ئىقتىدار ئۇسكۇنىڭىزدىكى «ئويۇن دۇكىنى»دىن باشقا جايلاردىن ئورنىتىلغان ئەپلەرنى سايىلاپ چىقالايدۇ.

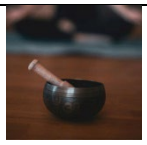
ئەپ نامى	ئۇرۇلما نامى	ئەپ سىمۋولى
ئاللاھنىڭ 99 ئىسمى	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine (پىنتو)	psyberia.pa.full	
AlpineQuest دالا كەزگۈچى	psyberia.alpinequest.full	

	psyberia.alpinequest.full	دالا AlpineQuest كەزگۈچى
	psyberia.alpinequest.free	دالا AlpineQuest كەزگۈچى (ئاددىي نۇسخا)
	com.alpha.applock	AppLock
	com.arabic.keyboard.arabic.language.keyboard.app	ئەرەبچە كۇنۇپكا تاختىسى
	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	ئۇن-سىن مونتاژلىغۇچ
	com.ziipin.softkeyboard	Badam ئۇيغۇرچە خەت كىرگۈزگۈچ
	com.bigkidsapps.buddhistsongs1	بۇددىست كۈيلىرى
	com.android2.calculator3	ھېسابلىغۇچ
	com.pro.app.compass	كومپاس 360 كەسپىي نۇسخا
	ru.vddevelopment.ref.enugen.free	ئىنگلىزچە -ئۇيغۇرچە لۇغەت ھەقسىز
	ewlat.com.ewlatuyghur	ئەۋلات

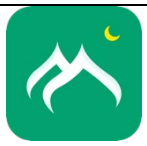
	com.netflix.Speedtest	FAST
	com.fmwhatsapp	FMWhatsApp
File Manager + 	com.alphainventor.filemanager	ھۆججەت باشقۇرغۇچى +
	org.telegram.FlyGram	FlyGram
	org.telegram.FlyGram	Flygram
	com.cl.wifipassword.share	WiFi ھەقسىز
	com.gbwhatsapp	GBWhatsApp
	com.golap.hefzquran	Hefz Quran
	com.ibrahim.hijricalendar	ھىجرىيە كالېندارى
	com.camerasideas.instashot	InShot

	com.kmplayer	KMPlayer
	com.nexstreaming.app.kinemasterfree	KineMaster
	ringtone.maker.mp3.cutter.audio	MP3 مونتاژلىغۇچ ۋە تېلېفون قوڭغۇرىقى ياسىغۇچ
	com.mallocprivacy.antistalkerfree	Malloc
	com.routemap.mapdownload.gpsroute planner	خەرىتە مۇساپىسىنى ھېسابلىغۇچ
	com.aaa.media.recovery.androidapp	ئۇن-سىننى ئەسلىگە كەلتۈرۈش
	com.nur.reader	Nur.cn
	com.nur.ime	Nur خەت كىرگۈزگۈچ
	com.gbwhatsapp3	OGWhatsApp
	com.mobisystems.mobiscanner	PDF قوشۇمچىلىرى
	pdf.pdfreader.pdfviewer.pdfeditor	PDF كۆرگۈچ

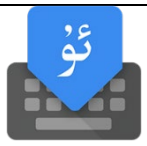
	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	PDF كۆرگۈچ
	com.iudesk.android.photo.editor	سۈرەت تەھرىرلىگۈچ
	recover.restore.undelete.photo.video.file	سۈرەتنى ئەسلىگە كەلتۈرگۈچ
	com.kvadgroup.photostudio	سۈرەت ئۇيى
	org.telegram.pluspro	Plus
	com.arashpayan.prayerbook	ناماز قوللانمىسى
	com.speedy.vpn	QuarkVPN
	com.tos.quranuighore	قۇرئان
	com.ewlat.qurankerim	قۇرئان كەرىم
	com.restore.deleted.pictures.video	ئۆچۈرۈلگەن سۈرەتلەرنى ئەسلىگە كەلتۈرۈش
	org.thoughtcrime.securesms	Signal

	org.thoughtcrime.securesmsplus	Signal Plus
	org.thoughtcrime.securesmsplus	SignalPlus
	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	كۈي قاچسى ساداسى HD
	com.skype.raider	Skype
	com.snaptube.premium	Snaptube
	com.snaptube.gold	Snaptube Plus
	com.touchtype.swiftkey	SwiftKey Keyboard
	com.mmmoussa.iqra	Tarteel
	org.zhifeijihj.messenger	Telegram
	org.telegramfbo.messenger	Telegram
	org.thunderdog.challegram	Telegram X

	net.rhombapp.mo	تىبەت پالچىلىق سىستېمىسى MO
	com.chorig.tibetanprayer	تىبەتچە ئىبادەت
	free_translator.artr	تەرجىمانAR-TR
	com.truecaller	Truecaller
	com.techshop.videocraft	TubePlus
	us.ultrasurf.mobile.ultrasurf	Ultrasurf
	com.mykeyboard.myphotokeyboard.uyghurkeyboard	ئۇيغۇرچە كۇنۇپكا تاختىسى
	com.ziipin.softkeyboard	ئۇيغۇرچە كىرگۈزگۈچ
	com.inverseai.video_converter	ۋىدىيو ئايلاندۇرغۇچ
	com.naing.cutter	ۋىدىيو مونتاژلىغۇچ
	downloader.video.download.free	ۋىدىيو چۈشۈرگۈچ

	com.bstech.slideshow.videomaker	ۋىدىيو ئىشلىگۈچ
	com.zgz.supervideo	ئاندرويىد ئۇچۇن ۋىدىيو قويغۇچ
	com.prime.story.android	Vieka
	com.quvideo.vivavideo.lite	VivaVideo Lite
	com.quvideo.xiaoying.pro	VivaVideo PRO
	com.alhiwar	Vmuslim
	com.media.bestrecorder.audiorecorder	ئاۋاز خاتىرىلىگۈچ
	com.rebelvox.voxer	Voxer
	com.graph.weather.forecast.channel	ھاۋا رايىدىن ئالدىن مەلۇمات
	com.whatsapp	WhatsApp
	com.whatsapp	WhatsApp

	com.WhatsApp3Plus	WhatsApp
	com.whatsapp	WhatsApp
	com.WhatsApp2Plus	WhatsApp
	gogolook.callgogolook2	Whoscall
	com.example.dat.a8andoserverx	مەخپىي نومۇر WiFi ئۇستىسى v1.4 _
	com.windyty.android	Windy
	com.transferwise.android	Wise
	com.yowhatsapp	YoWhatsApp
	dentex.youtube.downloader	YouTubeچۈشۈرگۈچ
	im.zom.messenger	Zom

	com.guidedways.iQuran	iQuran Lite
	com.ewlat.eserler	ئاۋازلىق ئەسەرلەر
	com.c9.utilim	ئاۋازلىق قۇرئان
	com.yelken.izchi	ئىزچى
	com.uygur.apkstore	ئۇيغۇرچە APK ئىزدىگۈچى
	com.c9.uyghurquran	ئۇيغۇرچە قۇرئان
	com.maher4web.quran	القرآن الكريم
	com.my.newproject5	زىكىرلەر
	ru.omdevelopment.ref.quranuyghur.free	قۇرئان كەرىم
	com.kuhiqap.lughitim	كۇھىقاپ لۇغىتى
	com.nur.ime	نۇر كىرگۈزگۈچ

《心灵法门》念佛机 	com.guanyincitta.chant	《心灵法门》念佛机
	com.dacd.dictionary	汉藏英辞典
	com.example.astronomicalcalendarapp	藏历基本数据
	com.tibetan.translate	阳光藏汉翻译