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

උපදේශනය

BADBAZAAR සහ MOONSHINE: උයිගර්,තායිවාන හා ටිබෙට් කෂ්ඩායම් සහ සිවිල් සමාජ ක්‍රියාකාරීන්ව ඉලක්ක කරගත් ඔත්තු මෘදුකාංග

2025 අප්‍රේල් 9

BADBAZAAR සහ MOONSHINE: උයිගර්, තායිවාන හා ටිබෙට් කණ්ඩායම් සහ සිවිල් සමාජ ක්‍රියාකාරීන්ව ඉලක්ක කරගත් ඔත්තු මෘදුකාංග

NCSC සහ හවුල්කරුවන් විසින් ඔත්තු මෘදුකාංග ප්‍රභේද දෙකක්මගින් ඉහළ අවදානමක් ඇති අය සඳහා නව තොරතුරු සහ ලිහිල් කිරීමේ පියවර ප්‍රකාශයට පත් කරයි.

සාරාංශය

එක්සත් රාජධානියේ සයිබර් ලීගයේ සහාය ඇතිව, මෙම උපදේශනය ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය (NCSC UK) සහ ජාත්‍යන්තර හවුල්කරුවන් විසින් ඒකාබද්ධව උත්පාදනය කරන ලදී:

- **ඔස්ට්‍රේලියානු සංඥා අධ්‍යක්ෂ මණ්ඩලයේ කොටසක් වන, ඔස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානය**
- **සන්නිවේදන ආරක්ෂක ආයතනයේ කොටසක් වන, කැනේඩියානු සයිබර් ආරක්ෂාව පිළිබඳ මධ්‍යස්ථානය**
- **ජර්මානු ෆෙඩරල් බුද්ධි සේවය**
- **ආණ්ඩුක්‍රම ව්‍යවස්ථාව ආරක්ෂා කිරීම සඳහා වූ ජර්මානු ෆෙඩරල් කාර්යාලය**
- **රජයේ සන්නිවේදන ආරක්ෂක කාර්යාංශයේ කොටසක් වන, නවසීලන්ත ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය**
- **ජනපදයේ විමර්ශන පිළිබඳ ෆෙඩරල් කාර්යාංශය**
- **එක්සත් ජනපදයේ ජාතික ආරක්ෂක ඒජන්සිය**

එහි අරමුණ වන්නේ තායිවානය, ටිබෙටය, ෂින්ජියැං උයිගර් ස්වයං පාලන කලාපය, ප්‍රජාතන්ත්‍රවාදී ව්‍යාපාර සහ ෆලුන් ගොං ඇතුළත් වන මාතෘකාවලට සම්බන්ධ පුද්ගලයින්ට ද්වේෂසහගත සයිබර් ක්‍රියාකාරීන් විසින් එල්ල කරන වැඩෙන තර්ජනය පිළිබඳව දැනුවත් කිරීමයි.

චීන රාජ්‍යය උනන්දුවක් දැක්විය හැකි ස්මාර්ට්ෆෝන් ඇතුළු ජංගම උපාංගවල ඇති දත්ත ඉලක්ක කර ගැනීම සඳහා BADBAZAAR සහ MOONSHINE ලෙස හඳුන්වන ඔත්තු මෘදුකාංග උපයෝගිකර ගනිමින් ද්වේෂසහගත සයිබර් ක්‍රියාකාරීන් විසින් භාවිතා කරන ශිල්පීය ක්‍රම විස්තර කරන ප්‍රත්‍යෙක අධ්‍යයන දෙකක් මෙම උපදේශනයේ ඇතුළත් වේ. පුද්ගලයන්ට තමන්ව, තමන්ගේ උපාංග සහ තමන්ගේ දත්ත ආරක්ෂා කර ගැනීමට උපකාර කිරීම සඳහා මඟ පෙන්වීමක් ද එමගින් සපයයි.

මෙම උපදේශනය සමඟ, NCSC වෙනම මඟ පෙන්වීමක් සහිත සම්පූර්ණ තාක්ෂණික විස්තර ප්‍රකාශයට පත් කර ඇත

අවදානමට ලක් වී සිටින්නේ කවුරුන් ද?

චීන රාජ්‍යය ඔවුන්ගේ දේශීය අධිකාරියට, අභිලාෂයන්ට සහ ගෝලීය කීර්ති නාමයට තර්ජනයක් ලෙස සලකනු ලබන මානෘකාවලට සම්බන්ධ පුද්ගලයින්ව BADBAZAAR සහ MOONSHINE මගින් විශේෂයෙන් ඉලක්ක කර ගන්නා බව මෙම කර්තෘ ආයතන සහ කර්මාන්ත හවුල්කරුවන් නිරීක්ෂණය කර ඇත. පහත දේවල් හා සම්බන්ධ, (නමුත් ඒවාට පමණක් සීමා නොවන), ඕනෑම අයෙකු වඩාත්ම අවදානමට ලක්ව ඇති කාණ්ඩයට ඇතුළත් වේ,:

- **තායිවානයේ නිදහස**
- **ටිබෙට්යේ අයිතිවාසිකම්**
- **උයිගර් මුස්ලිම්වරුන් සහ අනෙකුත් චීනයේ ෂින්ජියැං උයිගර් ස්වයං පාලන කලාපයේ හෝ ඉන් පැමිණි ජනවාර්ගික සුළුතරයන්**
- **ප්‍රජාතන්ත්‍රවාදය වෙනුවෙන් පෙනී සිටීම (හොංකොං ඇතුළුව)**
- **ෆලුන් ගොං අධ්‍යාත්මික ව්‍යාපාරය**

මෙයට රාජ්‍ය නොවන සංවිධාන (NGOs), මාධ්‍යවේදීන්, ව්‍යාපාර සහ මෙම කණ්ඩායම් වෙනුවෙන් පෙනී සිටින, හඳුනා ගන්නා හෝ වෙනත් ආකාරයකින් ඒවා නියෝජනය කරන පුද්ගලයින් ඇතුළත් වේ. මෙම ඔත්තු මෘදුකාංගය මාර්ගගතව අවිචාරවත් ලෙස ව්‍යාප්ත වන ආකාරය මගින් අදහස් කෙරෙන්නේ අපේක්ෂිත වින්දිතයින්ගෙන් ඔබ්බට ආසාදන පැතිර යා හැකි අවදානමක් ඇති බවය.

මෙම උපදේශනය BADBAZAAR සහ MOONSHINE ඔත්තු මෘදුකාංග මගින් එල්ලවන නිශ්චිත තර්ජනයට ඵලදායී ලෙස ප්‍රතිචාර දැක්වීමට අවදානමට ලක්ව සිටින අයට උපකාර කිරීම අරමුණු කරයි. යෝජිත අවම කිරීම් පුළුල් සයිබර් ආරක්ෂණ උපදෙස් වලට අනුපූරක වන අතර ඒවා හුදකලා ලෙස නොසැලකිය යුතුය.

මෙම උපදේශනයේ සඳහන් කර ඇති මාර්ගෝපදේශ අනුගමනය කිරීමෙන්, පරිශීලකයින්ට ඔවුන්ගේ ජංගම උපාංග සහ දත්ත ආසාදනය වීමේ අවදානම අඩු කර ගත හැකිය.

නර්ජනය

MOONSHINE සහ BADBAZAAR, ට්‍රෝජන් (මතුපිටින් අනතුරුදායක බවක් නොපෙනෙන අයුරු සකස් කළ දේ) සඳහා උදාහරණ වේ; යෙදුම් ගබඩා (app stores) හෝ මාර්ගගත ගොනු බෙදාගැනීමේ සේවාවන්ගෙන් බාගත කළ හැකි වෙනත් ආකාරයකින් ක්‍රියාත්මක වන යෙදුමක් තුළ ඒවායේ ද්වේශසහගත කාර්යයන් සැඟවී ඇත.

මෙම යෙදුම් නිර්මාණය කර ඇත්තේ රැවටිලි ලෙසින් පරිශීලකයෙකු ලවා ඒවා බාගත කර උපාංගයකට ස්ථාපනය කරවා ගැනීමට ය. යෙදුමක් ස්ථාපනය කළ පසු, එය අනවසර කාර්යයන් සිදු කිරීම සඳහා උපාංගයේ අවදානම් තත්වයන් භාවිතා කරයි. නැතහොත් එය උපාංගයෙන් තොරතුරු ලබා ගැනීමට සහ බාගත කිරීමට යෙදුම් අවසර ලබා දෙන පරිශීලකයෙකු මත විශ්වාසය තැබිය හැකිය. එයට ඇතුළත් වන්නේ:

- **තත්‍ය කාලීන සෙවුම් ඇතුළුව ස්ථාන දත්ත**
- **මයික්‍රොෆෝනයට හා කැමරාවට ප්‍රවේශ වීම**
- **පිනිවිඩ, පින්තූර සහ උපාංගයේ තැන්පත් කර ඇති වෙනත් ගොනු**
- **උපාංගයේ තොරතුරු සහ වෙනත් දේ**

ඉන්පසු ක්‍රියාකාරීන් අවදානමට ලක්විය හැකි කණ්ඩායම්වල නීත්‍යානුකූල උවමනාවන් ගසාකමින්, හැකි තරම් විස්තීරණ ලෙස හඳුනාගෙන, ඔවුන්ව ආසාදනයට පත්කර, ඔවුන්ගේ දත්ත වෙත ප්‍රවේශ වීමට කටයුතු කරයි. ඔවුන් මෙය කරන එක් ක්‍රමයක් වන්නේ, ඔවුන්ගේ මව් භාෂාවන්ට සහාය දක්වන යෙදුම්, හෝ චීනයට අයත් ටිබෙට් ප්‍රදේශ හෝ ෂින්ජියැං වැනි ස්ථානවලට විශේෂිත අන්තර්ගතයන් අඩංගු යෙදුම් වැනි ඔවුන්ගේ විස්තීරණ කැමැත්තක් දක්වන බව ඔවුන් දන්නා යෙදුම් නිර්මාණය කිරීමයි.

මෙම උපදේශනයේ ඇති ප්‍රත්‍යෙක අධ්‍යයනයන් මේ සඳහා TibetOne සහ උයිගර් කුරාන යෙදුම් ඇතුළු උදාහරණ කිහිපයක් සපයයි.

ක්‍රියාකරුවන් ඔවුන්ගේ අපේක්ෂිත විස්තීරණයින්ගේ පරිශීලක පදනමක් ඇති මාර්ගගත සංසදවල ක්‍රියාකාරී වන අතර, එමඟින් විස්තීරණයින්ව ආසාදනයට පත් වීමේ අවස්ථාව උපරිම වේ. ටිබෙට් ආශ්‍රිත ටෙලිග්‍රාම් නාලිකා සහ Reddit (රෙඩිට්) සංසදවල ඔවුන් හිතාමතාම ඔත්තු මෘදුකාංග බෙදා ගන්නා බව නිරීක්ෂණය වී තිබේ. මෙම උපදේශනයේ ඇති ප්‍රත්‍යෙක අධ්‍යයනයඅධ්‍යයනයන් මෙම ක්‍රමවේදයන් සඳහා උදාහරණ ද සපයයි.

ද්වේශසහගත යෙදුම් බොහෝ විට Android හි APK ගොනු වැනි ස්වාධීන ගොනු ලෙස බෙදා ගන්නා අතර ඒවා පරිශීලකයින් බාගත කර ස්ථාපනය කළ යුතුය. ක්‍රියාකරුවන් ඔවුන්ගේ ඔත්තු මෘදුකාංග Google Play Store සහ Apple App Store වැනි නිල යෙදුම් ගබඩා වෙත උඩුගත කිරීමෙන් හෝ මීට කලින් හානිකර නොවුණු යෙදුම් වලට ද්වේශසහගත කේත එකතු කිරීමෙන් වඩාත් නීත්‍යානුකූල ලෙස පෙනෙන්නට උත්සාහ කරයි. නමුත් නිල ගබඩාවල ආරක්ෂක විශේෂාංග සහ පරීක්ෂා කිරීමේ ක්‍රියාවලීන් ඇති බැවින් මෙම උපක්‍රම අඩු සාර්ථකත්වයක් පෙන්නුම් කරයි. මෙය නිල ගබඩා වලින් ලබා ගන්නා යෙදුම් වඩාත් ආරක්ෂිත කරයි. නමුත් ප්‍රත්‍යෙක අධ්‍යයනයන් සහ NCSC හි App Store Threat Report පෙන්නුම් කර ඇති පරිදි, මෙම ක්‍රියාවලීන් පරිපූර්ණ නොවේ.

මෙම උපදෙස් 4 අනුගමනය කිරීමෙන් මෙම උපදේශනයේ දක්වා ඇති තර්ජන වලින් ඔබව ආරක්ෂා කර ගත හැක.

වඩාත් සවිස්තරාත්මක උපදෙස් සඳහා, අවම කිරීමේ කොටස බලන්න.

ප්‍රත්‍යක අධ්‍යයන

මෙම කරුණු ප්‍රත්‍යක අධ්‍යයන දෙක මගින් MOONSHINE සහ BADBAZAAR ක්‍රියා කරන ආකාරය, සහ ද්වේෂසහගත සයිබර් ක්‍රියාකාරීන් වඩාත් අවදානමට ලක්ව සිටින අය ඉලක්ක කරන ආකාරය නිරූපණය කෙරේ.

පළමු ප්‍රත්‍යක අධ්‍යයනය: MOONSHINE

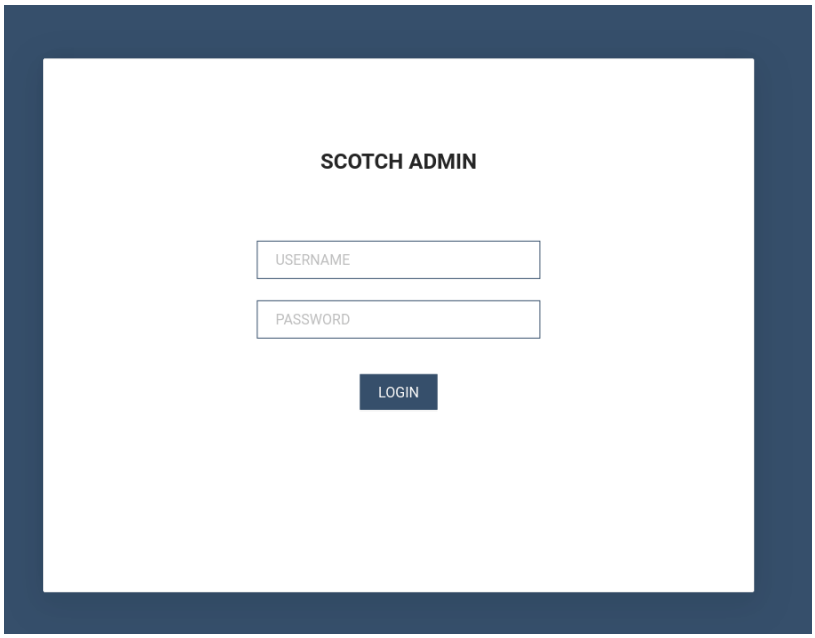
MOONSHINE යනු 2019 දී Citizen Lab විසින් වාර්තා කරන ලද Android ඔත්තු මෘදුකාංගයකි. එය ටිබෙට් කණ්ඩායම් ඉලක්ක කර ගනී. MOONSHINE වින්දිතයින් ලවා එය ස්ථාපනය කිරීමට පොළඹවා ගැනීම සඳහා නීත්‍යානුකූල යෙදුමක් ලෙස බොරු වේශයෙන් පෙනී සිටියි. එය ටෙලිග්‍රෑම් නාලිකා සහ WhatsApp හරහා යවන ලද සබැඳි හරහා බෙදා ගනියි.

MOONSHINE සතුව පුළුල් නිරීක්ෂණ හැකියාවන් ඇත. ඒවා නම්:

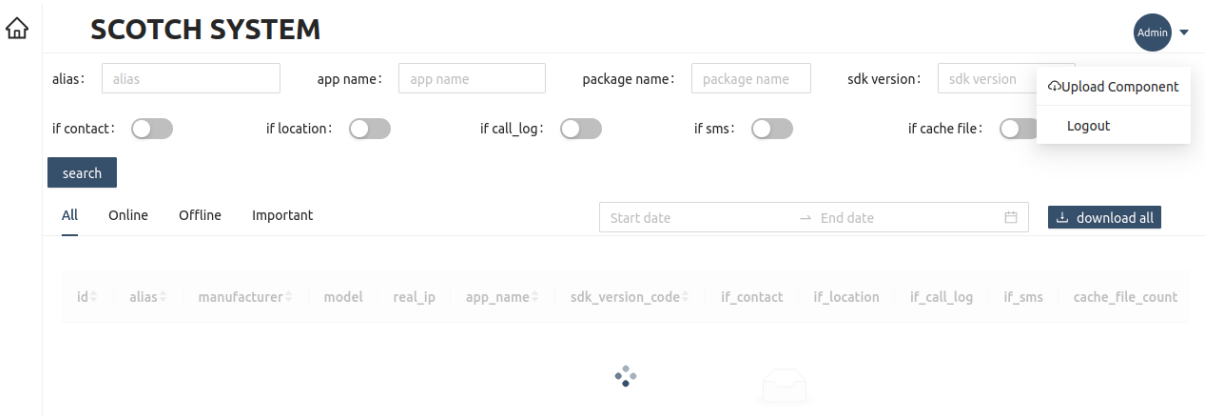
- **තථ්‍ය කාලීන ලුහුබැඳීම ඇතුළුව ස්ථාන දත්ත**
- **සජීවී ශ්‍රව්‍ය සහ ඡායාරූප ග්‍රහණය**
- **උපාංගයෙන් ගොනු බාගත කිරීම**
- **උපාංග තොරතුරු ලබා ගැනීම**
- **උපාංගයේ ශ්‍රව්‍ය වාදනය කිරීම**

‘**Audio Quran.apk**’ ලෙස පරිවර්තනය කරන ලද ‘ **ئاۋازلىق قۇرئان .apk**’ යෙදුම උයිගර් පුද්ගලයන් ඉලක්කගත කිරීම සඳහා MOONSHINE භාවිතා කරන ආකාරය පිළිබඳ උදාහරණයකි. කුරානයේ යෙදුමක් දක්වමින්, ගොනු නාමයේ උයිගර් භාෂාව භාවිතා කිරීම මගින් උයිගර් මුස්ලිම්වරුන්ව ආකර්ෂණය කිරීම සඳහා එය නිර්මාණය කර ඇති බව පෙනේ.

ස්ථාපනය කළ පසු, ද්වේෂසහගත සයිබර් ක්‍රියාකාරීන්ට වින්දිතයින්ගේ උපාංගවලින් තොරතුරු රැස් කළ හැකිය. මෙම තොරතුරු ‘SCOTCH ADMIN’ පැනලය හරහා ලබා ගනියි.



පරිගණකයට ඇතුලු වූ පසු, ක්‍රියාකරුවන්ට පහත තිර රුවෙහි පෙන්වා ඇති පිටුවට ප්‍රවේශ විය හැකිය. මෙම පිටුව ආසාදිත උපාංග පිළිබඳ විස්තර සහ ආසාදිත උපාංග වෙත ක්‍රියාකරුට ඇති ප්‍රවේශ මට්ටම පෙන්නුම් කරයි:



අනිෂ්ට මෘදුකාංග කළමනාකරණ පැනලය එකතු කරන ලද දත්ත පෙන්වයි. එයට ඇතුළත් වන්නේ:

- **උපාංගයට ප්‍රවේශ වන මට්ටම**
- **කෙටි පණිවිඩ**
- **ඇමතුම් සටහන්**
- **ස්ථාන දත්ත**
- **උපාංග තොරතුරු**

සයිබර් ලීගය සමඟ සහයෝගයෙන් යුතුව, NCSC විසින් MOONSHINE අයුතු ලෙස ප්‍රයෝජනයට ගන්නා කට්ටලය සහ HTML නාමයේ 'UPSEC' අඩංගු පිටුසුම් පැනල් අතර අනිච්ඡාදනය සොයා ගැනීම සඳහා Trend Micro වෙතින් වාර්තා කිරීම කර්මාන්තය මත ගොඩනගා ඇත. සම්පූර්ණ විස්තර මේ සමඟ ඇති තාක්ෂණික උපදේශනයේ ඇත.

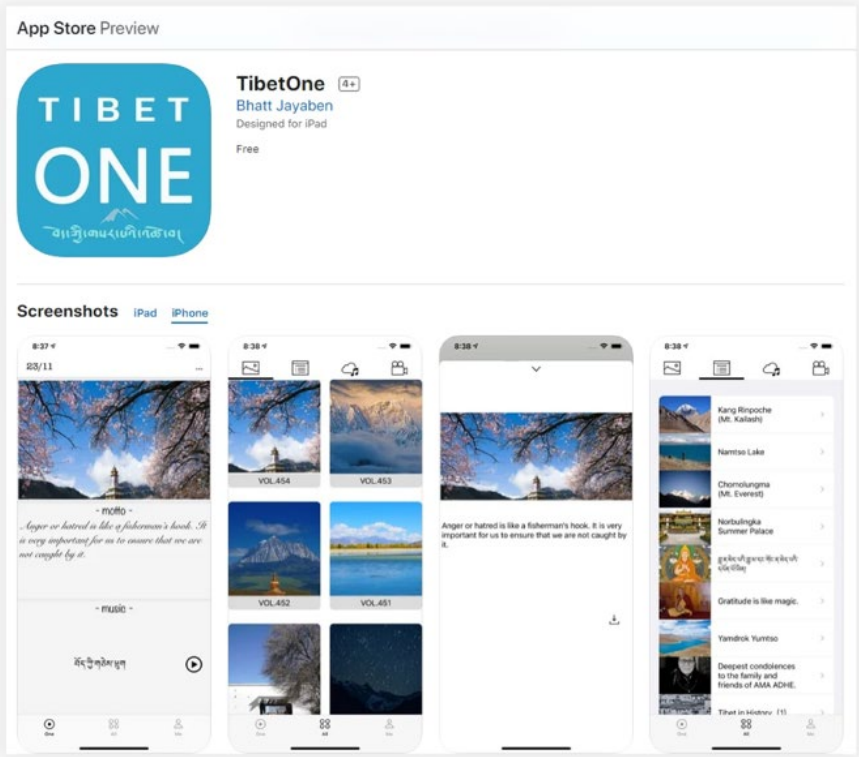
Intelligence Online වලට අනුව , UPSEC යනු 'Sichuan Dianke Network Security Technology Co. Ltd' වෙත යොමු කිරීමකි. කර්තෘ /උත්පාදන ආයතන මෙම ප්‍රකාශය සත්‍යාපනය කර නොමැත.

දෙවැනි ප්‍රතෙයක අධ්‍යයනය BADBAZAAR

BADBAZAAR යනු iOS සහ Android ප්‍රභේද සහිත ජංගම අනිෂ්ට දුෂ්ට මෘදුකාංගයක් වන අතර එය උයිගර්, ටිබෙට් සහ තායිවාන පුද්ගලයින් ඉලක්ක කර ගෙන ඇත. මෙම අනිෂ්ට මෘදුකාංගය සමාජ මාධ්‍ය වේදිකා සහ නිල යෙදුම් ගබඩා හරහා ව්‍යාප්ත වී ඇත.

Lookout සහ Volexity විසින් වාර්තා කරන ලද පරිදි, **'TibetOne'** යෙදුම හරහා ටිබෙට් ජාතිකයන් ඉලක්ක කර ගැනීම සඳහා BADBAZAAR භාවිතා කර ඇත. **TibetOne** යනු උපාංග තොරතුරු සහ ස්ථාන දත්ත වෙත ප්‍රවේශ වීමේ හැකියාව ඇති ද්වේෂසහගත ක්‍රියාකාරීන් විසින් නිර්මාණය කරන ලද iOS යෙදුමකි. එය 2021 දෙසැම්බර් මාසයේදී Apple App Store වෙත උඩුගත කරන ලද නමුත් මෙය තවදුරටත් ලබා ගත නොහැක. මෙම අනිෂ්ට මෘදුකාංගය තවදුරටත් ව්‍යාප්ත කිරීමට, ක්‍රියාකාරීන් '**tibetanphone**' නම් ටෙලිග්‍රාම් නාලිකාවක යෙදුම ප්‍රචාරය කළේය.

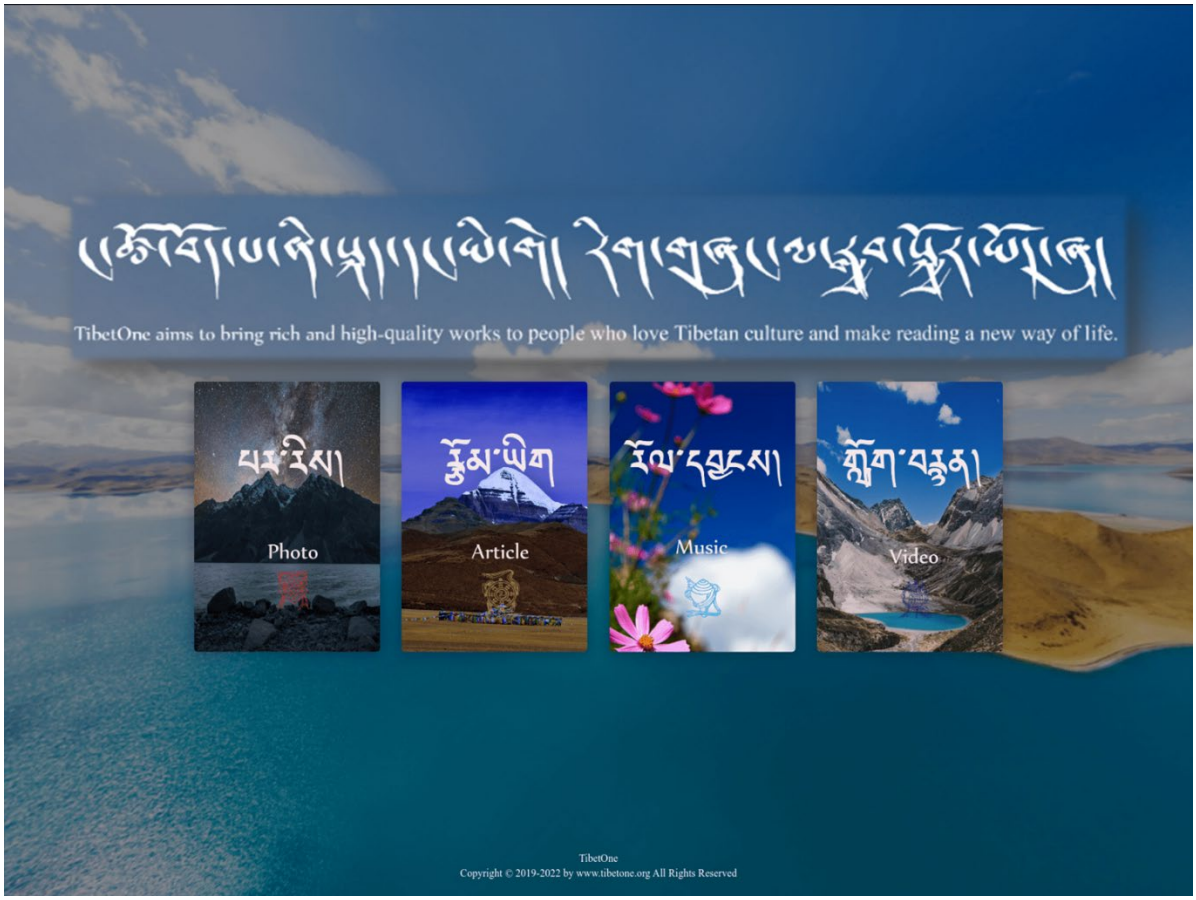
TibetOne



රූපසටහන 1: TibetOne යෙදුම් පිටුව Apple App Store මත. එනැන් සිට මෙම යෙදුම ඉවත් කර ඇත.

රූපසටහන 2 TibetOne ටෙලිග්‍රෑම් නාලිකා තුළ බෙදාගෙන ඇති පරිදි.

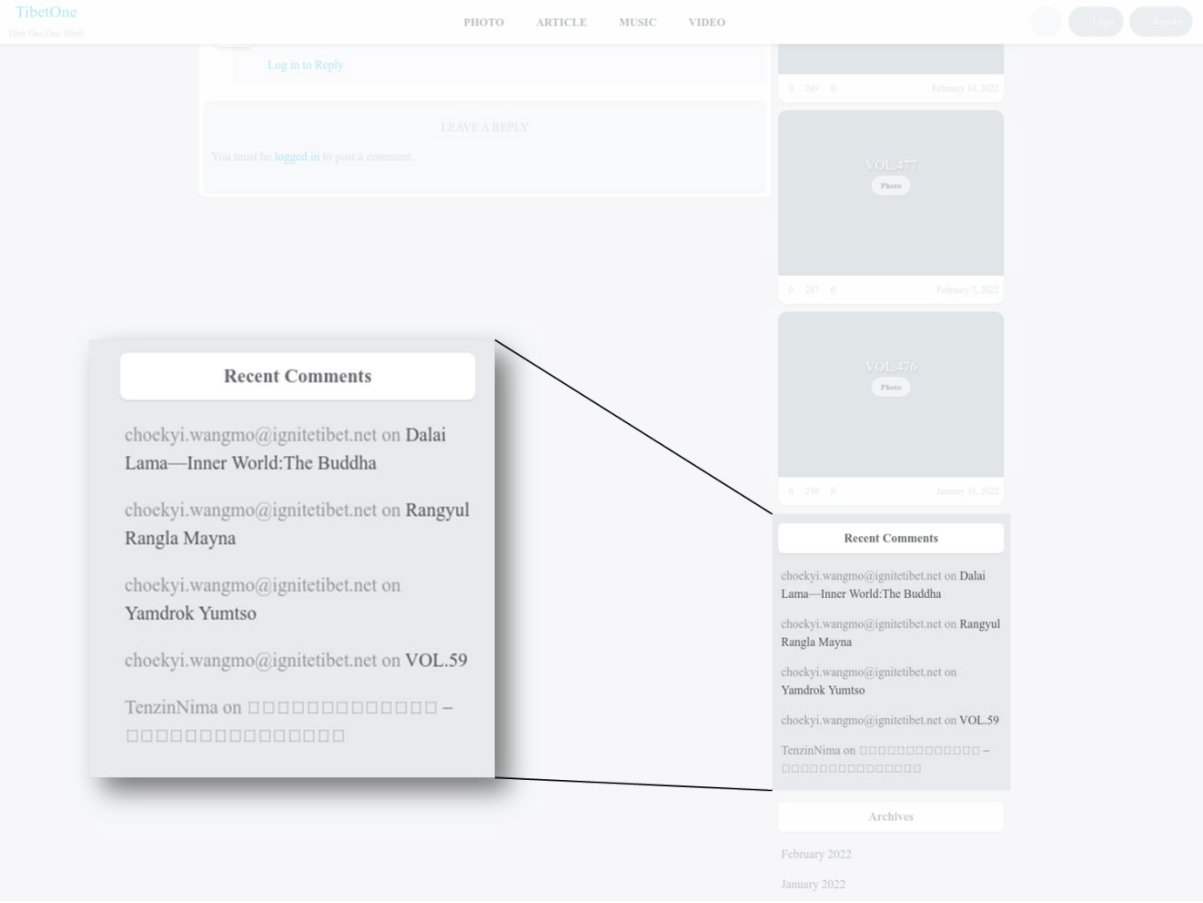
යෙදුමට නීත්‍යානුකූලභාවයක් එක් කිරීම සඳහා, ක්‍රියාකාරීන් විසින් **‘tibetone\[.]org’** නමින් වෙබ් අඩවියක් ද නිර්මාණය කළේය. එය විස්තර කෙරුනේ *‘bring\[ing] rich and high-quality works to people who love Tibetan culture and make reading a new way of life’* ලෙසින්ය.



රූපසටහන 3: 'tibetone[.]org' හි මුල් පිටුව..

අදාළ කොටස් වඩාත් පැහැදිලි කිරීම සඳහා මෙම රූපය සංස්කරණය කර ඇත.

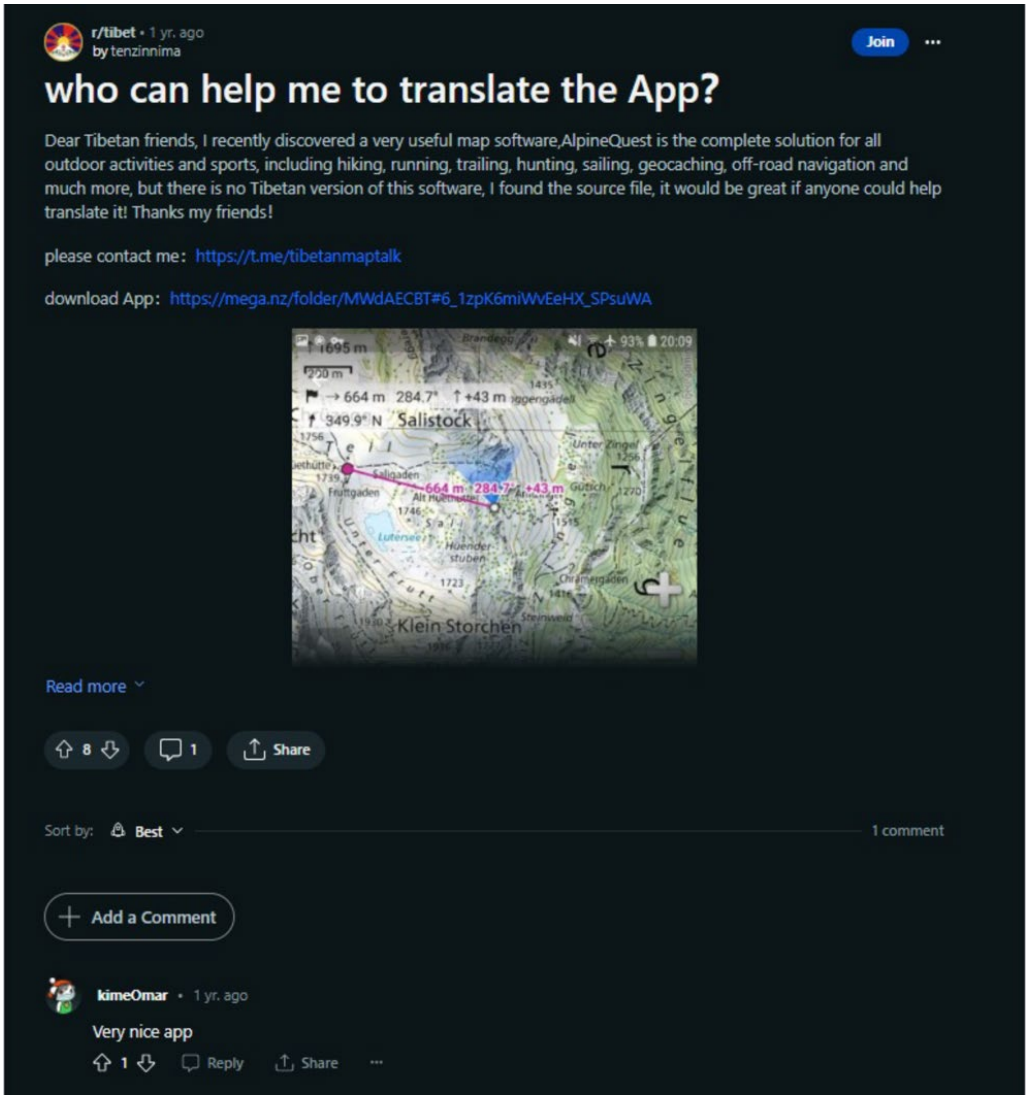
මෙම වෙබ් අඩවියේ පරිශීලකයින්ට අදහස් දැක්වීමට ඉඩ සලසන ලිපි පළ කිරීම සඳහා පිටුවක් නිබුණි. ද්වේෂසහගත ක්‍රියාකාරීන් විසින් පාලනය කරනු ලබන බවට විශ්වාස කෙරෙන **'choekyi.wangmo@ignitetibet.net'** ඊමේල් ලිපිනය මගින් කළ අදහස් දැක්වීමක්, **'Choekyi Wangmo'** ලෙසින් පෙනී සිටින්නෙක් විසින් කිරීමට ඉඩ ඇත.ඔහු මානව හිමිකම් සහ ප්‍රජාතන්ත්‍රවාදය පිළිබඳ ටිබෙට් මධ්‍යස්ථානයේ ටිබෙට් ගැනි විරෝධතාකරුවෙකු වේ. මෙම යෙදුම ටිබෙට් නිදහස සඳහා සැබවින්ම පෙනී සිටින බවට හැඟීමක් ලබාදීම් සඳහා කෙරෙන තවත් උත්සාහයක් විය හැකිය.



රූපසටහන 4: 'tibetone[.]org' පිටුවෙන් ද්වේෂසහගත ක්‍රියාකරුවා විසින් පාලනය කරනු ලබන බවට විශ්වාස කරන පරිශීලකයින්ගේ අදහස් පෙන්වයි.

අදාළ කොටස් වඩාත් පැහැදිලි කිරීම සඳහා මෙම රූපය සංස්කරණය කර ඇත.

'TenzinNima' නැමති වෙනත් පරිශීලක නාමයකින් මෙම අඩවිය මත අදහස් දැක්වීම් සිදුකර ඇත. Volexity විසින් වාර්තා කර ඇත්තේ මෙම පරිශීලක නාමය Reddit හි **'Tibetanmaptalk'** ටෙලිග්‍රාම් නාලිකාව ප්‍රචාරය කිරීම සඳහා ද භාවිතා කරන බවයි. Android උපාංගවලට ලබා ගත හැකි මඟ හසුරුවන සංචලන යෙදුමක් වන 'AlpineQuest' හි ද්වේශසහගත සාම්පලයක් බාගත කිරීම සඳහා සබැඳියක් එහි ඇතුළත් වේ. ලබා දී ඇති බාගත කිරීමේ සබැඳිය Mega නමින් හැඳින්වෙන තෙවන පාර්ශවීය ගොනු බෙදාගැනීමේ සේවාවක් සඳහා වේ.



රූපසටහන 5: Reddit ප්‍රචාරය කරන ද්වේෂසහගත යෙදුම ද්වේෂසහගත ක්‍රියාකරුවකු විසින් පාලනය කරනු ලබන බවට විශ්වාස කෙරෙන ගිණුමක් මගිනි.

සටහනක් වෙත අදහස් දැක්වූ 'KimeOmar' ලෙසින් හඳුන්වන පරිශීලකයෙකු තවත් උප-Reddit සංසදයක ද ද්වේෂසහගත යෙදුම් බෙදා ගන්නා බව නිරීක්ෂණය වී ඇති බව Volexity සනිටුහන් කරයි. මෙයින් ඇඟවෙන්නේ ද්වේෂසහගත ක්‍රියාකාරීන් තම සටහන් සැබෑ ඒවා ලෙස පෙන්වීමට බහු සමාජ මාධ්‍ය පැතිකඩ භාවිතා කරන බවයි.

ඇගයීම

උයිගර්, ටිබෙට් සහ තායිවාන ප්‍රජාවන් විශේෂයෙන් ඉලක්ක කර ගැනීම සඳහා BADBAZAAR සහ MOONSHINE සමාජ ඉංජිනේරු ක්‍රමවේදයන් කිහිපයක් භාවිතා කරයි. එනම්:

- උයිගර් භාෂාවෙන් කුරානයේ යෙදුමක් වැනි මෙම ප්‍රජාවන් කැමැත්තක් දක්වන යෙදුම් ට්‍රෝජනීකරණය කිරීම, නියත වශයෙන්ම ඉලක්කගත විඳිනයන්ට ගැලපෙන පරිදි සකස් කර ඇත.
- මෙම ට්‍රෝජනීකරණය කළ යෙදුම් නිල යෙදුම් ගබඩා වලට එකතු කිරීම මගින් ඒවා සැබෑ බවට හැඟීමක් ලබා දෙන අතර, කණ්ඩායම් අතර කතාබස් වල බෙදා ගැනීමෙන් මෙම ප්‍රජාවන් තුළ විශ්වාසදායක සබඳතා ගසාකෑමට බොහෝ දුරට අදහස් කෙරේ.

BADBAZAAR සහ MOONSHINE මගින් නියත වශයෙන් චීන රජයට වටිනා දත්ත රැස් කළ හැකිය. BADBAZAAR සහ MOONSHINE උයිගර්, ටිබෙට් සහ තායිවාන පුද්ගලයින් ඉලක්ක කර ගන්නා බවට නිරීක්ෂණය කර ඇතත්, චීනයේ අනෙකුත් සුළුතර කණ්ඩායම් ඉලක්ක කර ගන්නා වෙනත් අනිෂ්ට මෘදුකාංග තිබේ. චීනයේ සහ විදේශයන්හි සිටින, පාලන තන්ත්‍රයේ ස්ථාවරත්වයට තර්ජනයක් වන හේතූන් සඳහා සහාය දක්වන බව සැලකෙන, වෙනත් රටවලින් පැමිණි පුරවැසියන්, BADBAZAAR සහ MOONSHINE වැනි ජංගම අනිෂ්ට මෘදුකාංග වලින් නිසැකවම තර්ජනයට ලක්ව ඇත. ස්ථානය, ශ්‍රව්‍ය සහ ඡායාරූප දත්ත ග්‍රහණය කර ගැනීමේ හැකියාව, ඉලක්කයේ ක්‍රියාකාරකම් පිළිබඳ තත්‍ය කාලීන තොරතුරු ලබා දීම මගින් අනාගත නිරීක්ෂණ සහ හිරිහැර මෙහෙයුම් දැනුම් දීමට නිසැකවම අවස්ථාව ලබා දෙයි.

ජංගම යෙදුම් භාවිතා කරන්නන් සඳහා ලිහිල් කිරීමේ පියවර

ප්‍රත්‍යෙක අධ්‍යයනයන්හි විස්තර කර ඇති තර්ජන වලින් ආරක්ෂා වීමට කර්තෘ ආයතන පහත ආරක්ෂක පිළිවෙත් දිරිමත් කරයි. මෙම නිර්දේශවලට හොඳම ප්‍රායෝගික NCSC මාර්ගෝපදේශය මගින් ශක්තියක් ලබා දෙයි. ඔස්ට්‍රේලියාවේ සහ ඇමරිකා එක්සත් ජනපදයේ පාඨකයින් වෙනුවෙන් හොඳම ප්‍රායෝගික මාර්ගෝපදේශ සඳහා සබැඳි සඳහා 'වැඩිදුර කියවීමේ' කොටස බලන්න.

ඔබගේ උපාංගය ආරක්ෂිතව තබා ගන්න

- **Google හි Play Store හෝ Apple හි App Store වැනි නිල යෙදුම් ගබඩාවලින් පමණක් යෙදුම් බාගන්න.** Google හි Play Store සහ Apple හි App Store මෘදුකාංග ලබා ගත හැකි වීමට පෙර ඒවා වෛරස සඳහා පරීලෝකනය කරයි. එමගින් ඔබ බාගත කරන දේ ආරක්ෂිත බවට වැඩි සහතිකයක් ලබා දෙයි, විශ්වාසදායක ගබඩා වලින් ලබා ගන්නා යෙදුම් අවදානම්සහගත විය හැකි නමුත්, වෙනත් මූලාශ්‍ර වලින් කෙරෙන බාගත කිරීම් සඳහා කිසිදු ආරක්ෂාවක් නොතිබිය හැකිය. යෙදුම් ගබඩා පිළිබඳ තර්ජන වාර්තාවක් NCSC සතුව ඇත: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **ඔබේ උපාංගය සහ යෙදුම් යාවත්කාලීනව තබා ගන්න.** ඔබගේ යෙදුම් සහ උපාංග මෘදුකාංග සඳහා යාවත්කාලීන කිරීම්, ඒවා ලබා ගත හැකි ඉක්මනින් ස්ථාපනය කරන්න. ඔබේ උපාංගයේ සැකසුම් තුළ 'ස්වයංක්‍රීය යාවත්කාලීන කිරීම්' කට්ටල අංග තිබේ නම්, ක්‍රියාත්මක කරන්න. එවිට ඔබට එය කිරීමට මතක තබා ගැනීමට අවශ්‍ය නොවේ. දැන හඳුනන වෛරස් සහ වෙනත් ආකාරයේ අනිෂ්ට මෘදුකාංග වලින් ආරක්ෂා වීමට, මාර්ගගතව ආරක්ෂිතව සිටීම පිළිබඳ NCSC මාර්ගෝපදේශය බලන්න. යාවත්කාලීන කිරීම් වලට බොහෝ විට වැඩිදියුණු කිරීම් සහ නව විශේෂාංග ඇතුළත් වේ: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **ඔබගේ උපාංගය 'jailbreak' හෝ 'root' නොකරන්න**, මන්ද යත් එමගින් ක්‍රියාත්මක කර ඇති ආරක්ෂක පාලනයන් මඟ හැරවීම සඳහා නොගැලපෙන අවදානම් භාවිතා කරයි. මෙය උපාංගයන් ප්‍රහාරවලට ගොදුරු වීමේ අවදානම වැඩි කරයි. NCSC මාර්ගෝපදේශය බලන්න: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

ඔබේ යෙදුම් කළමනාකරණය කර ගන්න

- **ඔබේ යෙදුම් සහ ඒවායේ අවසරයන් සමාලෝචනය කරන්න.** ඔබට තවදුරටත් යෙදුමක් අවශ්‍ය නොවේ නම්, එය ඉවත් කරන්න. අනිෂ්ට මෘදුකාංග බොහෝ විට කැමරා සහ මයික්‍රෆෝන වැනි ආරක්ෂිත ගොනු හෝ පර්යන්ත වෙත ප්‍රවේශ වීමට නිර්මාණය කර ඇති බැවින්, ඔබට හැකි අවස්ථාවකදීම, දත්ත නිරාවරණය අවම කිරීම සඳහා යෙදුම් අවසර සීමා කරන්න
  - ඇපල් පරිශීලකයින් සඳහා යෙදුම් අවසර පරීක්ෂා කරන ආකාරය: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Android පරිශීලකයින් සඳහා යෙදුම් අවසර පරීක්ෂා කරන ආකාරය: https://support.google.com/android/answer/9431959?hl=en-GB

- **නොදන්නා යෙදුම් ස්වයංක්‍රීයව Google වෙත යවන්න.** ඔබ Android පරිශීලකයෙකු නම් සහ Google හි Play Store වෙතින් නොවන යෙදුමක් බාගත කර ඇත්නම්, 'Play Protect' යටතේ Google හි Play Store යෙදුම් සැකසුම් තුළ 'හානිකර යෙදුම් හඳුනාගැනීම වැඩි දියුණු කරන්න' සක්‍රීය කිරීමෙන් ඔබට එය Google වෙත යැවිය හැකිය. පරිශීලකයින් ආරක්ෂා කිරීමට උපකාරී වෙමින්, මෙය අනිෂ්ට මෘදුකාංග හඳුනාගැනීම සඳහා යෙදුම පරිලෝකනය කරනු ඇත. මෙය සකසන්නේ කෙසේද යන්න පිළිබඳ තොරතුරු: https://support.google.com/android/answer/2812853?hl=en-GB

සයිබර් සේවාවන් භාවිතා කරන්න

- **සබැඳියක් ක්ලික් කිරීමට පෙර කීර්තිනාමයක් ඇති URL සේවා භාවිතා කරන්න.** Google Transparency Report හෝ Virus Total වැනි සේවාවන් භාවිතයෙන් එය පළමුව ස්කෑන් කිරීම මගින්, ඔබට විද්‍යුත් තැපෑලකින්, කෙටි පණිවිඩයකින් හෝ වෙනත් තැනකින් ලැබෙන සබැඳියක් ආරක්ෂිත දැයි පරීක්ෂා කළ හැකිය. ගොනුවක් ද්වේශසහගතද යන්න හඳුනා ගැනීමට උපකාරී වන Virus Total වැනි අනිෂ්ට මෘදුකාංග විශ්ලේෂකයෙක් වෙතට ඔබට සැක සහිත ගොනු සහ යෙදුම් උඩුගත කළ හැකිය. ස්කෑන් කිරීමේ සේවාවන් ව්‍යාජ නිෂේධක පෙන්නුම් කළ හැකි බව මතක තබා ගන්න.{

- **Google Advanced Protection වැඩසටහනට ලියාපදිංචි වන්න.**මෙය ඉලක්කගත වීමේ අවදානමට ලක්ව සිටින Google සේවාවන් (Gmail, Play Store, ආදිය) භාවිතා කරන පුද්ගලයින් ආරක්ෂා කිරීම සඳහා නිර්මාණය කර ඇති නොමිලේ සැපයෙන සේවාවකි. Google සේවාවන් භාවිතා කරන විට මෙම සේවාව ඉහළ ආරක්ෂාවක් සපයයි: https://landing.google.com/advancedprotection/

- **ඔරොත්තු දිය හැකි සේවාවන් සඳහා, ඒවා ලබාගත් හැකි අවස්ථාවලදී, ලියාපදිංචි වන්න.** උදාහරණයක් ලෙස, එක්සත් රාජධානියේ ඉහළ අවදානම් සහිත පුද්ගලයින්ට ඔවුන්ගේ සයිබර් ආරක්ෂාවට උපකාරී වීම සඳහා අමතර ආරක්ෂක සේවාවන් සඳහා සුදුසුකම් ලැබිය හැකිය. සුදුසුකම් පරීක්ෂා කර වැඩිදුර සොයා බලන්න: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

තර්ජන වාර්තා කරන්න

- **ව්‍යාජ ගිණුම් හඳුනා ගැනීම සහ වාර්තා කිරීම.** ද්වේෂසහගත සයිබර් ක්‍රියාකරුවන් තම අරමුණු ඉටුකර ගැනීම සඳහා ව්‍යාජ ගිණුම් නිර්මාණය කිරීම් හෝ සැබෑ ගිණුම්වලින් දත්ත ලබා ගැනීම් සිදු කරයි. ගිණුමක් ව්‍යාජ හෝ අවදානමට ලක් වූ බවට ඔබ සැක කරන්නේ නම්, එය වේදිකාවට වාර්තා කර එය අවහිර කරන්න. ඉන්ස්ටග්‍රෑම් සහ මුහුනුපොත සඳහා ‘සත්‍යාපිත ලාංඡන’ වැනි ගිණුම් සත්‍යාපනය කිරීමේ ක්‍රියාවලියක් බොහෝ සේවාවන් සතුව ඇත. මෙය ගිණුමක් අව්‍යාජ බව හඳුනා ගැනීමට උපකාරී වේ. NCSC සතුව සමාජ මාධ්‍ය ආරක්ෂිතව භාවිතා කිරීම පිළිබඳ මාර්ගෝපදේශයක් ඇත. අවදානමට ලක් වූ ගිණුම් සත්‍යාපනය කර වාර්තා කරන්නේ කෙසේද යන්න පිළිබඳ විස්තර එහි ඇතුළත් වේ: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **වංචනික ඊමේල්, කෙටි පණිවුඩ සහ සබැඳි භාවිතයෙන් වංචනික සන්නිවේදනයන් යැවීම.** ...NCSC හට සැක සහිත ඊමේල් ලිපින සහ වෙබ් අඩවි විමර්ශනය කළ හැකිය. ඔබ වෙබ් අඩවියක්, විද්‍යුත් තැපෑලක් හෝ පණිවිඩයක් සැක සහිත යැයි සිතන්නේ නම්, ඔබට එය වාර්තා කළ හැකිය: NCSC හට සැක සහිත ඊමේල් ලිපින සහ වෙබ් අඩවි විමර්ශනය කළ හැකිය. ඔබ වෙබ් අඩවියක්, විද්‍යුත් තැපෑලක් හෝ පණිවිඩයක් සැක සහිත යැයි සිතන්නේ නම්, ඔබට එය වාර්තා කළ හැකිය: https://www.ncsc.gov.uk/collection/phishing-scams

NCSC පාරිභාෂික ශබ්ද මාලාව

Android

Google හි ජංගම මෙහෙයුම් පද්ධතිය, ස්මාර්ට්ෆෝන් සහ ටැබ්ලට් නිෂ්පාදකයින් කිහිප දෙනෙකු විසින් භාවිතා කරනු ලැබේ.

යෙදුම

භාවිතයක්, හෝ යෙදුමක්, යනු පරිශීලකයින්ට තම උපාංගයට අමතර කර්යිකත්වයක් හෝ අන්තර්ගතයක් ලබා දීම සඳහා උපාංගයක ස්ථාපනය කළ හැකි හෝ පෙර ස්ථාපනය කළ හැකි මෘදුකාංග පැකේජයකි.

සයිබර් ආරක්ෂණය

උපාංග, සේවා සහ ජාල - සහ ඒවායේ අඩංගු තොරතුරු - අනවසර ප්‍රවේශය, සොරකම් කිරීම් හෝ හානි වලින් ආරක්ෂා කර ගැනීම.

උපාංගය

ඩෙස්ක්ටොප් පරිගණකයක්, ස්මාර්ට් ජංගම දුරකථනයක් හෝ ටැබ්ලටයක් වැනි භෞතිකව පවතින පරිගණක පාදක දෘඩාංග.

iOS

Apple ජංගම උපාංග කට්ටලයේ භාවිතා කරන එහි ජංගම මෙහෙයුම් පද්ධතිය.

අනිෂ්ට මෘදුකාංග

'ද්වේෂසහගත මෘදුකාංග' වලින් ව්‍යුත්පන්න වූ, අනිෂ්ට මෘදුකාංග යනු පරිගණක පද්ධති, ජාල හෝ උපාංග වලට හානි කළ හැකි ඕනෑම ආකාරයක මෘදුකාංගයකි. වෛරස්, කප්පම් සඳහා යොදා ගන්න මෘදුකාංග සහ ට්‍රෝජන් ඇතුළත් වේ.

මෙහෙයුම් පද්ධතිය

පරිගණක, ටැබ්ලට් සහ ස්මාර්ට්ෆෝන් මත භාවිතා වන, අමතර යෙදුම් සහ දෘඩාංග ක්‍රියාත්මක කිරීමට අවශ්‍ය වන මූලික මෘදුකාංග.

වංචනික සන්නිවේදනයන් යැවීම.

අනිෂ්ට මෘදුකාංග අඩංගු විය හැකි, හෝ සංවේදී තොරතුරු (මුරපද වැනි) හෙළි කිරීම හෝ මුදල් මාරු කිරීම සඳහා පරිශීලකයින් රවටා ගත හැකි වෙබ් අඩවි හා සම්බන්ධ සබැඳි අඩංගු වංචනික ඊමේල් හෝ කෙටි පණිවිඩ.

ඔත්තු මෘදුකාංග

පරිශීලකයාගේ අවසරයකින් තොරව උපාංගයක ස්ථාපනය කර, දත්ත රැස් කර තෙවන පාර්ශවයකට යවන අනිෂ්ට මෘදුකාංග වර්ගයකි.

- **සමාජ මාධ්‍ය**

පරිශීලකයන් විසින් ජනනය කරන ලද අන්තර්ගතයන් (කෙටි පණිවිඩ, ඡායාරූප සහ වීඩියෝ) බෙදා ගැනීමට සහ ප්‍රතිචාර දැක්වීමට පුද්ගලයින්ට ඉඩ සලසන ෆේස්බුක්, X සහ ඉන්ස්ටග්‍රෑම් වැනි වෙබ් අඩවි සහ යෙදුම්.

- **ස්මාර්ට්ෆෝන්**

ඇන්ඩ්‍රොයිඩ් සහ iOS මෙහෙයුම් පද්ධති සහිත සංකීර්ණ ක්‍රියාකාරිත්වයක් ඉටු කරන නවීන ජංගම දුරකථන.

- **ට්‍රෝජන්**

නීත්‍යානුකූල මෘදුකාංගයක් ලෙස වෙස්වලාගත්, වින්දිතයෙකුගේ උපාංගයට අනවසර ලෙස ප්‍රවේශය වීමට භාවිතා කරන අනිෂ්ට මෘදුකාංග වර්ගයකි.

- **URL**

ඒකාකාර සම්පත් ස්ථානගත කරන්නා. අඩවි වසම් නාමයක් වැනි ලෝක ව්‍යාප්ත වෙබයේ ලිපිනයක් (උදාහරණයක් ලෙස www.bbc.co.uk).

- **වෛරස්**

නීත්‍යානුකූල මෘදුකාංග වැඩසටහන් ආසාදනය කිරීමට නිර්මාණය කර ඇති සහ එම වැඩසටහන් සක්‍රිය කළ විට ජාල හරහා ප්‍රතිනිර්මාණය වන අනිෂ්ට මෘදුකාංග වර්ගයකි.

වැඩිදුර කියවීම

ඔස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානයේ මග පෙන්වීම

- Report a cybercrime, incident or vulnerability සයිබර් අපරාධයක්, සිද්ධියක් හෝ අවදානමක් වාර්තා කරන්න
- How to secure your devices ඔබගේ උපාංග සුරක්ෂිත කර ගන්නේ කෙසේද
- Secure your mobile phone ඔබගේ ජංගම දුරකථනය සුරක්ෂිත කර ගන්න
- Phishing වංචනිකව යවනු ලබන
- Scams වංචනික ක්‍රියා
- Secure your social media ඔබගේ සමාජ මාධ්‍ය සුරක්ෂිත කර ගන්න
- Security tips for social media and messaging apps සමාජ මාධ්‍ය සහ පණිවිඩ යෙදුම් සඳහා ආරක්ෂක උපදෙස්

Guidance from the UK NCSC and NPSA

- Defending Democracy ප්‍රජාතන්ත්‍රවාදය ආරක්ෂා කිරීම
- Social Media: how to use it safely සමාජ මාධ්‍ය: එය ආරක්ෂිතව භාවිතා කරන්නේ කෙසේද
- Device Security Guidance for organisations including mobile සංවිධාන සඳහා උපාංග, ජංගම උපාංග ඇතුළු, ආරක්ෂක මාර්ගෝපදේශ
- Threat report on application stores. යෙදුම් ගබඩා පිළිබඳ තර්ජන වාර්තාව.
- Personal safety and security for high-risk individuals අධි අවදානම් සහිත පුද්ගලයින් සඳහා පුද්ගලික ආරක්ෂාව සහ සුරක්ෂිත භාවය

ඇමරිකා එක්සත් ජනපද NSA වෙතින් මග පෙන්වීමක්

- Mobile Device Best Practices ජංගම උපාංග සම්බන්ධ හොඳම පිළිවෙත්

හිමිකම් අත්හැරීම

මෙම උපදේශනයේ සැපයෙන තොරතුරු එය ප්‍රකාශනය කරන අවස්ථාවේ වලංගු ඒවා බව කරුණාවෙන් සලකන්න.

මෙම වාර්තාව කර්තෘ ආයතනයේ සහ කර්මාන්ත මූලාශ්‍රවලින් ලබාගත් තොරතුරු මත පදනම් වේ. සියලු අවදානම් වළක්වා ගැනීමේ සහ නිර්දේශ අනුගමනය කිරීමේ අරමුණින් නොකරන ලද යම් සොයාගැනීම් හා සහ නිර්දේශ මගින් එවැනි සියලු අවදානම් ඉවත් නොවේ. තොරතුරු අවදානම් වල හිමිකාරිත්වය සෑම විටම අදාළ පද්ධති හිමිකරු සමඟ පවතී.

එක්සත් රාජධානියේ, මෙම තොරතුරු Freedom of Information Act 2000 (FOIA) පනත යටතේ වගකීමෙන් නිදහස් කර ඇති අතර අනෙකුත් එක්සත් රාජධානියේ තොරතුරු නීති යටතේ වගකීමෙන් නිදහස් කළ හැකිය.

ඕනෑම FOIA විමසුමක් ncscinfoleg@ncsc.gov.uk වෙත යොමු කරන්න.

ඇමුණුම: නිරීක්ෂණය කරන ලද MOONSHINE & BADBAZAAR සාම්පල

පසුගිය වසර දෙක තුළ MOONSHINE සහ BADBAZAAR ක්‍රියා මාලාවල නිරත වීම සඳහා භාවිතා කළ යෙදුම් මෙම වගුවේ ලැයිස්තුගත කර ඇත.

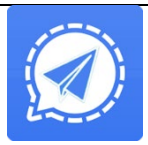
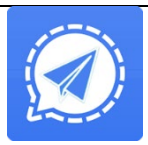
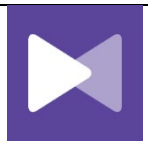
මෙම යෙදුම් බොහොමයක් හා ස්ථාපිත යෙදුම් අතර පැහැදිලි සමානකමක් පෙන්නුම් කරයි. මෙය ප්‍රසිද්ධ වෙළඳ නාම 'රැවටීමට' හිතාමතාම භාවිතා කරන උපක්‍රමයක් වීමට ඉඩ ඇත.

යෙදුමේ නම, පැකේජයේ නම, සහ අයිකොන යන සියල්ලටම සැබෑ භාවිත අනුකරණය කිරීමට හෝ ගැළපීමට හැකි බවත්, එබැවින් උපාංගයක් ආසාදනය වී ඇත්දැයි හඳුනා ගැනීමට පමණක් ඒවා භාවිතා නොකළ යුතු බවත් සැලකිල්ලට ගැනීම වැදගත්ය.

ලිහිල් කිරීම පිළිබඳ කොටසේ ඇතුළත් කර ඇති පරිදි, 'හානිකර යෙදුම් හඳුනාගැනීම වැඩි දියුණු කිරීම' මගින් Android උපාංගයේ ඇති ඔබේ යෙදුම් Google වෙත යැවිය හැකිය.එවිට Play Store වලට පිටතින් ස්ථාපනය කර ඇති ඔබගේ උපාංගයේ යෙදුම් පරිලෝකනය සක්‍රීය කරනු ඇත.

යෙදුමේ නාමය	පැකේජයේ නම	යෙදුමේ අයිකොනය
අල්ලා දෙවියන්වහන්සේගේ නම් 99	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	
කැල්කියුලේටරය	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	

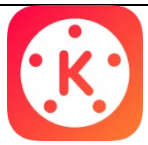
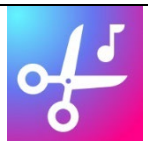
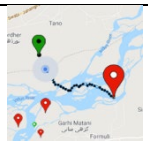
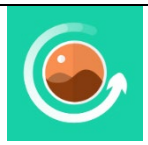
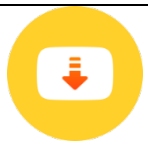
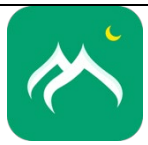
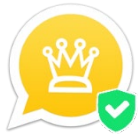
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

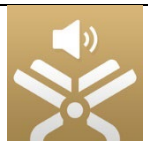
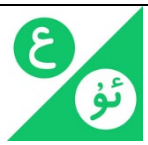
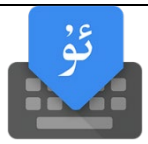
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore 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	
ස්කයිප්	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	
උයිගර් යර්හුරු පුවරුව	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	
හඬ පටිගත කරන යන්ත්‍රය	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast missing trans?	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	
ئەسەرلەر ئاۋازلىق	com.ewlat.eserler	

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