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

အကြံပြုချက်

BADBAZAAR နှင့် MOONSHINE- ဝဂါလူမျိုး၊ ထိုင်ဝမ်နှင့် တိဘက်လူမျိုးများနှင့် လူမှုအဖွဲ့အစည်းများကို ပစ်မှတ်ထားကာ ထောက်လှမ်းသည့် ဆော့ဖ်ဝဲ Spyware

၉ ဧပြီ ၂၀၂၁

BADBAZAAR နှင့် MOONSHINE- ဝဂါလူမျိုး၊ ထိုင်ဝမ်နှင့် တိဘက်လူမျိုးများနှင့် လူမှုအဖွဲ့အစည်းများကို ပစ်မှတ်ထားကာ ထောက်လှမ်းသည့် ဆော့ဖ်ဝဲ Spyware

NCSC နှင့် ပါတနာများမှ ထောက်လှမ်းရေး ဆော့ဖ်ဝဲ spyware မျိုးကွဲ နှစ်ခုနှင့် ပတ်သက်သည့် အချက်အလက်များနှင့် အန္တရာယ်များကို လျှော့ချနိုင်မည့် နည်းလမ်းများအား ထုတ်ဝေထားပါသည်။

အကျဉ်းချုပ်

ယူကေနိုင်ငံမှ Cyber League ပံ့ပိုးမှုဖြင့် အမျိုးသား ဆိုင်ဘာလုံခြုံရေးစင်တာ National Cyber Security Centre (NCSC UK) နှင့် အောက်ပါ နိုင်ငံတကာ ပါတနာများ ပူးပေါင်းကာ ဤအကြံပြုချက်အား ပူးပေါင်းထုတ်ဝေခြင်း ဖြစ်ပါသည်။

- **ဆက်သွယ်ညွှန်ကြားရေးမှူးရုံး၏ အစိတ်အပိုင်းဖြစ်သည့် ဩစတြေးလျ ဆိုင်ဘာ လုံခြုံရေးစင်တာ The Australian Cyber Security Centre**
- **ဆက်သွယ်မှုဆိုင်ရာ လုံခြုံရေး ဦးစီးဌာန၏ အစိတ်အပိုင်းဖြစ်သည့် ကနေဒါ ဆိုင်ဘာလုံခြုံရေး စင်တာ The Canadian Centre for Cyber Security**
- **ဂျာမန်နိုင်ငံ ဗဟို ထောက်လှမ်းရေး ဝန်ဆောင်မှုရုံး The German Federal Intelligence Service**
- **ဂျာမန်နိုင်ငံ ဖွဲ့စည်းအုပ်ချုပ်ပုံ အခြေခံ ဥပဒေ ကာကွယ်ရေး ဗဟိုရုံး The German Federal Office for the Protection of the Constitution**
- **အစိုးရ၏ ဆက်သွယ်မှုဆိုင်ရာ လုံခြုံရေးဗဟိုဌာန၏ အစိတ်အပိုင်းဖြစ်သည့် နယူးဇီလန်နိုင်ငံ ဆိုင်ဘာလုံခြုံရေး စင်တာ The New Zealand National Cyber Security Centre**
- **အမေရိကန် ဗဟိုထောက်လှမ်းရေး ဌာန The United States Federal Bureau of Investigation**
- **အမေရိကန်နိုင်ငံ အမျိုးသား လုံခြုံရေး အေဂျင်စီ The United States National Security Agency**

ဤအကြံပြုချက်၏ ရည်ရွယ်ချက်မှာ ထိုင်ဝမ်အရေး၊ တိဘက်နှင့် ရှင်ကျန် ပြည်နယ်မှ ဝိဂါ ကိုယ်ပိုင်အုပ်ချုပ်ခွင့်ရဒေသ အကြောင်းများ၊ ဒီမိုကရေစီ လှုပ်ရှားမှုနှင့် Falun Gong အကြောင်းနှင့် ပတ်သက်လာလျှင် မသမာသည့် ဆိုင်ဘာတိုက်ခိုက်ရေးသမားများ၏ ခြိမ်းခြောက်မှုများ ပိုများလာနေသည့်အကြောင်း လူအများ သိစေရန် ရည်ရွယ်ထုတ်ဝေခြင်း ဖြစ်ပါသည်။

ဤအကြံပြုချက်ထဲတွင် မသမာသည့် ဆိုင်ဘာ တိုက်ခိုက်ရေး သမားများ တိုက်ခိုက်မှုလုပ်စဉ်အတွင်း အသုံးပြုသည့် နည်းလမ်းများကို ဖြစ်ရပ်မှန် ဥပမာ နှစ်ခုဖြင့် အသေးစိတ် ဖော်ပြထားပါသည်။ ထိုထောက်လှမ်းရေး ဆော့ဖ်ဝဲများမှာ BADBAZAAR နှင့် MOONSHINE ဆိုသည့် spyware များဖြစ်ကြပြီး ၎င်းတို့သည် စမတ်ဖုန်း အပါအဝင် တရုတ်နိုင်ငံနှင့် ပတ်သက်နိုင်သည့် မိုဘိုင်းပစ္စည်းများ၏ အချက်အလက်များကို ပစ်မှတ်ထားသည့် ထောက်လှမ်းရေး ဆော့ဖ်ဝဲများ ဖြစ်ပါသည်။ ထို့အပြင် ဤအကြံပြုချက်သည် တစ်ဦးတစ်ယောက်ချင်းစီ အနေဖြင့် မိမိကိုယ်ကိုနှင့် မိမိကိုင်ဆောင်သည့် စက်ပစ္စည်း၏ အချက်အလက်များအား မည်ကဲ့သို့ ကာကွယ်နိုင်ကြောင်း လမ်းညွှန်ချက်များလည်း ဖော်ပြပေးထားပါသည်။

ဤအကြံပြုချက်နှင့်အတူ NCSC မှ ပညာရပ်ဆန်သည့် အသေးစိတ် သီးသန့် လမ်းညွှန်ချက် ဖြင့်လည်း ဖော်ပြမှု လုပ်ထားပါသည်။

မည်သူ့အတွက် အန္တရာယ် ရှိနိုင်သနည်း။

အာဏာပိုင် အေဂျင်စီများနှင့် ကဏ္ဍအတွင်းမှ ပါတနာများ၏ စောင့်ကြည့်ချက်အရ BADBAZAAR နှင့် MOONSHINE တို့သည် တရုတ်နိုင်ငံ၏ ပြည်တွင်းအာဏာပိုင်များ၊ တရုတ်၏ ရည်ရွယ်ချက်နှင့် ကမ္ဘာတွင် တရုတ်၏ နာမည်အား ထိခိုက်အောင် ခြိမ်းခြောက်လုပ်ဆောင်နိုင်သည့် လူတစ်ဦးတစ်ယောက်ချင်းကို အထူးပစ်မှတ်ထားကြောင်း တွေ့ရှိရပါသည်။ ဤကဲ့သို့ ပစ်မှတ်ထား အခံရနိုင်ဆုံးသော သူများမှာ - ထိုထက်မကသောသူများလည်း ပါနိုင်ပြီး - အောက်ပါ လှုပ်ရှားမှုများနှင့် ဆက်စက်မှု ရှိသည့် ပုဂ္ဂိုလ်များ ဖြစ်ပါသည်။

- **ထိုင်ဝမ် လွတ်လပ်ရေး**
- **တိဘက်လူမျိုး အခွင့်အရေးများ**
- **ဝိဂါ မွတ်ဆလင်နှင့် တရုတ်နိုင်ငံ ရှင်ကျန်း ဝိဂါ ကိုယ်ပိုင်အုပ်ချုပ်ခွင့်ရ ဒေသမှ အခြားသော လူနည်းစုများ**
- **ဒီမိုကရေစီအရေး ဆောင်ရွက်မှုများ (ဟောင်ကောင် အပါအဝင်)**
- **Falun Gong ဝိညာဉ်ရေးဆိုင်ရာ လှုပ်ရှားမှုတို့ ပါဝင်ပါသည်။**

ထိုပစ်မှတ်ထားခံရသည့် စာရင်းတွင် (NGOs) အစိုးရမဟုတ်သည့် အဖွဲ့အစည်းများ၊ သတင်းထောက်များနှင့် အထက်ဖော်ပြပါ လှုပ်ရှားမှုများကို အားပေးထောက်ခံသည့် လုပ်ငန်းများ၊ တသီးပုဂ္ဂလများနှင့် ထိုအဖွဲ့အစည်းများနှင့် ရင်းနှီးဆက်စပ်မှု သို့မဟုတ် ကိုယ်စားပြုမှု ရှိသည့် သူများလည်း ပါဝင်ပါသည်။ ထို spyware များသည် အွန်လိုင်းပေါ် ပျံ့နှံ့ကာ ၎င်းတို့ပစ်မှတ်ထားသည့် ပုဂ္ဂိုလ်များကိုသာ သီးသန့်တိုက်ခိုက်ခြင်းမဟုတ်ဘဲ ရည်ရွယ်မထားသည့် သူများလည်း တိုက်ခိုက်မှုတွင် ထိခိုက်နစ်နာတာမျိုး ဖြစ်နိုင်ပါသည်။

ဤအကြံပြုချက်သည် BADBAZAAR နှင့် MOONSHINE spyware များ၏ အချို့သော ခြိမ်းခြောက်မှုများအား ထိရောက်စွာ တုန့်ပြန်ရာတွင် အထောက်အကူပြုရန်အတွက် ရည်ရွယ်ထုတ်ဝေထားပါသည်။ ခြိမ်းခြောက်မှုကို လျော့ချစေသည့် အကြံပြုချက်များသည် ပိုမိုကျယ်ပြန့်သည့် ဆိုင်ဘာလုံခြုံရေး အကြံပြုချက်များအတွက်လည်း အကျုံးဝင်သည့်အတွက် ဤအကြံပြုချက်များကို သီးသန့်ခွဲထားခြင်းမျိုး မလုပ်သင့်ပေ။

ဤလမ်းညွှန်ချက်များကို လိုက်နာခြင်းဖြင့် အသုံးပြုသူများသည် ၎င်းတို့၏ မိုဘိုင်းပစ္စည်းနှင့် အချက်အလက်များ တိုက်ခိုက်ခံရမှု အန္တရာယ်ကို လျော့ချနိုင်မည် ဖြစ်သည်။

ခြိမ်းခြောက်မှု

MOONSHINE နှင့် BADBAZAAR တို့သည် ကောင်းမွန်သည့် ဆော့ဖ်ဝဲများကဲ့သို့ ဟန်ဆောင်ကာ မသမာမှုများ လုပ်ဆောင်သည့် trojans ၏ ဥပမာများ ဖြစ်သည်။ ၎င်းတို့တွင် ဖျက်ဆီးနိုင်သည့် အရာများကို app ထဲတွင် ထည့်သွင်းကာ ထို app အား app store များနှင့် အွန်လိုင်းဖိုင် မျှဝေခြင်း ဝန်ဆောင်မှုများမှတစ်ဆင့် ၎င်းအား ဒေါင်းလုဒ် လုပ်နိုင်ရန် လုပ်ဆောင်ထားတတ်ပါသည်။

ထို app များသည် ၎င်းတို့ကို အသုံးပြုသူများ ဒေါင်းလုဒ် လုပ်ရန်၊ ဖုန်းကဲ့သို့ စက်ပစ္စည်းထဲတွင် ထည့်သွင်းရန်အတွက် လူများကို လှည့်ဖျားနိုင်အောင် ပြုလုပ်ထားပါသည်။ ထို app ကို ထည့်သွင်းပြီးသည်နှင့် မိမိထည့်သွင်းလိုက်သည့် စက်ပစ္စည်း၏ ပျော့ကွက်ဟာကွက်များကို အသုံးပြုကာ မိမိခွင့်မပြုထားသည့် အရာများကို လုပ်ဆောင်ခြင်း သို့မဟုတ် ၎င်း app ကို အသုံးပြုလိုပါက အောက်ပါ အချက်အလက်များကို ရယူခွင့် ပြုပါသည်ဟု ခွင့်ပြုချက် ပါရှိသည့် app များကို အသုံးပြုပါသည်။ ထိုအချက်များမှာ-

- **အချိန်နှင့် တပြေးညီ မိမိ၏ လက်ရှိတည်နေရာကို သိနိုင်သည့် အချက်အလက်များ**
- **မိမိ၏ မိုက်ခရိုဖုန်းနှင့် ကင်မရာကို ဝင်ရောက်ခွင့်**
- **မိမိ၏ စာတိုမက်ဆေ့ချ်များ၊ ဓာတ်ပုံများနှင့် အခြား သိမ်းထားသည့် ဖိုင်များထဲ ဝင်ရောက်နိုင်ခွင့်**
- **မိမိအသုံးပြုသည့် ပစ္စည်းနှင့် အခြား အချက်အလက်များကို သိရှိခွင့်ပေးခြင်းတို့ ပါဝင်ပါသည်။**

ထိုမသမာသူများသည် ၎င်း၏ app ကို အမှန်တကယ် စိတ်ဝင်စားရာက app ကို ရယူသည့် အချက်ကို အခွင့်ကောင်းယူကာ မသမာမှုများကို များနိုင်သမျှ များအောင် ပြုလုပ်ပြီး လူများ၏ အချက်အလက်ကို ရယူခြင်းများ ပြုလုပ်လျက်ရှိသည်။ ထိုကဲ့သို့ လုပ်ဆောင်သည့် နည်းလမ်းတစ်ခုမှာ ၎င်းတို့လှည့်စားလိုသည့်လူများ ကြိုက်နှစ်သက်မည့် app များ ဥပမာ ဌာနေဘာသာစကားနှင့် အသုံးပြုနိုင်ခြင်း သို့မဟုတ် တရုတ်နိုင်ငံ တိဘက်ဒေသ သို့မဟုတ် ရှင်ကျန်းဒေသ စသည်တို့ဖြင့် ၎င်းတို့ပစ်မှတ်ထားသူများ ကြိုက်နှစ်သက်နိုင်သော app များကို တီထွင်ကာ ဆွဲဆောင်နိုင်ပါသည်။

ဤအကြံပြုချက်ထဲတွင် အဆိုပါ ဥပမာ app များကို ဖော်ပြထားပြီး ထိုအထဲတွင် TibetOne နှင့် Uyghur Quran app တို့ ပါဝင်ပါသည်။

ထိုမသမာသူများသည် ၎င်းတို့ ပစ်မှတ်ထားလိုသူများ စုဝေးရာ အွန်လိုင်းဖိုရမ်တွင် တက်ကြွစွာ ပါဝင်တတ်ပြီး ထိုမှတစ်ဆင့် ပစ်မှတ်ထားသူများကို အများဆုံး တိုက်ခိုက်မှု လုပ်နိုင်ခြင်း ဖြစ်ပါသည်။ ၎င်းတို့သည် တိဘက်နှင့် ဆက်စပ်သည့် တယ်လီဂရမ်များနှင့် Reddit ဖိုရမ်များတွင် spyware များကို

တမင်တကာ ဖြန့်ဖြူး မျှဝေမှုများလည်း ပြုလုပ်ကြကြောင်း တွေ့ရှိရပါသည်။ ဤအကြံပြုချက်မှ ဖော်ပြသည့် ဖြစ်ရပ်မှန် နမူနာများထဲတွင် ထိုကဲ့သို့သော လုပ်ဆောင်ချက်များအား ဥပမာအနေဖြင့်လည်း ဖော်ပြထားပါသည်။

မသမာသည့် apps များသည် APK file များကဲ့သို့ တစ်ခုတည်းသော သီးသန့်ဖိုင်အဖြစ် မျှဝေမှု လုပ်ဆောင်ပြီး အသုံးပြုသူများမှ ထိုဖိုင်အား ဒေါင်းလုဒ်လုပ်ရန် သို့မဟုတ် ထည့်သွင်းခြင်း ပြုလုပ်အောင် လုပ်ဆောင်ထားပါသည်။ ထိုမသမာသူများသည် ၎င်းတို့၏ ထောက်လှမ်းရေး ဆော့ဖ်ဝဲများ အစစ်အမှန်ဖြစ်ကြောင်း ထင်ယောင်ထင်မှား ဖြစ်စေရန်အတွက် ထို app များကို တရားဝင်ဖြစ်သည့် Google Play Store နှင့် Apple App Store တို့တွင် တင်ထားခြင်း သို့မဟုတ် နဂိုက ကောင်းမွန်သည့် app ထဲတွင် မသမာသည့် ကုဒ်များ ထည့်သွင်းခြင်းများကို ပြုလုပ်နိုင်ပါသည်။ သို့သော် တရားဝင် App Store များတွင် မသမာသည့် ကုဒ်များ ထည့်သွင်းခြင်းများ မလုပ်နိုင်ရန် လုံခြုံရေးနှင့် စိစစ်မှု လုပ်ငန်းစဉ်များ ရှိသည့်အတွက် ထိုကဲ့သို့သော နည်းဗျူဟာများ အထမမြောက်စေခြင်းမျိုး ဖြစ်စေနိုင်ပါသည်။ App Store မှ App များကို အသုံးပြုခြင်းသည် ပိုမို လုံခြုံမှုရှိသော်လည်း ဖြစ်ရပ်မှန် နမူနာများတွင် ဖော်ပြချက်နှင့် NCSC တို့၏ App Store ခြိမ်းခြောက်ခံရမှု အစီရင်ခံစာ App Store Threat Report အရ ထိုလုံခြုံရေး နည်းလမ်းများသည်လည်း ပြည့်စုံခြင်း မရှိကြောင်းကို တွေ့ရှိထားပါသည်။

ဤအကြံပြုချက်ပါ အချက် ၄ ချက်အတိုင်း ဆောင်ရွက်ပါက သင့်အား ခြိမ်းခြောက်မှု အန္တရာယ်မှ အကာအကွယ်ပေးနိုင်ပါသည်။
အသေးစိတ် အကြံဉာဏ်များအား အန္တရာယ် လျှော့ချဖြေရှင်းခြင်း ကဏ္ဍတွင် ကြည့်ရှုပါ။

ဖြစ်ရပ်မှန် နမူနာများ

ဤဖြစ်ရပ်မှန် နမူနာ နှစ်ခုတို့သည် MOONSHINE နှင့် BADBAZAAR တို့ မည်ကဲ့သို့ အလုပ်လုပ်ကြသည်ကို ဖော်ပြထားပြီး အန္တရာယ်ဖြစ်နိုင်ခြေ ရှိသူတို့အပေါ် ဆိုင်ဘာမသမာ သူများမှ မည်ကဲ့သို့ ပစ်မှတ်ထားသနည်း ဆိုတာကို ဖော်ပြထားပါသည်။

ဖြစ်ရပ်မှန် နမူနာ တစ် - MOONSHINE

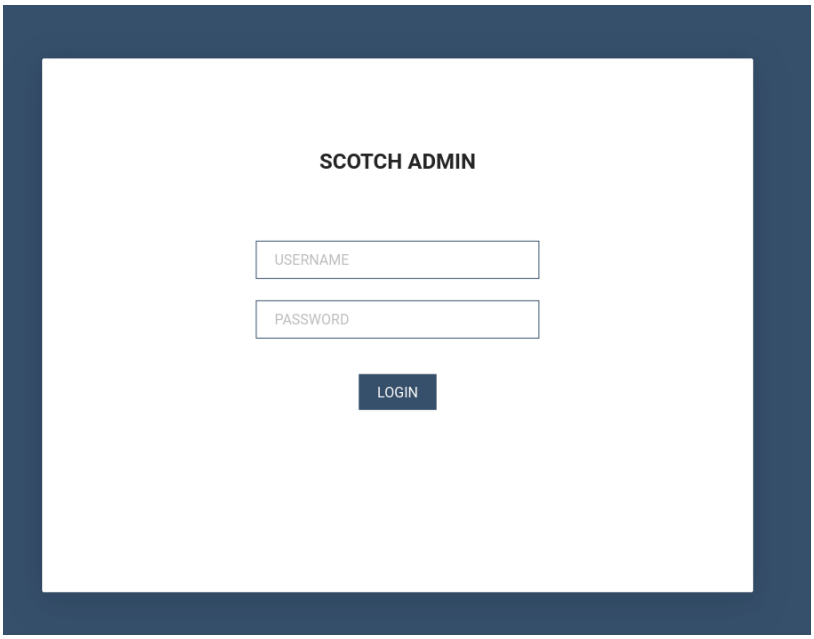
MOONSHINE သည် Android spyware တစ်ခုဖြစ်ပြီး တိဘက်အုပ်စုများကို ပစ်မှတ်ထားသည့် ထောက်လှမ်းရေး ဆော့ဖ်ဝဲဖြစ်ကြောင်း ၂၀၁၉ ခုနှစ်က Citizen Lab မှ ဖော်ထုတ်ခဲ့သည့် spyware ဖြစ်ပါသည်။ MOONSHINE သည် တရားဝင်သည့် app တစ်ခုကဲ့သို့ဟန်ဆောင်ကာ ၎င်းပစ်မှတ်ထားလိုသူများ ထို app ကို ထည့်သွင်းအောင် လုပ်ဆောင်ခြင်း ဖြစ်ပါသည်။ ထို app ကို တယ်လီဂရမ် ချန်နယ်များနှင့် WhatsApp တို့မှတစ်ဆင့် လင့်ခ်များကဲ့သို့ ဖြန့်ချီမှုဝေမှု ပြုလုပ်ခဲ့ပါသည်။

MOONSHINE တွင် ကျယ်ပြန့်သည့် အောက်ပါ ထောက်လှမ်းရေး အစွမ်းအစများ ရှိပါသည်။ ထိုအထဲတွင်

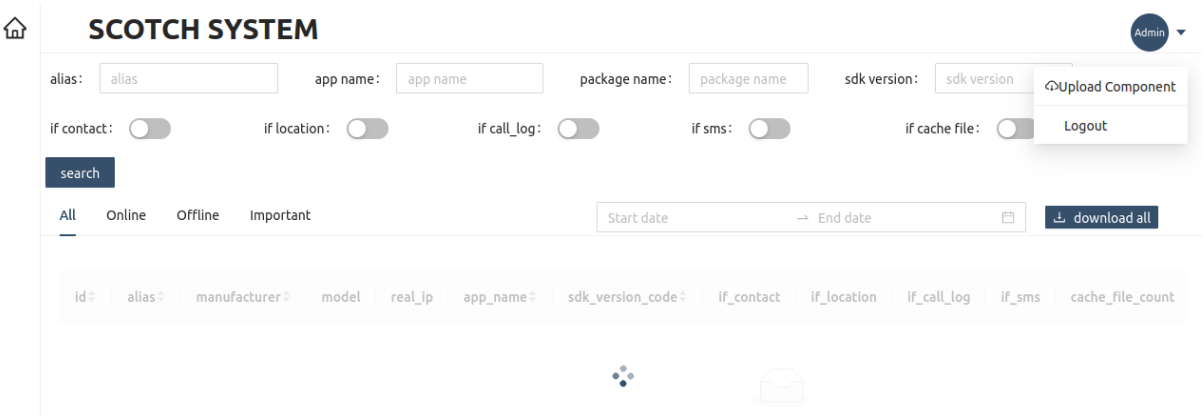
- **အချိန်နှင့် တပြေးညီ မိမိ၏ တည်နေရာကို သိနိုင်ခြင်း**
- **ဖုန်းနှင့် အသံများကို တိုက်ရိုက် ရယူခြင်း**
- **မိမိစက်ပစ္စည်းထဲ ဖိုင်များကို ဒေါင်းလုဒ် ဆွဲခြင်းများ**
- **စက်ပစ္စည်း၏ အချက်အလက်ကို ရယူခြင်းများ**
- **စက်ပစ္စည်းတွင် အသံဖိုင်များ ဖွင့်လှစ်ခြင်းများ ပါဝင်ပါသည်။**

'ئاۋازلىق قۇرئان**.apk**' ဟုခေါ်သည့် app ၏ ဘာသာပြန် အဓိပ္ပာယ်မှာ '**Audio Quran.apk**' ဖြစ်ပြီး MOONSHINE သည် ထို app ကို ဝိဂါ မွတ်ဆလင်များအား ပစ်မှတ်ထားရန်အတွက် အသုံးပြုပါသည်။ ဝိဂါဘာသာစကားဖြင့် ဖိုင်နာမည်ပေးထားသကဲ့သို့ Quran ကိုရမ် ဆိုသည့် app ကြောင့် ဝိဂါမွတ်ဆလင်များ၏ စိတ်ဝင်စားမှုကို ရရှိစေသည့် app ဖြစ်ပါသည်။

ထို app ကို ထည့်သွင်းလိုက်သည်နှင့် တပြိုင်နက် မိမိစက်ပစ္စည်းထဲမှ အချက်အလက်များကို ထိုမသမာသည့် app က စုဆောင်းရယူမှု လုပ်နိုင်ပါသည်။ ထိုအချက်အလက်များကို 'SCOTCH ADMIN' panel မှ တစ်ဆင့် ရယူနိုင်ပါသည်။



ထိုအထဲ log in ဝင်သည်နှင့် တပြိုင်နက် မသမာသူများသည် အောက်ပါ screenshot တွင် ဖော်ပြထားသည့် အရာများကို ရယူနိုင်ပါသည်။ ဤစာမျက်နှာတွင် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းများ၏ အသေးစိတ်အချက်နှင့် မည်သည့်အတိုင်းအတာအထိ မသမာသူများက တိုက်ခိုက်နိုင်သည်ကို ဖော်ပြထားပါသည်။



ထိုမသမာသည့် malware ၏ စီမံချက်တွင် အောက်ပါ ဒေတာ အချက်အလက်များကို စုဆောင်းနေကြောင်း ဖော်ပြထားပါသည်-

- **စက်ပစ္စည်းအတွင်း ဝင်ရောက်နိုင်သည့် အနေအထား**
- **SMS messages များ**
- **ဖုန်းခေါ်ဆိုမှု စာရင်းများ**
- **တည်နေရာဆိုင်ရာ အချက်အလက်များ**
- **စက်ပစ္စည်းဆိုင်ရာ အချက်အလက်များတို့ ပါဝင်ပါသည်။**

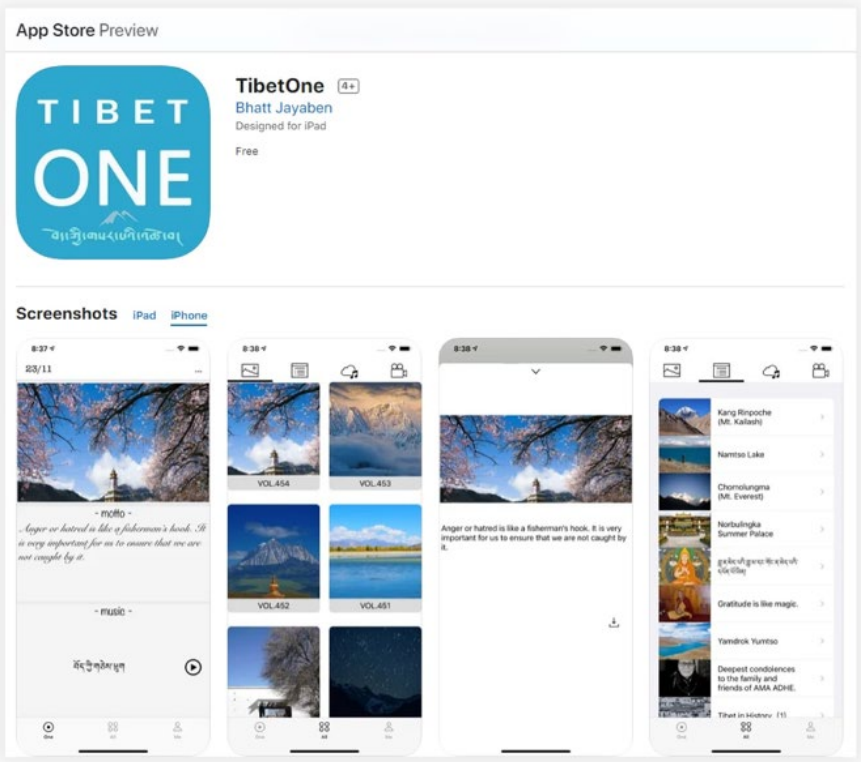
ဆိုင်ဘာအဖွဲ့ချုပ် Cyber League နှင့် ပူးပေါင်းမှုဖြင့် NCSC သည် လုပ်ငန်း၏ reporting from Trend Micro ကို တည်ထောင်ကာ'UPSEC' တွင် HTML ခေါင်းစဉ်အတွင်း MOONSHINE ၏ အမြတ်ထုတ်မှုနှင့် log in panels များ၏ ထပ်တူဖြစ်ပွားမှုကို စောင့်ကြည့်ခဲ့ပါသည်။ ပညာရပ်ဆန်သည့် အကြံပြုချက်တွင် အသေးစိတ် အပြည့်အစုံ ဖော်ပြထားပါသည်။

Intelligence Online အရ UPSEC ဆိုသည်မှာ 'Sichuan Dianke Network Security Technology Co. Ltd' ကို ဆိုလိုသည်ဟု ဖော်ပြထားပါသည်။ ထိုထုတ်ပြန်ချက်နှင့် ပတ်သက်၍ အာဏာပိုင် အေဂျင်စီများမှ အတည်မပြုနိုင်ပါ။

ဖြစ်ရပ်မှန် နမူနာ နှစ် - BADBAZAAR

BADBAZAAR ဆိုသည်မှာ iOS နှင့် Android မျိုးကွဲ မိုဘိုင်းပစ္စည်းများကို တိုက်ခိုက်နိုင်သည့် malware ဖြစ်ပြီး ဝိဂါ၊ တိဘက်နှင့် ထိုင်ဝမ်အရေး လှုပ်ရှားသူ ပုဂ္ဂိုလ်တချို့ကို ပစ်မှတ်ထားသည့် ဆော့ဖ်ဝဲ ဖြစ်ပါသည်။ ထို malware သည် ဆိုရှယ်မီဒီယာနှင့် တရားဝင် app store များမှ တစ်ဆင့် ပျံ့နှံ့လျက်ရှိသည်။

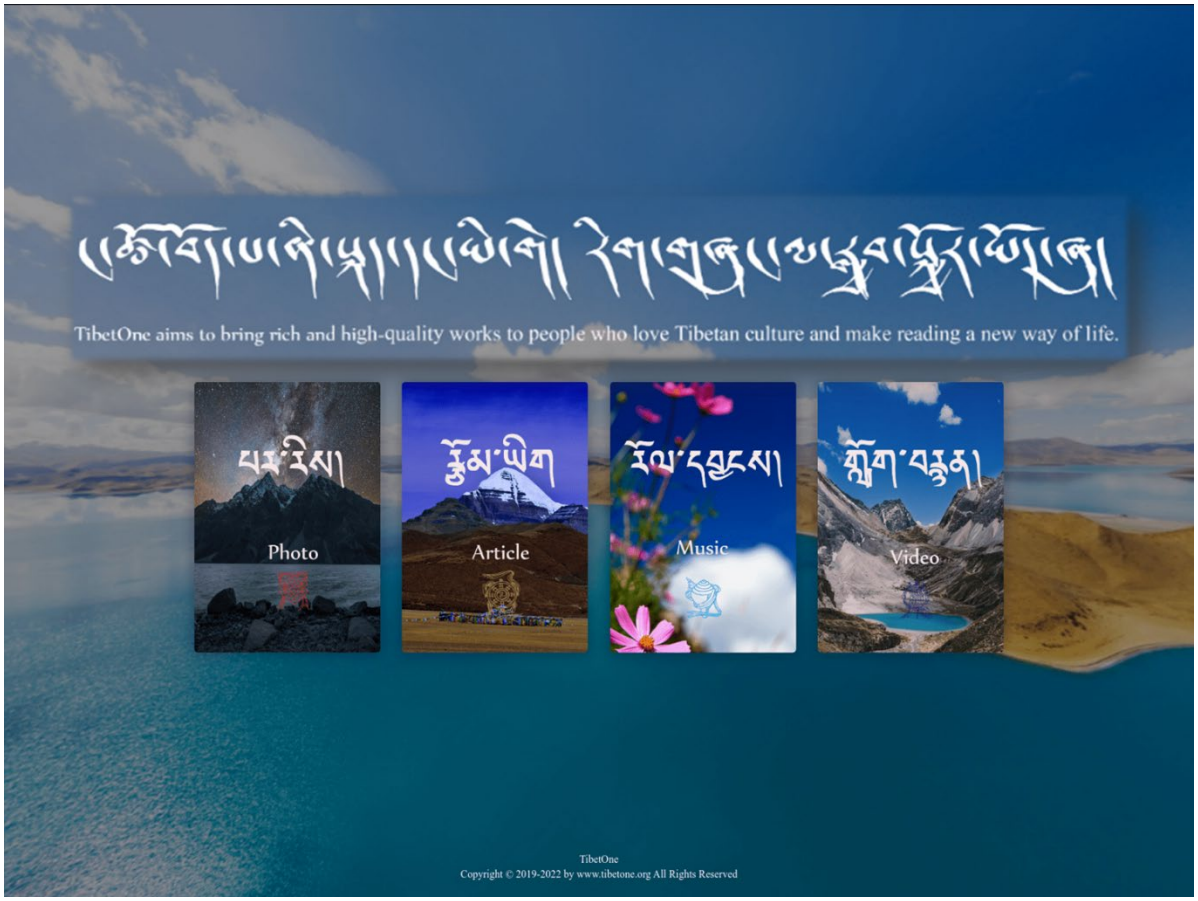
BADBAZAAR သည် '**TibetOne**' app မှတစ်ဆင့် တိဘက်လူမျိုးများကို ပစ်မှတ်ထားသည်ဟု Lookout နှင့် Volexity တို့မှ ဖော်ပြထားပါသည်။ **TibetOne** သည် မသမာသူများက တီထွင်ထားသည့် iOS app ဖြစ်ပြီး စက်ပစ္စည်းပါ အချက်အလက်များနှင့် တည်နေရာ အချက်အလက်များကို ရယူနိုင်သည့် app ဖြစ်ပါသည်။ ၂၀၂၁ ခုနှစ် ဒီဇင်ဘာလက Apple App Store တွင် တင်ထားသော်လည်း ယခုအခါတွင် တင်ထားခြင်း မရှိတော့ပေ။ ထိုမသမာသည့် App ပိုမို ပျံ့နှံ့စေရန်အတွက် မသမာသူများသည် ထို App အား တယ်လီဂရမ် ချန်နယ်တွင် '**tibetanphone**' ဆိုသည့် နာမည်ဖြင့် ကြော်ငြာခြင်းများ ပြုလုပ်ခဲ့ပါသည်။



ပုံ 1: Apple App Store တွင် တွေ့ရသည့် TibetOne app၊ ၎င်း app အား ဖယ်ရှားထားပြီး ဖြစ်ပါသည်။

ပုံ 2. တယ်လီဂရမ် ချန်နယ်တွင် မျှဝေထားသည့် TibetOne

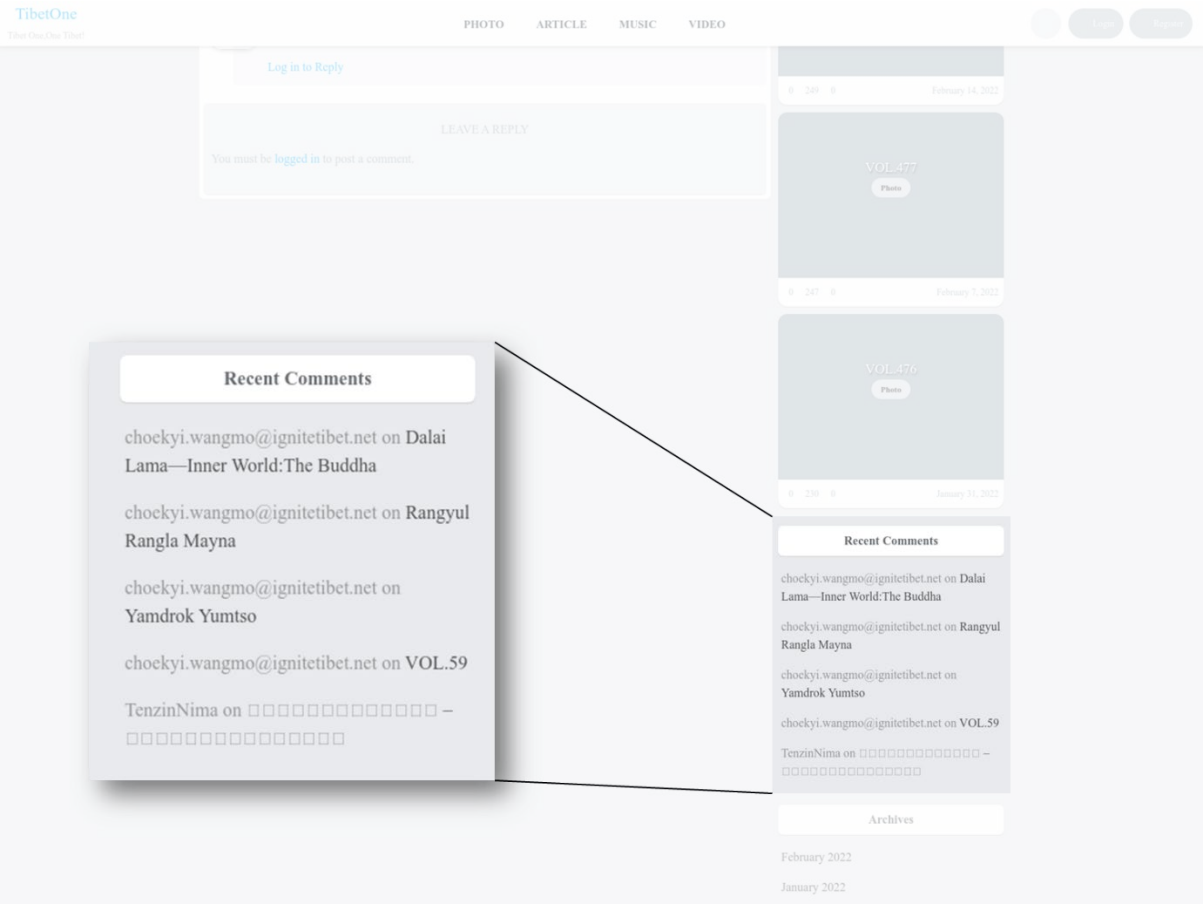
ထို app သည် တရားဝင်ဖြစ်ကြောင်း ထင်ယောင်ထင်မှား ဖြစ်စေရန်အတွက် မသမာသူများက **'tibetone[.]org'** ဟုခေါ်သည့် ဝဘ်ဆိုက်ကိုပါ တည်ထောင်ကာ "တိဘက် ရိုးရာ ယဉ်ကျေးမှုကို ချစ်မြတ်နိုးသူများအတွက် ကြွယ်ဝမှုရှိပြီး အရည်အသွေးမြင့်မားသည့် လုပ်ရပ်များကို ယူဆောင်ခြင်းနှင့် စာဖတ်ခြင်းဖြင့် ဘဝသစ်ကို စတင်ခြင်း" ဆိုသည့် စကားလုံးမျိုးဖြင့် ဝဘ်ဆိုက်တွင် ဖော်ပြထားပါသည်။



ပုံ 3. 'tibetone[.]org' ၏ ပင်မ စာမျက်နှာ

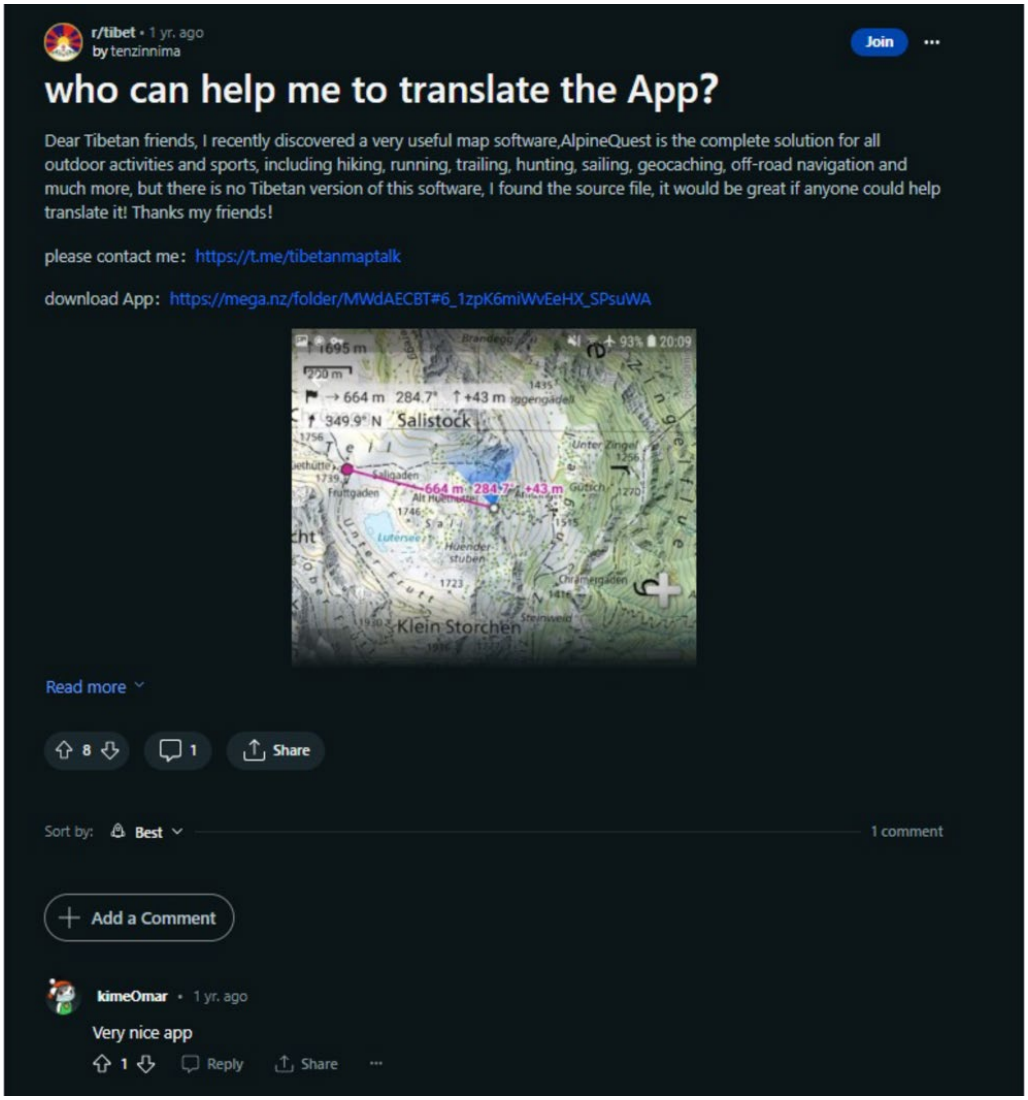
ဆီလျော်သော အပိုင်းကို ရှင်းလင်းစွာ ဖော်ပြရန်အတွက် ဤပုံအား တည်းဖြတ်မှု လုပ်ထားပါသည်။

ထိုဝဘ်ဆိုက်တွင် ဆောင်းပါးများ ပါရှိပြီး စာဖတ်သူများမှ မှတ်ချက်များ ရေးသားနိုင်ရန်အတွက်လည်း လုပ်ဆောင်ပေးထားပါသည်။ **'choekyi.wangmo@ignitetibet.net'** ဆိုသည့် အီးမေးလ် လိပ်စာဖြင့် မှတ်ချက်ကို ကြည့်လိုက်ပါက မသမာသူများက ထိန်းချုပ်ထားသည့် အီးမေးလ်ဟု ယူဆရကာ တိဘက်၏ လူ့အခွင့်အရေးနှင့် ဒီမိုကရေစီအကြောင်း ရေးသားသည့် တိဘက်အရေးလှုပ်ရှားသူ **'Choekyi Wangmo'** ကဲ့သို့ ဟန်ဆောင်ထားဟန် ရှိပါသည်။ ထိုကဲ့သို့ လုပ်ရပ်ကို ကြည့်ခြင်းအားဖြင့် ဤ app သည် တရားဝင် app ဖြစ်ကာ တိဘက်လူမျိုးတို့၏ လွတ်လပ်ရေး အတွက် အရေးဆိုပေးသည့် app အဖြစ် ထင်ယောင်ထင်မှားဖြစ်အောင် လုပ်ဆောင်သည့် အခြားကြိုးပမ်းချက်တစ်ခု ဖြစ်နိုင်ပါသည်။



ပုံ 4: 'tibetone[.]org' စာမျက်နှာတွင် မသမာသူများ ထိန်းချုပ်ထားသည့် မှတ်ချက်များကို ဖော်ပြထားပါသည် - ဆီလျော်သော အပိုင်းကို ရှင်းလင်းစွာ ဖော်ပြရန်အတွက် ဤ ပုံအား တည်းဖြတ်မှု လုပ်ထားပါသည်။

ထိုဝဘ်ဆိုက်တွင် မှတ်ချက်ပြုသူ နောက်တစ်ဦးမှာ '**TenzinNima**' ဖြစ်ပါသည်။ Volexity ၏ ဖော်ပြချက်အရ ထိုနာမည်ဖြင့် Reddit တွင် တယ်လီဂရမ် ချန်နယ်ဖြစ်သည့် '**Tibetanmaptalk**' ကို ကြော်ငြာထားသည့်အကြောင်း ဖော်ပြထားပါသည်။ ထိုကြော်ငြာထဲတွင် မသမာသည့် လမ်းခရီးညွှန်းသည့် app **AlpineQuest**' ၏ နမူနာကို ပြသထားပြီး Android စက်ပစ္စည်းများအတွက် ရယူနိုင်ကြောင်း ဖော်ပြထားပါသည်။ ဒေါင်းလုဒ်လုပ်သည့်အခါ ဖိုင်မျှဝေခြင်း ဝန်ဆောင်မှုပေးသည့် Mega ခေါ် တတိယပါတီတစ်ခု၏ လင့်ခ်ကို ဖော်ပြထားပါသည်။



ပုံ 5: မသမာသူများ ထိန်းချုပ်ထားကြောင်း ယူဆရသည့် အကောင့်မှ Reddit တွင် မသမာသည့် app ကို ကြော်ငြာထားပါသည်။

Volexity ၏ စောင့်ကြည့်မှုအရ '**KimeOmar**' ဆိုသည့် နာမည်ဖြင့် မှတ်ချက်ပြုသောအကောင့်သည် အခြား Reddit အစိတ်အပိုင်းဖြစ်သည့် ဖိုရမ်များတွင် မသမာသည့် app များကို မျှဝေခြင်းများ ပြုလုပ်ထားသည်ကို တွေ့ရှိရပါသည်။ ထိုလုပ်ရပ်များကို ကြည့်ခြင်းအားဖြင့် မသမာသူများသည် ဆိုရှယ်မီဒီယာ ပရိုဖိုင်း အမျိုးမျိုးကို အသုံးပြုကာ ၎င်းတို့၏ ရေးသားမျှဝေမှုများအား ဘောင်ဝင်အောင် ကြိုးစားလုပ်ဆောင်နေကြောင်း သိသာစေနိုင်ပါသည်။

လေ့လာဆန်းစစ်ချက်

BADBAZAAR နှင့် MOONSHINE တို့သည် လူစိတ်ဇေဒနှင့် ဆက်သွယ်မှုကို အသုံးချကာ မသမာသည့်နည်းဖြင့် အချက်အလက်ရယူခြင်း ဆိုရှယ်အင်ဂျင်နီယာနည်းလမ်းကို အသုံးပြုကာ ဝါဂါလူမျိုး၊ တိဘက်လူမျိုးနှင့် ထိုင်ဝမ်လူမျိုးတို့ကို ပစ်မှတ်ထားလေ့ရှိပြီး အဓိကအားဖြင့်

- ဝါဂါလူမှုအသိုင်းအဝိုင်းများ စိတ်ဝင်စားနိုင်သည့် ဝါဂါဘာသာဖြင့် ပြုလုပ်ထားသည့် ကိုရမ် Quran app ကို တီထွင်ကာ တရားဝင် ဆော့ဖ်ဝဲများကဲ့သို့ ဟန်ဆောင်ပြီး မသမာမှုများ လုပ်ဆောင်သည့် trojans app များဖြင့် ပစ်မှတ်ထားခြင်းများ
- ထိုမသမာမှုများ လုပ်ဆောင်သည့် trojans app များကို တရားဝင် app store များပေါ်တွင် ထားရှိကာ စစ်မှန်သည့် app ဖြစ်ကြောင်း ထင်ယောင်ထင်မှားမှု ဖြစ်အောင် လုပ်ဆောင်ခြင်းနှင့် group chat များတွင် ၎င်းတို့ ပစ်မှတ်ထားသည့် လူမှုအသိုင်းအဝိုင်းတို့၏ ယုံကြည်မှုကို အလွဲသုံးစားလုပ်ခြင်း

BADBAZAAR နှင့် MOONSHINE တို့သည် တရုတ်အစိုးရအတွက် တန်ဖိုးရှိသည့် အချက်အလက်များကို စုဆောင်းပေးခြင်းမျိုးများ ပြုလုပ်လျက်ရှိသည်။ BADBAZAAR နှင့် MOONSHINE တို့သည် ဝါဂါလူမျိုး၊ တိဘက်လူမျိုးနှင့် ထိုင်ဝမ်မှ တသီးပုဂ္ဂလများအား ပစ်မှတ်ထားသည်ကို သိရပြီး အခြားသော မသမာသည့် malware များသည် တရုတ်နိုင်ငံအတွင်းမှ အခြားသော လူနည်းစုများကိုလည်း ပစ်မှတ်ထားကြောင်း သိရပါသည်။ တရုတ်နိုင်ငံ၏ တည်ငြိမ်မှုအားခြိမ်းခြောက်နိုင်သည်ဟု ယူဆရသော တရုတ်နိုင်ငံပြည်တွင်းနှင့် ပြည်ပနိုင်ငံမှာ နေထိုင်သည့် အတူတကွ လက်မှတ်ရေးထိုးထားသည့် နိုင်ငံသားများသည် BADBAZAAR နှင့် MOONSHINE ကဲ့သို့သော မိုဘိုင်း malware တို့၏ တိုက်ခိုက်မှုအန္တရာယ်ကို ခံရရန် သေချာလုနီးပါးဖြစ်သည်။ ထိုလူများ၏ တည်နေရာ၊ အသံဖိုင်၊ ဓာတ်ပုံစသည့် အချက်အလက်များကို ရရှိနိုင်သည့်အတွက် အနာဂတ်တွင် ထိုပစ်မှတ်ထား ခံရသူများ၏ လှုပ်ရှားမှု အချက်အလက်များအား အချိန်နှင့် တပြေးညီ ထောက်လှမ်းခြင်းများနှင့် နှောင့်ယှက်ခြင်းများ ပြုလုပ်နိုင်ရန် အခွင့်အလမ်း ရစေနိုင်ပါသည်။

မိုဘိုင်း app အသုံးပြုသူများအနေဖြင့် ခြိမ်းခြောက်မှုကို လျော့ချနိုင်မည့် နည်းလမ်းများ

အာဏာပိုင် အေဂျင်စီများအနေဖြင့် အောက်ပါ လုံခြုံရေး နည်းလမ်းများကို အသုံးပြုကာ ဖြစ်ရပ်မှန်ပါ နမူနာများတွင် ဖော်ပြခဲ့သည့် တိုက်ခိုက်ခံရမှုများ မဖြစ်အောင် ကာကွယ်လုပ်ဆောင်ထားရန် တိုက်တွန်းလိုပါသည်။ ဤအကြံပြုချက်များသည် NCSC ၏ လမ်းညွှန်ချက်များထဲတွင် အကောင်းဆုံး အကြံပြုချက်များ ဖြစ်ပါသည်။ "ထပ်မံ ဖတ်ရှုလေ့လာရန်" ကဏ္ဍကို သွားရောက်ကာ ဩစတြေးလျနှင့် အမေရိကမှ ဖတ်ရှုသူများအတွက် အကောင်းဆုံး လမ်းညွှန်ချက်များကို ဖော်ပြထားသည့် လင့်ခ်များတွင် လေ့လာနိုင်ပါသည်။

သင်အသုံးပြုသည့် စက်ပစ္စည်းအား လုံခြုံစွာ လုပ်ဆောင်ထားခြင်း

- App **များကို ဒေါင်းလုဒ်လုပ်မည်ဆိုပါက တရားဝင် app stores များဖြစ်သည့် Google's Play Store သို့မဟုတ် Apple's App Store ကဲ့သို့သော app store များကို အသုံးပြုပါ။** Google's Play Store နှင့် Apple's App Store တို့သည် ၎င်းတို့ပေါ်တွင် app များ တင်ခွင့် မပေးခင်တွင် ထို app များတွင် ဗိုင်းရပ်စ်ရှိမရှိ အရင်ဆုံး စိစစ်သည့်အတွက် သင်ဒေါင်းလုဒ်ရယူသည့် app သည် လုံခြုံဘေးကင်းသည့်အရာ ဖြစ်သည် ဟူသည့် ခံစားချက်မျိုး ရရှိစေနိုင်ပါသည်။ ယုံကြည်စိတ်ချရသည့် app store များပေါ်တွင် ရနိုင်သည့် app များကို ဒေါင်းလုဒ် လုပ်သည့်တိုင် အန္တရာယ် ရှိနိုင်သေးသော်လည်း အခြားသော နေရာမှ ဒေါင်းလုဒ် ရယူလျှင် မည်သည့်ကာကွယ်မှုဆိုင်ရာ တစုံတရာမှ ရရှိမည် မဟုတ်ပါ။ NCSC တွင် App store များတွင် ရှိသည့် ခြိမ်းခြောက်မှုဆိုင်ရာ အစီရင်ခံစာ ရှိပါသည် - https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **သင်အသုံးပြုသည့် စက်ပစ္စည်းနှင့် app များကို ပုံမှန် update လုပ်ပါ** သင်၏ စက်ပစ္စည်းအတွက် ဆော့ဖ်ဝဲများနှင့် app များအတွက် update များ ထည့်လို့ရသည်နှင့်

တပြိုင်တည်း ထည့်သွင်းပါ။ Update လုပ်ဖို့ လိုသည့်အခါ မေ့သွားမည်ကို စိုးရိမ်နေစရာ မလိုအောင် သင့်ပစ္စည်း၏ setting တွင် အလိုအလျောက် update လုပ်ပေးသည့် 'automatic updates' ကို ဖွင့်ထားပါ။ NCSS ၏ အွန်လိုင်းတွင် လုံခြုံဘေးကင်းစွာ နေထိုင်ခြင်း လမ်းညွှန်ချက်ကို ကြည့်ပြီး ဗိုင်းရပ်စ်များနှင့် တခြားသော malware တို့ရန်မှ ကာကွယ်ထားနိုင်ပါသည်။ Update လုပ်သည့်အခါတွင် ပိုပြီး ခေတ်မီတိုးတက်သည့် အင်္ဂါရုပ်များကို ထည့်သွင်းပါဝင်ပါသည် - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- သင်၏ ပစ္စည်း ကန့်သတ်ချက်များကြံုရသည့်အခါ ကန့်သတ်ချက်များကို ဖယ်ရှားခြင်း **'Jailbreak'** သို့မဟုတ် မူရင်းကို ဖယ်ရှားခြင်း **'root'** များ **မလုပ်ပါနှင့်**၊ [3 ထိုလုပ်ရပ်များသည် သင်၏ စက်ပစ္စည်းအတွက် ထားရှိပေးထားသည့် လုံခြုံရေးကို အားနည်းသွားစေနိုင်ပါသည်။ ထိုကဲ့သို့ လုပ်ရပ်သည် စက်ပစ္စည်းကို ခုခံနိုင်စွမ်း မရှိအောင် လုပ်ရာကြပြီး တိုက်ခိုက်ခံရမှု အလားအလာပိုများစေပါသည်။ . NCSC လမ်းညွှန်ချက်ကို ကြည့်ပါ - https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

သင်၏ App များကို စီမံခြင်း

- **သင်၏ App များနှင့် ခွင့်ပြုချက်ပေးထားသည်များကို ပြန်လည် ဆန်းစစ်ပါ** အကယ်၍ သင့်အနေဖြင့် app တစ်ခုကို မလိုအပ်တော့ပါက ဖျက်ပစ်လိုက်ပါ။ ဖြစ်နိုင်ပါက အချက်အလက်များ ရယူခြင်းကို ကန့်သတ်ရန်အတွက် app ထံမှ တောင်းဆိုချက်ကို ကန့်သတ်ခြင်းများ ပြုလုပ်ပါ၊ အကြောင်းရင်းမှာ မသမာသည့် app များသည် ကင်မရာနှင့် မိုက်ခရိုဖုန်း တို့ကဲ့သို့ ကာကွယ်ထားသည့် ဖိုင်များ သို့မဟုတ် အရန်အချက်အလက်များထဲသို့ ဝင်ရောက်နိုင်ရန် ကြိုးစားလေ့ရှိသည့်အတွက် ဖြစ်ပါသည်။

- Apple အသုံးပြုသူများအနေဖြင့် app အား မည်သည့် ခွင့်ပြုချက်များ ပေးထားသည်ကို သိနိုင်ရန် ဘယ်လို လုပ်ဆောင်နိုင်သနည်း ဆိုသည်ကို လေ့လာနိုင်ပါသည်။ https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
- Android အသုံးပြုသူများအနေဖြင့် app အား မည်သည့် ခွင့်ပြုချက်များ ပေးထားသည်ကို သိနိုင်ရန် ဘယ်လို လုပ်ဆောင်နိုင်သနည်း ဆိုသည်ကို လေ့လာနိုင်ပါသည်။ https://support.google.com/android/answer/9431959?hl=en-GB

› **မသိသော app များကို Google ထံ အလိုအလျောက် အသိပေးပို့ဆောင်ပါ။** အကယ်၍ သင်သည် Android အသုံးပြုသူဖြစ်ပြီး Google Play Store ထဲမှ မဟုတ်သည့် App တစ်ခုကို
ဒေါင်းလုဒ် လုပ်မိပါက Google ထံ ပို့ဆောင်ပြီး Play Store ၏ app settings မှ 'Play Protect' ကို သွားရောက်ကာ Ïmprove harmful app detection
ဖျက်လိုဖျက်ဆီးပြုနိုင်သည့် App ကို ပိုမိုသိအောင် လုပ်ခြင်း' ဆိုသည့် အရာကို ဖွင့်ထားနိုင်ပါသည်။ ထိုကဲ့သို့ လုပ်ထားလျှင် ထို app တွင် မသမာမှုများ ရှိမရှိ ဆန်းစစ်မှု လုပ်ပေးကာ အသုံးပြုသူများအား ကာကွယ်ပေးနိုင်ပါသည်။ မည်ကဲ့သို့ ပြုလုပ်နိုင်သနည်း ဆိုသည့် အကြောင်းအရာကို ဖတ်ရှုပါ။
https://support.google.com/android/answer/2812853?hl=en-GB

ဆိုင်ဘာ ဝန်ဆောင်မှုများကို အသုံးပြုပါ

› **လင့်ခ် တစ်ခုအား မနှိပ်ခင်တွင် လုံခြုံသည့် လင့်ခ် ဟုတ်မဟုတ် သိရအောင် URL reputation services ကို အသုံးပြုပါ။** အီးမေးလ်၊ မက်ဆေ့ချ်နှင့် အခြားနေရာမှ ရရှိသော လင့်ခ်သည် လုံခြုံဘေးကင်းခြင်း ရှိမရှိ သိလိုပါက Google Transparency Report သို့မဟုတ် Virus Total. တို့ကို အသုံးပြုပြီး ဆန်းစစ်မှု လုပ်နိုင်ပါသည်။ မသမာသည့်ဖိုင်ဟု သံသယ ရှိပါက ထိုဖိုင်ကို malware များတွင် ဗိုင်းရပ်စ်ပါမပါ ဆန်းစစ်ပေးသည့် Virus Total ကဲ့သို့သော စိစစ်ရေးဝန်ဆောင်မှုကို အသုံးပြုနိုင်ပါသည်။ ထိုကဲ့သို့ စိစစ်မှုတွင်လည်း လုံခြုံဘေးကင်းသည်ဟု မှားယွင်းစာဖော်ပြသည့် false negative အဖြေများလည်း ထွက်နိုင်သည်ကို သတိပြုပါ။

- **Google Advanced Protection programme တွင် စာရင်းသွင်းပါ။**
  ဤဝန်ဆောင်မှုသည် Google ၏ ဝန်ဆောင်မှုများ (Gmail, Play Store စသည်တို့) ကို အသုံးပြုသူများ ပစ်မှတ်ထားခံရခြင်းမှ ကာကွယ်နိုင်ရန်အတွက် အခမဲ့ပေးသည့် ဝန်ဆောင်မှု ဖြစ်ပါသည်။ ဤဝန်ဆောင်မှုသည် Google ဝန်ဆောင်မှုများအား အသုံးပြုသည့်အခါတွင် မြင့်မားသည့် လုံခြုံရေးများ ထားရှိပေးပါသည်။
  https://landing.google.com/advancedprotection/

- **ရန်ုင်သည့်အခါတွင် ပိုမို ကြံခိုင်နိုင်သော ဝန်ဆောင်မှုအတွက် စာရင်းသွင်းထားပါ။** ဥပမာ - ယူကေနိုင်ငံမှ ပစ်မှတ်ထားခံရနိုင်ခြေများသူများသည် ၎င်းတို့၏ ဆိုင်ဘာလုံခြုံရေးအတွက် ပိုသာသော လုံခြုံရေးနှင့် ကာကွယ်ရေး ဝန်ဆောင်မှုကို ရရှိနိုင်ပါသည်။ မည်သည့် အနေအထားတွင် ထိုဝန်ဆောင်မှု ရရှိနိုင်သနည်းဆိုတာကို လေ့လာပါ။
  https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

ခြိမ်းခြောက်မှုများကို တိုင်တန်းပါ။

- **အကောင့်တုများကို ဖော်ထုတ်ပြီး တိုင်တန်းမှု လုပ်ပါ။** မသမာသည့် ဆိုင်ဘာ ရာဇဝတ်သားများသည် အကောင့်တုများ အသုံးပြုခြင်း သို့မဟုတ် အကောင့်စစ်များကို hack လုပ်ကာ ၎င်းတို့၏ ရည်ရွယ်ချက်များကို အကောင်အထည်ဖော်နိုင်ပါသည်။ အကယ်၍ သင့်အနေဖြင့် အကောင့်တုဟု သံသယဖြစ်ပါက သို့မဟုတ် အကောင့် hack ခံရပါက မိမိအသုံးပြုနေသည့် ပလက်ဖောင်းဆီ တိုင်တန်းမှုလုပ်ပြီး ဘလော့ခ်လိုက်ပါ။ ဝန်ဆောင်မှုပေးသည့် အဖွဲ့များတွင် အကောင့်စစ် ဟုတ်မဟုတ် စိစစ်နိုင်သည့် နည်းလမ်းများရှိပြီး Instagram နှင့် Facebook အကောင့်များအတွက် အကောင့်စစ်ဖြစ်ကြောင်း ထောက်ခံပေးသည့် 'verified badges' ဝန်ဆောင်မှုလည်း ရှိပါသည်။ ထိုကဲ့သို့ လုပ်ရပ်များက အကောင့်စစ် ဟုတ်မဟုတ်ကို သိသာစေနိုင်ပါသည်။ NCSC တွင် ဆိုရှယ်မီဒီယာကို လုံခြုံဘေးကင်းစွာ အသုံးပြုခြင်းဆိုင်ရာ လမ်းညွှန်ချက်ရှိပြီး ထိုအထဲတွင် အကောင့် စစ်မစစ် မည်ကဲ့သို့ ဆန်းစစ်နိုင်သနည်းနှင့် အကောင့် hack ခံရပါက မည်ကဲ့သို့

တိုင်တန်းနိုင်သနည်း စသည့် လမ်းညွှန်ချက်များ ရှိပါသည်။
https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **အန္တရာယ်ရှိသည့် emails, SMS နှင့် လင့်ခ်များကို အသုံးပြုကာ အစစ်အမှန်ကဲ့သို့ လှည့်ဖြားခြင်း။** NCSC အနေဖြင့် သံသယဖြစ်ဖွယ်ရာ အီးမေးလ်နှင့် ဝဘ်ဆိုက်များအပေါ် စုံစမ်းစစ်ဆေးမှု လုပ်နိုင်ပါသည်။ အကယ်၍ သင့်အနေဖြင့် ဝဘ်ဆိုက်၊ အီးမေးလ် သို့မဟုတ် မက်ဆေ့ချ်တစ်ခုခုကို သံသယဖြစ်ပါက တိုင်တန်းမှု လုပ်နိုင်ပါသည်။
https://www.ncsc.gov.uk/collection/phishing-scams

NCSC ၏ ခက်ဆစ်များ

Android

Google ၏ မိုဘိုင်း လည်ပတ်မှု စနစ်ဖြစ်ပြီး စမတ်ဖုန်းနှင့် တက်ဘလက် ထုတ်လုပ်သူအချို့ အသုံးပြုသည့် စနစ် ဖြစ်ပါသည်။

App

Aapplication သို့မဟုတ် အတိုကောက် app ဟု ခေါ်ဆိုသည့် အရာသည် ဆော့ဖ်ဝဲဖြစ်ပြီး ၎င်းတို့ကို စက်ပစ္စည်း ကောင်းမွန်စွာ ပိုအလုပ်လုပ်ရန် သို့မဟုတ် အချက်အလက်များ ပိုမိုစုံလင်ရန်အတွက် ထုတ်လုပ်သူများမှ စက်ပစ္စည်းထဲ ကြိုတင်ထည့်သွင်းခြင်း သို့မဟုတ် နောက်မှ ထည့်သွင်းခြင်း လုပ်နိုင်ပါသည်။

ဆိုင်ဘာ လုံခြုံရေး

စက်ပစ္စည်းများ၊ ဝန်ဆောင်မှုများနှင့် ကွန်ရက်များနှင့် ၎င်းတို့၏ အချက်အလက်များကို တရားမဝင် ရယူခြင်း၊ ခိုးယူခြင်း သို့မဟုတ် ပျက်စီးခြင်းတို့မှ ကာကွယ်ပေးသည့် အရာဖြစ်သည်။

စက်ပစ္စည်း

ကွန်ပြူတာ အခြေခံထားသည့် hardware ဖြစ်ပြီး လက်ဆုပ်လက်ကိုင် တည်ရှိသည့် စက်ပစ္စည်းဖြစ်ပြီး ဥပမာ အချို့မှာ desktop ကွန်ပြူတာ၊ စမတ်ဖုန်း သို့မဟုတ် တက်ဘလက်တို့ ပါဝင်သည်။

iOS

Apple ၏ မိုဘိုင်းစနစ်ဖြစ်ကာ ၎င်း၏ မိုဘိုင်းပစ္စည်းများအတွက် အသုံးပြုသည့်စနစ် ဖြစ်ပါသည်။

Malware

“မသမာသည့် ဆော့ဖ်ဝဲ” မှ ဆင်းသက်လာသည့် စကားလုံးဖြစ်ပြီး ကွန်ပြူတာစနစ်နှင့် ကွန်ပြူတာကွန်ရက် သို့မဟုတ် စက်ပစ္စည်းမှန်သမျှကို ဖျက်လိုဖျက်ဆီးပြုလိုသည့် ဆော့ဖ်ဝဲမှန်သမျှသည် malware ဖြစ်ပါသည်။ ထိုအထဲတွင် ဗိုင်းရပ်စ်များ၊ ငွေညှစ်သည့် ransomware နှင့် trojans တို့ ပါဝင်ပါသည်။

Operating system လည်ပတ်ရေး စနစ်

ကွန်ပြူတာများ၊ တဘ်ဘလက်နှင့် စမတ်ဖုန်းစသည့် applications နှင့် hardware များ လည်ပတ်ရန်အတွက် လိုအပ်သည့် အခြေခံ ဆော့ဖ်ဝဲ ဖြစ်ပါသည်။

- **Phishing**

အီးမေးလ် သို့မဟုတ် မက်ဆေ့ချ်များပို့ကာ ထိုအထဲတွင် မသမာသည့် ဆော့ဖ်ဝဲများ ထည့်ထားသည့် လင့်ခ်များ သို့မဟုတ် ဝဘ်ဆိုက်လိပ်စာများ ပါဝင်ပြီး ၎င်းတို့ကို ဖွင့်သည့်အခါ အသုံးပြုသူ၏ ထိလွယ်ရှလွယ်သော အချက်များ (ဥပမာ password) သို့မဟုတ် ငွေလွှဲပေးရန် တောင်းခံနိုင်ပါသည်။

- **ထောက်လှမ်းရေး ဆော့ဖ်ဝဲ Spyware**

မသမာသည့် ဆော့ဖ်ဝဲ တစ်မျိုးဖြစ်ပြီး အသုံးပြုသူဖက်မှ ခွင့်ပြုချက်မရှိသော်လည်း ထိုသူ၏ စက်ပစ္စည်းထဲသို့ မသမာသည့် ဆော့ဖ်ဝဲ ထည့်သွင်းကာ အချက်အလက်များ ရယူပြီး တခြားလူများကို ပို့ပေးခြင်းများ လုပ်သည့် ဆော့ဖ်ဝဲ ဖြစ်သည်။

- **ဆိုရှယ် မီဒီယာ Social media**

ဝဘ်ဆိုက်နှင့် Facebook၊ X နှင့် Instagram ကဲ့သို့သော app များကို ဆိုလိုပြီး အသုံးပြုသူများအနေဖြင့် (စာ၊ ဓာတ်ပုံ နှင့် ဗီဒီယို) စသည့် အရာများကို အပြန်အလှန် ကြည့်ရှုပို့ဆောင်နိုင်သည့် အရာ ဖြစ်ပါသည်။

- **စမတ်ဖုန်း Smartphone**

ခေတ်မီသည့် မိုဘိုင်းဖုန်းများဖြစ်ပြီး Android နှင့် iOS လည်ပတ်ရေး စနစ်များ အသုံးပြုကာ အရာမျိုးစုံကို ပြုလုပ်နိုင်သည့် ဖုန်းများ ဖြစ်ပါသည်။

- **Trojan**

မသမာသည့် ဆော့ဖ်ဝဲ တစ်မျိုးဖြစ်ပြီး ၎င်းပစ်မှတ်ထားလိုသည့် စက်ပစ္စည်းထဲ ခွင့်ပြုချက်မပါဘဲ ဝင်ရောက်နိုင်ရန်အတွက် ကောင်းမွန် တရားဝင်သော ဆော့ဖ်ဝဲ တစ်ခုကဲ့သို့ ဟန်ဆောင်ကာ လှည့်စားမှုလုပ်ထားသည့် မသမာသည့် ဆော့ဖ်ဝဲ တစ်မျိုးဖြစ်သည်။

- **URL**

Uniform Resource Locator. ဝဘ်ဆိုက် လိပ်စာများ သို့မဟုတ် ဒိုမိန်းနာမည်များဖြစ်သည် (ဥပမာ www.bbc.co.uk)

- **ဗိုင်းရပ်စ် Virus**

မသမာသည့် ဆော့ဖ်ဝဲ တစ်မျိုးဖြစ်ပြီး တရားဝင် ဆော့ဖ်ဝဲပရိုဂမ်များ ထိခိုက်ပျက်စီးသွားစေရန်အတွက် တီထွင် ဝင်ရောက်ကာ ထိုကဲ့သို့ ဗိုင်းရပ်စ်ကူးစက်ခံရသည့် ပရိုဂမ်များ လည်ပတ်မှုလုပ်သည့်အခါ ပျံ့နှံ့သွားသည့် မသမာသည့် ဆော့ဖ်ဝဲ အမျိုးအစား ဖြစ်ပါသည်။

ထပ်မံဖတ်ရှု လေ့လာရန်အကြံပြုစာရင်း

ဩစတြေးလျ ဆိုင်ဘာလုံခြုံရေးစင်တာ၏ လမ်းညွှန်ချက်များ

- ဆိုင်ဘာရာဇာဝတ်မှု၊ အခင်းဖြစ်ပွားမှုနှင့် အားနည်းချက်များအား တိုင်တန်းပါ
- သင်၏ စက်ပစ္စည်း လုံခြုံရန် မည်ကဲ့သို့ လုပ်နိုင်သနည်း
- သင်၏ မိုဘိုင်းဖုန်းအား လုံခြုံအောင် လုပ်ဆောင်ခြင်း
- Phishing
- Scams လိမ်လည်ခြင်း
- သင်၏ ဆိုရှယ်မီဒီယာ အကောင့်ကို လုံခြုံအောင် လုပ်ဆောင်ခြင်း
- ဆိုရှယ်မီဒီယာနှင့် မက်ဆေ့ချ် app များ လုံခြုံဘေးကင်းရန်အတွက် အကြံပြုချက်များ

UK ၏ NCSC နှင့် NPSA တို့၏ လမ်းညွှန်ချက်များ

- ဒီမိုကရေစီကို ကာကွယ်ခြင်း
- ဆိုရှယ်မီဒီယာ - လုံခြုံဘေးကင်းစွာ မည်ကဲ့သို့ အသုံးပြုနိုင်သနည်း
- မိုဘိုင်းအပါအဝင် အဖွဲ့အစည်းများ၏ စက်ပစ္စည်းများ လုံခြုံရေးအတွက် လမ်းညွှန်ချက်များ
- Application store များပေါ်မှ ခြိမ်းခြောက်မှုဆိုင်ရာ အစီရင်ခံစာ 3]
- ပစ်မှတ်ထားခံရနိုင်ခြေများသော သူများအတွက် ဘေးကင်းရေးနှင့် လုံခြုံရေးများ Personal safety and security for high-risk individuals

အမေရိကန် NSA မှ လမ်းညွှန်ချက်များ

- မိုဘိုင်းပစ္စည်းများ လိုက်နာရန် အကောင်းဆုံး နည်းလမ်းများ

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤအကြံပြုချက်ပါ အချက်အလက်များသည် ထုတ်ဝေသည့် အချိန်အထိ အတည်ပြုပြီးကြောင်း အသိပေးလိုပါသည်။

ဤအစီရင်ခံစာသည် အာဏာပိုင် အေဂျင်စီနှင့် ဤကဏ္ဍတို့မှ ရရှိသည့် အချက်အလက် ရင်းမြစ်များအပေါ် အခြေခံကာ ထုတ်ဝေထားခြင်း ဖြစ်ပါသည်။ တွေ့ရှိချက်များနှင့် အကြံပြုချက်များ အားလုံးကြောင့်

အန္တရာယ် လုံးဝ မရှိတော့ကြောင်း မဆိုလိုသကဲ့သို့ ဤအကြံပြုချက်များအားလုံး လိုက်နာလုပ်ဆောင်ပါက အန္တရာယ်အားလုံးကို ဖယ်ရှားနိုင်သည်ဟုလည်း မဆိုလိုပါ။ အချက်အလက်ဆိုင်ရာ အန္တရာယ်များ၏ ပိုင်ဆိုင်မှုသည် သင့်တော်သက်ဆိုင်ရာ စနစ်နှင့် သက်ဆိုင်ရာ တာဝန်ခံသူနှင့်သာ သက်ဆိုင်ပါသည်။

ယူကေနိုင်ငံတွင် ဤအချက်အလက်များသည် ၂၀၀၀ ခုနှစ် သတင်းအချက်အလက်လွတ်လပ်ခွင့် အက်ဥပဒေ (Freedom of Information Act 2000 (FOIA)) အရ ကင်းလွတ်ခွင့် ရရှိထားကာ အခြားသော ယူကေနိုင်ငံ၏ ဆက်သွယ်ရေးဆိုင်ရာ ဥပဒေ ကင်းလွတ်ခွင့်လည်း ရရှိနိုင်ပါသည်။

FOIA နှင့် ပတ်သက်သည့် စုံစမ်းမေးမြန်းမှု မှန်သမျှအတွက် ncscinfoleg@ncsc.gov.uk ကို ဆက်သွယ်ပါ။.

ပူးတွဲစာရွက် – လေ့လာထားသည့် **MOONSHINE** နှင့် **BADBAZAAR** ဥပမာများ

ဤဖောင်းထဲတွင် လွန်ခဲ့သည့် နှစ်နှစ်ကာလအတွင်း MOONSHINE နှင့် BADBAZAAR ကမ်ပိန်းအတွင်း အသုံးပြုခဲ့သည့် app များ၏ စာရင်းကိုထည့်သွင်းထားပါသည်။

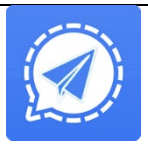
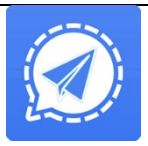
ထို app အများစုတို့သည် အတည်တကျရှိနေပြီးသား app များနှင့် အများကြီး ဆင်တူကြောင်း ပြသထားပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းသည် လူသိများကျော်ကြားသည့် အမှတ်တံဆိပ်များအား တမင်တကာ “လှောင်ပြောင်” ခြင်း ဖြစ်နိုင်ပါသည်။

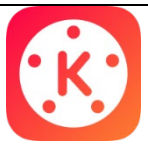
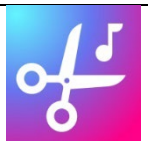
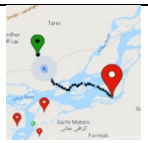
သတိပြုရမည့် အချက်မှာ app များ၏ နာမည်၊ package နာမည်နှင့် သင်္ကေတများ အားလုံးသည် တုပနိုင်သည့် အရာဖြစ်ပြီး application အစစ်များအတိုင်း လုပ်ဆောင်နိုင်သည့်အတွက် စက်ပစ္စည်းတစ်ခု တိုက်ခိုက်ခံရခြင်း ရှိမရှိ စစ်ဆေးရာတွင် app အစစ်အဖြစ် မှတ်ယူကာ အသုံးမပြုသင့်ပါ။

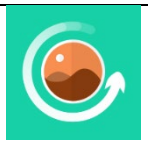
အန္တရာယ်လျှော့ချရေး အပိုင်းတွင် ဖော်ပြသည့်အတိုင်း သင်၏ Android စက်ပစ္စည်းမှ app ကို Google ဆီ ပို့ဆောင်ကာ ‘Improve harmful app detection ဖျက်လိုဖျက်ဆီးပြုနိုင်သည့် App ကို ပိုမိုသိအောင် လုပ်ခြင်း’ ကို ဖွင့်ထားပါက Play Store ပြင်ပမှ app များ ဟုတ်မဟုတ် စစ်စိမ့် လုပ်ပေးနိုင်ပါသည်။

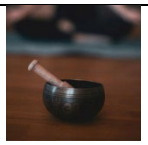
App ခေါင်းစဉ်	Package အမည်	App **သင်္ကေတ**
99 Names of ALLAH အလွာအရှင်မြတ်၏ အမည် ၉၉ ခု	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	

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	

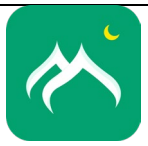
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	

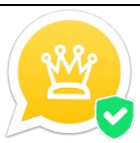
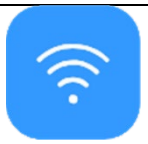
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	

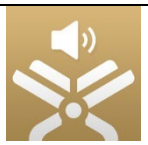
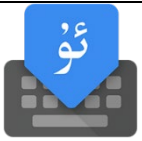
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
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	
زىكىرلەر	com.my.newproject5	
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	
نۇر كىرگۈزگۈچ	com.nur.ime	

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