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

ຄຳແນະນຳ

BADBAZAAR ແລະ MOONSHINE: ສະປາຍແວທີ່ແນເປົ້າໝາຍໄປຍັງກຸ່ມອຸຍກູ, ຊາວໄຕ້ຫວັນ ແລະ ຊາວທິເບດ ແລະ ລວມທັງຜູ້ມີບົດບາດໃນສັງຄົມພົນລະເມືອງ

ວັນທີ 9 ເມສາ 2025

BADBAZAAR ແລະ MOONSHINE: ສະປາຍແວທີ່ແນເປົ້າໝາຍໄປຍັງກຸ່ມອຸຍກູ, ຊາວໄຕ້ຫວັນ ແລະ ຊາວທິເບດ ແລະ ລວມທັງຜູ້ມີບົດບາດໃນສັງຄົມພົນລະເມືອງ

NCSC ແລະ ຄູ່ຮ່ວມມືເຜີຍແຜ່ຂໍ້ມູນໃໝ່ ແລະ ມາດຕະການບັນເທົາຜົນກະທົບສຳລັບຜູ້ທີ່ມີຄວາມສ່ຽງສູງຈາກສະປາຍແວສອງສາຍພັນ.

ບົດສະຫຼຸບ

ດ້ວຍການສະໜັບສະໜູນໄຊເບີລີກຈາກອັງກິດ, ຄຳແນະນຳນີ້ໄດ້ຮັບການຜະລິດຮ່ວມກັນໂດຍສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດ (NCSC UK) ແລະ ຄູ່ຮ່ວມງານສາກົນ:

- **ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕາລີ, ເຊິ່ງເປັນສ່ວນໜຶ່ງຂອງສຳນັກງານສັນຍານຂອງອົດສະຕາລີ**
- **ສູນຄວາມປອດໄພທາງໄຊເບີຂອງການາດາ, ເຊິ່ງເປັນສ່ວນໜຶ່ງຂອງການສ້າງຕັ້ງຄວາມປອດໄພດ້ານການສື່ສານ**
- **ບໍລິການຂ່າວລັບຂອງລັດຖະບານກາງຂອງເຢຍລະມັນ**
- **ສຳນັກງານລັດຖະບານກາງເຢຍລະມັນເພື່ອປົກປ້ອງລັດຖະທຳມະນູນ**
- **ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດນິວຊີແລນ, ເຊິ່ງເປັນສ່ວນໜຶ່ງຂອງສຳນັກງານຄວາມປອດໄພດ້ານສື່ສານຂອງລັດຖະບານ**
- **ສຳນັກງານສືບສວນຂອງລັດຖະບານກາງສະຫະລັດ**
- **ອົງການຄວາມໝັ້ນຄົງແຫ່ງຊາດຂອງສະຫະລັດ**

ຈຸດປະສົງຂອງແມ່ນເພື່ອປູກຈິດສຳນຶກກ່ຽວກັບໄພຂົ່ມຂູ່ທີ່ເພີ່ມຂຶ້ນ ຜູ້ບໍ່ປະສົງດີທາງໄຊເບີກໍ່ຂຶ້ນຕໍ່ບຸກຄົນທີ່ກ່ຽວຂ້ອງກັບຫົວຂໍ້ຕ່າງໆລວມທັງໄຕ້ຫວັນ, ທິເບດ, ເຂດປົກຄອງຕົນເອງຊິນຈຽງອຸຍກູ, ຂະບວນການປະຊາທິປະໄຕ ແລະ ຟາລູນໂກງ.

ຄຳແນະນຳນີ້ປະກອບມີສອງກໍລະນີສຶກສາລາຍລະອຽດກ່ຽວກັບເຕັກນິກທີ່ໃຊ້ໂດຍຜູ້ບໍ່ປະສົງດີທາງໄຊເບີທີ່ໃຊ້ສະປາຍແວທີ່ເອີ້ນວ່າ BADBAZAAR ແລະ MOONSHINE
ເພື່ອກຳນົດເປົ້າໝາຍຂໍ້ມູນໃນອຸປະກອນມືຖືລວມທັງໂທລະສັບສະມາດໂຟນເຊິ່ງອາດເປັນທີ່ສົນໃຈຂອງລັດຖະບານຈີນ. ນອກຈາກນີ້, ຍັງເປັນປ້າຍຊີ້ບອກທາງໄປຍັງຄຳແນະນຳເພື່ອຊ່ວຍໃຫ້ບຸກຄົນຕ່າງໆປົກປ້ອງຕົນເອງ, ອຸປະກອນ ແລະ ຂໍ້ມູນຂອງຕົນອີກດ້ວຍ.

ນອກເໜືອຈາກຄຳແນະນຳນີ້, NCSC ຍັງໄດ້ເຜີຍແຜ່ ລາຍລະອຽດດ້ານເທັກນິກສະບັບເຕັມພ້ອມຄຳແນະນຳແຍກຕ່າງຫາກ.

ໃຜແດ່ທີ່ມີຄວາມສ່ຽງ?

ໜ່ວຍງານຜູ້ປະພັນ ແລະ ຄູ່ຮ່ວມມືໃນອຸດສາຫະກຳພົບວ່າ BADBAZAAR ແລະ MOONSHINE ມຸ່ງເປົ້າໄປຍັງບຸກຄົນທີ່ກ່ຽວຂ້ອງກັບຫົວຂໍ້ທີ່ລັດຖະບານຈີນພິຈາລະນາວ່າເປັນໄພຂົ່ມຂູ່ຕໍ່ອຳນາດພາຍໃນປະເທດ, ຄວາມທະເຍີທະຍານ ແລະ ຊື່ສຽງລະດັບໂລກຂອງພວກເຂົາໂດຍສະເພາະ. ຜູ້ທີ່ມີຄວາມສ່ຽງສູງສຸດປະກອບມີ, ແຕ່ບໍ່ຈຳກັດ, ຜູ້ທີ່ກ່ຽວຂ້ອງກັບ:

- **ເອກະສານຂອງໄຕ້ຫວັນ**
- **ສິດຂອງຊາວທິເບດ**
- **ຊາວມຸດສະລິມອຸຍກູ ແລະ ຊົນເຜົ່າອື່ນໆຢູ່ໃນ ຫຼື ຈາກເຂດປົກຄອງຕົນເອງຊິນຈຽງອຸຍກູຂອງຈີນ**
- **ການສະໜັບສະໜູນປະຊາທິປະໄຕ (ລວມທັງຮົ່ງກົ່ງ)**
- **ການເຄື່ອນໄຫວທາງຈິດວິນຍານຟາລຸນໂກງ**

ນີ້ປະກອບມີອົງກອນທີ່ບໍ່ຂຶ້ນກັບລັດຖະບານ (NGOs), ນັກຂ່າວ, ທຸລະກິດ ແລະ ບຸກຄົນທີ່ສະໜັບສະໜູນ, ລະບຸ ຫຼື ເປັນຕົວແທນຂອງກຸ່ມເຫຼົ່ານີ້.
ການແຜ່ກະຈາຍສະປາຍແວແບບບໍ່ເລືອກປະຕິບັດທາງອອນລາຍຍັງໝາຍເຖິງຄວາມສ່ຽງທີ່ການຕິດເຊື້ອອາດແຜ່ລາມໄປໄກກວ່າຜູ້ຖືກເຄາະຮ້າຍທີ່ຕັ້ງໃຈໄວ້.

ຄຳແນະນຳນີ້ມີຈຸດປະສົງເພື່ອຊ່ວຍໃຫ້ຜູ້ທີ່ມີຄວາມສ່ຽງຕອບສະໜອງຢ່າງມີປະສິດທິພາບຕໍ່ກັບໄພຂົ່ມຂູ່ສະເພາະຈາກສະປາຍແວ BADBAZAAR ແລະ MOONSHINE.
ມາດຕະການບັນເທົາບັນຫາທີ່ແນະນຳນັ້ນເປັນສ່ວນເສີມຂອງຄຳແນະນຳດ້ານຄວາມປອດໄພທາງໄຊເບີຢ່າງກວ້າງຂວາງ ແລະ ບໍ່ຄວນພິຈາລະນາແຍກກັນ.

ໂດຍປະຕິບັດຕາມຄຳແນະນຳທີ່ອ້າງອີງໃນຄຳແນະນຳນີ້, ຜູ້ໃຊ້ສາມາດຫຼຸດຜ່ອນຄວາມສ່ຽງຕໍ່ການຕິດໄວຣັດໃນອຸປະກອນມືຖື ແລະ ຂໍ້ມູນຂອງຕົນໄດ້.

ໄພຂົ່ມຂູ່

MOONSHINE ແລະ BADBAZAAR ແມ່ນຕົວຢ່າງຂອງໂທຈັນ; ພວກມັນມີຟັງຊັນທີ່ເປັນອັນຕະລາຍທີ່ເຊື່ອງໄວ້ຢູ່ໃນແອັບທີ່ເຮັດວຽກຢ່າງອື່ນທີ່ສາມາດດາວໂຫຼດໄດ້ຈາກຮ້ານຄ້າແອັບ ຫຼື ບໍລິການແບ່ງປັນໄຟລ໌ອອນລາຍ.

ແອັບເຫຼົ່ານີ້ໄດ້ຮັບການອອກແບບມາເພື່ອຫຼອກລວງຜູ້ໃຊ້ໃຫ້ດາວໂຫຼດ ແລະ ຕິດຕັ້ງພວກມັນລົງໃນອຸປະກອນ. ເມື່ອແອັບຖືກຕິດຕັ້ງແລ້ວ, ມັນຈະໃຊ້ຊ່ອງໂຫວ່ຢູ່ໃນອຸປະກອນເພື່ອເຮັດໜ້າທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ ຫຼື ມັນອາດຈະອີງໃສ່ຜູ້ໃຊ້ທີ່ໃຫ້ການອະນຸຍາດແອັບເພື່ອເຂົ້າເຖິງ ແລະດາວໂຫຼດຂໍ້ມູນຈາກອຸປະກອນ, ລວມທັງ:

- **ຂໍ້ມູນສະຖານທີ່ລວມທັງການຕິດຕາມເວລາທີ່ແທ້ຈິງ**
- **ການເຂົ້າເຖິງໄມໂຄຣໂຟນ ແລະ ກ້ອງຖ່າຍຮູບ**
- **ຂໍ້ຄວາມ, ຮູບພາບ ແລະ ໄຟລ໌ອື່ນໆທີ່ເກັບໄວ້ໃນອຸປະກອນ**
- **ຂໍ້ມູນອຸປະກອນ ແລະ ອື່ນໆອີກ**

ຫຼັງຈາກນັ້ນ,ຜູ້ກະທຳຈະສະແຫວງຫາຜົນປະໂຫຍດທີ່ຖືກຕ້ອງຕາມກົດໝາຍຂອງກຸ່ມທີ່ມີຄວາມສ່ຽງ, ເພື່ອກຳນົດ ແລະ ແຜ່ເຊື້ອໃຫ້ຜູ້ຖືກເຄາະຮ້າຍໃຫ້ໄດ້ຫຼາຍທີ່ສຸດ ແລະ ເຂົ້າເຖິງຂໍ້ມູນຂອງພວກເຂົາ. ວິທີໜຶ່ງທີ່ເຂົາເຈົ້າເຮັດຄືການອອກແບບແອັບທີ່ເຂົາເຈົ້າຮູ້ວ່າຈະດຶງດູດຜູ້ເຄາະຮ້າຍຂອງເຂົາເຈົ້າ, ເຊັ່ນແອັບທີ່ຮອງຮັບພາສາພື້ນເມືອງຂອງເຂົາເຈົ້າ ຫຼື ມີເນື້ອຫາສະເພາະກັບສະຖານທີ່ຕ່າງໆ ເຊັ່ນ: ເຂດຕິເບດຂອງຈີນ ຫຼື ຊິນຈຽງ.

ກໍລະນີສຶກສາຢູ່ໃນຄຳແນະນຳນີ້ໃຫ້ບາງຕົວຢ່າງຂອງເລື່ອງນີ້, ເຊິ່ງລວມທັງແອັບ TibetOne ແລະ Uyghur Quran.

ຜູ້ກະທຳມັນຈະຢູ່ໃນຟອມສົນທະນາອອນລາຍທີ່ມີພື້ນຖານຜູ້ໃຊ້ຂອງຜູ້ຖືກເຄາະຮ້າຍທີ່ມີຈຸດປະສົງ, ເຊິ່ງເຮັດໃຫ້ໂອກາດຂອງພວກເຂົາຕິດເຊື້ອຜູ້ຖືກເຄາະຮ້າຍສູງສຸດ. ພວກເຂົາມີການສັງເກດເຫັນວ່າພວກເຂົາເຈດຕະນາແບ່ງປັນ Telegram ທີ່ກ່ຽວຂ້ອງກັບທິເບດ ແລະ ຟໍຣັມ Reddit. ກໍລະນີສຶກສາຢູ່ໃນຄຳແນະນຳນີ້ຍັງໃຫ້ຕົວຢ່າງຂອງວິທີການເຫຼົ່ານີ້ດ້ວຍ.

ແອັບທີ່ເປັນອັນຕະລາຍມັກຈະຖືກແບ່ງປັນເປັນໄຟລ໌ແບບດ່ຽວ ເຊັ່ນ: ໄຟລ໌ APK ຢູ່ໃນ Android, ເຊິ່ງຜູ້ໃຊ້ຈຳເປັນຕ້ອງໄດ້ດາວໂຫຼດ ແລະ ຕິດຕັ້ງ. ຜູ້ກະທຳຄວາມຜິດພະຍາຍາມເຮັດໃຫ້ສະປາຍແວ ຂອງເຂົາເຈົ້າເບິ່ງຄືໜ້າເຊື່ອຖືຫຼາຍຂຶ້ນ ໂດຍການອັບໂຫຼດໄປຫາຮ້ານຄ້າແອັບຢ່າງເປັນທາງການເຊັ່ນ Google Play Store ແລະ Apple App Store ຫຼື ໂດຍການເພີ່ມລະຫັດທີ່ເປັນອັນຕະລາຍລົງໃນແອັບທີ່ບໍ່ເຄີຍອັນຕະລາຍ, ເຖິງແມ່ນວ່າຮ້ານຄ້າຢ່າງເປັນທາງການຈະມີລັກສະນະຄວາມປອດໄພ ແລະ ຂະບວນການກວດສອບທີ່ເຮັດໃຫ້ກົນລະຍຸດນີ້ປະສົບຜົນສຳເລັດໜ້ອຍລົງ. ເຊິ່ງເຮັດໃຫ້ແອັບຈາກຮ້ານຄ້າທີ່ເປັນທາງການມີຄວາມປອດໄພຂຶ້ນ, ແຕ່ຕາມທີ່ໄດ້ສະແດງໃນກໍລະນີສຶກສາ ແລະ ລາຍງານໄພຂົ່ມຂູ່ຂອງ App Store ຂອງ NCSC, ຂະບວນການເຫຼົ່ານີ້ບໍ່ສົມບູນແບບ.

ປະຕິບັດຕາມຄຳແນະນຳ 4 ປະການເຫຼົ່ານີ້ອາດຊ່ວຍປົກປ້ອງທ່ານຈາກໄພຂົ່ມຂູ່ທີ່ລະບຸໄວ້ໃນຄຳແນະນຳນີ້ໄດ້.

ສຳລັບຄຳແນະນຳໂດຍລາຍລະອຽດເພີ່ມເຕີມ,ໃຫ້ເບິ່ງສ່ວນການບັນເທົາຜົນກະທົບ.

ກໍລະນີສຶກສາ

ກໍລະນີສຶກສາທັງສອງນີ້ສະແດງໃຫ້ເຫັນວ່າ MOONSHINE ແລະ BADBAZAAR ເຮັດວຽກແນວໃດ ແລະ ຜູ້ກະທຳຜິດທາງໄຊເບີຕັ້ງເປົ້າໄປທີ່ຜູ້ທີ່ມີຄວາມສ່ຽງສູງທີ່ສຸດແນວໃດ.

ກໍລະນີສຶກສາທີ່ໜຶ່ງ: MOONSHINE

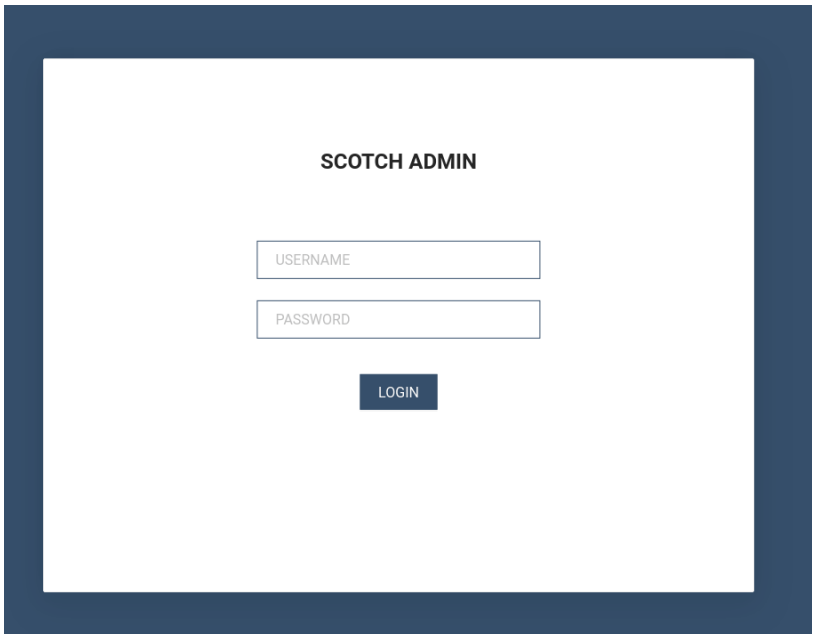
MOONSHINE ເປັນ ສະປາຍແວລະບົບປະຕິບັດການ Android ທີ່ລາຍງານໃນປີ 2019 ໂດຍ ຫ້ອງທົດລອງພົນລະເມືອງ ເປັນເປົ້າໝາຍກຸ່ມຊາວທິເບດ. MOONSHINE ປອມຕົວເປັນແອັບຖືກກົດໝາຍເພື່ອລໍ້ລວງຜູ້ຖືກເຄາະຮ້າຍໃຫ້ຕິດຕັ້ງແອັບນີ້. ມີການແບ່ງປັນຜ່ານຊ່ອງທາງ Telegram ແລະ ມີການສົ່ງລິ້ງຜ່ານ WhatsApp ດ້ວຍ.

MOONSHINE ມີຄວາມສາມາດໃນການເຝົ້າລະວັງຢ່າງກວ້າງຂວາງ, ເຊັ່ນ:

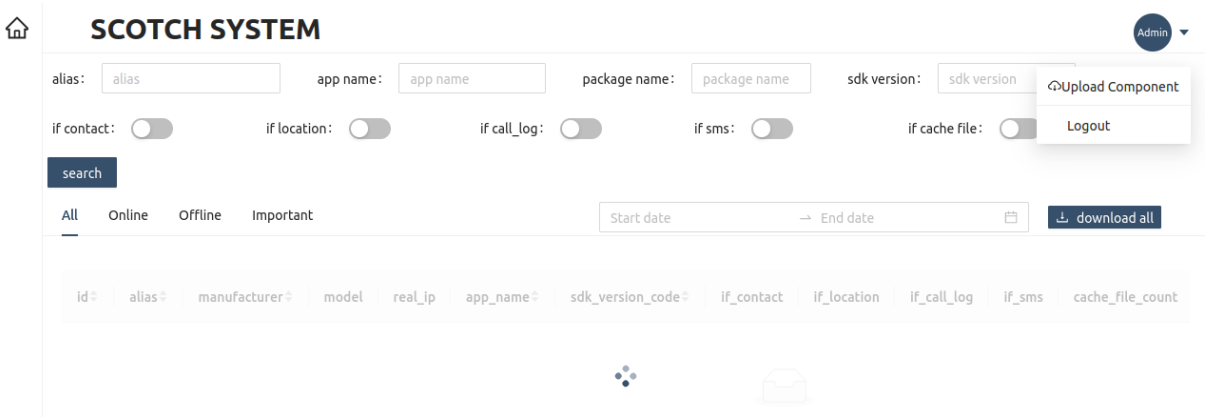
- **ຂໍ້ມູນສະຖານທີ່ລວມທັງການຕິດຕາມເວລາທີ່ແທ້ຈິງ**
- **ບັນທຶກສຽງ ແລະ ຖ່າຍພາບສົດ**
- **ການດາວໂຫຼດໄຟລ์ຈາກອຸປະກອນ**
- **ການດຶງຂໍ້ມູນອຸປະກອນ**
- **ການຫຼິ້ນສຽງຢູ່ໃນອຸປະກອນ**

ແອັບພລິເຄຊັນ ‘**ئاۋازلىق قۇرئان.apk**’ ເຊິ່ງແປວ່າ ‘**Audio Quran.apk**’, ເປັນຕົວຢ່າງຂອງການໃຊ້ MOONSHINE ເພື່ອກຳນົດເປົ້າໝາຍຊາວອຸຍເກີ. ການໃຊ້ພາສາອຸຍກູໃນຊື່ໄຟລ์, ສະແດງໃຫ້ເຖິງແອັບພລິເຄຊັນຄູຣານອາດໄດ້ຮັບການ ອອກແບບມາເພື່ອດຶງດູດໃຈຊາວຊາວມຸດສະລິມອຸຍກູ.

ເມື່ອຕິດຕັ້ງແລ້ວ, ຜູ້ບໍ່ຫວັງດີທາງໄຊເບີຈະສາມາດລວບລວມຂໍ້ມູນຈາກອຸປະກອນຂອງຜູ້ຖືກເຄາະຮ້າຍໄດ້. ສາມາດເຂົ້າເຖິງຂໍ້ມູນນີ້ໄດ້ຜ່ານແຜງຄວບຄຸມ ‘SCOTCH ADMIN’.



ເມື່ອເຂົ້າສູ່ລະບົບແລ້ວ, ຜູ້ກະທຳຜິດສາມາດເຂົ້າເຖິງໜ້າທີ່ສະແດງຢູ່ໃນພາບໜ້າຈໍຂ້າງລຸ່ມນີ້ໄດ້.
ໜ້ານີ້ສະແດງລາຍລະອຽດຂອງອຸປະກອນທີ່ຕິດເຊື້ອ ແລະ ລະດັບການເຂົ້າເຖິງອຸປະກອນທີ່ຕິດເຊື້ອຂອງຜູ້ກະທຳຜິດ:



ແຜງການຈັດການມັນແວຈະສະແດງຂໍ້ມູນທີ່ເກັບກຳ, ລວມທັງ:

- **ລະດັບການເຂົ້າເຖິງອຸປະກອນ**
- **ຂໍ້ຄວາມ SMS**
- **ບັນທຶກການໂທ**
- **ຂໍ້ມູນສະຖານທີ່**
- **ຂໍ້ມູນອຸປະກອນ**

NCSC ຮ່ວມມືກັບ Cyber League, ພັດທະນາລາຍງານຂອງອຸດສາຫະກຳ ການລາຍງານຈາກ Trend Micro ເພື່ອຊອກຫາການທັບຊ້ອນກັນລະຫວ່າງຊຸດສະແຫວງຜົນປະໂຫຍດ MOONSHINE ກັບແຜງຄວບຄຸມການເຂົ້າສູ່ລະບົບທີ່ມີຄຳວ່າ 'UPSEC' ໃນຊື່ HTML. ລາຍລະອຽດຄົບຖ້ວນມີຢູ່ໃນຄຳແນະນຳທາງເທັກນິກທີ່ແນບມາ.

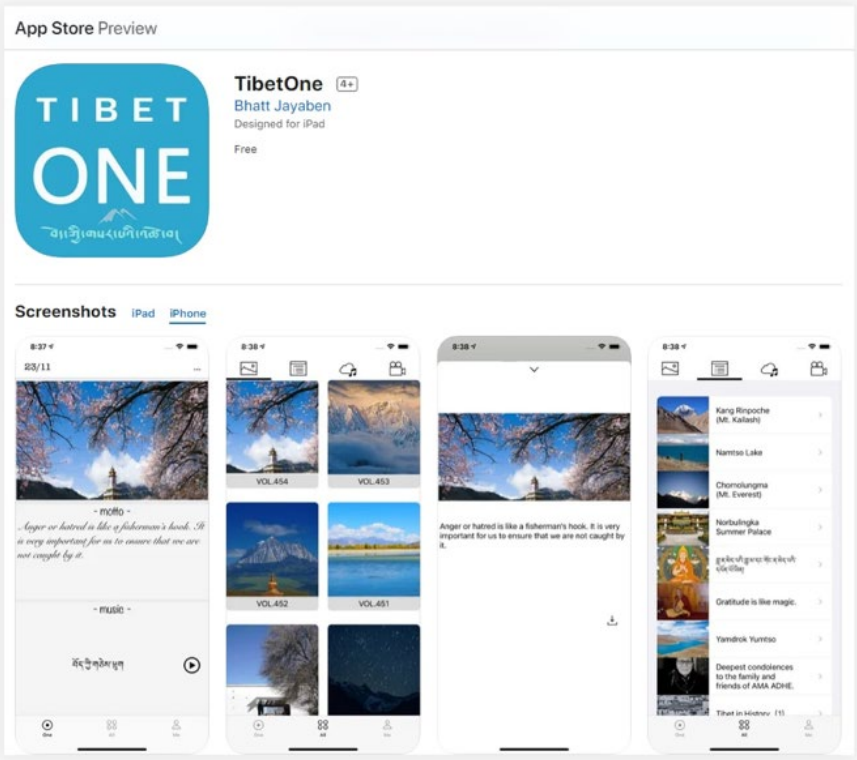
ອີງຕາມລາຍງານຂອງ Intelligence Online, UPSEC ແມ່ນການອ້າງອີງເຖິງ ‘Sichuan Dianke Network Security Technology Co. Ltd’. ໜ່ວຍງານຜູ້ປະພັນຍັງບໍ່ໄດ້ກວດຢືນຢັນຄຳຖະແຫຼງການນີ້.

ກໍລະນີສຶກສາສອງ: BADBAZAAR

BADBAZAAR ແມ່ນ ມັນແວໃນອຸປະກອນມືທີ່ມີເວີຊັນ iOS ແລະ Android ທີ່ກຳນົດເປົ້າໝາຍທີ່ເປັນຊາວອຸຍກູ, ຊາວທິເບດ ແລະ ໄຕ້ຫວັນ. ມັນແວນີ້ແຜ່ກະຈາຍຜ່ານແພລະຕະຟອມສື່ສັງຄົມ ແລະ ຮ້ານຄ້າແອັບຢ່າງເປັນທາງການ.

BADBAZAAR ຖືກໃຊ້ເພື່ອກຳນົດເປົ້າໝາຍຊາວທິເບດຜ່ານແອັບ **‘TibetOne’**, ຕາມການລາຍງານຂອງ Lookout ແລະ Volexity. **TibetOne** ເປັນແອັບ iOS ທີ່ສ້າງຂຶ້ນໂດຍຜູ້ກະທຳທີ່ເປັນອັນຕະລາຍ, ທີ່ມີຄວາມສາມາດໃນການເຂົ້າເຖິງຂໍ້ມູນອຸປະກອນ ແລະ ຂໍ້ມູນສະຖານທີ່. ໄດ້ຮັບການອັບໂຫຼດໄປຍັງ Apple App Store ໃນເດືອນທັນວາ 2021 ແຕ່ບໍ່ສາມາດໃຊ້ໄດ້ອີກຕໍ່ໄປ. ເພື່ອແຜ່ກະຈາຍມັນແວໃຫ້ເພີ້ມຫຼາຍຂຶ້ນ, ຜູ້ກະທຳຄວາມຜິດຍັງໄດ້ໂຄສະນາແອັບດັ່ງກ່າວໃນຊ່ອງ Telegram ທີ່ເອີ້ນວ່າ **'tibetanphone'** ອີກດ້ວຍ.

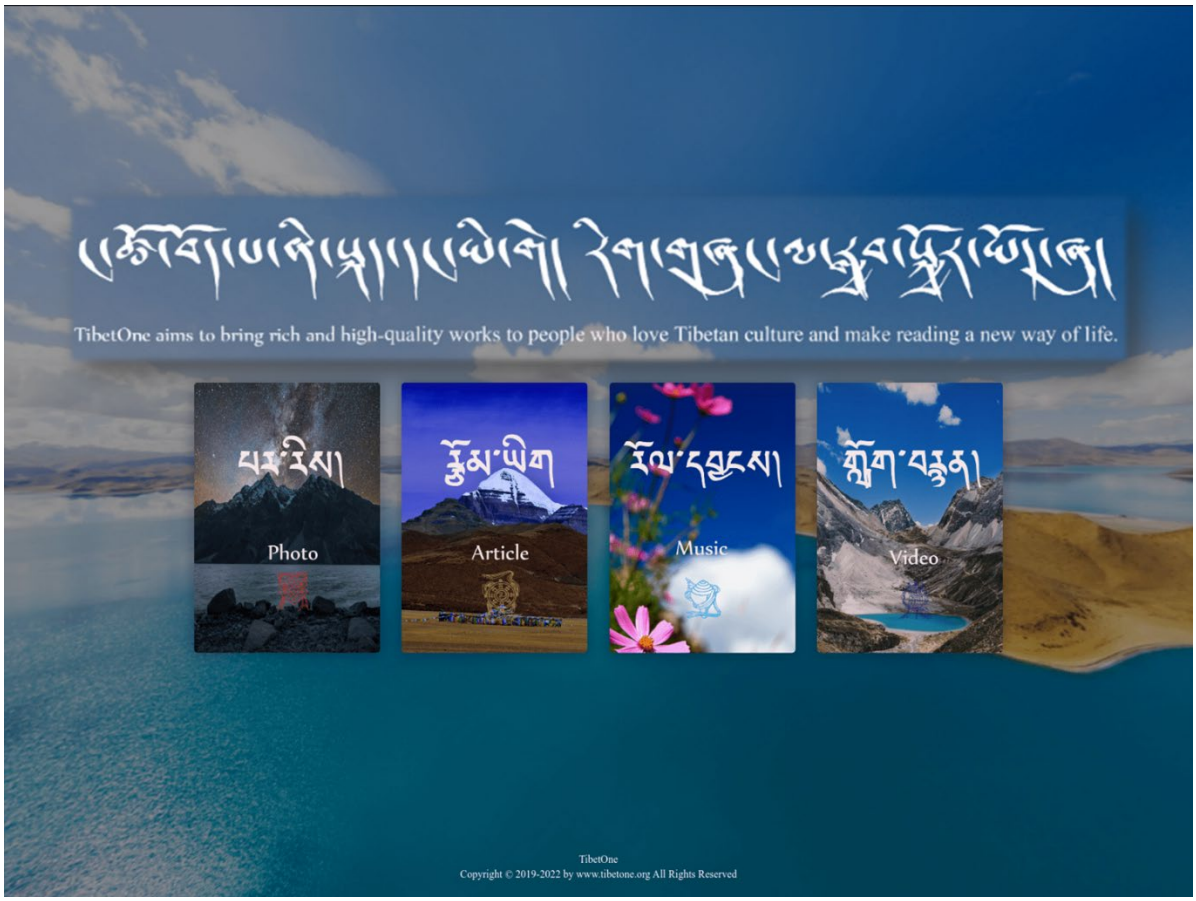
TibetOne



ຮູບທີ 1: ໜ້າແອັບ TibetOne ໃນ Apple App Store. ແອັບດັ່ງກ່າວໄດ້ຖືກລຶບອອກແລ້ວ.

ຮູບທີ 2: TibetOne ທີ່ຖືກແບ່ງປັນໃນຊ່ອງ Telegram.

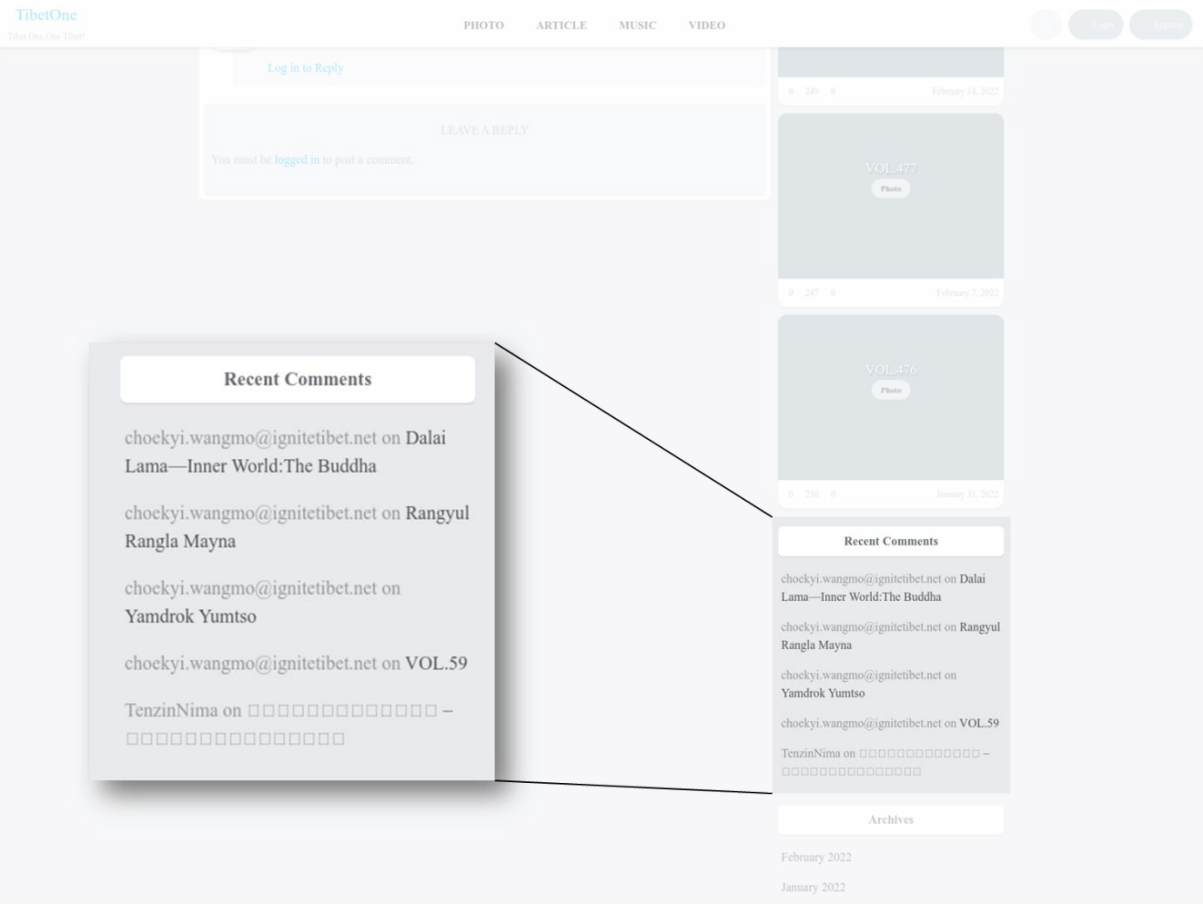
ເພື່ອເພີ່ມຄວາມໜ້າເຊື່ອຖືໃຫ້ກັບແອັບ, ຜູ້ກະທຳຍັງໄດ້ພັດທະນາເວັບໄຊທ໌ທີ່ເອີ້ນວ່າ **'tibetone[.]org'**, ເຊິ່ງອະທິບາຍຕົວເອງວ່າ '*ນຳເອົາຜົນງານທີ່ມີຄຸນນະພາບສູງ ແລະ ມີຄຸນນະພາບສູງມາສູ່ຜູ້ທີ່ຮັກວັດທະນະທຳທິເບດ ແລະ ເຮັດໃຫ້ການອ່ານເປັນວິຖີຊີວິດໃໝ່*'.



ຮູບທີ 3: ໜ້າທຳອິດຂອງ 'tibetone[.]org'.

ຮູບພາບນີ້ໄດ້ຮັບການແກ້ໄຂເພື່ອເຮັດໃຫ້ພາກສ່ວນທີ່ກ່ຽວຂ້ອງຊັດເຈນຍິ່ງຂຶ້ນ.

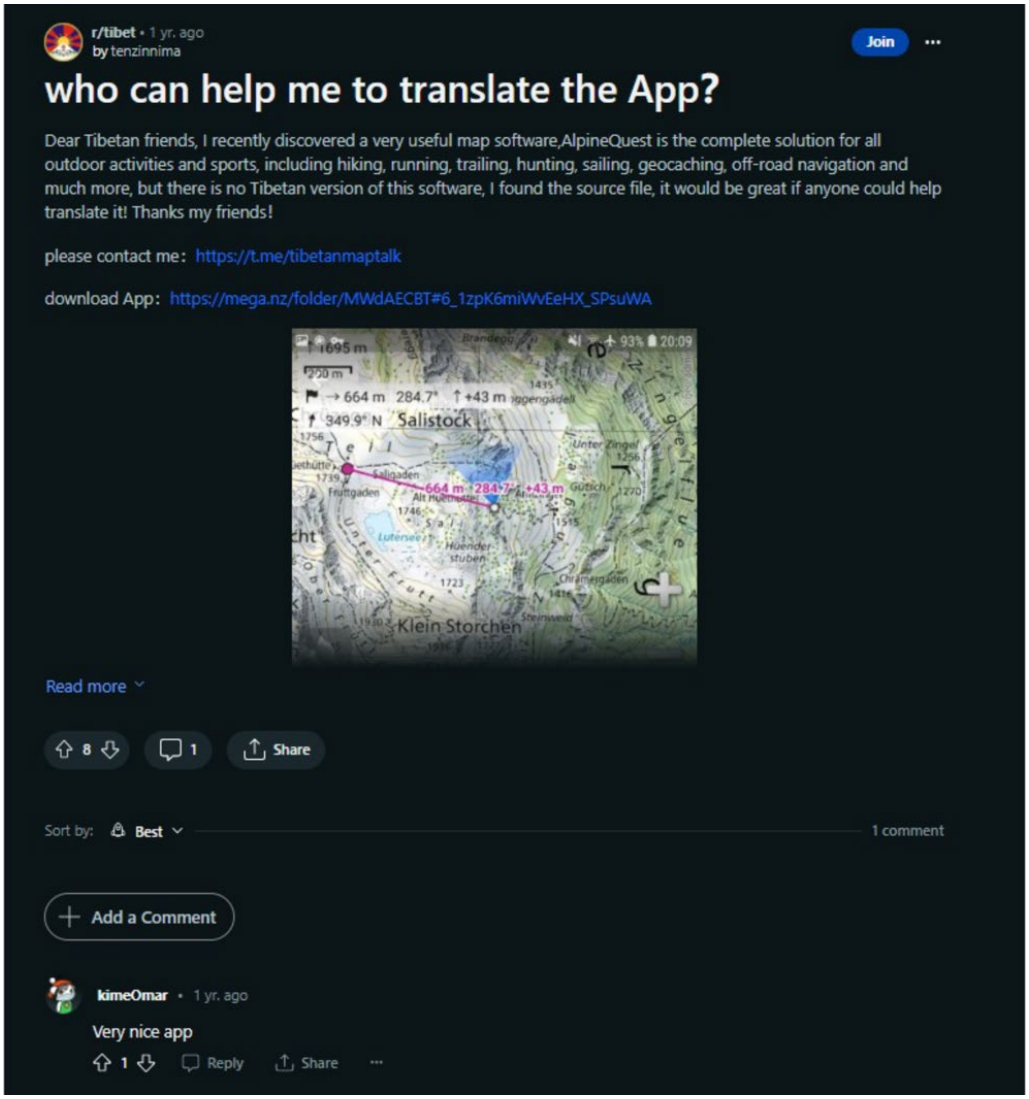
ເວັບໄຊທ໌ນີ້ມີໜ້າສຳລັບບົດຄວາມທີ່ອະນຸຍາດໃຫ້ຜູ້ໃຊ້ສາມາດສະແດງຄຳຄິດເຫັນ. ຄວາມຄິດເຫັນທີ່ສະແດງເປັນ ອີເມວ ທີ່ຢູ່ **'choekyi.wangmo@ignitetibet.net'**, ເຊື່ອວ່າຖືກຄວບຄຸມໂດຍຜູກະທຳຄວາມຜິດ ແລະ ມີແນວໂນ້ມທີ່ຈະປອມຕົວເປັນ **'Choekyi Wangmo'** ເຊິ່ງເປັນຜູ້ປະທ້ວງທີ່ສະໜັບສະໜູນທິເບດໃນນາມ ສູນສິດທິມະນຸດຊົນ ແລະປະຊາທິປະໄຕທິເບດ. ນີ້ອາດຈະເປັນຄວາມພະຍາຍາມອີກອັນໜຶ່ງທີ່ຈະໃຫ້ຄວາມປະທັບໃຈ ທີ່ແອັບດັ່ງກ່າວສະໜັບສະໜູນຄວາມເປັນເອກະລາດຂອງຊາວທິເບດຢ່າງແທ້ຈິງ.



ຮູບທີ 4: ໜ້າ 'tibetone[.]org' ສະແດງຄຳຄິດເຫັນຈາກຜູ້ໃຊ້ທີ່ເຊື່ອວ່າຖືກຄວບຄຸມໂດຍຜູ້ກະທຳທີ່ເປັນອັນຕະລາຍ.

ຮູບພາບນີ້ໄດ້ຮັບການແກ້ໄຂເພື່ອເຮັດໃຫ້ພາກສ່ວນທີ່ກ່ຽວຂ້ອງຊັດເຈນຍິ່ງຂຶ້ນ.

'TenzinNima' ຊື່ຜູ້ໃຊ້ອື່ນທີ່ໄດ້ເພີ່ມຄຳຄິດເຫັນຢູ່ໃນເວັບໄຊທ໌ນີ້. Volexity ໄດ້ລາຍງານ ວ່າຊື່ຜູ້ໃຊ້ນີ້ຍັງຖືກໃຊ້ຢູ່ໃນ Reddit ເພື່ອໂຄສະນາຊ່ອງ Telegram ທີ່ເຊື່ອວ່າ **'Tibetanmaptalk'** ອີກດ້ວຍ. ລວມທັງລິ້ງສຳລັບການດາວໂຫຼດຕົວຢ່າງທີ່ເປັນອັນຕະລາຍຂອງ **‘AlpineQuest’**, ເຊິ່ງເປັນແອັບນຳທາງທີ່ມີໃຫ້ໃຊ້ຢູ່ໃນອຸປະກອນ Android. ລິ້ງດາວໂຫຼດທີ່ໃຫ້ໄວ້ເປັນຂອງບໍລິການແບ່ງປັນໄຟລ໌ຂອງພາກສ່ວນທີສາມເອີ້ນວ່າ Mega.



ຮູບທີ່ *5: ໂພສ Reddit ໂຄສະນາແອັບພລິເຄຊັນທີ່ເປັນອັນຕະລາຍໂດຍບັນຊີທີ່ເຊື່ອວ່າເປັນຜູ້ຄວບຄຸມທີ່ເປັນອັນຕະລາຍ.*

ນອກຈາກນີ້ Volexity ຍັງສັງເກດເຫັນວ່າຜູ້ໃຊ້ທີ່ຮູ້ຈັກໃນນາມ **'KimeOmar'** ເຊິ່ງສະແດງຄວາມຄິດເຫັນໃນໂພສດັ່ງກ່າວຍັງຖືກພົບວ່າແບ່ງປັນແອັບທີ່ເປັນອັນຕະລາຍຢູ່ໃນເວທີສົນທະນາຍ່ອຍຂອງ Reddit ອີກດ້ວຍ. ເຊິ່ງອາດຊີ້ບອກໄດ້ວ່າຜູ້ກະທຳທີ່ເປັນອັນຕະລາຍໃຊ້ໂປຣໄຟລ໌ສື່ສັງຄົມຫຼາຍບັນຊີເພື່ອເຮັດໃຫ້ໂພສຂອງຕົນເບິ່ງຖືກຕ້ອງຕາມກົດໝາຍ.

ການປະເມີນ

BADBAZAAR ແລະ MOONSHINE ໃຊ້ວິທີການວິສະວະກຳສັງຄົມຈຳນວນໜຶ່ງເພື່ອກຳນົດເປົ້າໝາຍໄປທີ່ຊຸ່ມຊົນອຸຍກູ, ທິເບດ ແລະ ໄຕ້ຫວັນໂດຍສະເພາະ, ດັ່ງຕໍ່ໄປນີ້:

- ການໃຊ້ໂທຈັນໃນແອັບຕ່າງໆທີ່ມີຄວາມສົນໃຈກັບຊຸມຊົນເຫຼົ່ານີ້, ເຊັ່ນ ແອັບຄູຣານພາສາອຸຍກູ, ມີແນວໂນ້ມສູງວ່າຈະຖືກປັບແຕ່ງໃຫ້ເໝາະສົມກັບຖານຜູ້ເຄາະຮ້າຍເປົ້າໝາຍ.
- ການເພີ່ມແອັບໂທຈັນເຫຼົ່ານີ້ໄປຍັງຮ້ານຄ້າແອັບຢ່າງເປັນທາງການນັ້ນເປັນໄປໄດ້ສູງທີ່ຈະເຮັດໃຫ້ເກີດຄວາມສອບທຳ ແລະ ການແບ່ງປັນໃນກຸ່ມສົນທະນາແມ່ນມີຄວາມຕັ້ງໃຈສູງທີ່ຈະມີຈຸດປະສົງເພື່ອໃຊ້ປະໂຫຍດຈາກຄວາມສຳພັນທີ່ໄວ້ວາງໃຈໄດ້ພາຍໃນຊຸມຊົນເຫຼົ່ານີ້.

BADBAZAAR ແລະ MOONSHINE ເກັບກຳຂໍ້ມູນນີ້ເກືອບຈະແນ່ນອນວ່າຈະມີຄຸນຄ່າຕໍ່ລັດຖະບານຈີນ. ເຖິງແມ່ນວ່າ BADBAZAAR ແລະ MOONSHINE ໄດ້ຖືກພົບວ່າແນເປົ້າໃສ່ຊາວອຸຍກູ, ທິເບດ ແລະ ໄຕ້ຫວັນກໍ່ຕາມ, ຍັງມີມັນແວອື່ນໆທີ່ແນເປົ້າໃສ່ກຸ່ມຊົນເຜົ່າສ່ວນນ້ອຍອື່ນໆໃນປະເທດຈີນ. ພົນລະເມືອງຈາກບັນດາປະເທດພັນທະມິດ, ທັງໃນຈີນ ແລະ ຕ່າງປະເທດ,
ເຊິ່ງຖືກເບິ່ງວ່າສະໜັບສະໜູນສາເຫດທີ່ເປັນໄພຂົ່ມຂູ່ຕໍ່ຄວາມໝັ້ນຄົງຂອງລະບອບການປົກຄອງ,
ເກືອບຈະແນ່ນອນວ່າຕົກຢູ່ພາຍໃຕ້ໄພຂົ່ມຂູ່ຈາກມັນແວມືຖືເຊັ່ນ BADBAZAAR ແລະ MOONSHINE.
ຄວາມສາມາດໃນການເກັບກຳຂໍ້ມູນສະຖານທີ່, ສຽງ ແລະ ຮູບພາບຊ່ວຍໃຫ້ສາມາດແຈ້ງການດຳເນີນການເຝົ້າລະວັງ ແລະ ໄພຂົ່ມຂູ່ໃນອະນາຄົດໄດ້ຢ່າງແນ່ນອນໂດຍໃຫ້ຂໍ້ມູນໃນເວລາທີ່ແທ້ຈິງກ່ຽວກັບກິດຈະກຳຂອງເປົ້າໝາຍ.

ມາດຕະການບັນເທົາຜົນກະທົບສຳລັບຜູ້ໃຊ້ແອັບມືຖື

ໜ່ວຍງານຜູ້ປະພັນສະໜັບສະໜູນໃຫ້ໃຊ້ແນວທາງປະຕິບັດຮັກສາຄວາມປອດໄພຕໍ່ໄປນີ້ເພື່ອປ້ອງກັນໄພຂົ່ມຂູ່ທີ່ອະທິບາຍໄວ້ໃນກໍລະນີສຶກສາ. ຄຳແນະນຳເຫຼົ່ານີ້ແມ່ນໄດ້ຮັບການສະໜັບສະໜູນໂດຍແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດຂອງ NCSC. ເບິ່ງພາກສ່ວນ ‘ການອ່ານເພີ່ມເຕີມ’ ເພື່ອເບິ່ງລິ້ງໄປຍັງຄຳແນະນຳແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດ ສຳລັບຜູ້ອ່ານໃນອົດສະຕາລີ ແລະ ສະຫະລັດ.

ຮັກສາອຸປະກອນຂອງທ່ານໃຫ້ປອດໄພ

- **ດາວໂຫຼດສະເພາະແອັບຈາກຮ້ານແອັບຢ່າງເປັນທາງການ ເຊັ່ນ: Play Store ຂອງ Google ຫຼື App Store ຂອງ Apple.** Play Store ຂອງ Google ແລະ App Store ຂອງ Apple ສະແກນເຊີບເວີເພື່ອຊອກຫາໄວຣັສກ່ອນທີ່ຈະເຜີຍແຜ່, ເຮັດໃຫ້ທ່ານໝັ້ນໃຈໄດ້ຫຼາຍຂຶ້ນວ່າສິ່ງທີ່ທ່ານດາວໂຫຼດນັ້ນປອດໄພ. ແອັບຈາກຮ້ານຄ້າທີ່ເຊື່ອຖືໄດ້ອາດຈະມີຄວາມສ່ຽງ, ແຕ່ການດາວໂຫຼດຈາກແຫຼ່ງອື່ນອາດຈະບໍ່ມີການປ້ອງກັນເລີຍ. NCSC ມີລາຍງານໄພຂົ່ມຂູ່ໃນ App Store: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **ອັບເດດອຸປະກອນ ແລະ ແອັບຂອງທ່ານໃຫ້ທັນສະໄໝ. ຕິດຕັ້ງ ອັບເດດແອັບ ແລະ ຊອບແວອຸປະກອນຂອງທ່ານທັນທີທີ່ມີໃຫ້ບໍລິການ.** ເປີດ 'ການອັບເດດອັດຕະໂນມັດ' ໃນການຕັ້ງຄ່າອຸປະກອນຂອງທ່ານຖ້າມີໃຫ້, ເພື່ອທ່ານຈະບໍ່ຈຳເປັນຕ້ອງຈື່ຈຳເຮັດເຊັ່ນນີ້. ເບິ່ງຄຳແນະນຳຂອງ NCSC ກ່ຽວກັບການຮັກສາຄວາມປອດໄພອອນລາຍ, ເພື່ອປ້ອງກັນໄວຣັສທີ່ຮູ້ຈັກ ແລະ ມັນແວປະເພດອື່ນໆ. ການອັບເດດມັກຈະມີການປັບປຸງ ແລະ ຄຸນສົມບັດໃໝ່: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **ຢ່າເຮັດ 'jailbreak' ຫຼື 'root' ອຸປະກອນຂອງທ່ານ** ເນື່ອງຈາກວິທີນີ້ໃຊ້ຊ່ອງໂຫວ່ທີ່ບໍ່ໄດ້ຮັບການແກ້ໄຂ ເພື່ອຂ້າມການຄວບຄຸມຄວາມປອດໄພທີ່ວາງໄວ້. ສິ່ງນີ້ຈະເຮັດໃຫ້ອຸປະກອນມີຄວາມສ່ຽງຕໍ່ກັບການໂຈມຕີຫຼາຍຂຶ້ນ. ເບິ່ງຄຳແນະນຳຂອງ: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

ຈັດການແອັບຂອງທ່ານ

- **ກວດສອບແອັບຂອງທ່ານ ແລະ ສິດອະນຸຍາດຂອງແອັບເຫຼົ່ານັ້ນ.** ຖ້າ ທ່ານບໍ່ຕ້ອງການແອັບອີກຕໍ່ໄປ, ໃຫ້ລຶບອອກ. ຖ້າເຮັດໄດ້, ໃຫ້ຈຳກັດການອະນຸຍາດຂອງແອັບເພື່ອຫຼຸດຜ່ອນການເປີດເຜີຍຂໍ້ມູນ, ເນື່ອງຈາກວ່າມັນແວມັກຈະຖືກອອກແບບມາເພື່ອເຂົ້າເຖິງໄຟລ໌ທີ່ມີການປ້ອງກັນ ຫຼື ອຸປະກອນຕໍ່ພ່ວງ, ເຊັ່ນ: ກ້ອງຖ່າຍຮູບ ແລະ ໄມໂຄຣໂຟນ.
  - ວິທີກວດສອບການອະນຸຍາດແອັບສຳລັບຜູ້ໃຊ້ Apple: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - ວິທີກວດສອບການອະນຸຍາດແອັບສຳລັບຜູ້ໃຊ້ Android: https://support.google.com/android/answer/9431959?hl=en-GB

- **ສົ່ງແອັບທີ່ບໍ່ຮູ້ຈັກໄປໃຫ້ Google ໂດຍອັດຕະໂນມັດ.** ຖ້າ ທ່ານເປັນຜູ້ໃຊ້ Android ແລະ ໄດ້ດາວໂຫຼດແອັບທີ່ບໍ່ໄດ້ມາຈາກ Play Store ຂອງ Google, ທ່ານສາມາດສົ່ງແອັບດັ່ງກ່າວໄປໃຫ້ Google ໄດ້ໂດຍການເປີດໃຊ້ 'ປັບປຸງການກວດຫາແອັບທີ່ເປັນອັນຕະລາຍ' ໃນການຕັ້ງຄ່າແອັບ Play Store ຂອງ Google ພາຍໃຕ້ ‘Play Protect’. ການດຳເນີນການນີ້ຈະສະແກນແອັບເພື່ອກວດຫາມັນແວ ເພື່ອຊ່ວຍປົກປ້ອງຜູ້ໃຊ້. ຂໍ້ມູນກ່ຽວກັບວິທີການຕັ້ງຄ່ານີ້: https://support.google.com/android/answer/2812853?hl=en-GB

ໃຊ້ການບໍລິການທາງໄຊເບີ

- **ໃຊ້ບໍລິການຊື່ສຽງ URL ກ່ອນທີ່ຈະຄລິກລິ້ງ.** ທ່ານສາມາດກວດວ່າລິ້ງຈາກອີເມວ, ຂໍ້ຄວາມ ຫຼື ທີ່ອື່ນໆປອດໄພ ຫຼື ບໍ່ໂດຍການສະແກນກ່ອນໂດຍໃຊ້ບໍລິການເຊັ່ນ Google Transparency Report ຫຼື Virus Total ນອກນັ້ນທ່ານຍັງສາມາດອັບໂຫຼດໄຟລ໌ ແລະ ແອັບທີ່ໜ້າສົງໄສໄປຍັງເຄື່ອງວິເຄາະມັນແວໄດ້ເຊັ່ນ: Virus Total ທີ່ສາມາດຊ່ວຍກວດຫາວ່າໄຟລ໌ນັ້ນເປັນອັນຕະລາຍຫຼືບໍ່. ໃຫ້ຮູ້ວ່າການບໍລິການການສະແກນ ອາດສ້າງຜົນໄດ້ຮັບດ້ານລົບທີ່ບໍ່ຖືກຕ້ອງໄດ້.

- **ລົງທະບຽນໃນໂຄງການການປົກປ້ອງຂັ້ນສູງຂອງ Google.** ນີ້ແມ່ນການບໍລິການຟຣີທີ່ຖືກອອກແບບມາ ເພື່ອປົກປ້ອງບຸກຄົນທີ່ໃຊ້ບໍລິການຂອງ Google (Gmail, Play Store, ແລະ ອື່ນໆ) ທີ່ມີຄວາມສ່ຽງທີ່ຈະຕົກເປັນເປົ້າໝາຍ. ບໍລິການນີ້ໃຫ້ຄວາມປອດໄພສູງຂຶ້ນເມື່ອໃຊ້ບໍລິການ ຂອງ Google: https://landing.google.com/advancedprotection/

- **ລົງທະບຽນຮັບບໍລິການຄວາມຍືດຢຸ່ນເພີ່ມເຕີມ, ຖ້າມີໃຫ້ບໍລິການ.** ຕົວຢ່າງ, ບຸກຄົນທີ່ມີຄວາມສ່ຽງສູງໃນປະເທດອັງກິດອາດຈະມີສິດໄດ້ຮັບການບໍລິການປ້ອງກັນພິເສດເພື່ອຊ່ວຍເຫຼືອດ້ານຄວາມປອດໄພທາງໄຊເບີຂອງຕົນ. ກວດສອບຄຸນສົມບັດ ແລະ ຊອກຫາຂໍ້ມູນເພີ່ມເຕີມ: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

ລາຍງານໄພຂົ່ມຂູ່

- **ການລະບຸ ແລະ ລາຍງານບັນຊີປອມ.** ຜູ້ກໍ່ອາຊາຍາກຳທາງໄຊເບີສ້າງບັນຊີປອມ ຫຼື ແຮັກບັນຊີຈິງເພື່ອຈຸດປະສົງຂອງຕົນ. ຖ້າທ່ານສົງໃສວ່າບັນຊີໃດເປັນຂອງປອມ ຫຼື ຖືກບຸກລຸກ, ໃຫ້ລາຍງານໄປຍັງເວທີ ແລະ ບລັອກບັນຊີນັ້ນ. ການບໍລິການຕ່າງໆມີຂະບວນການສຳລັບການກວດສອບບັນຊີ, ເຊັ່ນ 'ປ້າຍຢືນຢັນ' ສຳລັບ Instagram ແລະ Facebook. ນີ້ສາມາດຊ່ວຍລະບຸໄດ້ວ່າບັນຊີນັ້ນເປັນຂອງແທ້. NCSC ມີຄຳແນະນຳກ່ຽວກັບການນຳໃຊ້ສື່ສັງຄົມຢ່າງປອດໄພ ເຊິ່ງລວມມີລາຍລະອຽດຂອງວິທີການກວດສອບ ແລະ ລາຍງານບັນຊີທີ່ຖືກບຸກລຸກ: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **ການຫຼອກເອົາຂໍ້ມູນໂດຍໃຊ້ອີເມວຫຼອກລວງ, SMS ແລະ ລິ້ງ.** NCSC ສາມາດສືບສວນທີ່ຢູ່ອີເມວ ແລະ ເວັບໄຊທ໌ທີ່ໜ້າສົງໄສ. ຖ້າທ່ານຄິດວ່າເວັບໄຊທ໌, ອີເມວ ຫຼື ຂໍ້ຄວາມໃດໜ້າສົງໄສ, ທ່ານສາມາດລາຍງານໄດ້ທີ່: https://www.ncsc.gov.uk/collection/phishing-scams

ຄຳສັບ NCSC

- **Android**

ລະບົບປະຕິບັດການມືຖືຂອງ Google, ທີ່ນຳໃຊ້ໂດຍຜູ້ຜະລິດໂທລະສັບສະມາດໂຟນ ແລະ ແທັບເລັດຈຳນວນໜຶ່ງ.

- **ແອັບ**

ແອັບພລິເຄຊັ່ນ ຫຼື ແອັບ, ແມ່ນຊຸດຊອບແວທີ່ຜູ້ໃຊ້ສາມາດຕິດຕັ້ງ ຫຼື ຕິດຕັ້ງໄວ້ລ່ວງໜ້າໃນອຸປະກອນເພື່ອສະໜອງຄວາມສາມາດພິເສດ ຫຼື ເນື້ອຫາໃຫ້ກັບອຸປະກອນຂອງຕົນ.

- **ຄວາມປອດໄພທາງໄຊເບີ**

ການປົກປ້ອງອຸປະກອນ, ການບໍລິການ ແລະ ເຄືອຂ່າຍ ແລະ ລວມໄປເຖິງຂໍ້ມູນໃນນັ້ນຈາກການເຂົ້າເຖິງ ການໂຈມລະກຳ ຫຼື ຄວາມເສຍຫາຍທີ່ບໍ່ໄດ້ຮັບອານຸຍາດ.

- **ອຸປະກອນ**

ຮາດແວທີ່ໃຊ້ໃນຄອມພິວເຕີທີ່ມີຢູ່ຈິງ ເຊັ່ນ: ຄອມພິວເຕີຕັ້ງໂຕະ, ໂທລະສັບສະມາດໂຟນ ຫຼື ແທັບເລັດ.

- **iOS**

ລະບົບປະຕິບັດການຂອງ Apple ທີ່ໃຊ້ໃນຊຸດອຸປະກອນມືຖືຂອງບໍລິສັດ.

- **ມັນແວ**

ມັນແວມາຈາກ 'ຊອບແວທີ່ເປັນອັນຕະລາຍ', ແມ່ນຊອບແວທຸກປະເພດທີ່ສາມາດສ້າງຄວາມເສຍຫາຍໃຫ້ກັບລະບົບຄອມພິວເຕີ, ເຄືອຂ່າຍ ຫຼື ອຸປະກອນຕ່າງໆ. ລວມມີໄວຣັສ, ແຣນຊັມແວ ແລະ ໂທຈັນ.

- **ລະບົບປະຕິບັດການ**

ຊອບແວພື້ນຖານທີ່ເຮັດວຽກຢູ່ໃນຄອມພິວເຕີ, ແທັບເລັດ ແລະ ໂທລະສັບສະມາດໂຟນ, ຈຳເປັນຕ້ອງດຳເນີນການສຳລັບການຮັບແອັບພລິເຄຊັ່ນ ແລະ ຮາດແວເພີ່ມເຕີມ.

- **ຟິດຊິ່ງ**

ອີເມວ ຫຼື ຂໍ້ຄວາມຫຼອກລວງທີ່ມີລິ້ງໄປຫາເວັບໄຊທີ່ອາດມີມັນແວ ຫຼື ອາດຈະຫຼອກລວງໃຫ້ຜູ້ໃຊ້ເປີດເຜີຍຂໍ້ມູນທີ່ລະອຽດອ່ອນ (ເຊັ່ນ: ລະຫັດຜ່ານ) ຫຼື ການໂອນເງິນ.

- **ສະປາຍແວ**

ມັນແວປະເພດໜຶ່ງທີ່ຕິດຕັ້ງຢູ່ໃນອຸປະກອນໂດຍບໍ່ມີການຍິນຍອມເຫັນດີຂອງຜູ້ໃຊ້, ເກັບກຳຂໍ້ມູນ ແລະ ສົ່ງຂໍ້ມູນດັ່ງກ່າວໄປຫາພາກສ່ວນທີສາມ.

- **ສື່ມວນຊົນສັງຄົມ**

ເວັບໄຊທ໌ ແລະ ແອັບ, ເຊັ່ນ: Facebook, X ແລະ Instagram, ທີ່ອະນຸຍາດໃຫ້ຜູ້ຄົນສາມາດແບ່ງປັນ ແລະ ຕອບສະໜອງຕໍ່ເນື້ອຫາທີ່ສ້າງໂດຍຜູ້ໃຊ້ (ຂໍ້ຄວາມ, ຮູບພາບ ແລະ ວິດີໂອ).

- **ສະມາດໂຟນ**

ໂທລະສັບມືຖືທີ່ທັນສະໄໝທີ່ມີຟັງຊັນທີ່ເຮັດວຽກສັບຊ້ອນລວມທັງລະບົບປະຕິບັດການ Android ແລະ iOS.

- **Trojan**

ປະເພດຂອງມັນແວ, ທີ່ປອມຕົວເປັນຊອບແວທີ່ຖືກຕ້ອງຕາມກົດໝາຍ, ໃຊ້ເພື່ອເຂົ້າເຖິງອຸປະກອນຂອງຜູ້ເຄາະຮ້າຍ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

- **URL**

ເຄື່ອງມືລະບຸຕຳແໜ່ງຊັບພະຍາກອນສາກົນ ທີ່ຢູ່ໃນເວັບທົ່ວໂລກເຊັ່ນຊື່ໂດເມນ (ຕົວຢ່າງ: www.bbc.co.uk).

- **ໄວຣັສ**

ມັນແວປະເພດໜຶ່ງທີ່ຖືກອອກແບບມາເພື່ອແຜ່ເຊື້ອໄປຍັງໂປຣແກຣມຊອບແວທີ່ຖືກຕ້ອງຕາມກົດໝາຍ ແລະ ເຮັດຊ້ຳກັນໃນທົ່ວເຄືອຂ່າຍເມື່ອເປີດໃຊ້ງານໂປຣແກຣມເຫຼົ່ານີ້.

ອ່ານເພີ່ມເຕີມ

ຄຳແນະນຳຈາກສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕຣາລີ

- ລາຍງານອາດຊະຍາກຳທາງໄຊເບີ, ເຫດການ ຫຼື ຊ່ອງໂຫວ່
- ວິທີຮັກສາອຸປະກອນຂອງທ່ານໃຫ້ປອດໄພ
- ຮັກສາຄວາມປອດໄພໂທລະສັບມືຖືຂອງທ່ານ
- ຟິດຊິງ
- ການຫຼອກລວງ
- ຮັກສາຄວາມປອດໄພສື່ສັງຄົມຂອງທ່ານ
- ເຄັດລັບຄວາມປອດໄພສຳລັບສື່ສັງຄົມ ແລະ ແອັບຮັບສົ່ງຂໍ້ຄວາມ

ຄຳແນະນຳຈາກ NCSC ແລະ NPSA ຂອງອັງກິດ

- ການປົກປ້ອງປະຊາທິປະໄຕ
- ສື່ສັງຄົມ: ວິທີໃຊ້ໃຫ້ປອດໄພ
- ຄຳແນະນຳດ້ານຄວາມປອດໄພອຸປະກອນສຳລັບອົງກອນລວມທັງມືຖື
- ລາຍງານໄພຂົ່ມຂູ່ໃນຮ້ານຄ້າແອັບພລິເຄຊັນ.
- ຄວາມປອດໄພສ່ວນຕົວ ແລະ ຄວາມໝັ້ນຄົງສຳລັບບຸກຄົນທີ່ມີຄວາມສ່ຽງສູງ

ຄຳແນະນຳຈາກ NSA ຈາກສະຫະລັດ

- ແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດຂອງອຸປະກອນມືຖື

ການປະຕິເສດຄວາມຮັບຜິດຊອບ

ກະລຸນາຮັບຊາບວ່າຄຳແນະນຳນີ້ໃຫ້ຂໍ້ມູນທີ່ໄດ້ຮັບການກວດສອບແລ້ວໃນເວລາທີ່ເຜີຍແຜ່.

ບົດລາຍງານນີ້ດຶງຂໍ້ມູນມາຈາກອົງກອນໜ່ວຍງານຜູ້ຈັດທຳ ແລະ ແຫຼ່ງທີ່ມາຈາກອຸດສາຫະກຳ. ຜົນການຄົ້ນພົບ ແລະ ຂໍ້ສະເໜີແນະໃດໆ ທີ່ເກີດຂຶ້ນບໍ່ໄດ້ຈັດທຳຂຶ້ນດ້ວຍຄວາມຕັ້ງໃຈທີ່ຈະຫຼີກເວັ້ນຄວາມສ່ຽງທັງໝົດ ແລະ ປະຕິບັດຕາມຄຳແນະນຳຈະບໍ່ສາມາດຈັດຄວາມສ່ຽງທັງໝົດດັ່ງກ່າວໄດ້. ຄວາມເປັນເຈົ້າຂອງຄວາມສ່ຽງດ້ານຂໍ້ມູນຍັງຄົງຢູ່ກັບເຈົ້າຂອງລະບົບທີ່ກ່ຽວຂ້ອງຕະຫຼອດເວລາ.

ໃນປະເທດອັງກິດ, ຂໍ້ມູນນີ້ຖືກຍົກເວັ້ນພາຍໃຕ້ກົດໝາຍວ່າດ້ວຍເສລີພາບຂອງຂໍ້ມູນຂ່າວສານ 2000 (FOIA) ແລະ ອາດໄດ້ຮັບການຍົກເວັ້ນພາຍໃຕ້ກົດໝາຍຂໍ້ມູນຂ່າວສານອື່ນໆຂອງອັງກິດ.

ອ້າງອີງຄຳຖາມ FOIA ໃດໆກໍຕາມໄປທີ່ ncscinfoleg@ncsc.gov.uk.

ເອກະສານຊ້ອນທ້າຍ: ພົບຕົວຢ່າງ MOONSHINE ແລະ BADBAZAAR

ຕາຕະລາງນີ້ສະແດງລາຍການແອັບທີ່ໃຊ້ໃນແຄມເປນ MOONSHINE ແລະ BADBAZAAR ໃນຊ່ວງສອງປີຜ່ານມາ.

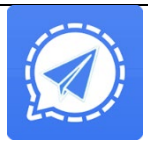
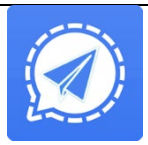
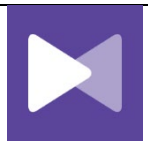
ຫຼາຍໆແອັບເຫຼົ່ານີ້ສະແດງໃຫ້ເຫັນຄວາມຄ້າຍຄືກັນຢ່າງຈະແຈ້ງຕໍ່ກັບແອັບທີ່ສ້າງຂຶ້ນ. ນີ້ແມ່ນແນວໂນ້ມທີ່ຈະເປັນເຕັກນິກ ນັກສະແດງໂດຍເຈດຕະນາເພື່ອ 'ຫຼອກລວງ' ຍີ່ຫໍ້ທີ່ມີຊື່ສຽງ.

ສິ່ງສຳຄັນທີ່ຈະຕ້ອງຮູ້ແມ່ນ, ຊື່ຂອງແອັບ, ຊື່ແພັກເກັດ ແລະ ໄອຄອນອາດຮຽນແບບ ຫຼື ກົງກັບແອັບພລິເຄຊັນທີ່ແທ້ຈິງ ແລະ ດັ່ງນັ້ນບໍ່ຄວນໃຊ້ສະເພາະເພື່ອກຳນົດວ່າອຸປະກອນໃດໜຶ່ງຕິດໄວຣັສ.

ຕາມທີ່ຮວມຢູ່ໃນພາກສ່ວນບັນເທົາຜົນກະທົບ, ທ່ານສາມາດສົ່ງແອັບໃນອຸປະກອນ Android ຂອງທ່ານໄປໃຫ້ Google ໂດຍການເປີດໃຊ້ງານ 'ປັບປຸງການກວດຫາແອັບທີ່ເປັນອັນຕະລາຍ', ເຊິ່ງຈະສະແກນແອັບໃນອຸປະກອນຂອງທ່ານທີ່ຕິດຕັ້ງ ຈາກນອກ Play Store.

ຊື່ແອັບ	ຊື່ແພັກເກດ	ໄອຄອນແອັບ
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	

FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

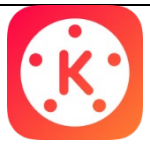
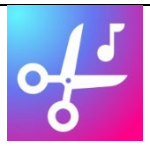
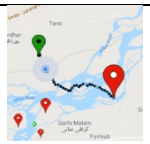
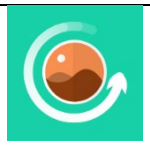
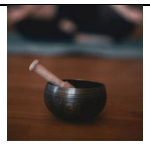
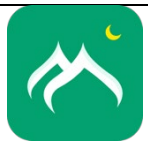
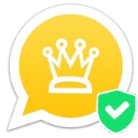
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

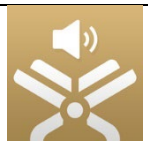
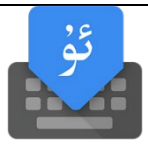
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

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

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

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

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

ئەسەرلەر ئاۋازلىق	com.ewlat.eserler	
قۇرئان ئاۋازلىق	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى ئۇيغۇرچە APK	com.uygur.apkstore	
قۇرئان ئۇيغۇرچە	com.c9.uyghurquran	
الكريم القرآن	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
كەرىم قۇرئان	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	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–{数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate