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

ஆலோசனை

BADBAZAAR மற்றும் MOONSHINE:

உய்குர், தைவானிய மற்றும் திபெத்திய குழுக்கள் மற்றும் சமூக ஆர்வலர்களைக் குறி வைக்கும் Spyware எனப்படும் உளவுமென்பொருள்

9 ஏப்ரல் 2025

BADBAZAAR மற்றும் MOONSHINE: உய்குர், தைவானிய மற்றும் திபெத்திய குழுக்கள் மற்றும் சமூக ஆர்வலர்களைக் குறி வைக்கும் Spyware எனப்படும் உளவுமென்பொருள்

இரண்டு உளவுமென்பொருள் வகைகளிலிருந்து அதிக ஆபத்தில் உள்ளவர்களுக்கான புதிய தகவல் மற்றும் தணிப்பு நடவடிக்கைகளை NCSC மற்றும் அதன் கூட்டாளர்கள் வெளியிடுகிறார்கள்.

தொகுப்பு

இந்த ஆலோசனை UKயின் Cyber League அமைப்பின் ஆதரவுடன், the National Cyber Security Centre (NCSC UK) என்ற தேசிய சைபர் பாதுகாப்பு மையம் மற்றும் பின்வரும் சர்வதேச கூட்டாளர்களால் கூட்டாகத் தயாரிக்கப்பட்டுள்ளது:

- **ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையம், ஆஸ்திரேலிய சமிக்ஞைகள் இயக்குநரகத்தின் ஒரு பகுதி**
- **சைபர் பாதுகாப்பிற்கான கனேடிய மையம், தகவல் தொடர்பு பாதுகாப்பு ஸ்தாபனத்தின் ஒரு பகுதி**
- **ஜெர்மன் ஃபெடரல் புலனாய்வு சேவை**
- **ஜெர்மன் ஃபெடரல் அரசியலமைப்பு பாதுகாப்பு அலுவலகம்**
- **நியூசிலாந்து தேசிய சைபர் பாதுகாப்பு மையம், அரசாங்க தகவல் தொடர்பு பாதுகாப்பு பணியகத்தின் ஒரு பகுதி**
- **அமெரிக்காவின் குற்றப் புலனாய்வுத்துறை - Federal Bureau of Investigation (FBI)**
- **அமெரிக்க தேசிய பாதுகாப்பு நிறுவனம் (NSA)**

தைவான், திபெத், சின்ஜியாங் உய்குர் தன்னாட்சி பிராந்தியம், ஜனநாயக இயக்கங்கள் மற்றும் ஃபாலுன் காங் உள்ளிட்ட விடயங்களுடன் தொடர்புடைய தனிநபர்களுக்குத் தீங்கிழைக்கும் இணைய நடவடிக்கைகள் ஏற்படுத்தும் வளர்ந்து வரும் அச்சுறுத்தல் குறித்து விழிப்புணர்வை ஏற்படுத்துவதே இதன் நோக்கம்.

இந்த ஆலோசனையில் சீன அரசுக்கு ஆர்வமுள்ள ஸ்மார்ட்ஃபோன்கள் உள்ளிட்ட மொபைல் சாதனங்களின் தரவை குறி வைக்க, BADBAZAAR மற்றும் MOONSHINE எனப்படும் உளவுமென்பொருளைப் பயன்படுத்தி தீங்கிழைப்பவர்கள் பயன்படுத்தும் நுட்பங்களை விவரிக்கும் இரண்டு

விரிவான ஆய்வுகள் அடங்கும். தங்களையும் தங்கள் சாதனங்களையும் தங்கள் தரவையும் ஒருவர் பாதுகாக்க உதவும் வழிகாட்டுதலாகவும் இது அமைகிறது.

இந்த ஆலோசனையுடன், full technical detail with separate guidance என்ற தொழில்நுட்ப விவரங்களையும் NCSC வெளியிட்டுள்ளது.

இதனால் யாருக்கு ஆபத்து?

BADBAZAAR மற்றும் MOONSHINE ஆகியவை குறிப்பாக சீன அரசால் அவர்களின் உள்நாட்டு அதிகாரம், இலட்சியங்கள் மற்றும் உலகளாவிய நற்பெயருக்கு அச்சுறுத்தலாகக் கருதப்படும் தலைப்புகளுடன் தொடர்புடையவர்களைக் குறி வைப்பதை, இந்த ஆவணத்தை எழுதிய அமைப்புகள் மற்றும் தொழில்துறை பங்காளிகள் கவனித்துள்ளனர். அவர்கள் மட்டும் தான் ஆபத்துக்குள்ளானவர்கள் என்று இல்லாவிட்டாலும், பட்டியலிடப்பட்டிருக்கும் பின்வரும் அமைப்புகளுடன் தொடர்புடையவர்கள் மிகவும் ஆபத்தில் உள்ளனர்:

- **தாய்வானின் விடுதலை**
- **திபெத்திய உரிமைகள்**
- **உய்குர் முஸ்லிம்கள் மற்றும் சீனாவின் சிஞ்சியாங் உய்குர் தன்னாட்சிப் பகுதியில் வாழும் பிற இன சிறுபான்மையினர்**
- **(ஹொங்கொங் உட்பட) ஜனநாயகத்திற்காகக் குரல் கொடுப்பவர்கள்**
- **ஃபாலுன் காங் ஆன்மீக இயக்கம்**

அரசு சாரா நிறுவனங்கள் (NGO), பத்திரிகையாளர்கள், வணிகங்கள் மற்றும் இந்த குழுக்களுக்காக வாதிடும், அடையாளம் காணும் அல்லது வேறு விதமாக பிரதிநிதித்துவப்படுத்தும் தனிநபர்களும் இதில் அடங்குவர். இந்த உளவுமென்பொருள் இணையத்தில் கண்மூடித்தனமாகப் பரவுவதனால், மேற்கூறிய பாதிக்கப்பட்டவர்களுக்கு அப்பால், இது மற்றைய பயனர்களிடமும் பரவும் அபாயம் அதிகமாக உள்ளது.

BADBAZAAR மற்றும் MOONSHINE உளவுமென்பொருளின் குறிப்பிட்ட அச்சுறுத்தலுக்கு ஆபத்தில் உள்ளவர்கள் அதற்குத் திறம்படப் பதிலளிக்க உதவுவதை நோக்கமாகக் கொண்டு இந்த ஆலோசனை எழுதப்பட்டுள்ளது. பரிந்துரைக்கப்பட்ட தணிப்பு நடவடிக்கைகள், பரந்த இணைய பாதுகாப்பு ஆலோசனையையும் கருத்தில் கொண்டு கொடுக்கப்படுகின்றன. அவற்றைத் தனியாகப் பார்ப்பதைத் தவிர்க்கவும்.

இந்த ஆலோசனையில் குறிப்பிடப்பட்டுள்ள வழிகாட்டுதலைப் பயனர்கள் பின்பற்றுவதன் மூலம், உளவுமென்பொருள் அவர்கள் மொபைல் சாதனங்கள் மற்றும் தரவுகளில் தொற்றும் அபாயத்தைக் குறைக்க முடியும்.

அச்சுறுத்தல்

MOONSHINE மற்றும் BADBAZAAR ஆகியவை ட்ரோஜன்களுக்கு எடுத்துக்காட்டுகள். முறையாக app storeகள் அல்லது ஆன்லைன் கோப்பு பகிர்வு சேவைகளிலிருந்து பதிவிறக்கம் செய்யக்கூடிய செயலிகளுக்குள் இந்த தீங்கிழைக்கும் செயல்பாடுகள் மறைத்து வைக்கப்பட்டுள்ளன.

ஒரு பயனரை ஏமாற்றி அவரது சாதனத்தில் பதிவிறக்கம் செய்து நிறுவும் வகையில் இந்த செயலிகள் வடிவமைக்கப்பட்டுள்ளன. அந்த செயலி நிறுவப்பட்டதும், சாதனத்தில் உள்ள பாதிப்புக்குள்ளாகக்கூடிய பகுதிகளை அந்த செயலி பயன்படுத்தி, அங்கீகரிக்கப்படாத செயல்பாடுகளைச் செய்ய சாதனத்திலிருந்து தகவலை அணுகவும் பதிவிறக்கவும் செயலியின் அனுமதிகளைப் பயனர் நம்பிக்கையுடன் வழங்க வழி செய்யலாம். அவற்றுள் அடங்குபவை:

- **நிகழ்நேர கண்காணிப்பு உட்பட இருப்பிடத் தரவு**
- **ஒலிவாங்கி மற்றும் கமரா ஆகியவற்றின் அணுகல்**
- **செய்திகள், புகைப்படங்கள் மற்றும் சாதனத்தில் சேமிக்கப்பட்ட பிற கோப்புகள்**
- **சாதனத் தகவல் மற்றும் பல**

அதன் பின்னர், ஆபத்தில் உள்ள குழுக்களில் உள்ளவர்களின் நியாயமான விருப்பங்களைப் பயன்படுத்தி, அவர்களின் தரவை அணுகவும், முடிந்தவரை பலரைப் பாதிக்கவும் செய்கிறார்கள். அவர்களின் சொந்த மொழிகளை ஆதரிக்கும் செயலிகள் அல்லது சீனாவின் திபெத்திய பகுதிகள் அல்லது சின்ஜியாங் போன்ற இடங்களின் குறிப்பிட்ட உள்ளடக்கத்தைக் கொண்டிருப்பதன் மூலம் பாதிக்கப்பட்டவர்களை ஈர்க்கும் செயலிகளை வடிவமைத்து அதனை அவர்கள் செய்கிறார்கள்.

இந்த ஆலோசனையில் உள்ள விரிவான ஆய்வுகள் TibetOne மற்றும் Uyghur Quran செயலிகள் உட்பட சில எடுத்துக்காட்டுகளை இதற்கு வழங்குகின்றன.

ஆன்லைன் மன்றங்களில் இவர்கள் செயற்படுகிறார்கள். அந்த மன்றங்களில் குறிப்பிட்ட நோக்கம் கொண்ட பயனர்கள் பலர் இணைந்திருப்பதால் அவர்கள் அனைவரது கருவிகளும் பாதிக்கப்படுவதற்கான வாய்ப்பு அதிகரிக்கிறது. திபெத் தொடர்பான Telegram channelகள் மற்றும் Reddit மன்றங்களில் உளவுமென்பொருட்கள் வேண்டுமென்றே பகிர்வது அவதானிக்கப்பட்டுள்ளது. இந்த ஆலோசனையில் வழங்கப்பட்டுள்ள விரிவான ஆய்வுகளில் சில எடுத்துக்காட்டுகள் தரப்பட்டுள்ளன.

தீங்கிழைக்கும் செயலிகள் பெரும்பாலும் Android இல் APK கோப்புகள் போன்ற முழுமையான கோப்புகளாகப் பகிரப்படுகின்றன, அவற்றை பயனர்கள் பதிவிறக்கம் செய்து நிறுவ வேண்டும். Google Play Store மற்றும் Apple App Store போன்ற அதிகார பூர்வ தளங்களில் பதிவேற்றுவதன் மூலம் அல்லது முன்னர் தீங்கற்ற செயலிகளில் தீங்கிழைக்கும் செயலியைச் சேர்ப்பதன் மூலம் தீங்கிழைப்பவர்கள் தங்கள் உளவுமென்பொருளை மிகவும் முறையானதாகத்

தோன்றச் செய்ய முயற்சிக்கின்றனர். அதிகார பூர்வ இடங்களில் பாதுகாப்பு அம்சங்கள் மற்றும் சோதனை செயல்முறைகள் உள்ளன. அதனால், இந்த தந்திரோபாயம் வெற்றி பெறுவது குறைவாகவே உள்ளது. இது அதிகார பூர்வ கடைகளிலிருந்து பெறப்படும் செயலிகளைப் பாதுகாப்பானதாக்குகிறது என்றாலும் இந்த ஆலோசனையில் வழங்கப்பட்டுள்ள விரிவான ஆய்வுகளில் குறிப்பிட்டது போலவும் NCSC இன் App Store Threat Reportஇல் நிரூபிக்கப்பட்டுள்ளபடியும், அவை எப்போதும் பாதுகாப்பானதாக அமைவதில்லை.

அச்சுறுத்தல்களிலிருந்து உங்களைப் பாதுகாக்க, இந்த ஆலோசனையில் கோடிட்டுக் காட்டப்பட்டுள்ள பின்வரும் நான்கு உதவிக் குறிப்புகளைப் பின்பற்றுவது உதவும்.

மேலும் விரிவான ஆலோசனைக்கு, தணிப்புகள் பகுதியைப் பார்க்கவும்.

விரிவான ஆய்வுகள்

இந்த இரண்டு விரிவான ஆய்வுகளும் MOONSHINE மற்றும் BADBAZAAR எவ்வாறு செயல்படுகின்றன என்பதையும், தீங்கிழைப்பவர்கள் எவ்வாறு ஆபத்தில் உள்ளவர்களை குறி வைக்கிறார்கள் என்பதையும் விளக்குகின்றன.

விரிவான ஆய்வு ஒன்று: MOONSHINE

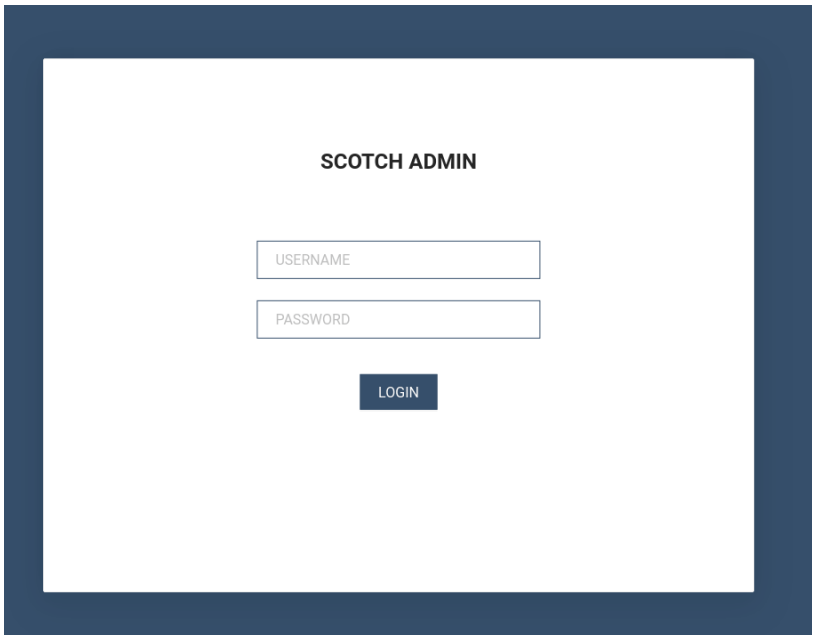
MOONSHINE என்ற Android உளவுமென்பொருள் திபெத்திய குழுக்களை குறி வைப்பதாக 2019ஆம் ஆண்டில் Citizen Lab அறிவித்தது. முறையான செயலியாக MOONSHINE காட்டிக் கொண்டு, அதை நிறுவ பாதிக்கப்பட்டவர்களைக் கவர்ந்திழுக்கிறது. அது Telegram சேனல்கள் மூலம் பகிரப்பட்டு, அதன் இணைப்புகள் WhatsApp வழியாகப் பகிரப்பட்டுள்ளது.

MOONSHINE விரிவான கண்காணிப்பு திறன்களைக் கொண்டுள்ளது. அதில்:

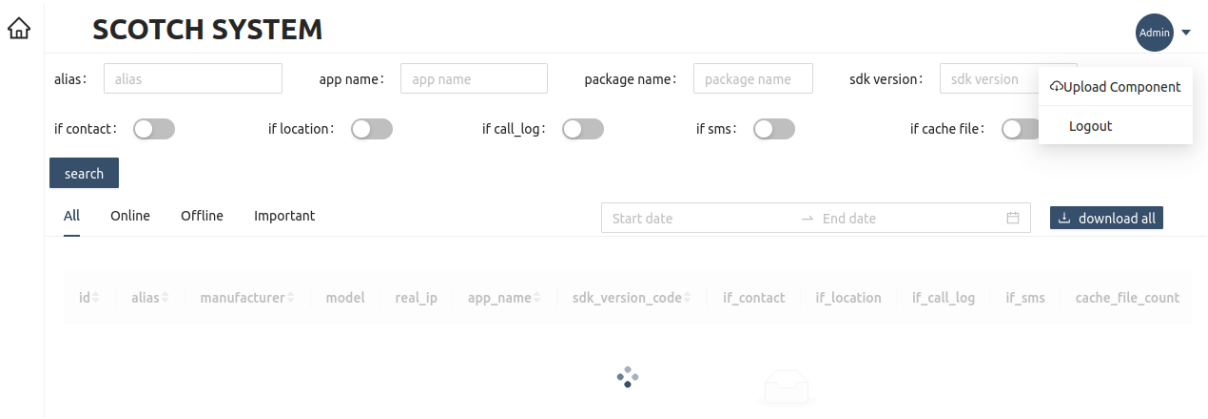
- **நிகழ்நேர கண்காணிப்பு உட்பட இருப்பிடத் தரவு**
- **நேரடி ஆடியோ மற்றும் புகைப்பட பிடிப்பு**
- **சாதனத்தில் இருந்து கோப்புகளைப் பதிவிறக்குகிறது**
- **சாதனத்தின் தகவல்களை மீட்டெடுக்கிறது**
- **சாதனத்தில் ஆடியோவை இயக்குகிறது**

உய்குர்களைக் குறிவைக்க MOONSHINE எவ்வாறு பயன்படுத்தப்படுகிறது என்பதற்கு,
‘Audio Quran.apk’ என மொழிபெயர்க்கப்பட்ட **'قۇرئان ئاۋازلىق.apk'** என்ற செயலி ஒரு எடுத்துக்காட்டு. குர்ஆன் செயலியைச் சுட்டிக்காட்டும் வகையில், உய்குர் மொழியில் கோப்பு பெயர் இடப்பட்டிருப்பதானது, உய்குர் முஸ்லிம்களின் கவனத்தை ஈர்ப்பதற்காகவே செய்யப்பட்டிருக்கலாம்.

செயலி நிறுவப்பட்டதும், பாதிக்கப்பட்டவர்களின் சாதனங்களிலிருந்து தீங்கிழைப்பவர்கள் தகவல்களை சேகரிக்க முடியும். இந்தத் தகவலை, 'SCOTCH ADMIN' குழு வழியாக அணுகலாம்.



செயலிக்குள் நுழைந்ததும், கீழே உள்ள படத்தில் காட்டப்பட்டுள்ள பக்கத்தைத் தீங்கிழைப்பவர்கள் அணுகலாம். பாதிக்கப்பட்ட சாதனங்களின் விவரங்கள் மற்றும் பாதிக்கப்பட்ட சாதனங்களை தீங்கிழைப்பவர்கள் அணுகும் அளவை இந்தப் பக்கம் காட்டுகிறது:



சேகரிக்கப்பட்ட தரவை, தீம்பொருள் மேலாண்மைப் பலகை காட்டுகிறது, அவற்றுள் பின்வருவன அடங்குகின்றன:

- **சாதனத்திற்கான அணுகல் நிலை**
- **குறுஞ்செய்திகள்**
- **அழைப்புகளின் பதிவுகள்**
- **இருப்பிடத் தரவு**
- **சாதனத்தின் தகவல்**

Cyber League உடன் இணைந்து, NCSC அமைப்பு, Trend Micro வழங்கிய தொழில்துறை அறிக்கையை அடிப்படையாக கொண்டு, 'UPSEC' கொண்ட HTML

தலைப்புள்ள உள்நுழைவு பலகையிலுள்ள விடயங்களும், MOONSHINE உளவுமென்பொருளிலுள்ள திருடும் செயற்பாடும் ஒன்றுடன் ஒன்று இணைந்து இருப்பதை கண்டுபிடித்துள்ளது. முழு விபரங்கள் இத்துடன் இணைக்கப்பட்டுள்ள தொழில்நுட்ப ஆலோசனையில் உள்ளன.

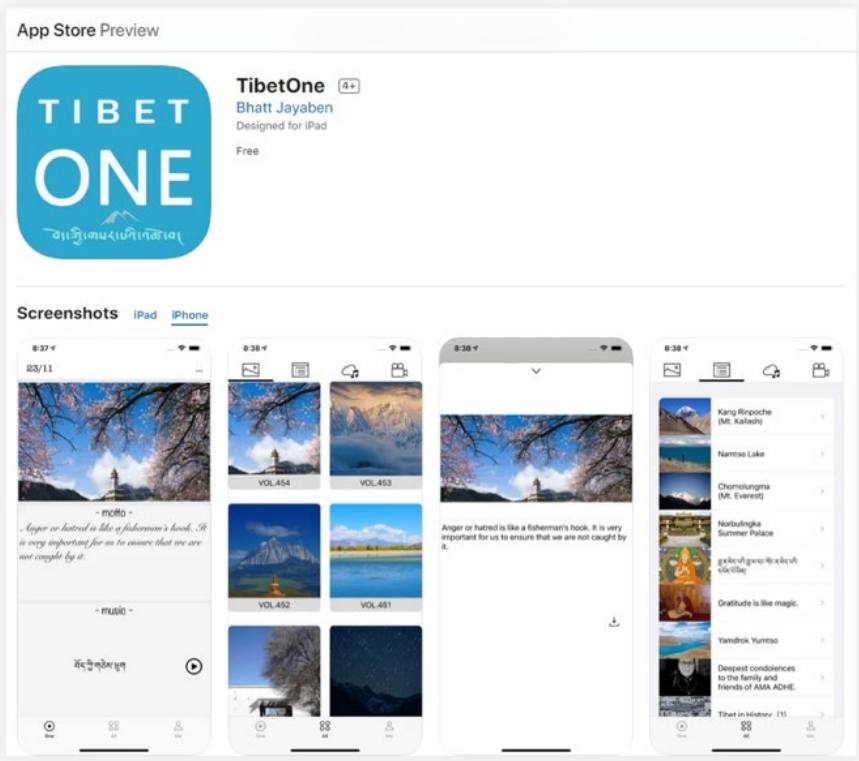
UPSEC என்பது 'Sichuan Dianke Network Security Technology Co. Ltd' என்பதைக் குறிக்கிறது என்று Intelligence Online குறிப்பிடுகிறது. இந்த ஆவணத்தை வெளியிடும் அமைப்புகள் இந்த அறிக்கையைச் சரிபார்க்கவில்லை.

விரிவான ஆய்வு இரண்டு: BADBAZAAR

BADBAZAAR என்பது உய்குர்கள், திபெத்தியர்கள் மற்றும் தைவானியர்களைக் குறி வைக்கும் iOS மற்றும் Android வகை மொபைல் தீம்பொருளாகும். இந்தத் தீம்பொருள் சமூக ஊடகத் தளங்கள் மற்றும் அதிகார பூர்வ App storeகள் வழியாக பரவியுள்ளது.

'TibetOne' என்ற செயலியின் மூலம் திபெத்தியர்களைக் குறிவைக்க, BADBAZAAR பயன்படுத்தப்பட்டுள்ளது என்பதை Lookout மற்றும் Volexity தெரிவிக்கின்றன. **'TibetOne'** என்பது தீங்கிழைப்பவர்களால் உருவாக்கப்பட்ட iOS செயலியாகும். இது சாதனத் தகவல் மற்றும் இருப்பிடத் தரவை அணுகும் திறனைக் கொண்டுள்ளது. இந்த செயலி, 2021ஆம் ஆண்டு டிசம்பர் மாதம் Apple App Storeஇல் பதிவேற்றப்பட்டது. ஆனால், தற்போது அது அங்கே கிடைக்காது. தீம்பொருளை மேலும் பரப்ப, **'tibetanphone'** என்ற Telegram சேனலில் அந்த செயலியை தீங்கிழைப்பவர்கள் விளம்பரப்படுத்தினர்.

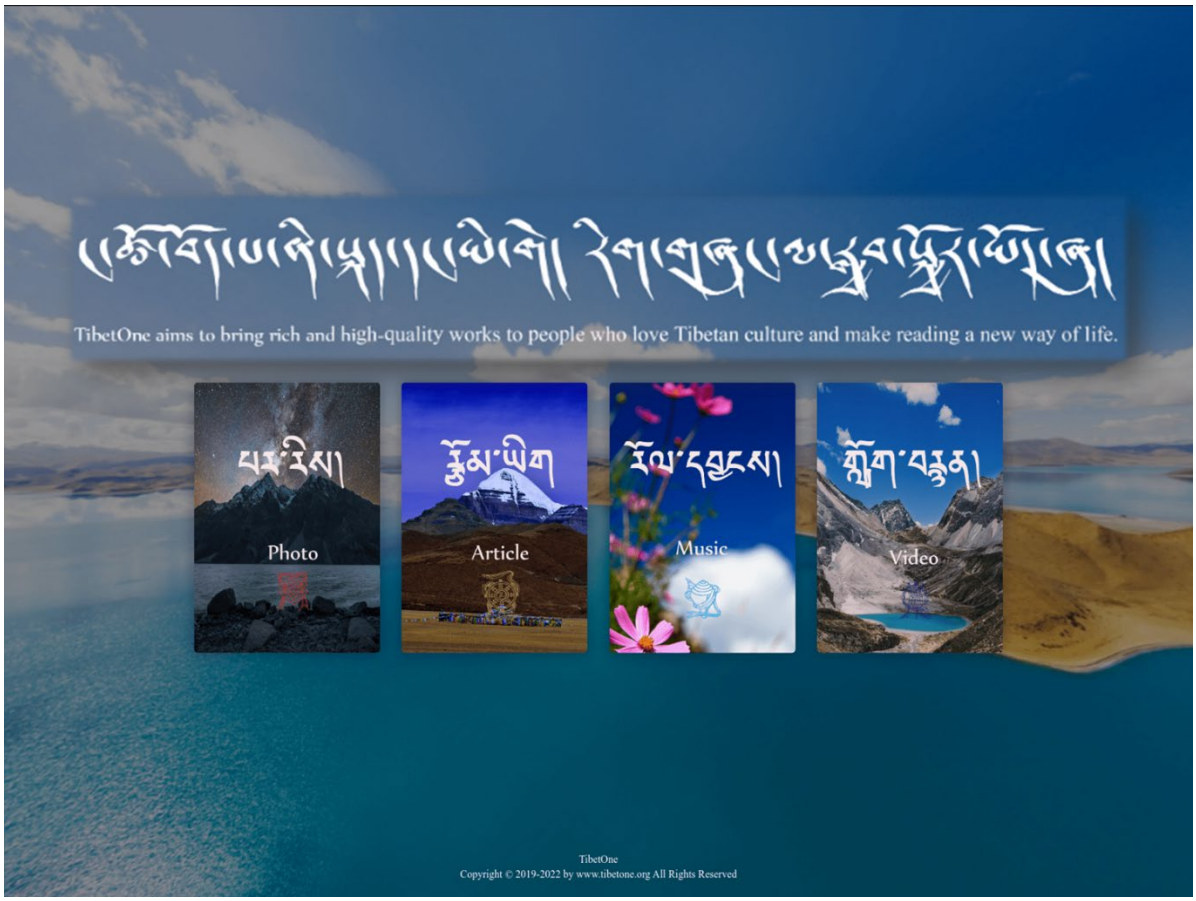
TibetOne



படம் *1: Apple App Store* இல் *TibetOne* செயலியின் பக்கம். தற்போது அந்த செயலி அங்கிருந்து நீக்கப்பட்டுள்ளது.

படம் *2:* Telegram சேனலில் பகிரப்பட்ட *TibetOne* செயலி.

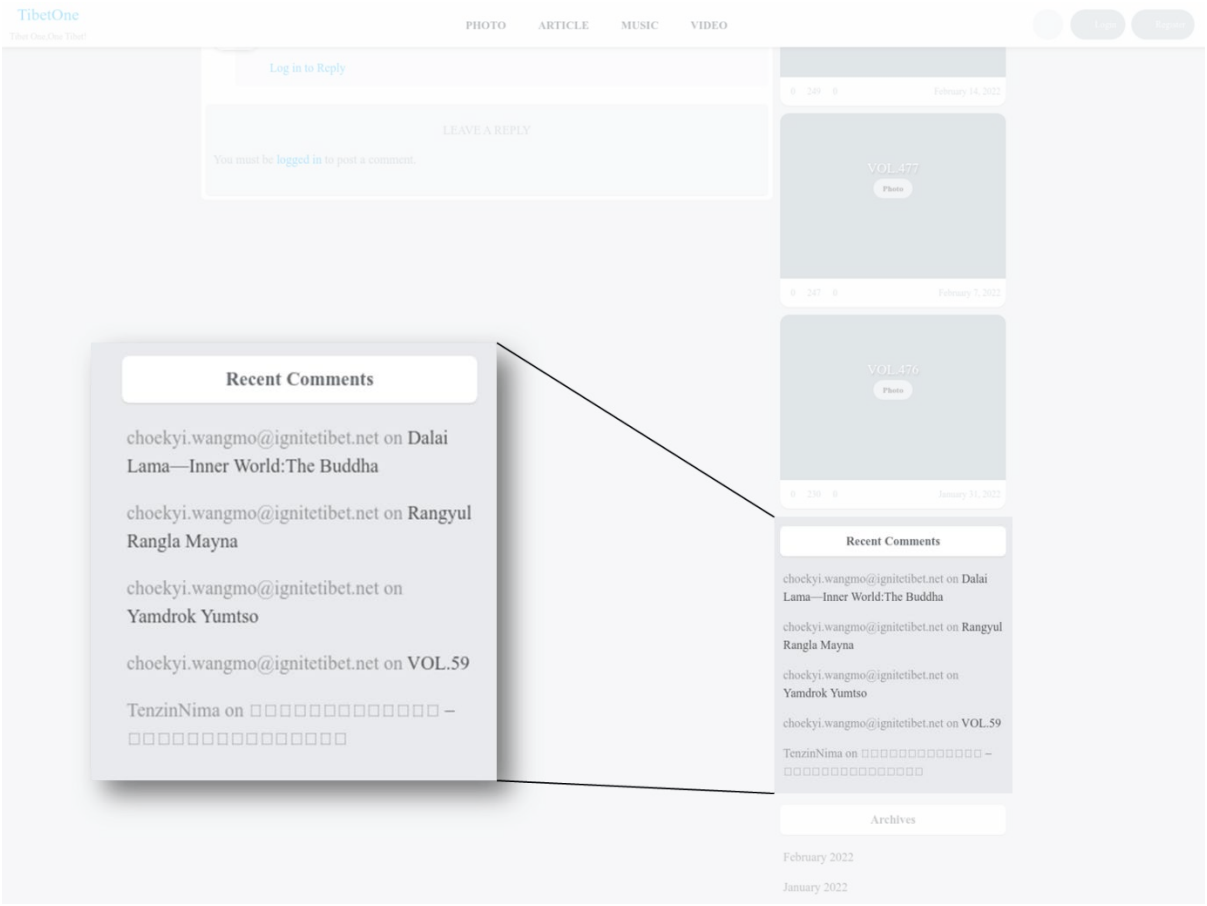
இந்த செயலிக்கு சட்ட பூர்வமான அங்கீகாரத்தை சேர்ப்பதற்காக, தீங்கிழைப்பவர்கள் **‘tibetone[.]org’** என்ற வலைத்தளத்தையும் உருவாக்கினார்கள். 'திபெத்திய கலாச்சாரத்தை நேசிக்கும் மற்றும் வாசிப்பை ஒரு புதிய வாழ்க்கை முறையாக மாற்றும் மக்களுக்கு பணக்கார மற்றும் உயர்தர படைப்புகளை கொண்டு வருவதாக ’தன்னை அதில் விவரித்தது.



படம் *3:* **‘tibetone[.]org’** இன் முகப்புப்பக்கம்

தொடர்புடைய பகுதிகளை தெளிவு படுத்தும் வகையில் இந்த படம் திருத்தப்பட்டுள்ளது.

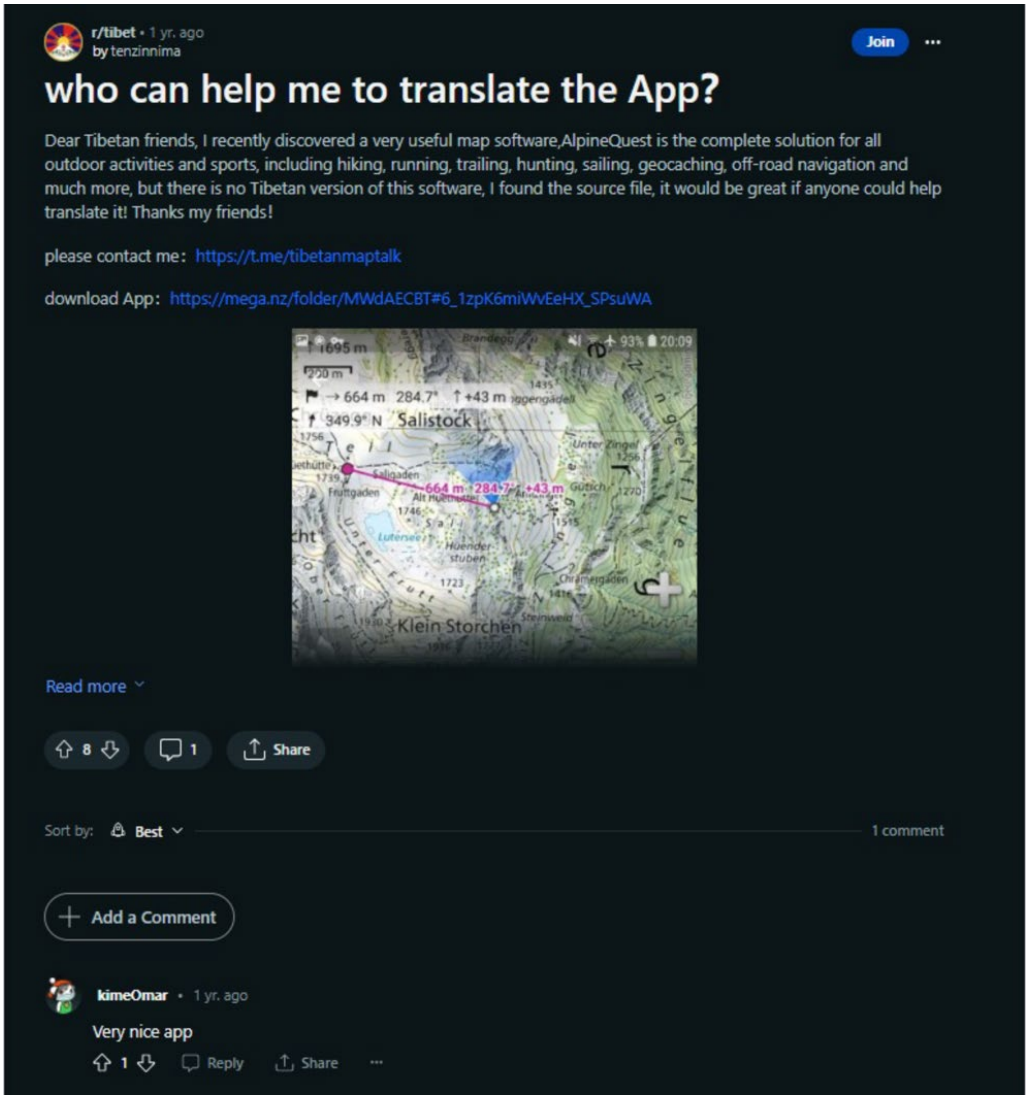
இந்த வலைத்தளத்தில் பயனர்கள் கருத்துகளை வெளியிட அனுமதிக்கும் ஒரு பக்கம் இருந்தது. '**choekyi.wangmo@ignitetibet.net**' என்ற மின்னஞ்சல் முகவரியால் இடப்பட்ட ஒரு கருத்து, தீங்கிழைப்பவரால் கட்டுப்படுத்தப்படுவதாகவும், அவர் ‘**Choekyi Wangmo**’ என்பவரை ஆள்மாறாட்டம் செய்திருக்க வாய்ப்புள்ளது எனவும் நம்பப்படுகிறது. ‘Choekyi Wangmo’ என்பவர், Tibetan Centre of Human Rights and Democracyஆல் திபெத்தை ஆதரிக்கும் போராளியாக பட்டியலிடப்பட்டுள்ளார். இந்த செயலி உண்மையிலேயே திபெத்திய சுதந்திரத்திற்காக வாதிடுகிறது என்ற தோற்றத்தை அளிக்கும் மற்றொரு முயற்சியாக இருக்கலாம்.



படம் *4:* தீங்கிழைப்பவர்களால் கட்டுப்படுத்தப்படுவதாக நம்பப்படும் பயனர்களின் கருத்துகளைக் காட்டும் *'tibetone[.]org '* பக்கம்.

தொடர்புடைய பகுதிகளை தெளிவு படுத்தும் வகையில் இந்த படம் திருத்தப்பட்டுள்ளது.

'**TenzinNima**' என்பது இந்தத் தளத்தில் பின்னூட்டல் கருத்துகளைப் பகிர்ந்து கொண்ட மற்றொரு பயனர் பெயர். Telegram சேனலில் **'Tibetanmaptalk'ஐ** விளம்பரப்படுத்த Redditடிலும் இந்த பயனர் பெயர் பயன்படுத்தப்படுகிறது என்று Volexity தெரிவித்துள்ளது. Android சாதனங்களில் கிடைக்கும் வழிசெலுத்தல் செயலியான **'AlpineQuest'** இல் தீங்கிழைக்கும் செயலியைப் பதிவிறக்குவதற்கான இணைப்பு இதில் அடங்கும். வழங்கப்பட்ட பதிவிறக்க இணைப்பு Mega எனப்படும் மூன்றாம் தரப்பு கோப்பு பகிர்வு சேவைக்கானது.



படம் *5:* தீங்கிழைப்பவர்களால் கட்டுப்படுத்தப்படுவதாக நம்பப்படும் கணக்கு மூலம் தீங்கிழைக்கும் செயலியை *Reddit*இல் பகிரப்பட்ட ஒரு இடுகை விளம்பரப்படுத்துகிறது.

இந்த இடுகையில் கருத்து தெரிவித்த **'KimeOmar'** என்று அழைக்கப்படும் ஒரு பயனரும் Reddit உடன் தொடர்புடைய இன்னொரு மன்றத்தில் தீங்கிழைக்கும் செயலியைப் பகிர்வது கவனிக்கப்பட்டுள்ளது என்றும் Volexity குறிப்பிடுகிறது. தீங்கிழைப்பவர்கள் தங்கள் இடுகைகள் முறையானதாகத் தோன்றச் செய்ய பல சமூக ஊடக சுய விவரங்களைப் பயன்படுத்துகிறார்கள் என்பதை இது குறிக்கலாம்.

மதிப்பீடு

BADBAZAAR மற்றும் MOONSHINE இரண்டும், குறிப்பாக உய்குர், தைவானிய மற்றும் திபெத்திய குழுக்களைக் குறி வைக்க, பல சமூக பொறியியல் முறைகளைப் பயன்படுத்துகின்றன. அதாவது:

- இந்த சமூகங்களுக்கு ஆர்வமுள்ள செயலிகளில் மறைந்திருந்து தாக்கக்கூடிய, உய்குர் மொழி குர்ஆன் செயலி போன்றவை, கிட்டத்தட்ட நிச்சயமாக இலக்கு வைத்து பாதிக்கப்பட்டவர்களுக்கு ஏற்ற வகையில் வடிவமைக்கப்பட்டுள்ளது
- உத்தியோக பூர்வ app storeகளில், இப்படி மறைத்து வைக்கப்பட்டுள்ள செயலிகளை சேர்ப்பதன் மூலம், அவை சட்டபூர்வமானவை என்ற உணர்வை அளிக்கிறது. மேலும் குழு அரட்டைகளில் அது குறித்துப் பகிர்வதன் மூலம், இந்த சமூகங்களுக்குள் நம்பகத்தன்மையை உருவாக்கி, அவர்களை சுரண்டுவதை நோக்கமாகக் கொண்டுள்ளது

BADBAZAAR மற்றும் MOONSHINE ஆகியவை சேகரிக்கும் தரவுகள் நிச்சயமாக சீன அரசுக்கு மதிப்பு மிக்கதாக இருக்கும். BADBAZAAR மற்றும் MOONSHINE ஆகியவை உய்குர், திபெத்திய மற்றும் தைவானியர்களைக் குறிவைத்துள்ளதாகப் பார்க்கப்பட்டாலும், சீனாவில் உள்ள பிற சிறுபான்மை குழுக்களை குறி வைக்கும் பிற தீம்பொருள்களும் உள்ளன. ஆட்சி நிலைத் தன்மையை அச்சுறுத்தும் காரணங்களை ஆதரிப்பதாகக் கருதப்படும் சீனா மற்றும் வெளிநாடுகளில் உள்ள co-sealing நாடுகளின் குடிமக்கள், BADBAZAAR மற்றும் MOONSHINE போன்ற மொபைல் தீம்பொருட்களால் நிச்சயமாக அச்சுறுத்தலுக்கு உள்ளாகியுள்ளனர். இருப்பிடம், ஆடியோ மற்றும் புகைப்படத் தரவைப் பிடிக்கும் திறன், கண்காணிக்கப்படுபவரின் செயல்பாடு குறித்த நிகழ்நேர தகவல்களை வழங்குவதன் மூலம் எதிர்காலத்தில், கண்காணிப்பு மற்றும் துன்புறுத்தல் நடவடிக்கைகளுக்கு வாய்ப்பளிக்கிறது.

மொபைல் செயலி பயனர்களுக்கான தணிப்பு நடவடிக்கைகள்

விரிவான ஆய்வுகளில் விவரிக்கப்பட்டுள்ள அச்சுறுத்தல்களுக்கு எதிராகப் பாதுகாக்க, பின்வரும் பாதுகாப்பு நடைமுறைகளை, இதை பிரசுரிக்கும் அமைப்புகள் ஊக்குவிக்கின்றன. NCSCயின் சிறந்த நடைமுறை வழிகாட்டுதல்களுடன் இந்த பரிந்துரைகள் தரப்படுகின்றன. ஆஸ்திரேலியா மற்றும் அமெரிக்காவில் உள்ளவர்களுக்கான, சிறந்த நடைமுறை வழிகாட்டுதலுக்கான இணைப்புகளுக்கு 'மேலும் படித்தல்' என்ற பகுதியைப் பார்க்கவும்.

உங்கள் சாதனத்தைப் பாதுகாப்பாக வைத்திருங்கள்

- **Googleஇன்** Play Store **அல்லது** Appleஇன் App Store **போன்ற அதிகார பூர்வ** App Store**களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கவும்.** Google இன் Play Store மற்றும் Apple இன் App Store முதலில் செயலியில் வைரஸ்கள் இருக்கின்றனவா என்பதை சோதித்துப் பார்த்த பின்னரே, நீங்கள் பதிவிறக்குவது பாதுகாப்பானது என்று உங்களுக்கு அதிக உத்தரவாதம் அளிக்கிறது. நம்பகமான கடைகளிலிருந்து வரும் செயலிகள் ஆபத்தைக் கொண்டிருக்கும் வாய்ப்பு இருக்கலாம், ஆனால் பிற மூலங்களிலிருந்து பதிவிறக்கம் செய்யப்படும் செயலிகளுக்கு எந்த பாதுகாப்பும் இருக்காது. App storeகளில் இருக்கும் அச்சுறுத்தல்கள் குறித்து NCSC ஒரு அறிக்கை வெளியிட்டுள்ளது: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **உங்கள் சாதனத்தையும் செயலிகளையும் புதுப்பித்த நிலையில் வைத்திருங்கள்.** உங்கள் செயலிகள் மற்றும் சாதன மென்பொருளுக்கு புதுப்பித்தல்கள் கிடைத்தவுடன் அவற்றை நிறுவவும். உங்கள் சாதனத்தின் அமைப்புகளில் "தானியங்கு புதுப்பிப்புகள்" கிடைக்குமானால் அவற்றை இயக்கவும். அப்படி செய்தால், புதுப்பித்தல் குறித்து நீங்கள் நினைவில் கொள்ள வேண்டியதில்லை. அறியப்பட்ட வைரஸ்கள் மற்றும் பிற வகையான தீம்பொருளிலிருந்து பாதுகாக்க, ஆன்லைனில் பாதுகாப்பாக இருப்பது பற்றிய NCSC வழிகாட்டலைப் பார்க்கவும். புதுப்பித்தல்கள் பெரும்பாலும் மேம்பாடுகள் மற்றும் புதிய அம்சங்களை உள்ளடக்குகின்றன: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **உங்கள் சாதனத்தை 'jailbreak' அல்லது 'root' செய்ய வேண்டாம். ஏனெனில்**, இது செயலிகளைப் புதுப்பிக்கப்படாத நிலையில் வைத்திருந்து பாதுகாப்புக் கட்டுப்பாடுகளைத் தவிர்த்து பாதுகாப்பற்ற தன்மையை ஏற்படுத்தும். இது சாதனத்தை தாக்குதல்களுக்கு மிகவும் பாதிக்கப்படக் கூடியதாக ஆக்குகிறது. இது குறித்த NCSC வழிகாட்டலைப் பார்க்கவும்: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

உங்கள் செயலிகளை நிர்வகிக்கவும்

- **உங்கள் செயலிகள் மற்றும் அவற்றிற்கு வழங்கப்பட்டுள்ள அனுமதிகளை மதிப்பாய்வு செய்யவும்**. உங்கள் பயன்பாட்டிற்கு இனி தேவையில்லை என்றால், அந்த செயலியை நீக்கவும். தீம்பொருள் பெரும்பாலும் பாதுகாக்கப்பட்ட கோப்புகள், கமராக்கள் மற்றும் ஒலிவாங்கிகள் போன்ற புறக் கருவிகளை அணுகுவதற்காக வடிவமைக்கப்பட்டுள்ளதால், தரவு வெளிப்பாட்டைக் குறைக்க செயலியின் பயன்பாட்டு அனுமதிகளைக் கட்டுப்படுத்தவும்.
  - Apple பயனர்கள் பயன்பாட்டு அனுமதிகளை சரிபார்க்க: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - Android பயனர்கள் பயன்பாட்டு அனுமதிகளை சரிபார்க்க: https://support.google.com/android/answer/9431959?hl=en-GB

- **அறியப்படாத செயலிகளைத் தானாகவே Googleற்கு அனுப்புதல்.** நீங்கள் Android பயனராக இருந்து, Google இன் Play Storeஇல் இல்லாத செயலியைப் பதிவிறக்கியிருந்தால், 'Play Protect' என்பதன் கீழ் Google இன் Play Store Apps இல் 'Improve harmful app detection' என்பதை இயக்குவதன் மூலம் அதை Googleற்கு அனுப்பலாம். தீம்பொருள் கண்டறிதலுக்காக செயலியை இது சோதனை செய்யும், அத்துடன் மற்றைய பயனர்களைப் பாதுகாக்க உதவும். இதை எப்படி செயல்படுத்துவது என்பது பற்றிய தகவல்: https://support.google.com/android/answer/2812853?hl=en-GB

சைபர் சேவைகளைப் பயன்படுத்தவும்

- **ஒரு இணைப்பைச் சொடுக்க முன்னர் URL நற் பெயர் சேவைகளைப் பயன்படுத்தவும்**. Google Transparency Report அல்லது Virus Total. ஒரு கோப்பு தீங்கிழைக்கிறதா என்பதைக் கண்டறிய உதவும் Virus Total போன்ற தீம்பொருள் பகுப்பாய்வில் சந்தேகத்திற்கிடமான கோப்புகள் மற்றும் செயலிகளை நீங்கள் பதிவேற்றலாம். சோதனை செய்யும் சேவைகள் தவறான எதிர்மறைகளை உருவாக்கக்கூடும் என்பதை அறிந்து கொள்ளுங்கள்.

- **Google மேம்பட்ட பாதுகாப்புத் திட்டத்தில் சேரவும்.** இது இலக்கு வைக்கப்படும் அபாயத்திலுள்ள, (Gmail, Play Store போன்ற) கூகிள் சேவைகளைப் பயன்படுத்துபவர்களைப் பாதுகாக்க வடிவமைக்கப்பட்ட இலவச சேவையாகும். Google சேவைகளைப் பயன்படுத்தும் போது இந்தச் சேவை உயர்ந்த பாதுகாப்பை வழங்குகிறது: https://landing.google.com/advancedprotection/

- கிடைக்கும் பட்சத்தில் கூடுதல் பின்னடைவு சேவைகளில் சேரவும். எடுத்துக்காட்டாக, இங்கிலாந்தில் அதிக ஆபத்திலுள்ள நபர்கள் தங்கள் இணைய பாதுகாப்புக்கு உதவ கூடுதல் தற்காப்பு சேவைகளுக்கு தகுதியுடையவர்களாக இருக்கலாம். தகுதியை சரிபார்த்து மேலும் கண்டுபிடிக்கவும்: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

அச்சுறுத்தல்கள் குறித்துப் புகாரளிக்கவும்

- **போலி கணக்குகளை அடையாளம் கண்டு புகாரளித்தல்**. தீங்கிழைக்கும் சைபர் குற்றவாளிகள் தங்கள் நோக்கங்களை முன்னெடுத்துச் செல்ல போலி கணக்குகளை உருவாக்குகிறார்கள் அல்லது உண்மையான கணக்குகளைத் திருடுகிறார்கள். ஒரு கணக்கு போலியானது அல்லது சமரசம் செய்யப்பட்டது என்று நீங்கள் சந்தேகித்தால், அந்தத் தளத்தில் அது குறித்துப் புகாரளித்து அந்தக்

கணக்கைத் தடுக்கவும். கணக்குகளைச் சரிபார்க்க பல சேவைகள் செயல்முறையில் உள்ளன. எடுத்துக் காட்டாக, Instagram மற்றும் Facebook போன்றவை சரி பார்க்கப்பட்ட கணக்குகளுக்கு, 'verified badges' என்ற சான்றிதழ் வழங்குகின்றன. ஒரு கணக்கு உண்மையானது என்பதை அடையாளம் காண இது உதவும். சமூக ஊடகங்களை பாதுகாப்பாகப் பயன்படுத்துவதற்கான NCSC வழிகாட்டுதல், சமரசம் செய்யப்பட்ட கணக்குகளை எவ்வாறு சரிபார்ப்பது மற்றும் புகாரளிப்பது என்பது பற்றிய விவரங்களை உள்ளடக்கியது:
https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **மோசடி மின்னஞ்சல்கள், குறுஞ்செய்திகள் மற்றும் இணைப்புகளைப் பயன்படுத்தி phishing என்ற மின் தூண்டிலிடல்.** சந்தேகத்திற்கிடமான மின்னஞ்சல் முகவரிகள் மற்றும் வலைத் தளங்களை NCSC விசாரிக்க முடியும். ஒரு தளம், மின்னஞ்சல் முகவரி அல்லது வரும் மின்னஞ்சல் செய்தி சந்தேகத்திற்குரியது என்று நீங்கள் நினைத்தால், நீங்கள் அது குறித்துப் புகாரளிக்கலாம்:
https://www.ncsc.gov.uk/collection/phishing-scams

NCSC சொற் களஞ்சியம்

› Android (அண்ட்ராய்ட்)

Googleஇன் மொபைல் இயக்க முறைமை, பல ஸ்மார்ட்ஃபோன் மற்றும் மடிக்கணினி உற்பத்தியாளர்களால் பயன்படுத்தப்படுகிறது.

› செயலி

செயலி என்பது பயனர்கள் தங்கள் சாதனத்திற்கு கூடுதல் செயல்பாடு அல்லது உள்ளடக்கத்தை வழங்குவதற்காக சாதனத்தில் முன்பே நிறுவப்பட்டுள்ள அல்லது பயனர் நிறுவக்கூடிய ஒரு மென்பொருள் தொகுப்பாகும்.

› சைபர் பாதுகாப்பு

அங்கீகரிக்கப்படாத அணுகல், திருட்டு அல்லது சேதத்திலிருந்து சாதனங்கள், சேவைகள் மற்றும் நெட்வொர்க்குகளைப் பாதுகாப்பது மற்றும் அவற்றைப் பற்றிய தகவல்கள் வெளியிடுவது

› சாதனம்

மேசைக்கணினி, ஸ்மார்ட்ஃபோன் அல்லது மடிக்கணினி போன்ற தொட்டு உணரக் கூடிய கணினி சார்ந்த வன்பொருள்.

› iOS (ஐஓஎஸ்)

Apple நிறுவனத்தின் மொபைல் சாதனங்களின் தொகுப்பில் பயன்படுத்தப்படும் மொபைல் இயக்க முறைமை.

› தீம்பொருள்

தீம்பொருள் என்பது கணினி அமைப்புகள், நெட்வொர்க்குகள் அல்லது சாதனங்களை சேதப்படுத்தும் எந்த வகையான 'தீங்கிழைக்கும் மென்பொருளிலிருந்து' பெறப்பட்ட மென்பொருளையும் குறிக்கும். அதில் வைரஸ்கள், ransomware மற்றும் ட்ரோஜன்கள் அடங்கும்.

› இயக்க அமைப்பு

மேசைக்கணினி, ஸ்மார்ட்ஃபோன் அல்லது மடிக்கணினி போன்றவற்றை இயக்கும் அடிப்படை மென்பொருள். கூடுதல் செயலிகள் மற்றும் வன்பொருளை இயக்க இது தேவைப்படுகிறது.

› Phishing என்ற மின் தூண்டிலிடல்

தீம்பொருளைக் கொண்டிருக்கக்கூடிய இணையதளங்களுக்கான இணைப்புகளைக் கொண்டிருக்கும் அல்லது பயனர்களை ஏமாற்றி (கடவுச் சொற்கள் போன்ற) முக்கியமான தகவலைத் திருடும் அல்லது பணத்தை வேறு கணக்கிற்கு மாற்றும் வகையில் அமைக்கப்பட்ட மோசடி மின்னஞ்சல்கள் அல்லது குறுஞ்செய்திகள்

› Spyware எனப்படும் உளவுமென்பொருள்

பயனரின் அனுமதியின்றி சாதனத்தில் நிறுவி, தரவைச் சேகரித்து மூன்றாம் தரப்புக்கு அனுப்பும் ஒரு வகை தீம்பொருள்.

சமூக ஊடகம்

பயனர் உருவாக்கிய (உரை இடுகைகள், படங்கள் மற்றும் வீடியோ போன்ற) உள்ளடக்கத்தைப் பகிரவும் பதிலளிக்கவும் மக்களை அனுமதிக்கும் Facebook, X மற்றும் Instagram போன்ற இணையதளங்களும் செயலிகளும்.

ஸ்மார்ட்ஃபோன்

Android மற்றும் iOS இயக்க முறைமைகள் உள்ளிட்ட சிக்கலான செயல்பாடுகளைச் செய்யும் நவீன மொபைல் ஃபோன்கள்.

ட்ரோஜன்

முறையான மென்பொருளாக மாறுவேடமிட்டு, பாதிக்கப்பட்டவரின் சாதனத்திற்கு அங்கீகரிக்கப்படாத அணுகலைப் பெற பயன்படும் ஒரு வகை தீம்பொருள்.

URL

இணைய முகவரி அல்லது டொமைன் பெயர் போன்ற உலகளாவிய வலையில் உள்ள ஒரு முகவரி. உலகளாவிய வலையில் ஒரு டொமைன் பெயர் போன்ற ஒரு முகவரி (எடுத்துக்காட்டாக www.bbc.co.uk).

வைரஸ்

முறையான மென்பொருளைப் பாதிக்கும் வகையில் வடிவமைக்கப்பட்ட மற்றும் அந்த மென்பொருள் அல்லது செயலி இயக்கப்படும் போது நெட்வொர்க்குகள் முழுவதும் பிரதிபலிக்கும் வகையில் வடிவமைக்கப்பட்ட ஒரு வகை தீம்பொருள்.

மேலதிக விபரங்களுக்கு

ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையத்தின் வழிகாட்டி

- சைபர் குற்றம், சம்பவம் அல்லது அதனால் ஏற்பட்ட பாதிப்பு குறித்து புகாரளிக்க
- உங்கள் சாதனங்களைப் பாதுகாக்க
- உங்கள் மொபைல் ஃபோனைப் பாதுகாக்க
- Phishing என்ற மின் தூண்டிலிடல்
- மோசடிகள்
- உங்கள் சமூக ஊடகத்தைப் பாதுகாக்க
- சமூக ஊடகங்கள் மற்றும் செய்தியிடல் செயலிகளின் பயன்பாடுகளுக்கான பாதுகாப்பு உதவிக் குறிப்புகள்

UK NCSC மற்றும் NPSA இன் வழிகாட்டுதல்

- ஜனநாயகத்தை பாதுகாத்தல்
- சமூக ஊடகம்: அதை எவ்வாறு பாதுகாப்பாக பயன்படுத்துவது
- மொபைல் உள்ளிட்ட சாதனங்களைப் பாதுகாக்க, நிறுவனங்களுக்கான வழிகாட்டல்
- App storeகளில் ஏற்படுத்தப்படும் அச்சுறுத்தல்கள் குறித்த அறிக்கை.
- அதிக ஆபத்திலுள்ள தனிநபர்களுக்கான பாதுகாப்பு மற்றும் தனிப்பட்ட பாதுகாப்பு

அமெரிக்க NSAயின் வழிகாட்டி

- மொபைல் சாதனங்கள் குறித்த சிறந்த நடைமுறைகள்

பொறுப்புத் துறப்பு

இந்த ஆலோசனை வெளியிடப்படும் நேரத்தில் தகவல்கள் சரிபார்க்கப்பட்டன என்பதை நினைவில் கொள்க.

இந்த அறிக்கையை எழுதும் நிறுவனத்திலிருந்தும் தொழில் துறையிலிருந்தும் பெறப்பட்ட தகவல்களைக் கொண்டு இந்த அறிக்கை எழுதப்பட்டுள்ளது. அனைத்து ஆபத்துகளையும் தவிர்க்கும் நோக்கத்துடன் இதில் கூறப்பட்டுள்ள கண்டுபிடிப்புகளும் பரிந்துரைகளும் வழங்கப்பட்டவில்லை, மேலும் பரிந்துரைகளைப் பின்பற்றுவதால் மட்டுமே அத்தகைய அனைத்து ஆபத்துகளையும் அகற்ற முடியாது. தொடர்புடைய கணினி உரிமையாளர்களிடமே அந்த தகவல் அபாயங்களின் உரிமை எல்லா நேரங்களிலும் இருக்கும்.

இங்கிலாந்தில், தகவல் சுதந்திரச் சட்டம் 2000 (FOIA) இன் கீழ் இந்த தகவலுக்கு விலக்கு அளிக்கப்பட்டுள்ளது, மேலும் பிற UK தகவல் சட்டங்களின் கீழ் விலக்கு அளிக்கப்படலாம்.

ஏதேனும் கேள்விகள் இருந்தால், ncscinfoleg@ncsc.gov.uk என்ற மின்னஞ்சல் முகவரிக்கு அனுப்பி வைக்கவும்.

இணைப்பு: MOONSHINE & BADBAZAAR மாதிரிகள் காணப்பட்ட இடங்கள்

கடந்த இரண்டு ஆண்டுகளில் MOONSHINE மற்றும் BADBAZAAR பிரச்சாரங்களில் பயன்படுத்தப்பட்ட செயலிகளை கீழே உள்ள அட்டவணை பட்டியலிடுகிறது.

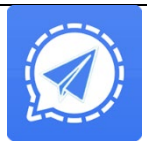
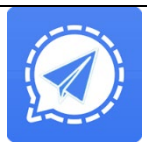
ஏற்கனவே உள்ள செயலிகளுடன் தெளிவான ஒற்றுமையை இந்த செயலிகளில் பல காட்டுகின்றன. வேண்டுமென்றே ஏமாற்றுவதற்காக, ஏற்கனவே நன்கு அறியப்பட்டவற்றைப் பயன்படுத்தும் உத்தியாக இருக்கலாம்.

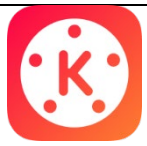
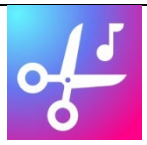
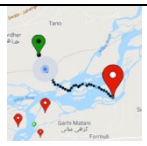
செயலியின் பெயர், அதன் தொகுப்பின் பெயர் மற்றும் குறியீட்டு சின்னம் அனைத்தும் உண்மையான செயலியைப் போன்றதாக இருக்கலாம் அல்லது பொருந்தலாம். எனவே ஒரு சாதனம் பாதிக்கப்பட்டுள்ளதா என்பதை அடையாளம் காண அதனைப் பிரத்தியேகமாகப் பயன்படுத்தப்படக்கூடாது என்பதைக் கவனத்தில் கொள்ள வேண்டும்.

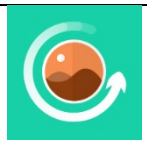
மட்டுப்படுத்தல்கள் பிரிவில் குறிப்பிடப்பட்டுள்ளபடி, Play Store Apps இல் 'Improve harmful app detection' என்பதை இயக்குவதன் மூலம் Android சாதனத்தில் உள்ள செயலிகளை Googleற்கு அனுப்பலாம். இது Play Storeருக்கு வெளியில் இருந்து நிறுவப்பட்ட உங்கள் சாதனத்தில் உள்ள செயலிகளை சோதனை செய்யும்.

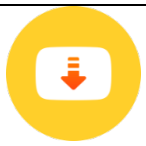
செயலியின் பெயர்	தொகுப்பின் பெயர்	செயலியின் குறியீட்டு சின்னம்
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	

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

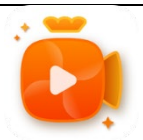
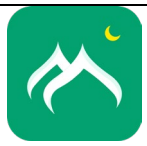
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar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

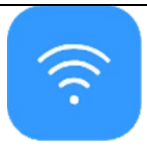
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader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

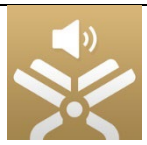
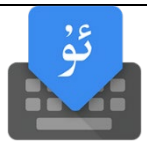
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	

Signal Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candle tibet.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	
بقاپ لۇغىتىaكۇ	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