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

परामर्श-सूचना

BADBAZAAR और MOONSHINE उइगर, ताइवानी और तिब्बती समूहों व नागरिक समाज कार्यकर्ताओं को लक्षित करने वाला स्पाइवेयर

9 अप्रैल 2025

BADBAZAAR और MOONSHINE: उइगर, ताइवानी और तिब्बती समूहों व नागरिक समाज कार्यकर्ताओं को लक्षित करने वाला स्पाइवेयर

एनसीएससी और साझेदार दो स्पाइवेयर वेरिएंट्स के ऊंचे खतरे वाले लोगों के लिए नई जानकारी और मिटिगेशन के लिए कदम प्रकाशित कर रहे हैं।

सारांश

यूके साइबर लीग के समर्थन से यह परामर्श-सूचना राष्ट्रीय साइबर सुरक्षा केंद्र (एनसीएससी यूके) और निम्नलिखित अंतर्राष्ट्रीय भागीदारों द्वारा संयुक्त रूप से तैयार की गई है:

- **ऑस्ट्रेलियन साइबर सिक्योरिटी सेंटर (एसीएससी), जो ऑस्ट्रेलियन सिग्नल्स डायरेक्टोरेट का हिस्सा है**
- **कैनेडियन सेंटर फॉर साइबर सिक्योरिटी, जो संचार सुरक्षा प्रतिष्ठान का हिस्सा है**
- **जर्मन संघीय खुफिया सेवा**
- **जर्मन संविधान संरक्षण संघीय कार्यालय**
- **न्यू ज़ीलैंड नैशनल साइबर सिक्योरिटी सेंटर, जो सरकारी संचार सुरक्षा ब्यूरो का हिस्सा है**
- **संयुक्त राज्य अमेरिका फेडरल ब्यूरो ऑफ इन्वेस्टिगेशन**
- **संयुक्त राज्य अमेरिका नैशनल सिक्योरिटी एजेंसी**

इसका उद्देश्य दुर्भाविनापूर्ण साइबर कर्ताओं के बढ़ते हुए खतरे के बारे में जागरूकता बढ़ाना है, जिनमें ताइवान, तिब्बत, झिंजियांग उइगर स्वायत्त क्षेत्र, लोकतंत्र आंदोलनों और फालुन गोंग सहित अन्य विषयों से जुड़े व्यक्ति-विशेष शामिल हैं।

इस परामर्श-सूचना में दुर्भाविनापूर्ण साइबर कर्ताओं द्वारा उपयोग की जाने वाली तकनीकों का विवरण देते हुए दो मामला अध्ययन शामिल हैं, जिन्हें BADBAZAAR और MOONSHINE के रूप में जाना जाता है। ये स्मार्टफोन सहित अन्य मोबाइल उपकरणों पर मौजूद डेटा को लक्षित करते हैं, जो चीनी राष्ट्र के लिए रुचिकर हो सकता है। यह व्यक्ति-विशेषों को अपनी, अपने उपकरणों और अपने डेटा के संरक्षण में मदद के लिए मार्गदर्शन देने के संकेतचिह्न भी प्रदान करती है।

इस परामर्श के साथ में एनसीएससी ने अलग से मार्गदर्शन सहित संपूर्ण तकनीकी विवरण भी प्रकाशित किया है।

किसे खतरा है?

संलेखन एजेंसियों और उद्योग भागीदारों ने BADBAZAAR और MOONSHINE को ऐसे व्यक्ति-विशेषों को लक्षित करते हुए देखा है, जिन्हें चीनी राष्ट्र विशेषकर अपने घरेलू प्राधिकार, महत्वाकांक्षाओं और वैश्विक प्रतिष्ठा के लिए खतरा माने जाने वाले विषयों से जुड़ा मानता है। जिनके लिए सबसे अधिक खतरा है, उनमें निम्नलिखित से जुड़े लोग शामिल हैं, लेकिन ये केवल इन्हीं तक ही सीमित नहीं हैं:

- **ताइवानी स्वतंत्रता**
- **तिब्बती अधिकार**
- **चीन के झिंजियांग उइघुर स्वायत्त क्षेत्र में या वहाँ के उइगर मुस्लिम और अन्य जातीय अल्पसंख्यक**
- **लोकतंत्र पक्ष-समर्थन (जिसमें हांग कांग शामिल है)**
- **फालुन गोंग आध्यात्मिक आंदोलन**

इसमें ऐसे गैर-सरकारी संगठन (एनजीओ), पत्रकार, व्यवसाय और व्यक्ति-विशेष शामिल हैं, जो इन समूहों का पक्ष-समर्थन करते हैं, इनके साथ अपनी पहचान करते हैं या अन्यथा इनका प्रतिनिधित्व करते हैं। जिस अव्यवस्थित तरह से यह स्पाइवेयर ऑनलाइन फैलता है, उसका अर्थ यह भी है कि इस संक्रमण का अपने इच्छित शिकारों से परे फैल सकने का खतरा है।

इस परामर्श-सूचना का उद्देश्य उन लोगों को BADBAZAAR और MOONSHINE स्पाइवेयर के विशिष्ट खतरे का प्रभावी ढंग से उत्तर देने में मदद करना है, जिन्हें इसका जोखिम है। सुझाए गए मिटिगेशन्स व्यापक साइबर सुरक्षा सलाह के संपूरक हैं और इन्हें अलग से नहीं माना जाना चाहिए।

इस परामर्श-सूचना में संदर्भित मार्गदर्शन का पालन करके उपयोगकर्ता अपने मोबाइल उपकरणों और डेटा में संक्रमण का खतरा कम कर सकते हैं।

खतरा

MOONSHINE और BADBAZAAR ट्रोजन्स के उदाहरण हैं; इनमें ऐप स्टोर या ऑनलाइन फाइल-शेयरिंग सेवाओं से डाउनलोड की जा सकने वाली एक अन्यथा कारगर ऐप के अंदर दुर्भाविनापूर्ण फंक्शन्स छिपे हुए हैं।

इन ऐप्स को उपयोगकर्ता को चकमा देकर डिवाइस पर डाउनलोड और इंस्टॉल करने के लिए डिज़ाइन किया गया है। एक बार ऐप के इंस्टॉल हो जाने पर यह अनधिकृत बातों के लिए डिवाइस की कमजोरियों का उपयोग करती है, अथवा यह पर्मिशन्स देने के लिए उपयोगकर्ता पर निर्भर कर सकती है ताकि डिवाइस से जानकारी को एक्सेस और डाउनलोड किया जा सके, जिसमें शामिल है:

- **स्थान से संबंधित डेटा, जिसमें रियल टाइम ट्रैकिंग भी शामिल है**
- **माइक्रोफ़ोन और कैमरे की एक्सेस**
- **डिवाइस पर स्टोर किए गए मैसेजेस, फोटो और अन्य फाइलें**
- **डिवाइस के बारे में जानकारी, तथा और भी बहुत कुछ**

इसके बाद कर्ता खतरे वाले समूहों के वैध हितों का फायदा उठाते हैं, ताकि वे यथासंभव अधिक से अधिक शिकारों की पहचान करके उन्हें संक्रमित कर सकें और उनके डेटा को एक्सेस कर सकें। ऐसा करने का एक तरीका यह है कि वे ऐसी ऐप्स डिज़ाइन करते हैं, जिनके बारे में उन्हें पता है कि वे उनके शिकारों को पसंद आएँगी, जैसे उनकी मूल भाषाओं को समर्थन देने वाली ऐप्स, या जिनमें चीन के तिब्बती क्षेत्रों या झिंजियांग जैसे स्थानों के बारे में विशिष्ट सामग्री होती है।

इस परामर्श-सूचना में शामिल मामला अध्ययनों में इसके कुछ उदाहरण दिए गए हैं, जिसमें TibetOne और Uyghur Quran ऐप्स शामिल हैं।

कर्ता ऐसे ऑनलाइन फोरमों में सक्रिय रहते हैं, जहां उनके इच्छित शिकारों का एक यूज़र बेस रहता है। इससे उन्हें शिकारों को संक्रमित करने का अधिकतम अवसर मिल पाता है। उन्हें तिब्बत से संबंधित टेलीग्राम चैनलों और रेडिट फोरमों में जानबूझकर स्पाइवेयर शेयर करते देखा गया है। इस परामर्श-सूचना में दिए गए मामले अध्ययन भी इन तरीकों के उदाहरण देते हैं।

दुर्भाविनापूर्ण ऐप्स को अक्सर स्टैंडएलोन फाइलों के रूप में साझा किया जाता है, जैसे एंड्रॉइड पर एपीके फाइलें, जिन्हें उपयोगकर्ताओं को डाउनलोड और इंस्टॉल करने की आवश्यकता होती है। कर्ता अपने स्पाइवेयर को गूगल प्ले स्टोर और एप्पल ऐप स्टोर जैसे आधिकारिक ऐप स्टोर्स पर अपलोड करके इन्हें अधिक वैध दिखाने की कोशिश करते हैं या फिर पहले से ही मौजूद गैर-दुर्भाविनापूर्ण ऐप्स में मैलिशियस कोड जोड़ देते हैं, किंतु आधिकारिक स्टोर्स में ऐसी सुरक्षा विशेषताएं और पुनरीक्षण प्रक्रियाएं होती हैं जो इस कार्यनीति की सफलता को कम कर सकती हैं। इस कारणवश आधिकारिक स्टोर्स पर उपलब्ध ऐप्स अधिक सुरक्षित होती हैं, लेकिन जैसाकि मामले अध्ययनों और एनसीएससी की ऐप स्टोर थ्रेट रिपोर्ट में दिखाया गया है, ये प्रक्रियाएं बिल्कुल सटीक नहीं होती हैं।

इन 4 सुझावों का पालन करके आपको इस परामर्श-सूचना में रेखांकित खतरों से बचने में सहायता मिल सकती है।
अधिक विस्तृत सलाह के लिए मिटिगेशन अनुभाग देखें।

मामले अध्ययन

ये दो मामले अध्ययन दर्शाते हैं कि MOONSHINE और BADBAZAAR कैसे काम करते हैं, और कैसे दुर्भाविनापूर्ण साइबर कर्ता सबसे अधिक खतरे वाले लोगों को लक्षित कर रहे हैं।

मामला अध्ययन एक: MOONSHINE

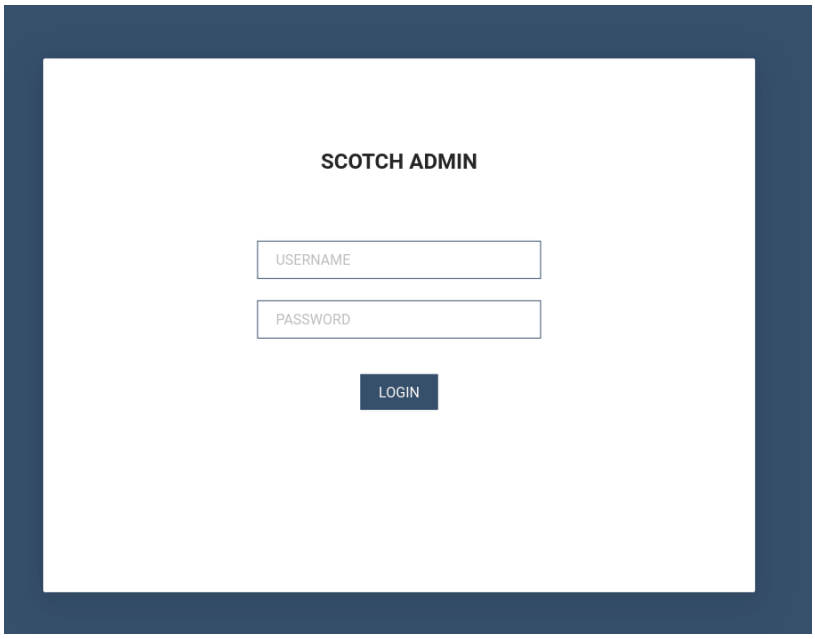
MOONSHINE एक एंड्रॉइड स्पाइवेयर है जिसके बारे में 2019 में सिटीज़न लैब द्वारा तिब्बती समूहों को लक्षित करने के रूप में रिपोर्ट की गई थी। MOONSHINE इंस्टॉल किए जाने के उद्देश्य से शिकारों को लुभाने के लिए इसे एक वैध ऐप के रूप में पेश करती है। इसे टेलीग्राम चैनलों और व्हॉट्सएप से भेजे गए लिंक्स के माध्यम से साझा किया गया है।

MOONSHINE के पास व्यापक निगरानी क्षमताएं हैं, जैसे:

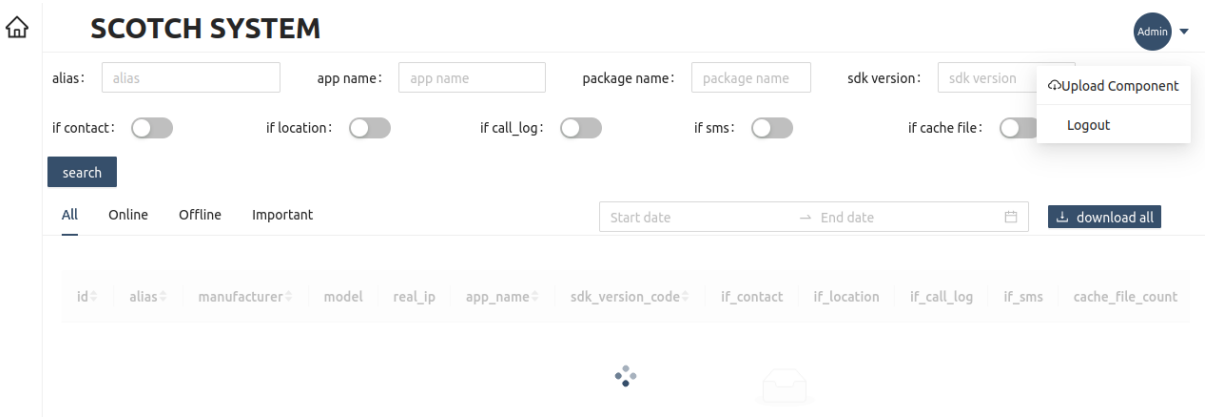
- **स्थान से संबंधित डेटा, जिसमें रियल टाइम ट्रैकिंग भी शामिल है**
- **लाइव ऑडियो और फोटो कैप्चर**
- **डिवाइस से फाइलें डाउनलोड करना**
- **डिवाइस से जानकारी प्राप्त करना**
- **डिवाइस पर ऑडियो चलाना**

यह ऐप, '**ئاۋازلىق قۇرئان.apk**' जिसका अनुवाद '**Audio Quran.apk**' है, उइगरों को लक्षित करने के लिए MOONSHINE का उपयोग किए जाने के तरीके का एक उदाहरण है। फाइल के नाम में उइगर भाषा का उपयोग, जोकि कुरान से संबंधित ऐप का संकेत देती है, संभवतः उइगर मुसलमानों को लुभाने के लिए डिज़ाइन किया गया था।

इसके इंस्टॉल हो जाने के बाद दुर्भाविनापूर्ण साइबर कर्ता शिकारों के डिवाइसेज़ से जानकारी एकत्र कर सकते हैं। इस जानकारी को 'SCOTCH ADMIN' पैनल के माध्यम से एक्सेस किया जाता है।



लॉग इन करने के बाद कर्ता नीचे स्क्रीनशॉट में दिखाए गए पेज को एक्सेस कर सकते हैं। यह पेज संक्रमित डिवाइसेज़ के विवरण व संक्रमित डिवाइसेज़ में कर्ता की एक्सेस का स्तर प्रदर्शित करता है:



मैलवेयर मैनेजमेंट पैनल एकत्र किया गया डेटा दिखाता है, जिसमें शामिल है:

- **डिवाइस की एक्सेस का स्तर**
- **एसएमएस मैसेजेस**
- **कॉल लॉग्स**
- **स्थान डेटा**
- **डिवाइस के बारे में जानकारी**

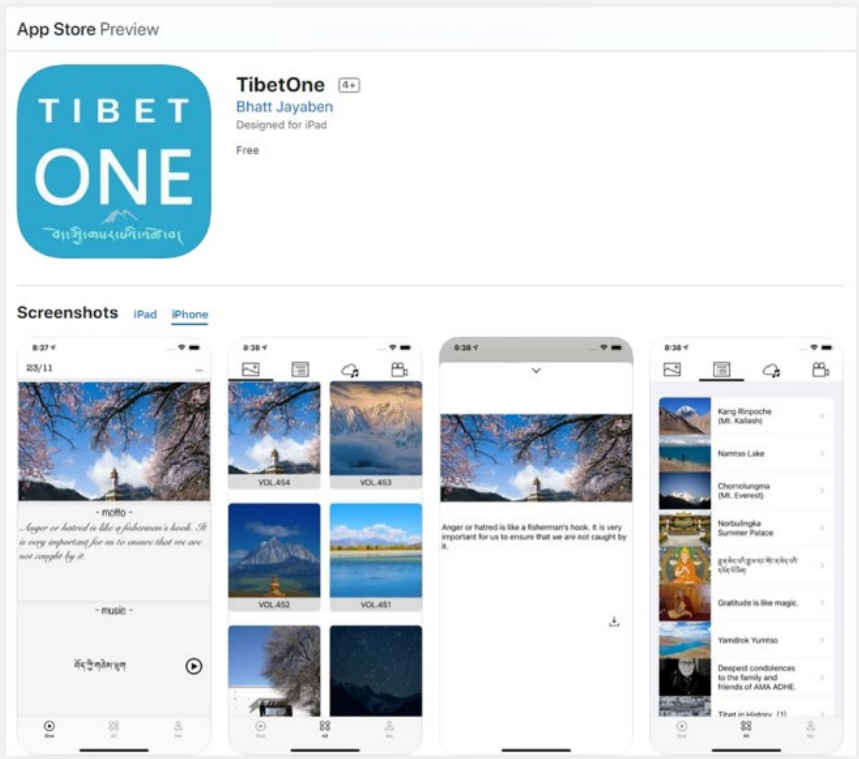
एनसीएससी ने साइबर लीग के सहयोग से MOONSHINE शोषण किट और एचटीएमएल शीर्षक में 'UPSEC' शामिल होने वाले लॉगिन पैनल के बीच ओवरलैप खोजने के लिए ट्रेंड माइक्रो से इंडस्ट्री रिपोर्टिंग पर आगे निर्माण किया है। संलग्न तकनीकी परामर्श-सूचना में संपूर्ण विवरण उपलब्ध हैं। इंटेलिजेंस ऑनलाइन के अनुसार UPSEC से संदर्भ 'सिचुआन डाएन्क नेटवर्क सिक्योरिटी टेक्नोलॉजी को. लि.' से है। संलेखन एजेंसियों ने इस कथन की पुष्टि नहीं की है।

मामला अध्ययन दो: BADBAZAAR

BADBAZAAR एक मोबाइल मैलवेयर है, जिसके आईओएस और एंड्रॉयड वेरिएंट्स हैं। इसने उइगर, तिब्बतियों और ताइवान के व्यक्ति-विशेषों को लक्षित किया है। इस मैलवेयर को सोशल मीडिया प्लेटफॉर्म्स और आधिकारिक ऐप स्टोर्स के माध्यम से फैलाया गया है।

लुकआउट और वोलेक्सिटी की रिपोर्ट के अनुसार, BADBAZAAR को **'TibetOne'** ऐप के जरिए तिब्बतियों को निशाना बनाने के लिए इस्तेमाल किया गया है। **TibetOne** दुर्भावनापूर्ण कर्ताओं द्वारा बनाई गई एक आईओएस ऐप है, जिसमें डिवाइस की जानकारी और स्थान से संबंधित डेटा को एक्सेस करने की क्षमता है। इसे दिसंबर 2021 में एप्पल ऐप स्टोर पर अपलोड किया गया था, लेकिन अब यह उपलब्ध नहीं है। मैलवेयर को और अधिक फैलाने के लिए कर्ताओं ने '**tibetanphone**' नाम के एक टेलीग्राम चैनल में इस ऐप को विज्ञापित भी किया था।

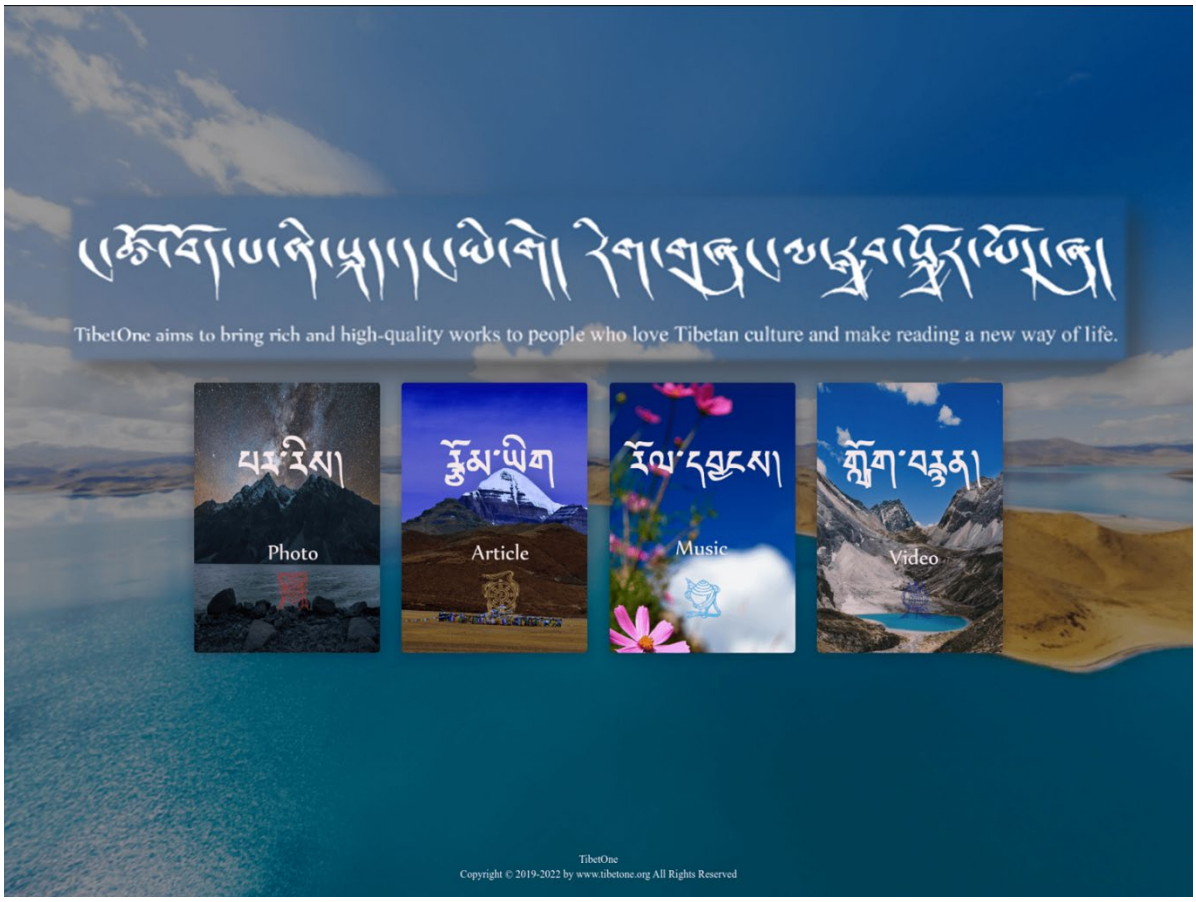
TibetOne



चित्र 1. एप्पल ऐप स्टोर पर TibetOne ऐप पेज। तब से ऐप को हटा दिया गया है।

चित्र 2. टेलीग्राम चैनलों में साझा किए गए TibetOne का स्वरूप।

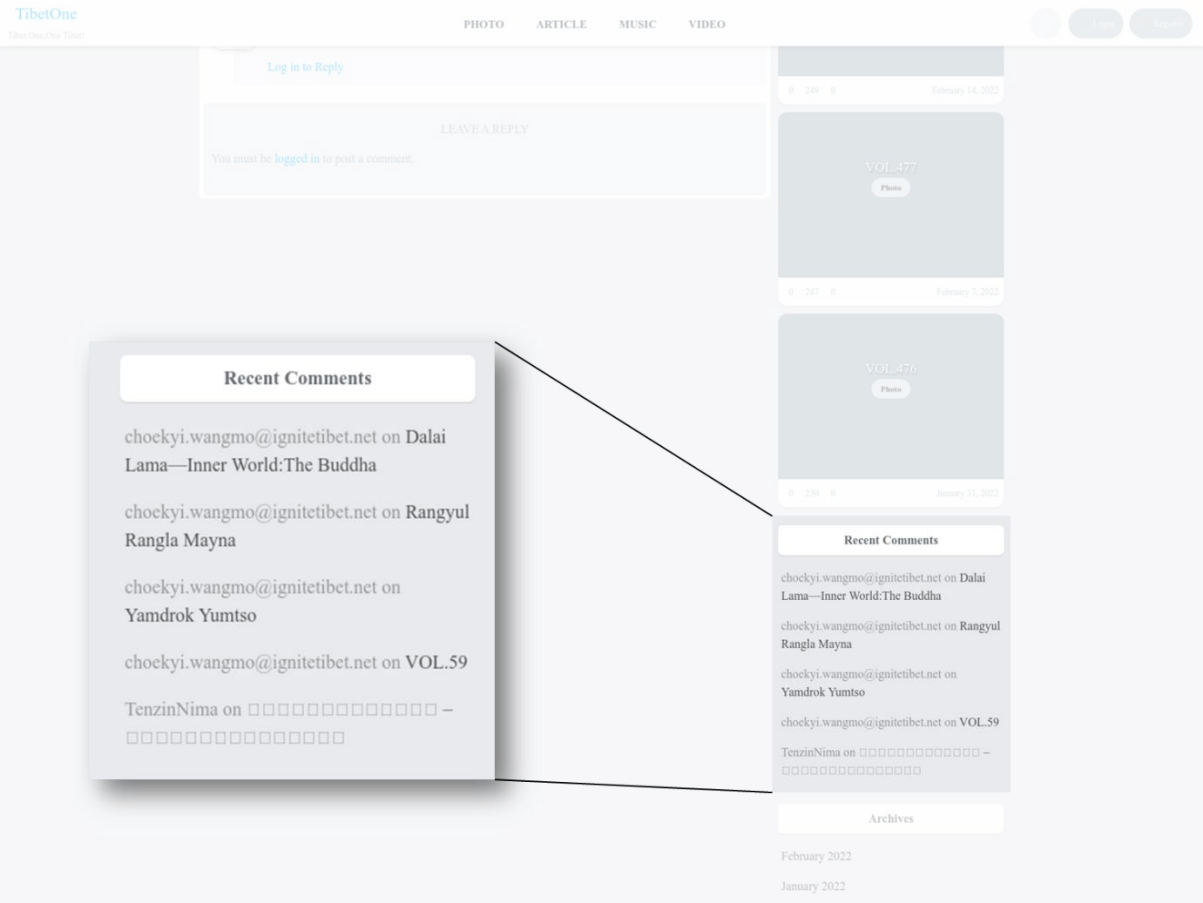
इस ऐप में और अधिक वैधता प्रदर्शित करने के लिए कर्ताओं ने '**tibetone[.]org**' नाम की एक वेबसाइट भी विकसित की, जिसका वर्णन था - *'bring[ing] rich and high-quality works to people who love Tibetan culture and make reading a new way of life'*।



चित्र 3: 'tibetone[.]org' का होमपेज।

संगत हिस्सों को स्पष्ट दिखाने के लिए इस इमेज को एडिट किया गया है।

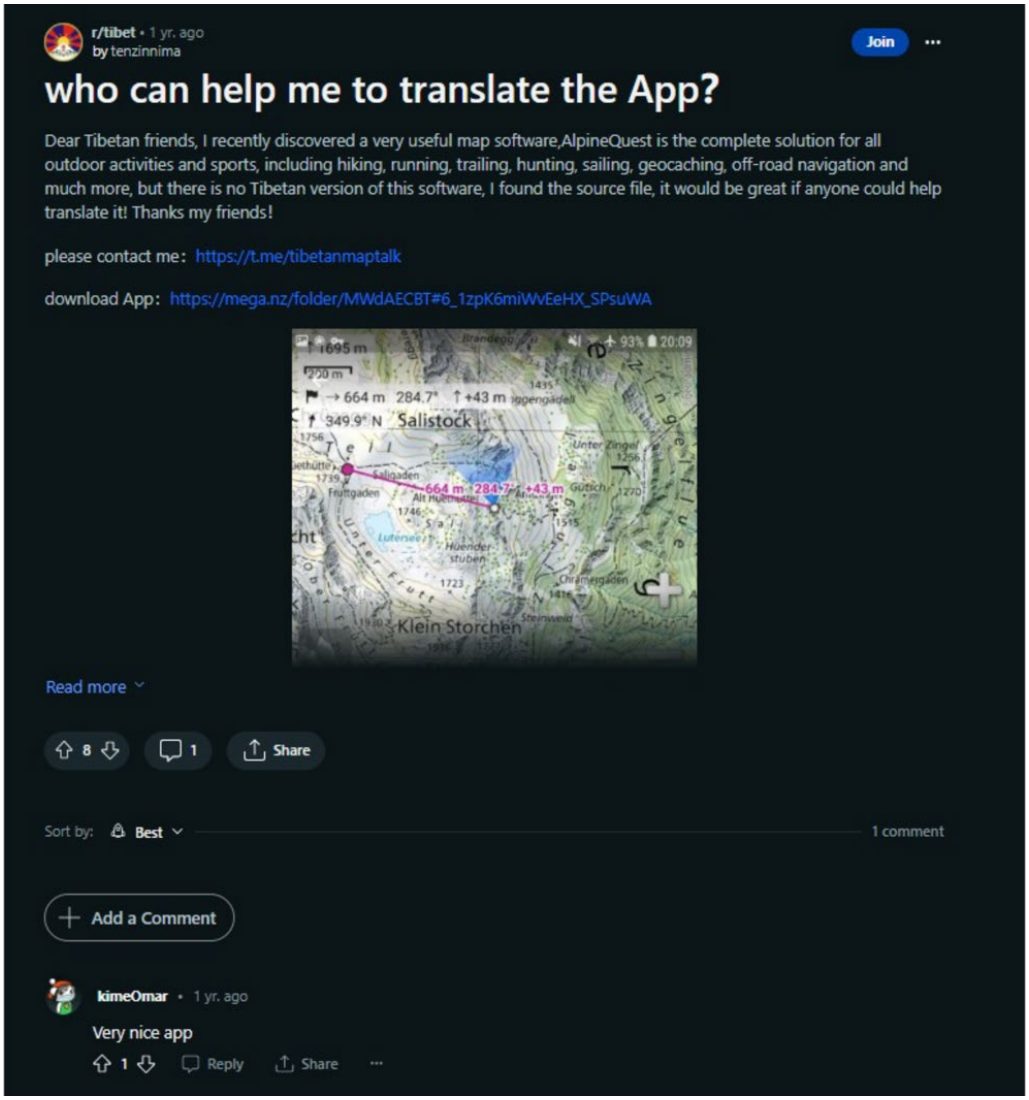
इस वेबसाइट पर उपयोगकर्ताओं को टिप्पणियाँ लिखने की अनुमति देने वाले लेखों का एक पेज शामिल था। माना जा रहा है कि ईमेल पते '**choekyi.wangmo@ignitetibet.net**' द्वारा लिखी गई एक टिप्पणी को दुर्भावनापूर्ण कर्ता द्वारा नियंत्रित किया जाता है और वह संभावित रूप से **'Choekyi Wangmo'** का प्रतिरूपण करता है, जिसे तिब्बती मानवाधिकार एवं लोकतंत्र केंद्र ने एक तिब्बत-समर्थक प्रदर्शनकारी के रूप में सूचीबद्ध किया है। संभावित रूप से यह ऐसी अवधारणा देने का एक और प्रयास है कि यह ऐप वास्तव में तिब्बती स्वतंत्रता के पक्ष-समर्थन में है।



चित्र 4: 'tibetone[.]org' पेज, जिसमें दुर्भावनापूर्ण कर्ता द्वारा संभवत: नियंत्रित किए जाने वाले उपयोगकर्ताओं की टिप्पणियाँ दिखाई गई हैं।

संगत हिस्सों को स्पष्ट दिखाने के लिए इस इमेज को एडिट किया गया है।

एक अन्य उपयोगकर्ता नाम '**TenzinNima**' है, जिसने इस साइट पर टिप्पणियाँ जोड़ी हैं। वोलेक्सिटी ने रिपोर्ट किया है कि इस उपयोगकर्ता नाम को रेडिट पर टेलीग्राम चैनल '**Tibetanmaptalk**' के विज्ञापन के लिए भी इस्तेमाल किया गया है। इसमें एंड्रॉइड डिवाइस पर उपलब्ध नेविगेशन ऐप '**AlpineQuest**' का एक दुर्भावनापूर्ण नमूना डाउनलोड करने के लिए लिंक शामिल है। दिया गया डाउनलोड लिंक Mega नाम की तृतीय-पक्ष फाइल-शेयरिंग सेवा के लिए है।



चित्र 5: मैलिशियस एप्लिकेशन का विज्ञापन देती हुई रेडिट पोस्ट, जो संभवतः दुर्भाविनापूर्ण कर्ता द्वारा नियंत्रित खाते से है।

वोलेक्सिटी इस बात पर भी ध्यान देती है कि इस पोस्ट पर टिप्पणी करने वाले एक उपयोगकर्ता को, जिसे '**KimeOmar**' के नाम से जाना जाता है, एक अन्य सब-रेडिट फोरम पर दुर्भाविनापूर्ण ऐप्स साझा करते हुए पाया गया है। इससे यह संकेत मिल सकता है कि अपनी पोस्ट्स को वैध दिखाने के लिए दुर्भाविनापूर्ण कर्ता कई सोशल मीडिया प्रोफाइलों का उपयोग करते हैं।

आकलन

BADBAZAAR और MOONSHINE विशेष रूप से उइगर, तिब्बती और ताइवानी समुदायों को निशाना बनाने के लिए कई सोशल इंजीनियरिंग तरीकों का उपयोग करते हैं, विशेषकर:

- इन समुदायों के लिए रुचिकर ऐप्स में ट्रोजन्स को जोड़ना, जैसे उइगर भाषा में कुरान ऐप, लगभग निश्चित रूप से शिकार आधारों को लक्षित करने के लिए अनुरूपित किया गया है
- आधिकारिक ऐप स्टोर में इन ट्रोज़न-युक्त ऐप्स को जोड़ने से वैधता का एहसास पैदा होने की संभावना है, और सामूहिक चैट में इन्हें साझा करने का उद्देश्य इन समुदायों के अंदर विश्वसनीय संबंधों का फायदा उठाना है

BADBAZAAR और MOONSHINE ऐसा डेटा एकत्र करते हैं, जो लगभग निश्चित रूप ही से चीनी राष्ट्र के लिए महत्वपूर्ण होगा। BADBAZAAR और MOONSHINE को उइगर, तिब्बती और ताइवान के व्यक्ति-विशेषों को लक्षित करते हुए देखा गया है, लेकिन ऐसे अन्य मैलवेयर्स भी हैं जो चीन में अन्य अल्पसंख्यक समूहों को लक्षित करते हैं। चीन और विदेशों में को-सीलिंग देशों के नागरिकों को, जिन्हें प्रशासन की स्थिरता के लिए खतरा पैदा करने वाले कारणों को समर्थन देने के रूप में माना जाता है, लगभग निश्चित रूप से ही BADBAZAAR और MOONSHINE जैसे मोबाइल मैलवेयर का खतरा है। स्थान, ऑडियो और फोटो डेटा को कैप्चर करने की क्षमता लक्ष्य की गतिविधि पर वास्तविक समय में जानकारी देकर भविष्य में निगरानी और उत्पीड़न कार्रवाइयों को सूचित करने का अवसर लगभग निश्चित रूप से ही उपलब्ध कराती हैं।

मोबाइल ऐप उपयोगकर्ताओं के लिए मिटिगेशन के कदम

मामले अध्ययनों में बताए गए खतरों से बचने के लिए संलेखन एजेंसियां निम्नलिखित सुरक्षा-प्रथाओं को प्रोत्साहन देती हैं। इन संस्तुतियों को सर्वोत्तम-कार्यप्रथा एनसीएससी मार्गदर्शन द्वारा रेखांकित किया गया है। ऑस्ट्रेलिया और अमेरिका में पाठकों के लिए सर्वोत्तम कार्यप्रथा मार्गदर्शन के लिंक्स के लिए 'आगे पढ़ने के लिए सामग्री' अनुभाग देखें।

अपने डिवाइस को सुरक्षित रखें

- **केवल आधिकारिक ऐप स्टोर्स से ही ऐप्स डाउनलोड करें, जैसे गूगल का प्ले स्टोर या एप्पल का ऐप स्टोर।** गूगल का प्ले स्टोर या एप्पल का ऐप स्टोर सॉफ्टवेयर उपलब्ध कराने से पहले वायरसों का पता लगाने के लिए सॉफ्टवेयर को स्कैन करते हैं, जिससे आपको इस बात का बेहतर आश्वासन मिलता है कि आप जो डाउनलोड कर रहे/ही हैं, वह सुरक्षित है। विश्वसनीय स्टोर्स से प्राप्त ऐप्स में फिर भी खतरा हो सकता है, लेकिन अन्य स्रोतों से प्राप्त डाउनलोड्स में संभवत: कोई भी संरक्षण नहीं हो सकता है। ऐप स्टोर्स के खतरों के बारे में एनसीएससी की रिपोर्ट यहाँ उपलब्ध है: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **अपने डिवाइस और ऐप्स को अप-टु-डेट रखें।** अपनी ऐप्स और डिवाइस सॉफ्टवेयर के लिए अपडेट्स के उपलब्ध होते ही उन्हें इंस्टॉल करें। अपने डिवाइस की सेटिंग्स में उपलब्धता के अनुसार 'automatic updates' को टर्न ऑन करें, ताकि आपको यह याद रखने की आवश्यकता न हो। ज्ञात वायरसों और अन्य प्रकार के मैलवेयर से बचने के लिए एनसीएससी का ऑनलाइन सुरक्षित रहने के बारे में मार्गदर्शन देखें। अपडेट्स में अक्सर सुधार और नए फीचर्स शामिल होते हैं: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **अपने डिवाइस को 'जेलब्रेक' या 'रूट' न करें**, क्योंकि यह लागू सुरक्षा नियंत्रणों को बायपास करने के लिए पैच न की गई कमजोरियों का उपयोग करता है। डिवाइस इससे हमलों के प्रति और भी अधिक कमजोर बन जाता है। एनसीएससी का मार्गदर्शन देखें: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

अपनी ऐप्स का प्रबंधन करें

- **अपनी ऐप्स और उनकी पर्मिशन्स की समीक्षा करें।** यदि अब आपको किसी ऐप की ज़रूरत न हो, तो उसे डिलीट कर दें। जहां हो सके, डेटा एक्सपोज़र को कम से कम करने के लिए ऐप पर्मिशन्स प्रतिबंधित करें, क्योंकि मैलवेयर को अक्सर संरक्षित फाइलों या बाहरी डिवाइसेज़ को एक्सेस करने के लिए डिज़ाइन किया जाता है, जैसे कैमरे और माइक्रोफोन।
  - एप्पल उपयोगकर्ताओं के लिए ऐप पर्मिशन्स की जांच कैसे करें: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - एंड्रॉयड उपयोगकर्ताओं के लिए ऐप पर्मिशन्स की जांच कैसे करें: https://support.google.com/android/answer/9431959?hl=en-GB

- **गूगल को अज्ञात ऐप्स स्वत: भेजें**। यदि आप एक एंड्रॉयड उपयोगकर्ता हैं और आपने कोई ऐसी ऐप डाउनलोड की है जो गूगल के प्ले स्टोर से नहीं है, तो आप गूगल की प्ले स्टोर ऐप्स सेटिंग्स में 'प्ले प्रोटेक्ट' के अंतर्गत 'Improve harmful app detection' को इनेबल करके उसे गूगल के पास भेज सकते/ती हैं। यह मैलवेयर का पता लगाने के लिए ऐप को स्कैन करेगा, ताकि उपयोगकर्ताओं की सुरक्षा में सहायता मिल सके। इसे सेट अप करने के तरीके के बारे में जानकारी: https://support.google.com/android/answer/2812853?hl=en-GB

साइबर सेवाओं का उपयोग करें

- **किसी भी लिंक पर क्लिक करने से पहले यूआरएल रेप्युटेशन सर्विसेज़ का उपयोग करें।** आप किसी ईमेल, टेक्स्ट मैसेज या किसी अन्य जगह से प्राप्त हुए किसी लिंक को पहले गूगल ट्रांसपैरेंसी रिपोर्ट या वायरस टोटल जैसी सेवाओं के इस्तेमाल से स्कैन करके इसकी सुरक्षितता की जांच कर सकते/ती हैं। आप संदिग्ध फाइलों और ऐप्स को वायरस टोटल जैसे किसी मैलवेयर एनालाइज़र पर अपलोड भी कर सकते/ती हैं, जो यह पता लगाने में सहायता कर सकता है कि कोई फाइल दुर्भावनापूर्ण है या नहीं। ध्यान रखें कि स्कैनिंग सेवाएं असत्य नकारात्मक परिणाम दे सकती हैं।

- **गूगल एडवांस्ड प्रोटेक्शन प्रोग्राम में शामिल हों।** इस निःशुल्क सेवा को गूगल सेवाओं (जीमेल, प्ले स्टोर, आदि) का उपयोग करने वाले व्यक्ति-विशेषों की सुरक्षा के लिए डिज़ाइन किया गया है, जिन्हें लक्षित किए जाने का खतरा है। यह सेवा गूगल सेवाओं का उपयोग करते समय ऊंचे स्तर की सुरक्षा प्रदान करती है: https://landing.google.com/advancedprotection/

- **अतिरिक्त प्रमाणन सेवाओं में उनकी उपलब्धतानुसार शामिल हों।** उदाहरण के लिए, यूके में ऊंचे खतरे वाले व्यक्ति-विशेष अपनी साइबर सुरक्षा में सहायता के लिए अतिरिक्त सुरक्षात्मक सेवाओं के पात्र हो सकते हैं। पात्रता की जांच तथा और अधिक जानकारी प्राप्त करें: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

धमकियों की रिपोर्ट करें

- **नकली खातों की पहचान और रिपोर्ट करना।** दुर्भावनापूर्ण साइबर कर्ता अपने उद्देश्य को आगे बढ़ाने के लिए नकली खाते बनाते हैं या वास्तविक खातों को हैक कर लेते हैं। यदि आपको संदेह है कि कोई खाता नकली है या उसे भंग किया गया है, तो उसके बारे में प्लेटफॉर्म पर रिपोर्ट करें और उसे ब्लॉक करें। कई सेवाओं में खातों के सत्यापन की एक प्रक्रिया होती है, जैसे इंस्टाग्राम और फेसबुक के लिए "verified badges"। इससे यह पहचान करने में सहायता मिल सकती है कि खाता वास्तविक है या नहीं। एनसीएससी के पास सोशल मीडिया का सुरक्षित रूप से उपयोग करने के बारे में मार्गदर्शन है, जिसमें भंग किए गए खातों के सत्यापन और उनकी रिपोर्ट करने के बारे में विवरण भी शामिल हैं: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **फिशिंग, जिसमें घोटाला ईमेल, एसएमएस और लिंक्स का उपयोग किया जाता है।** एनसीएससी संदिग्ध ईमेल पतों और वेबसाइटों की जांच कर सकती है। यदि आपको लगता है कि कोई साइट, ईमेल या मैसेज संदिग्ध है, तो आप उसकी रिपोर्ट कर सकते/ती हैं: https://www.ncsc.gov.uk/collection/phishing-scams

एनसीएससी शब्दावली

- **एनड्रॉयड**

गूगल का मोबाइल ऑपरेटिंग सिस्टम, जिसे कई स्मार्टफोन और टैबलेट निर्माताओं द्वारा इस्तेमाल किया जाता है।

- **एप**

एप्लिकेशन, या ऐप, एक सॉफ्टवेयर पैकेज होता है, जिसे डिवाइस पर अतिरिक्त फंक्शनैलिटी या सामग्री उपलब्ध कराने के लिए उपयोगकर्ता अपने डिवाइस पर इंस्टॉल कर सकते/ती हैं या फिर यह पहले से ही इंस्टॉल होता है।

- **साइबर सुरक्षा**

डिवाइसेज़, सेवाओं तथा नेटवर्क्स - और इनमें मौजूद जानकारी – की अनधिकृत एक्सेस, चोरी या क्षति से सुरक्षा।

- **डिवाइस**

भौतिक रूप से मौजूद कंप्यूटर-आधारित हार्डवेयर, जैसे डेस्कटॉप कंप्यूटर, स्मार्टफोन या टैबलेट।

- **आईओएस**

एप्पल का मोबाइल ऑपरेटिंग सिस्टम, जिसे इसके लिए अनुरूपित मोबाइल डिवाइसेज़ में इस्तेमाल किया जाता है।

- **मैलवेयर**

मैलवेयर, जिसे 'मैलिशियस सॉफ्टवेयर' शब्दों से निकाला गया है, ऐसा कोई भी प्रकार का सॉफ्टवेयर होता है जो कंप्यूटर सिस्टम्स, नेटवर्क्स या डिवाइसेज़ को नुकसान पहुंचा सकता है। इसमें वायरसेज़, रैंसमवेयर्स और ट्रोजन्स शामिल हैं।

- **ऑपरेटिंग सिस्टम**

कंप्यूटरों, टैबलेट्स और स्मार्टफोन्स पर चलने वाला बुनियादी सॉफ्टवेयर, जो अतिरिक्त एप्लिकेशन्स और हार्डवेयर को चलाने के लिए आवश्यक होता है।

- **फिशिंग**

धोखा देने वाली ईमेलें या टेक्स्ट मैसेजेस, जिनमें मैलवेयर युक्त वेबसाइटों के लिंक्स होते हैं या जो उपयोगकर्ताओं को धोखा देकर संवेदनशील जानकारी (जैसे पासवर्ड्स) का खुलासा करने या पैसे ट्रांस्फर करने के लिए उन्हें प्रेरित कर सकते हैं।

- **स्पाइवेयर**

उपयोगकर्ता की सहमति के बिना डिवाइस पर इंस्टॉल होने वाले मैलवेयर का एक प्रकार, जो डेटा एकत्र करता है और फिर इसे किसी तीसरे पक्ष को भेजता है।

- **सोशल मीडिया**

फेसबुक, X और इंस्टाग्राम जैसी वेबसाइटें और ऐप्स, जो लोगों को उपयोगकर्ता द्वारा पैदा की गई सामग्री (टेक्स्ट पोस्ट्स, फोटोज़ और वीडियो) को साझा करने और उनका जवाब देने की अनुमति देती हैं।

- **स्मार्टफोन**

कठिन फंक्शनैलिटी कर पाने में सक्षम आधुनिक मोबाइल फोन, जिनमें एंड्रॉयड और आईओएस ऑपरेटिंग सिस्टम्स शामिल हैं।

- **ट्रोजन**

वैध सॉफ्टवेयर के रूप में प्रस्तुत होने वाला एक प्रकार का मैलवेयर, जिसे लक्षित व्यक्ति के डिवाइस में अनधिकृत एक्सेस के लिए इस्तेमाल किया जाता है।

- **यूआरएल**

यूनिफॉर्म रिसोर्स लोकेटर। वर्ल्ड वाइड वेब पर एक पता, जैसे डोमेन नेम (उदाहरण के लिए www.bbc.co.uk)।

- **वायरस**

वैध सॉफ्टवेयर प्रोग्राम्स को संक्रमित करने के लिए डिज़ाइन किया गया एक प्रकार का मैलवेयर, जो उन प्रोग्राम्स के सक्रिय होने पर सभी नेटवर्क्स में व्याप्त हो जाता है।

आगे पढ़ने के लिए सामग्री

ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र से मार्गदर्शन

- साइबर अपराध, घटना या कमजोरी के बारे में रिपोर्ट करें
- अपने डिवाइसेज़ को सुरक्षित कैसे करें
- अपना मोबाइल फोन सुरक्षित करें
- फिशिंग
- घोटाले
- अपने सोशल मीडिया को सुरक्षित करें
- सोशल मीडिया और मैसेजिंग ऐप्स की सुरक्षा के लिए सुझाव

यूके एनसीएससी और एनपीएसए से मार्गदर्शन

- लोकतंत्र की रक्षा
- सोशल मीडिया: इसका सुरक्षापूर्वक उपयोग कैसे करें
- संगठनों के लिए डिवाइस सुरक्षा मार्गदर्शन, जिसमें मोबाइल भी शामिल है
- एप्लिकेशन स्टोर्स में खतरों की रिपोर्ट।
- ऊंचे खतरे वाले व्यक्ति-विशेषों के लिए व्यक्तिगत सुरक्षा और संरक्षण

यूएस एनएसए के लिए मार्गदर्शन

- मोबाइल डिवाइस के लिए सर्वोत्तम कार्यप्रथाएं

अस्वीकरण

कृपया ध्यान दें कि इस परामर्श-सूचना में प्रकाशन के समय प्रमाणित की गई जानकारी उपलब्ध कराई गई है।

यह रिपोर्ट संलेखन एजेंसी और उद्योग स्रोतों से प्राप्त जानकारी पर आधारित है। इसमें किसी भी निष्कर्ष और संस्तुति को सभी खतरों से बचाव के इरादे से प्रदर्शित नहीं किया गया है और संस्तुतियों का पालन करने से ऐसे सभी खतरे दूर नहीं होंगे। सिस्टम ओनर के लिए जानकारी के स्वामित्व से संबंधित खतरे हर समय मौजूद रहते है।

यूके में सूचना की स्वतंत्रता अधिनियम 2000 (एफओआईए) के तहत इस जानकारी के लिए अपवाद है और यूके के अन्य सूचना कानूनों के तहत भी इसके लिए अपवाद हो सकता है।

एफओआईए से संबंधित किसी भी पूछताछ को ncscinfoleg@ncsc.gov.uk पर भेजें।

परिशिष्ट: ध्यान में आए MOONSHINE और BADBAZAAR के नमूने

इस तालिका में पिछले दो वर्षों में MOONSHINE और BADBAZAAR अभियानों में इस्तेमाल की गई ऐप्स को सूचीबद्ध किया गया है।

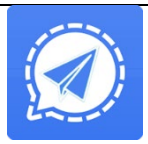
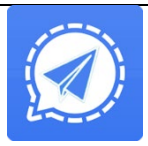
इनमें से कई ऐप्स भली-भांति स्थापित ऐप्स के साथ स्पष्ट रूप से समानता दिखाती हैं। इस बात की संभावना है कि यह प्रसिद्ध ब्रांडों को 'स्पूफ' करने के लिए कर्ता की एक सोची-समझी तकनीक है।

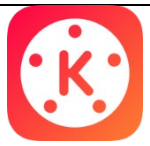
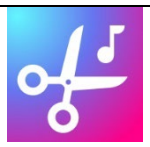
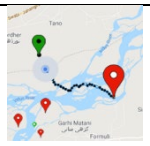
यह नोट करना महत्वपूर्ण है कि ऐप का नाम, पैकेज का नाम और आइकन, ये सभी वास्तविक एप्लिकेशन की नकल या इससे मिलते-जुलते हो सकते हैं, और इसलिए केवल इस बात की पहचान करने के लिए इसका उपयोग नहीं किया जाना चाहिए कि कोई डिवाइस संक्रमित है या नहीं।

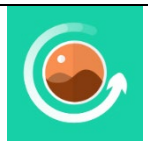
जैसा कि मिटिगेशन्स अनुभाग में शामिल है, आप 'Improve harmful app detection' इनेबल करके अपने एंड्रॉयड डिवाइस में मौजूद ऐप्स को गूगल के पास भेज सकते/ती हैं, जो आपके डिवाइस पर प्ले स्टोर के बाहर से इंस्टॉल की गई ऐप्स को स्कैन करेगा।

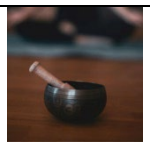
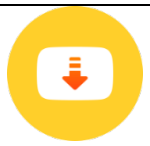
ऐप का नाम	पैकेज का नाम	ऐप का आइकन
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

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.buddhistssongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

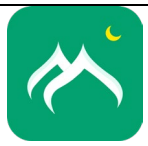
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
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	
com.mobisystems.mobiscanner	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	

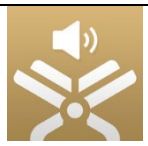
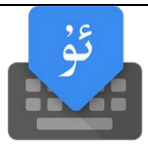
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
com.iudesk.android.photo.editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	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	TubePlus	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
com.ziipin.softkeyboard	Video Converter	
com.inverseai.video_converter	Video Cutter	
com.naing.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	
com.quvideo.xiaoying.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	
com.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