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

নির্দেশিকা

BADBAZAAR এবং MOONSHINE: উইঘুর, তাইওয়ানিজ এবং তিব্বতি গোষ্ঠী এবং নাগরিক সমাজের কর্মীদের লক্ষ্য করছে স্পাইওয়্যার

৯ এপ্রিল ২০২৫

BADBAZAAR এবং MOONSHINE: উইঘুর, তাইওয়ানিজ এবং তিব্বতি গোষ্ঠী এবং নাগরিক সমাজের কর্মীদের লক্ষ্য করছে স্পাইওয়্যার

NCSC এবং অংশীদারেরা দুটি স্পাইওয়্যার ভেরিয়েন্টের উচ্চ ঝুঁকিতে থাকা ব্যক্তিদের জন্য নতুন তথ্য এবং ঝুঁকি হ্রাসের পন্থা প্রকাশ করছে।

সারসংক্ষেপ

যুক্তরাজ্যের সাইবার লীগ এর সহায়তায় ন্যাশনাল সাইবার সিকিউরিটি সেন্টার (NCSC UK) এবং আন্তর্জাতিক অংশীদাররা যৌথভাবে এই নির্দেশিকাটি তৈরি করেছে:

- **অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টার, অস্ট্রেলিয়ান সিগন্যালস ডিরেক্টরেটের অংশ**
- **কানাডিয়ান সেন্টার ফর সাইবার সিকিউরিটি, কমিউনিকেশনস সিকিউরিটি এস্টাবলিশমেন্টের অংশ**
- **জার্মান ফেডারেল ইন্টেলিজেন্স সার্ভিস**
- **জার্মান ফেডারেল অফিস ফর দ্য প্রোটেকশন অফ দ্য কনস্টিটিউশন**
- **নিউজিল্যান্ড ন্যাশনাল সাইবার সিকিউরিটি সেন্টার, সরকারি যোগাযোগ নিরাপত্তা ব্যুরোর অংশ**
- **মার্কিন যুক্তরাষ্ট্রের ফেডারেল ব্যুরো অফ ইনভেস্টিগেশন**
- **মার্কিন যুক্তরাষ্ট্রের জাতীয় নিরাপত্তা সংস্থা**

এর উদ্দেশ্য হল তাইওয়ান, তিব্বত, জিনজিয়াং উইঘুর স্বায়ত্তশাসিত অঞ্চল, গণতন্ত্র আন্দোলন এবং ফালুন গং সহ বিভিন্ন বিষয়ের সাথে যুক্ত ব্যক্তিদের সাইবার অপরাধীরা যে ক্রমবর্ধমান হুমকি দিচ্ছে সে সম্পর্কে সচেতনতা বৃদ্ধি করা।

এই নির্দেশিকাটিতে দুটি কেস স্টাডি অন্তর্ভুক্ত রয়েছে যেখানে ক্ষতিকারক সাইবার অপরাধীরা যে কৌশলে BADBAZAAR এবং MOONSHINE নামে পরিচিত স্পাইওয়্যার ব্যবহার করে স্মার্টফোন সহ মোবাইল ডিভাইসের ডেটা লক্ষ্যবস্তু করে তার বিশদ বর্ণনা দেয়া হয়েছে যা চীনা রাষ্ট্রের জন্য আগ্রহের বিষয় হতে পারে। এটি নিজেকে, নিজের ফোন আর তাদের তথ্য নিরাপদ রাখতে কীভাবে সাহায্য পাওয়া যায়, সে ব্যাপারে মানুষকে দিকনির্দেশনা দেয়।

এই নির্দেশিকার পাশাপাশি, NCSC আলাদা নির্দেশাবলী সহ সম্পূর্ণ প্রযুক্তিগত বিবরণ প্রকাশ করেছে।

কারা ঝুঁকিতে রয়েছে

প্রতিবেদক সংস্থা এবং শিল্প অংশীদাররা লক্ষ্য করেছেন যে BADBAZAAR এবং MOONSHINE বিশেষভাবে চীনা রাষ্ট্র কর্তৃক তাদের অভ্যন্তরীণ কর্তৃত্ব, উচ্চাকাঙ্ক্ষা এবং বিশ্বব্যাপী খ্যাতির জন্য হুমকিস্বরূপ বিবেচিত বিষয়গুলির সাথে যুক্ত ব্যক্তিদের লক্ষ্য করে তৈরি করা হয়েছে। সবচেয়ে বেশি ঝুঁকির মধ্যে রয়েছে, তবে সীমাবদ্ধ নয়, এর সাথে যুক্ত যে কেউ:

- **তাইওয়ানি স্বাধীনতা**
- **তিব্বতের অধিকার**
- **উইঘুর মুসলিম এবং চীনের শিনজিয়াং উইঘুর স্বায়ত্তশাসিত অঞ্চলের অন্যান্য জাতিগত সংখ্যালঘু জনগণ**
- **গণতন্ত্রের পক্ষে (হংকং সহ)**
- **ফালুন গং আধ্যাত্মিক আন্দোলন**

এর মধ্যে রয়েছে বেসরকারি সংস্থা (এনজিও), সাংবাদিক, ব্যবসা প্রতিষ্ঠান এবং ব্যক্তি যারা এই গোষ্ঠীগুলির পক্ষে কথা বলেন, নিজেদেরকে তাদের অংশ মনে করেন, বা অন্য যেকোনোভাবে এই গোষ্ঠীগুলোর প্রতিনিধিত্ব করেন। এই স্পাইওয়্যারটি যেভাবে নির্বিচারে অনলাইনে ছড়িয়ে দেওয়া হচ্ছে তার অর্থ হল সম্ভাব্য ভুক্তভোগীদের বাইরেও সংক্রমণ ছড়িয়ে পড়ার ঝুঁকি রয়েছে।

এই নির্দেশিকার লক্ষ্য হল যারা ঝুঁকিতে আছেন তাদের BADBAZAAR এবং MOONSHINE স্পাইওয়্যারের সুনির্দিষ্ট হুমকি কার্যকরভাবে মোকাবেলায় সহায়তা করা। ঝুঁকি হ্রাসের প্রস্তাবিত পন্থাগুলি বৃহত্তর সাইবার নিরাপত্তা পরামর্শের পরিপূরক এবং এগুলিকে বিচ্ছিন্নভাবে বিবেচনা করা উচিত নয়।

এই নির্দেশিকাতে উল্লিখিত নির্দেশিকা অনুসরণ করে, ব্যবহারকারীরা তাদের মোবাইল ডিভাইস এবং ডেটা সংক্রমণের ঝুঁকি কমাতে পারেন।

হুমকি

MOONSHINE এবং BADBAZAAR হল ট্রোজানের দুটি উদাহরণ; এগুলোর ভেতরে ক্ষতিকর ফিচার লুকানো থাকে, যদিও দেখায় একেবারে সাধারণ অ্যাপের মতো, যেগুলো অ্যাপ স্টোর বা ফাইল শেয়ারিং সাইট থেকে ডাউনলোড করা যায়।

এই অ্যাপগুলি এমনভাবে তৈরি করা হয়েছে যাতে ব্যবহারকারীরা না বুঝে এগুলিকে তাদের ডিভাইসে ডাউনলোড এবং ইনস্টল করে। একবার অ্যাপটি ইনস্টল হয়ে গেলে, এটি ডিভাইসের দুর্বলতা ব্যবহার করে অনুমতি ছাড়া কিছু কাজ করতে পারে, অথবা ব্যবহারকারীর কাছ থেকে অনুমতি নিয়ে ফোন থেকে তথ্য এক্সেস বা ডাউনলোড করতে পারে, যেমন:

- **রিয়েল টাইম ট্র্যাকিং সহ অবস্থানের ডেটা**
- **মাইক্রোফোন এবং ক্যামেরায় অ্যাক্সেস**
- **মেসেজ, ফটো এবং ডিভাইসে সংরক্ষিত অন্যান্য ফাইল**
- **ডিভাইসের তথ্য এবং আরও অনেক কিছু**

তারপর এই সাইবার হামলাকারীরা ঝুঁকিতে থাকা মানুষের ন্যায্য স্বার্থকে কাজে লাগিয়ে যত বেশি সম্ভব লোককে শনাক্ত করে এবং সংক্রমিত করে, যাতে তারা তাদের ডিভাইসের তথ্যে ঢুকতে পারে। এটি করার একটি উপায় হল তারা এমন অ্যাপ ডিজাইন করে যা তারা জানে যে তাদের ভুক্তভোগীদের কাছে পছন্দসই হবে, যেমন এমন অ্যাপ যা তাদের মাতৃভাষায় ব্যবহারযোগ্য, অথবা চীনের তিব্বতি অঞ্চল বা জিনজিয়াংয়ের মতো জায়গা-ভিত্তিক কনটেন্ট থাকে।

এই নির্দেশিকার কেস স্টাডিতে এর কিছু উদাহরণ দেওয়া হয়েছে, যার মধ্যে রয়েছে TibetOne এবং Wyghur Quran অ্যাপ।

এই সাইবার অপরাধীরা অনলাইন ফোরামে সক্রিয় যেখানে তাদের অভিপ্রেত শিকারদের একটি ব্যবহারকারী দল রয়েছে, যা তাদের শিকারদের সংক্রমিত করার সম্ভাবনা বাড়িয়ে তোলে। তিব্বত-সম্পর্কিত টেলিগ্রাম চ্যানেল এবং রেডডিট ফোরামে তাদের ইচ্ছাকৃতভাবে স্পাইওয়্যার শেয়ার করতে দেখা গেছে। এই নির্দেশিকার কেস স্টাডিগুলিতে এই পদ্ধতিগুলির উদাহরণও দেওয়া হয়েছে।

ক্ষতিকারক অ্যাপগুলি প্রায়শই স্বতন্ত্র ফাইল হিসাবে শেয়ার করা হয়, যেমন অ্যান্ড্রয়েডে APK ফাইল, যা ব্যবহারকারীদের ডাউনলোড এবং ইনস্টল করতে হয়। সাইবার অপরাধীরা তাদের স্পাইওয়্যারটিকে গুগল প্লে স্টোর এবং অ্যাপল অ্যাপ স্টোরের মতো অফিসিয়াল অ্যাপ স্টোরে আপলোড করে অথবা পূর্বে ব্যবহারযোগ্য অ্যাপগুলিতে ক্ষতিকারক কোড যুক্ত করে আরও বৈধ দেখানোর চেষ্টা করে, যদিও অফিসিয়াল স্টোরগুলিতে সুরক্ষা বৈশিষ্ট্য এবং যাচাই প্রক্রিয়া রয়েছে যা এই কৌশলটির সফলতা হ্রাস করে দেয়। এটি অফিসিয়াল স্টোর থেকে আসা অ্যাপগুলিকে নিরাপদ করে তোলে, কিন্তু কেস স্টাডি এবং NCSC এর অ্যাপ স্টোর থ্রেট রিপোর্ট এ যেমন দেখানো হয়েছে, এই প্রক্রিয়াগুলি নিখুঁত নয়।

এই ৪টি টিপস অনুসরণ করলে এই নির্দেশিকাতে বর্ণিত হুমকি থেকে আপনাকে রক্ষা করা যেতে পারে।

আরও বিস্তারিত পরামর্শের জন্য, মিটিগেশন বিভাগটি দেখুন।

কেস স্টাডি

এই দুটি কেস স্টাডি দেখায় MOONSHINE এবং BADBAZAAR কীভাবে কাজ করে এবং কীভাবে সাইবার অপরাধীরা সবচেয়ে বেশি ঝুঁকিতে থাকা ব্যক্তিদের লক্ষ্যবস্তু করছে।

কেস স্টাডি একঃ MOONSHINE

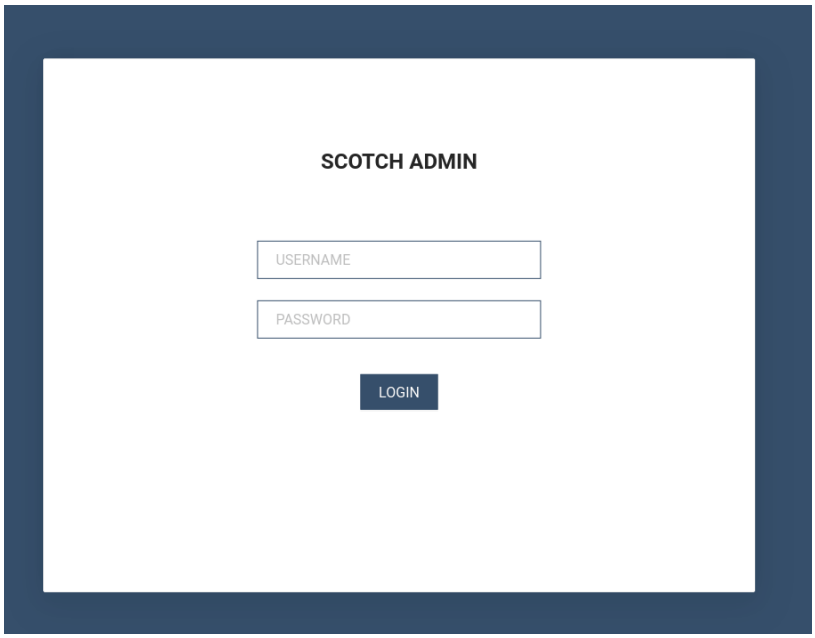
MOONSHINE হল একটি অ্যান্ড্রয়েড স্পাইওয়্যার যা তিব্বতি গোষ্ঠীগুলির উপর নজরদারি করছিল বলে ২০১৯ সালে Citizen Lab রিপোর্ট করেছিল। MOONSHINE একটি বৈধ অ্যাপ হিসেবে ছদ্মবেশ ধারণ করে যাতে এটি ইনস্টল করার জন্য ভুক্তভোগীদের প্রলুব্ধ করা যায়। টেলিগ্রাম চ্যানেল ও হোয়াটসঅ্যাপ লিংকের মাধ্যমে এটি ছড়ানো হয়েছে।

MOONSHINE-এর নজরদারি ক্ষমতা অনেক বিস্তৃত, যেমনঃ

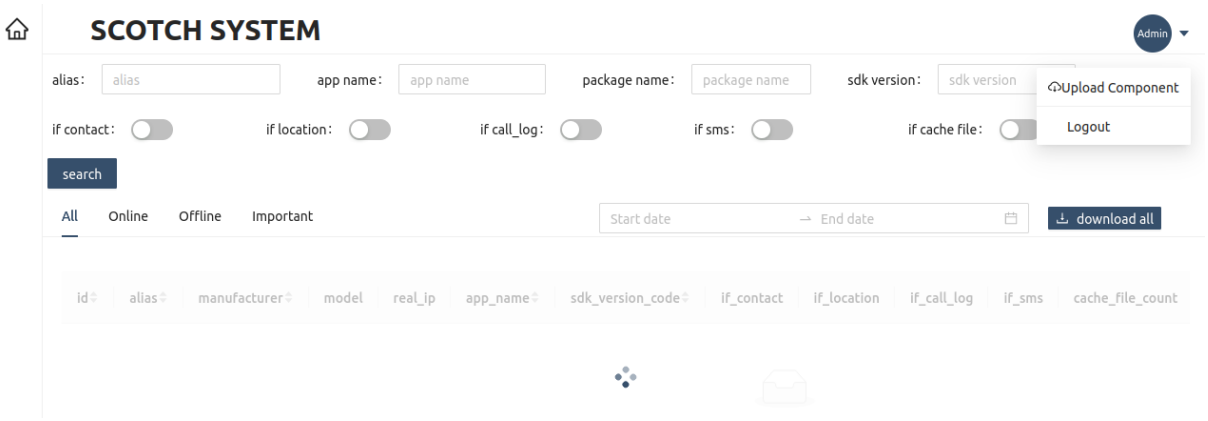
- **আপনি কোথায় আছেন তা তাৎক্ষনিক দেখতে পারে**
- **তাৎক্ষনিক অডিও এবং ছবি ধারন করতে পারে**
- **ডিভাইস থেকে ফাইল ডাউনলোড করতে পারে**
- **ডিভাইস সম্পর্কিত তথ্য জেনে নিতে পারে**
- **ডিভাইসে অডিও বাজাতে পারে**

‘ئاۋازلىق قۇرائن.apk’ অ্যাপ্লিকেশনটি, যার অনুবাদ ‘অডিও কুরআন.apk’, উইঘুরদের লক্ষ্য করার জন্য কীভাবে MOONSHINE ব্যবহার করা হয় তার একটি উদাহরণ। ফাইলের নামে কুরআন অ্যাপ্লিকেশন নির্দেশ করে উইঘুর ভাষা ব্যবহার করা হয়, যা সম্ভবত উইঘুর মুসলমানদের আবেদন করার জন্য তৈরি করা হয়েছিল।

একবার ইনস্টল হয়ে গেলে, সাইবার অপরাধীরা ভুক্তভোগীদের ডিভাইস থেকে তথ্য সংগ্রহ করতে পারে। এই তথ্য ‘SCOTCH ADMIN’ প্যানেলের মাধ্যমে অ্যাক্সেস করা হয়।



লগ ইন করার পরে, সাইবার অপরাধীরা নীচের স্ক্রিনশটে দেখানো পৃষ্ঠাটি অ্যাক্সেস করতে পারে। এই পৃষ্ঠায় সংক্রামিত ডিভাইসের বিবরণ এবং সংক্রামিত ডিভাইসগুলিতে সাইবার অপরাধীদের অ্যাক্সেসের পরিমাণ প্রদর্শন করা হয়েছে:



ম্যালওয়্যার ব্যবস্থাপনা প্যানেলে সংগৃহীত ডেটা দেখানো হয় যার মধ্যে রয়েছে:

- **ডিভাইসে নিয়ন্ত্রণের পরিমান**
- **এসএমএস বার্তা**
- **কল লগ**
- **অবস্থান সম্পর্কিত ডেটা**
- **ডিভাইসের তথ্য**

সাইবার লিগের সহযোগিতায়, NCSC Trend Micro-এর রিপোর্টের ভিত্তিতে গবেষণা চালিয়ে দেখেছে যে MOONSHINE স্পাইওয়্যারের এক্সপ্লয়টেশন কিটের সঙ্গে কিছু লগইন প্যানেলের মিল রয়েছে, যেগুলোর HTML টাইটেলে 'UPSEC' লেখা আছে। সংযুক্ত প্রযুক্তিগত নির্দেশিকাতে সম্পূর্ণ বিবরণ রয়েছে।

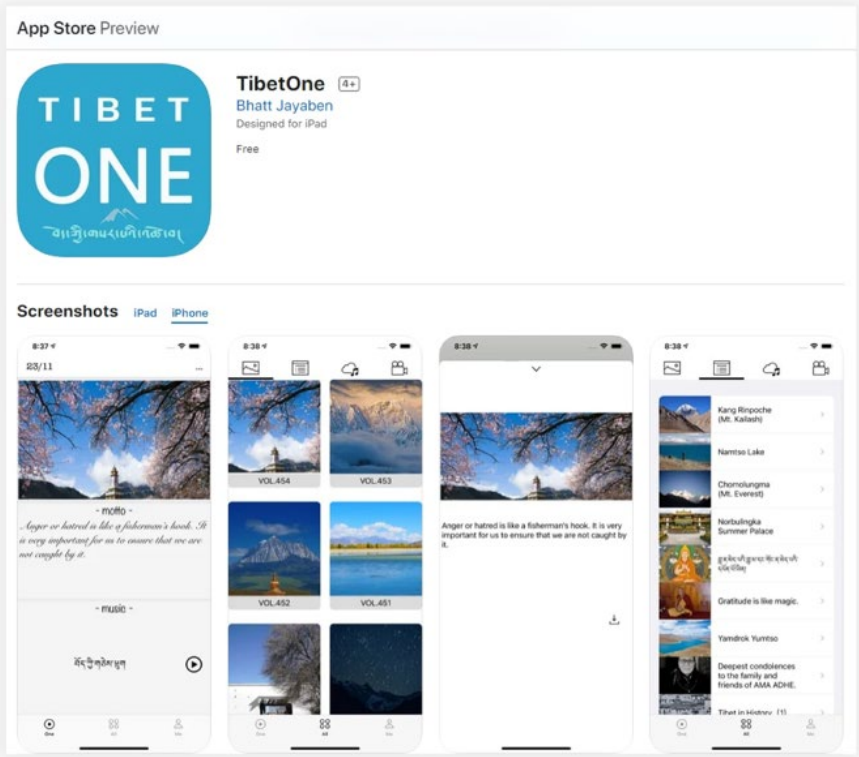
ইন্টেলিজেন্স অনলাইন অনুসারে, UPSEC" নামটি আসলে 'সিচুয়ান ডিয়াঙ্কে নেটওয়ার্ক সিকিউরিটি টেকনোলজি কোং লিমিটেড' কে বোঝাতে ব্যবহার করা হয়েছে। রিপোর্ট প্রদানকারী সংস্থাগুলি এই বিবৃতিটি নিজেরা যাচাই করেনি।

কেস স্টাডি দুইঃ BADBAZAAR

BADBAZAAR হল iOS এবং Android ভেরিয়েন্ট সহ একটি মোবাইল ম্যালওয়্যার যা উইঘুর, তিব্বতি এবং তাইওয়ানিজদের লক্ষ্যবস্তু করেছে। এই ম্যালওয়্যারটি সোশ্যাল মিডিয়া প্ল্যাটফর্ম এবং অফিসিয়াল অ্যাপ স্টোরের মাধ্যমে ছড়িয়ে পড়েছে।

Lookout এবং Volexity এর রিপোর্ট অনুসারে, 'TibetOne' অ্যাপের মাধ্যমে তিব্বতিদের উপর নজরদারির জন্য BADBAZAAR ব্যবহার করা হয়েছে। TibetOne হল একটি iOS অ্যাপ যা সাইবার অপরাধীরা তৈরি করেছে, যার রয়েছে ডিভাইসের তথ্য এবং অবস্থানের ডেটা অ্যাক্সেস করার সক্ষমতা। এটি ২০২১ সালের ডিসেম্বরে অ্যাপল অ্যাপ স্টোরে আপলোড করা হয়েছিল কিন্তু এখন আর পাওয়া যাচ্ছে না। ম্যালওয়্যারটি আরও ছড়িয়ে দেওয়ার জন্য, সাইবার অপরাধীরা 'tibetanphone' নামে একটি টেলিগ্রাম চ্যানেলেও অ্যাপটির বিজ্ঞাপন দিয়েছে।

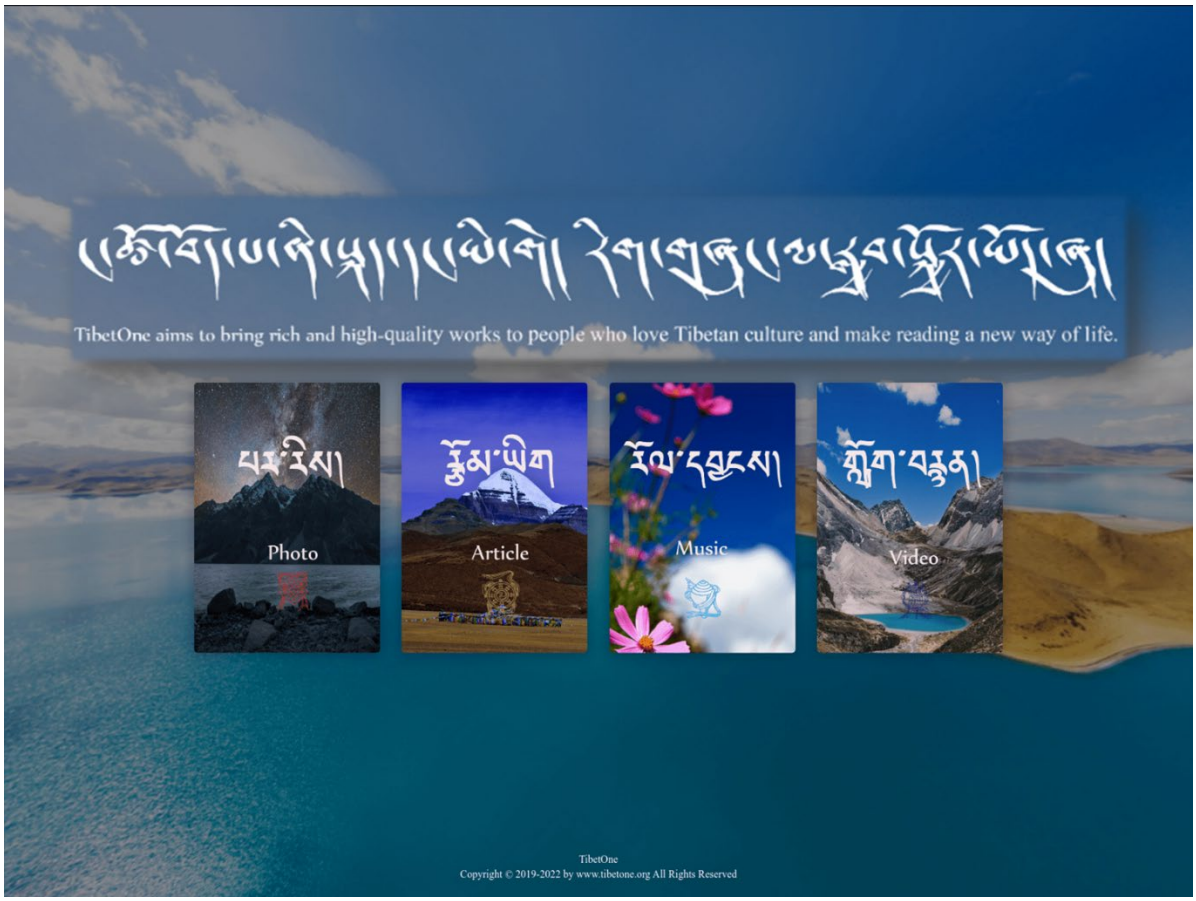
TibetOne



চিত্র 1: অ্যাপল অ্যাপ স্টোরে TibetOne অ্যাপ পেইজ। অ্যাপটি তখন থেকে সরিয়ে ফেলা হয়েছে।

চিত্র 2: টেলিগ্রাম চ্যানেলগুলিতে ছড়িয়ে পড়া TibetOne।

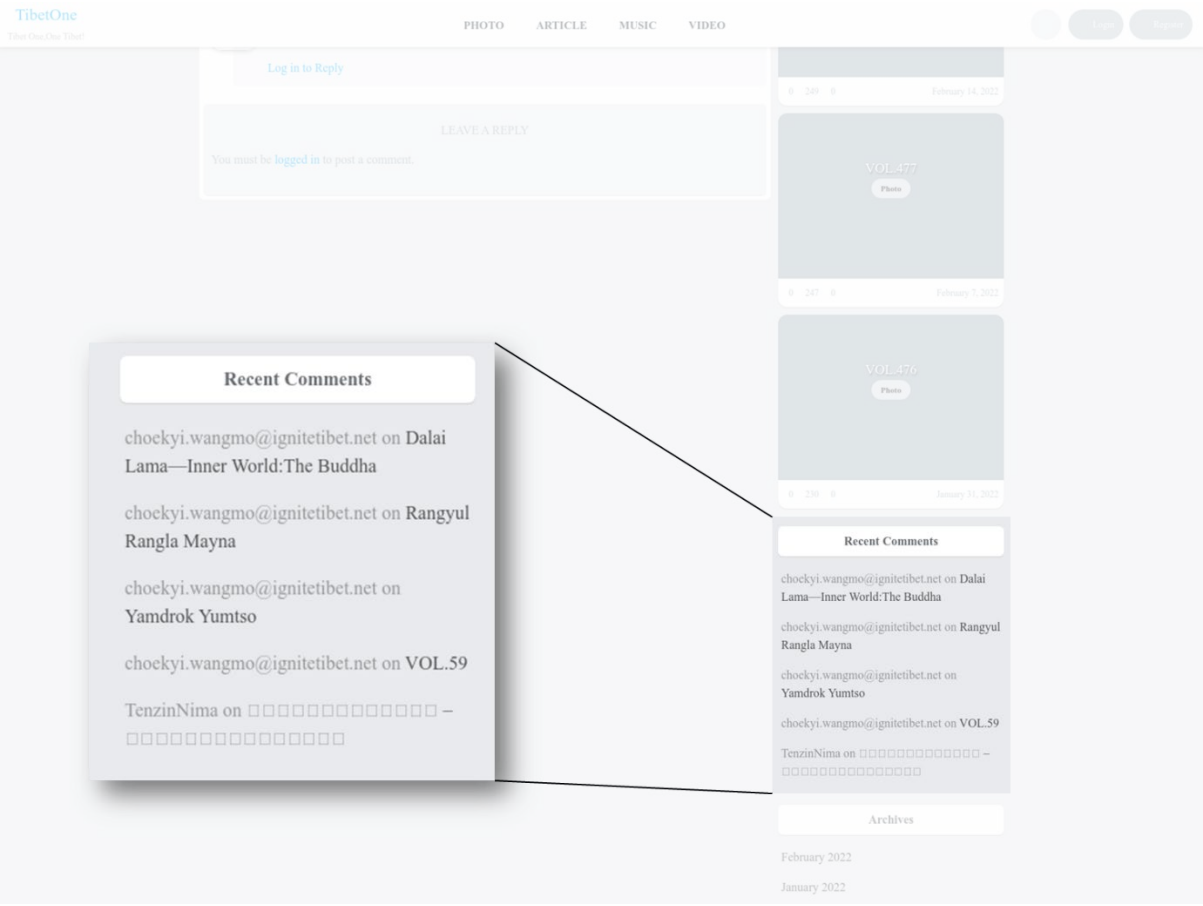
অ্যাপটিকে বৈধতা দেওয়ার জন্য, সাইবার অপরাধীরা **'tibetone[.]org'** নামে একটি ওয়েবসাইটও তৈরি করেছে, যা নিজেকে *'তিব্বতি সংস্কৃতি ভালোবাসে এমন লোকেদের কাছে সমৃদ্ধ এবং উচ্চমানের কাজ নিয়ে আসে এবং পড়াকে জীবনের একটি নতুন উপায় করে তোলে'* বলে বর্ণনা করেছে।



চিত্র 3: 'tibetone[.]org'-এর হোমপেজ।

সংশ্লিষ্ট বিভাগগুলি আরও স্পষ্ট করার জন্য এই ছবিটি সম্পাদনা করা হয়েছে।

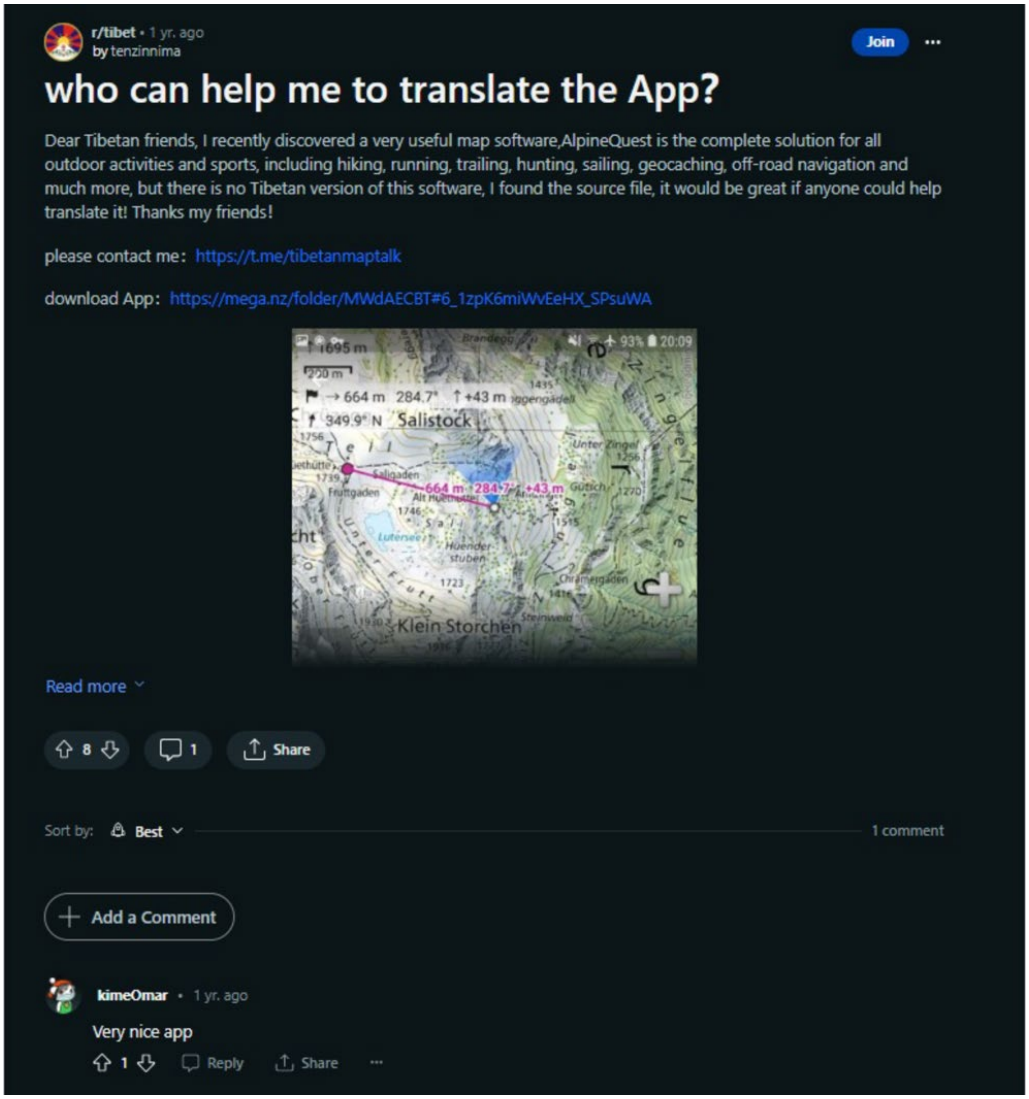
এই ওয়েবসাইটে নিবন্ধগুলির জন্য একটি পৃষ্ঠা ছিল যেখানে ব্যবহারকারীদের মন্তব্য করার সুযোগ ছিল। **'choekyi.wangmo@ignitetibet.net'** ইমেল ঠিকানা থেকে একটি মন্তব্য করা হয়েছে, যা ধারণা করা হচ্ছে সাইবার অপরাধীদের নিয়ন্ত্রণে ছিল এবং সম্ভবত তারা **'Choekyi Wangmo'**-এর ছদ্মবেশ ধারণ করছে যাকে তিবেতান সেন্টার অফ হিউম্যান রাইটস অ্যান্ড ডেমোক্রেসি একজন তিব্বতপন্থী আন্দোলনকারী হিসেবে চিহ্নিত করে। এটি সম্ভবত এই ধারণা দেওয়ার আরেকটি প্রচেষ্টা যে অ্যাপটি প্রকৃতপক্ষে তিব্বতের স্বাধীনতার পক্ষে।



চিত্র 2: 'tibetone[.]org' পৃষ্ঠাটিতে এমন কিছু ব্যবহারকারীদের মন্তব্য দেখা যাচ্ছে যাদের সাইবার অপরাধীদের দ্বারা নিয়ন্ত্রিত বলে ধারণা করা হচ্ছে।

সংশ্লিষ্ট বিভাগগুলি আরও স্পষ্ট করার জন্য এই ছবিটি সম্পাদনা করা হয়েছে।

'TenzinNima' হল আরেকটি ব্যবহারকারীর নাম যা এই সাইটে মন্তব্য যুক্ত করেছে। Volexity রিপোর্ট করেছে যে এই ইউজারনেমটি Reddit-এ টেলিগ্রাম চ্যানেল **'Tibetanmaptalk'**-এর বিজ্ঞাপন দেওয়ার জন্যও ব্যবহার করা হয়েছে। এতে Android ডিভাইসে পাওয়া যায় একটি নেভিগেশন অ্যাপ 'AlpineQuest'-এর একটি ক্ষতিকারক নমুনা ডাউনলোড করার লিঙ্ক রয়েছে। প্রদত্ত ডাউনলোড লিঙ্কটি Mega নামক একটি তৃতীয়-পক্ষের ফাইল-শেয়ারিং পরিষেবার জন্য।



চিত্র 3: Reddit পোস্টে ক্ষতিকারক অ্যাপ্লিকেশনের বিজ্ঞাপন সাইবার অপরাধীদের অ্যাকাউন্ট দ্বারা নিয়ন্ত্রিত বলে মনে করা হচ্ছে।

Volexity আরও উল্লেখ করেছে যে 'KimeOmar' নামে পরিচিত একজন ব্যবহারকারী যিনি পোস্টটিতে মন্তব্য করেছিলেন তাকে অন্য একটি সাব-রেডডিট ফোরামে ক্ষতিকারক অ্যাপ শেয়ার করতে দেখা গেছে। এতে বুঝা যায় যে সাইবার অপরাধীরা একাধিক সোশ্যাল মিডিয়া প্রোফাইল ব্যবহার করে, যাতে তাদের পোস্টগুলো সত্যি বা বিশ্বাসযোগ্য মনে হয়।

মুল্যায়ন

BADBAZAAR এবং MOONSHINE উইঘুর, তিব্বতি এবং তাইওয়ানিজ সম্প্রদায়কে বিশেষভাবে লক্ষ্য করার জন্য বেশ কয়েকটি সামাজিক প্রকৌশল পদ্ধতি ব্যবহার করে, যেমনঃ

- এই সম্প্রদায়ের আগ্রহের অ্যাপগুলির ট্রোজানাইজেশন, যেমন উইঘুর ভাষার কুরআন অ্যাপ, প্রায় নিশ্চিতভাবেই ভুক্তভোগীদের উদ্দেশ্য করে তৈরি করা হয়েছে
- অফিসিয়াল অ্যাপ স্টোরগুলিতে এই ট্রোজানাইজড অ্যাপগুলি যুক্ত করার ফলে বৈধতার গ্রহণযোগ্যতা খুব বেশি হয় বলে মনে হয়, এবং গ্রুপ চ্যাটে ছড়িয়ে দেয়ার উদ্দেশ্য হল খুব সম্ভবত এই সম্প্রদায়ের মধ্যে বিশ্বস্ত সম্পর্কগুলিকে কাজে লাগানো।

BADBAZAAR এবং MOONSHINE এমন তথ্য সংগ্রহ করে যা চীনা রাষ্ট্রের জন্য প্রায় নিশ্চিতভাবেই মূল্যবান হবে। যদিও BADBAZAAR এবং MOONSHINE উইঘুর, তিব্বতি এবং তাইওয়ানিজ ব্যক্তিদের লক্ষ্য করে বলে দেখা গেছে, অন্যান্য ম্যালওয়্যারও রয়েছে যা চীনের অন্যান্য সংখ্যালঘু গোষ্ঠীকে লক্ষ্যবস্তু করে। চীন এবং বিদেশে একাত্মতা ঘোষণাকারী দেশগুলির নাগরিক, যারা চীন সরকারের শাসনের স্থিতিশীলতার জন্য হুমকিস্বরূপ বিষয়গুলিকে সমর্থন করে বলে মনে করা হয়, তারা প্রায় নিশ্চিতভাবেই BADBAZAAR এবং MOONSHINE এর মতো মোবাইল ম্যালওয়্যারের হুমকির মুখে আছে। লোকেশন, অডিও ও ছবি সংগ্রহ করার ক্ষমতা থাকায়, ম্যালওয়্যারগুলো প্রায় নিশ্চিতভাবেই ভবিষ্যতে নজরদারি ও হয়রানির জন্য ব্যবহার করা যেতে পারে—কারণ এগুলোর মাধ্যমে টার্গেটকৃত ব্যক্তি সম্পর্কে সকল তথ্য রিয়েল-টাইমে জানা যায়।

মোবাইল অ্যাপ ব্যবহারকারীদের জন্য ঝুঁকি হ্রাসের পন্থা

কেস স্টাডিতে বর্ণিত হুমকি থেকে রক্ষা করার জন্য রিপোর্ট প্রদানকারী সংস্থাগুলি নিম্নলিখিত সুরক্ষা পদ্ধতিগুলি ব্যবহার করার জন্য উৎসাহিত করে। এই সুপারিশগুলি NCSC কর্তৃক প্রদত্ত এমন নির্দেশনা, যা সর্বোত্তম ও কার্যকর পদ্ধতি হিসেবে স্বীকৃত। অস্ট্রেলিয়া এবং মার্কিন যুক্তরাষ্ট্রের পাঠকদের জন্য সর্বোত্তম নির্দেশিকা সম্পর্কিত লিঙ্ক পেতে 'আরও পড়ুন' অংশটি দেখুন।

আপনার ডিভাইসটি সুরক্ষিত রাখুন

- **শুধুমাত্র অফিসিয়াল অ্যাপ স্টোর থেকেই অ্যাপ ডাউনলোড করুন, যেমন Google এর Play Store বা Apple এর App Store।** গুগলের প্লে স্টোর এবং অ্যাপলের অ্যাপ স্টোর সফটওয়্যারটিকে লভ্য করার আগে ভাইরাসের জন্য স্ক্যান করে, যা আপনাকে আরও নিশ্চিত করে যে আপনি যা ডাউনলোড করছেন তা নিরাপদ। বিশ্বস্ত স্টোর থেকে অ্যাপ কিনলেও ঝুঁকি থেকে যেতে পারে, তবে অন্যান্য উৎস থেকে ডাউনলোডের কোনও সুরক্ষা নাও থাকতে পারে। NCSC অ্যাপ স্টোরগুলির উপর একটি হুমকি প্রতিবেদন প্রকাশ করেছে: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **আপনার ডিভাইস এবং অ্যাপগুলিকে আপডেট রাখুন।** আপনার অ্যাপ এবং ডিভাইস সফ্টওয়্যারের আপডেট পাওয়া মাত্রই ইনস্টল করুন। যদি অপশন থাকে তবে আপনার ডিভাইসের সেটিংসে 'স্বয়ংক্রিয় আপডেট' চালু করুন যাতে আপনাকে এটি করার কথা মনে রাখতে না হয়। পরিচিত ভাইরাস এবং অন্যান্য ধরণের ম্যালওয়্যার থেকে রক্ষা পেতে অনলাইনে সুরক্ষিত থাকার বিষয়ে NCSC নির্দেশিকা দেখুন। আপডেটগুলিতে প্রায়শই আগের চেয়ে ভাল এবং নতুন বৈশিষ্ট্য অন্তর্ভুক্ত থাকে: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **আপনার ডিভাইসটিকে 'জেলব্রেক' বা 'রুট' করবেন না** কারণ এটি বিদ্যমান নিরাপত্তা ব্যবস্থাগুলিকে বাইপাস করার জন্য আনপ্যাচড ফাঁকফোকরগুলি ব্যবহার করে। এর ফলে ডিভাইসটি আরও বেশি আক্রমণের ঝুঁকিতে থাকে। NCSC নির্দেশিকা দেখুন: https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

আপনার অ্যাপগুলি ঠিকভাবে ব্যবহার এবং নিয়ন্ত্রণ করুন

- **আপনার অ্যাপ এবং এগুলির অনুমতিগুলি পর্যালোচনা করুন।** যদি আপনার কোনও অ্যাপের আর প্রয়োজন না হয়, তাহলে এটি মুছে ফেলুন। সম্ভব হলে, ডেটা এক্সপোজার কমাতে অ্যাপের অনুমতি সীমাবদ্ধ করুন, কারণ ম্যালওয়্যার প্রায়শই সুরক্ষিত ফাইল বা পেরিফেরাল, যেমন ক্যামেরা এবং মাইক্রোফোনে অ্যাক্সেস করার জন্য ডিজাইন করা হয়।
  - অ্যাপল ব্যবহারকারীদের জন্য অ্যাপের অনুমতি কীভাবে পরীক্ষা করবেন: https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - অ্যান্ড্রয়েড ব্যবহারকারীদের জন্য অ্যাপের অনুমতি কীভাবে পরীক্ষা করবেন: https://support.google.com/android/answer/9431959?hl=en-GB

- **অজানা অ্যাপগুলি স্বয়ংক্রিয়ভাবে Google-এ পাঠান।** যদি আপনি একজন Android ব্যবহারকারী হন এবং এমন একটি অ্যাপ ডাউনলোড করে থাকেন যা Google-এর Play Store থেকে আসে না, তাহলে আপনি Google-এর Play Store অ্যাপ সেটিংসে 'Play Protect'-এর অধীনে 'ক্ষতিকারক অ্যাপ সনাক্তকরণ উন্নত করুন' এই অপশনটি চালু করে Google-এ পাঠাতে পারেন। এটি ম্যালওয়্যার সনাক্তকরণের জন্য অ্যাপটি স্ক্যান করে ব্যবহারকারীদের সুরক্ষায় সহায়তা করবে। এটি কীভাবে সেট আপ করবেন সে সম্পর্কে তথ্য: https://support.google.com/android/answer/2812853?hl=en-GB

সাইবার পরিষেবা ব্যবহার করুন

- **কোনও লিঙ্কে ক্লিক করার আগে URL রেপুটেশন পরিষেবা ব্যবহার করুন।** গুগল ট্রান্স প্যারেন্সি রিপোর্ট অথবা ভাইরাস টোটাল এর মতো পরিষেবা ব্যবহার করে প্রথমে স্ক্যান করে আপনি কোনও ইমেল, টেক্সট মেসেজ বা অন্য কোথাও থেকে আসা কোনও লিঙ্ক **নিরাপদ কিনা তা পরীক্ষা করতে পারেন ।** আপনি ভাইরাস টোটালের মতো ম্যালওয়্যার বিশ্লেষকে সন্দেহজনক ফাইল এবং অ্যাপ আপলোড করতে পারেন যা কোনও ফাইল ক্ষতিকারক কিনা তা শনাক্ত করতে সহায়তা করতে পারে। সচেতন থাকুন যে স্ক্যানিং পরিষেবাগুলি মিথ্যা নেতিবাচক ফলাফল তৈরি করতে পারে।

- **গুগল অ্যাডভান্সড প্রোটেকশন প্রোগ্রামে নাম লেখান।** এটি একটি বিনামূল্যের পরিষেবা যা Google পরিষেবা (যেমন Gmail, Play Store, ইত্যাদি) ব্যবহার করে এবং ক্ষতিগ্রস্ত হওয়ার ঝুঁকিতে থাকা ব্যক্তিদের সুরক্ষার জন্য ডিজাইন করা হয়েছে। এই পরিষেবাটি Google পরিষেবাগুলি ব্যবহার করার সময় উচ্চতর সুরক্ষা প্রদান করে: https://landing.google.com/advancedprotection/

- **যেসব জায়গায় অতিরিক্ত সহায়তা পাওয়ার সুযোগ আছে, সেগুলোতে নাম লেখান।** উদাহরণস্বরূপ, যুক্তরাজ্যে যারা সাইবার আক্রমণের ঝুঁকিতে রয়েছেন তারা অতিরিক্ত সুরক্ষা সেবার জন্য যোগ্য হতে পারেন। যোগ্যতা পরীক্ষা করুন এবং আরও তথ্য জেনে নিন: https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

হুমকিসমূহ রিপোর্ট করুন

- **জাল অ্যাকাউন্ট সনাক্তকরণ এবং রিপোর্ট করা।** ক্ষতিকারক সাইবার অপরাধীরা তাদের লক্ষ্য অর্জনের জন্য জাল অ্যাকাউন্ট তৈরি করে অথবা আসল অ্যাকাউন্ট হ্যাক করে। যদি আপনার সন্দেহ হয় যে কোনও অ্যাকাউন্ট জাল বা হ্যাক করা হয়েছে, তাহলে প্ল্যাটফর্মে রিপোর্ট করুন এবং ব্লক করে দিন। অনেক সার্ভিসেই অ্যাকাউন্ট যাচাই করার একটি পদ্ধতি থাকে, যেমন ইনস্টাগ্রাম ও ফেসবুকে 'ভেরিফায়েড ব্যাজ' দেওয়া হয়। এটি কোনো অ্যাকাউন্ট আসল কিনা তা শনাক্ত করতে সাহায্য করতে পারে। নিরাপদে সোশ্যাল মিডিয়া ব্যবহারের জন্য NCSC-এর নির্দেশিকা রয়েছে যার মধ্যে হ্যাক করা অ্যাকাউন্টগুলি কীভাবে যাচাই এবং রিপোর্ট করতে হয় তার বিশদ বিবরণ রয়েছে: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **স্ক্যাম ইমেল, এসএমএস এবং লিঙ্ক ব্যবহার করে ফিশিং।** NCSC সন্দেহজনক ইমেল ঠিকানা এবং ওয়েবসাইটগুলি তদন্ত করতে পারে। যদি আপনি মনে করেন যে কোনও সাইট, ইমেল বা বার্তা সন্দেহজনক, তাহলে এটি রিপোর্ট করতে পারেন: https://www.ncsc.gov.uk/collection/phishing-scams

NCSC শব্দকোষ

- **অ্যান্ড্রয়েড**

গুগলের মোবাইল অপারেটিং সিস্টেম, যা বেশ কয়েকটি স্মার্টফোন এবং ট্যাবলেট নির্মাতারা ব্যবহার করে।

- **অ্যাপ**

একটি অ্যাপ্লিকেশন, বা অ্যাপ, হল একটি সফটওয়্যার প্যাকেজ যা ব্যবহারকারীরা তাদের ডিভাইসে অতিরিক্ত কার্যকারিতা বা কন্টেন্ট সরবরাহ করার জন্য ইনস্টল করতে পারে বা আগে থেকে ইনস্টল করা থাকে।

- **সাইবার নিরাপত্তা**

ডিভাইস, সার্ভিস এবং নেটওয়ার্ক—এবং সেগুলোর মধ্যে থাকা তথ্যকে—অননুমোদিত প্রবেশ, চুরি বা ক্ষতি থেকে রক্ষা করা।

- **ডিভাইস**

কম্পিউটার-ভিত্তিক হার্ডওয়্যার যা হাতে ধরা যায় বা দেখা যায়, যেমন একটি ডেস্কটপ কম্পিউটার, স্মার্টফোন বা ট্যাবলেট।

- **iOS**

অ্যাপলের মোবাইল ডিভাইসগুলোতে ব্যবহৃত অপারেটিং সিস্টেম

- **ম্যালওয়্যার**

'ক্ষতিকারক সফ্টওয়্যার' থেকে উদ্ভূত, ম্যালওয়্যার হল এমন যেকোনো ধরণের সফ্টওয়্যার যা কম্পিউটার সিস্টেম, নেটওয়ার্ক বা ডিভাইসের ক্ষতি করতে পারে। ভাইরাস, র‍্যানসমওয়্যার এবং ট্রোজান এর অন্তর্ভুক্ত।

- **অপারেটিং সিস্টেম**

কম্পিউটার, ট্যাবলেট এবং স্মার্টফোনে ব্যবহৃত মৌলিক সফ্টওয়্যার, যা অতিরিক্ত অ্যাপ্লিকেশন এবং হার্ডওয়্যার চালানোর জন্য দরকার হয়।

- **ফিশিং**

স্ক্যাম ইমেল বা টেক্সট বার্তা যাতে ওয়েবসাইটের লিঙ্ক থাকে যেখানে ম্যালওয়্যার থাকতে পারে, অথবা কৌশলে ব্যবহারকারীদের কাছ থেকে সংবেদনশীল তথ্য (যেমন পাসওয়ার্ড) বা অর্থ হাতিয়ে নিতে পারে।

- **স্পাইওয়্যার**

এক ধরণের ম্যালওয়্যার যা ব্যবহারকারীর সম্মতি ছাড়াই একটি ডিভাইসে ইনস্টল করে, ডেটা সংগ্রহ করে এবং তারপর এটি তৃতীয় পক্ষের কাছে পাঠায়।

- **সোশ্যাল মিডিয়া**

ফেসবুক, এক্স এবং ইনস্টাগ্রামের মতো ওয়েবসাইট এবং অ্যাপ, যেখানে মানুষ নিজেদের তৈরি কন্টেন্ট (টেক্সট পোস্ট, ছবি এবং ভিডিও) শেয়ার করতে পারে এবং অন্যদের পোস্টে মতামত জানাতে পারে।

- **স্মার্টফোন**

আধুনিক মোবাইল ফোন যেগুলো অনেক জটিল কাজ করতে পারে—যেমন অ্যান্ড্রয়েড বা আইওএস অপারেটিং সিস্টেমযুক্ত স্মার্টফোন।

- **ট্রোজান**

বৈধ সফটওয়্যারের ছদ্মবেশে এক ধরণের ম্যালওয়্যার, যা একজন ভুক্তভোগীর ডিভাইসে অননুমোদিত অ্যাক্সেস পেতে ব্যবহৃত হয়।

- **ইউআরএল**

ইউনিফর্ম রিসোর্স লোকেটর। ওয়ার্ল্ড ওয়াইড ওয়েবে একটি ঠিকানা যেমন একটি ডোমেন নেম (উদাহরণস্বরূপ www.bbc.co.uk)।

- **ভাইরাস**

এক ধরণের ম্যালওয়্যার যা বৈধ সফ্টওয়্যার প্রোগ্রামগুলিকে সংক্রামিত করার জন্য ডিজাইন করা হয়েছে এবং যখন সেই প্রোগ্রামগুলি সক্রিয় করা হয় তখন নেটওয়ার্কগুলিতে প্রতিলিপি তৈরি করে।

আরও পড়ুন

অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টারের নির্দেশিকা

- সাইবার অপরাধ, ঘটনা বা ঝুঁকি রিপোর্ট করুন
- আপনার ডিভাইসগুলিকে কীভাবে সুরক্ষিত করবেন
- আপনার মোবাইল ফোন সুরক্ষিত করুন
- ফিশিং
- স্ক্যাম
- আপনার সোশ্যাল মিডিয়া সুরক্ষিত করুন
- সোশ্যাল মিডিয়া এবং মেসেজিং অ্যাপের জন্য নিরাপত্তা টিপস

যুক্তরাজ্যের NCSC এবং NPSA এর নির্দেশিকা

- গণতন্ত্র রক্ষা
- সামাজিক মাধ্যম: কীভাবে এটি নিরাপদে ব্যবহার করবেন
- সংস্থাগুলির জন্য মোবাইল সহ ডিভাইস সুরক্ষা নির্দেশিকা
- অ্যাপ্লিকেশন স্টোরগুলিতে হুমকি রিপোর্ট করুন।
- যাদের ঝুঁকি বেশি তাদের জন্য ব্যক্তিগত নিরাপত্তা ও সুরক্ষা

যুক্তরাষ্ট্র NSA এর নির্দেশিকা

- মোবাইল ডিভাইসের সর্বোত্তম ব্যবহার

দাবিত্যাগ

অনুগ্রহ করে মনে রাখবেন যে এই নির্দেশিকাটি এমন তথ্য প্রদান করে যা প্রকাশের সময় যাচাই করা হয়েছে।

এই প্রতিবেদনটি প্রতিবেদন প্রদানকারী সংস্থা এবং শিল্প উৎস থেকে প্রাপ্ত তথ্যের উপর ভিত্তি করে তৈরি। যে তথ্য ও পরামর্শ দেওয়া হয়েছে, তা সব ধরনের ঝুঁকি এড়ানোর জন্য নয়—এবং এসব পরামর্শ মেনে চললেও সব ঝুঁকি পুরোপুরি দূর হবে না। তথ্য-সম্পর্কিত ঝুঁকির দায়িত্ব সব সময় সংশ্লিষ্ট সিস্টেম মালিকের উপরেই থাকে।

যুক্তরাজ্যে এই তথ্য ফ্রিডম অব ইনফরমেশন অ্যাক্ট 2000 (FOIA) এর আওতায় অব্যাহতিপ্রাপ্ত এবং যুক্তরাজ্যের অন্যান্য কিছু তথ্য সম্পর্কিত আইনের আওতায় অব্যাহতিপ্রাপ্ত হতে পারে।

যেকোনো FOIA সম্পর্কিত প্রশ্ন ncscinfoleg@ncsc.gov.uk ঠিকানায় পাঠান।

সংযোজন: MOONSHINE এবং BADBAZAAR নমুনা পর্যবেক্ষণ করা হয়েছে

এই টেবিলে গত দুই বছরে MOONSHINE এবং BADBAZAAR প্রচারণায় ব্যবহৃত অ্যাপগুলির তালিকা রয়েছে।

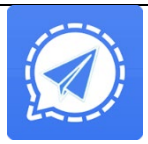
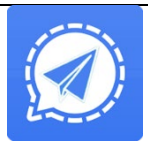
এই অ্যাপগুলোর অনেকগুলিই পরিচিত বা জনপ্রিয় অ্যাপগুলোর মতো দেখতে। এটি সম্ভবত সুপরিচিত ব্র্যান্ডগুলিকে 'নকল' করার জন্য একটি ইচ্ছাকৃত কৌশল।

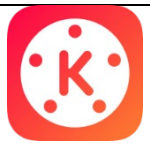
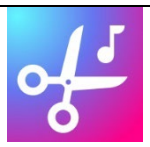
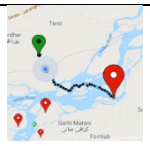
এটি মনে রাখা গুরুত্বপূর্ণ যে অ্যাপের নাম, প্যাকেজের নাম বা আইকন—এই তিনটি জিনিসই আসল অ্যাপের মতো দেখাতে পারে, তাই শুধু এগুলো দেখে বোঝা যাবে না যে ডিভাইসটি আক্রান্ত হয়েছে কি না।

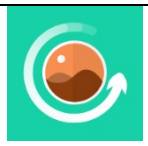
মিটিগেশন অংশে যেমনটি বলা হয়েছে, আপনি চাইলে আপনার অ্যান্ড্রয়েড ফোনে 'ক্ষতিকারক অ্যাপ সনাক্তকরণ উন্নত করুন' এই অপশনটি চালু করে গুগলে অ্যাপ পাঠাতে পারেন—যা প্লে স্টোরের বাইরে থেকে ইনস্টল করা অ্যাপগুলো স্ক্যান করে দেখে সেগুলো ক্ষতিকর কি না।

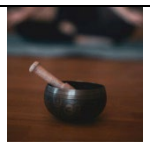
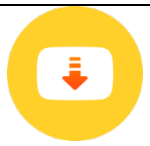
অ্যাপ এর টাইটেল	প্যাকেজের নাম	অ্যাপ এর আইকন
আল্লাহর ৯৯ নাম	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
অ্যাডোবি অ্যাক্রোব্যাট	com.adobe.reader	
অ্যালপাইন(پښتو)	psyberia.pa.full	
অ্যালপাইন কোয়েস্ট অফ-রোড এক্সপ্লোরার	psyberia.alpinequest.full	

অ্যালপাইন কোয়েস্ট অফ-রোড এক্সপ্লোরার	psyberia.alpinequest.full	
অ্যালপাইন কোয়েস্ট অফ-রোড এক্সপ্লোরার (লাইট)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
অ্যারাবিক কিবোর্ড	com.arabic.keyboard.arabic.language.keyboard.app	
অডিও ভিডিও ক্লাটার	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
বাদাম维语输入法	com.ziipin.softkeyboard	
বৌদ্ধ সংগীত (1)	com.bigkidsapps.buddhistsongs1	
ক্যালকুলেটর	com.android2.calculator3	
কম্পাস ৩৬০ প্রো	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

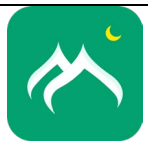
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
ফাইল ম্যানেজার +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
ফ্রি ওয়াইফাই পাস	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
হেফজ কোরআন	com.golap.hefzquran	
হিজরি ক্যালেন্ডার	com.ibrahim.hijricalendar	
ইনশট	com.camerasideas.instashot	

KMপ্লেয়ার	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
কাটার এবং রিংটোন মেকার	ringtone.maker.mp3.cutter.audio	
ম্যালক	com.mallocprivacy.antistalkerfree	
ম্যাপ ডিসটেন্স ক্যালকুলেটর	com.routemap.mapdownload.gpsrouteplanner	
মিডিয়া রিকোভারি	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
নুর输入法	com.nur.ime	
OGহোয়াটসঅ্যাপ	com.gbwhatsapp3	
PDF এক্সট্রা	com.mobisystems.mobiscanner	
PDF রিডার	pdf.pdfreader.pdfviewer.pdfeditor	

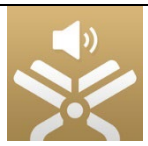
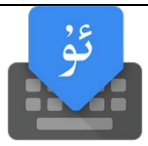
PDF রিডার	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo এডিটর	com.iudesk.android.photo.editor	
ফটো রিকভারি	recover.restore.undelete.photo.video.file	
ফটো স্টুডিও	com.kvadgroup.photostudio	
প্লাস	org.telegram.pluspro	
প্রেয়ার বুক	com.arashpayan.prayerbook	
কোয়ার্কVPN	com.speedy.vpn	
কোরআন	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
মুছে যাওয়া ছবি আবার ফিরিয়ে আনুন	com.restore.deleted.pictures.video	
সিগন্যাল	org.thoughtcrime.securesms	

সিগন্যাল প্লাস	org.thoughtcrime.securesmsplus	
সিগন্যাল প্লাস	org.thoughtcrime.securesmsplus	
সিগন্যাল বোল সাউন্ডস HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
স্কাইপ	com.skype.raider	
স্ন্যাপটিউব	com.snaptube.premium	
স্ন্যাপটিউব প্লাস	com.snaptube.gold	
সুইফটকি কিবোর্ড	com.touchtype.swiftkey	
টারটীল	com.mmmoussa.iqra	
টেলিগ্রাম	org.zhifeijihj.messenger	
টেলিগ্রাম	org.telegramfbo.messenger	
টেলিগ্রাম X	org.thunderdog.challegram	

তিবেতান ডিভিনেশন সিস্টেম MO	net.rhombapp.mo	
তিবেতান প্রেয়ার	com.chorig.tibetanprayer	
ট্রান্সলেটর AR-TR	free_translator.artr	
ট্রুকলার	com.truecaller	
টিউবপ্লাস	com.techshop.videocraft	
আলট্রাসার্ফ	us.ultrasurf.mobile.ultrasurf	
উইগুর কিবোর্ড	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
উইগুরচি কিরগুজগুচ	com.ziipin.softkeyboard	
ভিডিও কনভার্টার	com.inverseai.video_converter	
ভিডিও ক্লাটার	com.naing.cutter	
ভিডিও ডাউনলোডার	downloader.video.download.free	

ভিডিও মেকার	com.bstech.slideshow.videomaker	
অ্যান্ডয়েড এর জন্য ভিডিও প্লেয়ার	com.zgz.supervideo	
ভিয়েকা	com.prime.story.android	
ভিভাভিডিও লাইট	com.quvideo.vivavideo.lite	
ভিভাভিডিও প্রো	com.quvideo.xiaoying.pro	
ভিমুসলিম	com.alhiwar	
ভিডিও রেকর্ডার	com.media.bestrecorder.audiorecorder	
ভক্সার	com.rebelvox.voxer	
আবহাওয়ার পূর্বাভাষ	com.graph.weather.forecast.channel	
হোয়াটসঅ্যাপ	com.whatsapp	
হোয়াটসঅ্যাপ	com.whatsapp	

হোয়াটসঅ্যাপ	com.WhatsApp3Plus	
হোয়াটসঅ্যাপ	com.whatsapp	
হোয়াটসঅ্যাপ	com.WhatsApp2Plus	
হুজকল	gogolook.callgogolook2	
ওয়াইফাই পাসওয়ার্ড মাস্টার_ v1.4	com.example.dat.a8andoserverx	
উইন্ডি	com.windyty.android	
ওয়াইজ	com.transferwise.android	
ইওহোয়াটসঅ্যাপ	com.yowhatsapp	
ইউটিউব ডাউনলোডার	dentex.youtube.downloader	
জম	im.zom.messenger	

আইকোরআন লাইট	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	
زىكرلەر	com.my.newproject5	
كەرىم قۇرئان	ru.omdevelopment.ref.quranuyghur.free	
لۇغىتى كۇھىقاپ	com.kuhiqap.lughitim	
كىرگۈزگۈچ نۇر	com.nur.ime	

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