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

คำแนะนำ

BADBAZAAR และ MOONSHINE:

สปายแวร์ที่มุ่งเป้าไปยังกลุ่มชาวอุยกูร์ ชาวไต้หวัน และชาวทิเบตและนักเคลื่อนไหวภาคประชาสังคม

9 เมษายน 2025

BADBAZAAR และ MOONSHINE: สปายแวร์ที่มุ่งเป้าไปยังกลุ่มชาวอุยกูร์ ชาวไต้หวัน และชาวทิเบต และนักเคลื่อนไหวภาคประชาสังคม

NCSC

และพันธมิตรเป็นผู้เผยแพร่ข้อมูลใหม่และมาตรการบรรเทาปัญหาสำหรับผู้ที่มีความเสี่ยงสูงจากสปายแวร์สองสายพันธุ์

บทสรุป

ด้วยการสนับสนุนจาก Cyber League ของสหราชอาณาจักร คำแนะนำนี้จัดทำขึ้นโดยความร่วมมือระหว่างศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาติของสหราชอาณาจักร (NCSC UK) และพันธมิตรสากลดังต่อไปนี้

- **ศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย (Australian Cyber Security Centre) ซึ่งเป็นส่วนหนึ่งของหน่วยข่าวกรองสัญญาณออสเตรเลีย (Australian Signals Directorate)**
- **ศูนย์รักษาความปลอดภัยทางไซเบอร์แคนาดา (Canadian Centre for Cyber Security) ส่วนหนึ่งของหน่วยงานการรักษาความปลอดภัยทางการสื่อสาร (Communications Security Establishment)**
- **สำนักงานข่าวกรองกลางแห่งสหพันธรัฐเยอรมัน (German Federal Intelligence Service)**
- **สำนักงานสหพันธรัฐเยอรมันเพื่อการปกป้องรัฐธรรมนูญ (German Federal Office for the Protection of the Constitution)**
- **ศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาตินิวซีแลนด์ (New Zealand National Cyber Security Centre) ซึ่งเป็นส่วนหนึ่งของสำนักการรักษาความปลอดภัยทางการสื่อสารของรัฐบาล (Government Communications Security Bureau)**
- **สำนักงานสอบสวนกลางสหรัฐอเมริกา (United States Federal Bureau of Investigation)**
- **หน่วยงานรักษาความปลอดภัยแห่งชาติสหรัฐอเมริกา (United States National Security Agency)**

จุดประสงค์ของคำแนะนำนี้คือ เพื่อยกระดับความตระหนักรู้เกี่ยวกับภัยคุกคามที่เพิ่มมากขึ้น ซึ่งผู้ไม่ประสงค์ดีทางไซเบอร์ก่อให้เกิดต่อบุคคลที่เกี่ยวข้องกับประเด็นต่าง ๆ รวมถึงไต้หวัน ทิเบต เขตปกครองตนเองซินเจียงอุยกูร์ การเคลื่อนไหวเพื่อประชาธิปไตย และฝ่าหลุนกง

คำแนะนำนี้ประกอบด้วยกรณีศึกษา 2 กรณีที่ให้รายละเอียดเกี่ยวกับเทคนิคของผู้ไม่ประสงค์ดีทางไซเบอร์ ซึ่งใช้สปายแวร์ที่รู้จักกันในชื่อว่า BADBAZAAR และ MOONSHINE เพื่อมุ่งเป้าสู่ข้อมูลบนอุปกรณ์เคลื่อนที่ต่าง ๆ รวมถึงสมาร์ทโฟน ซึ่งอาจเป็นที่สนใจของรัฐบาลจีน คำแนะนำนี้ยังช่วยชี้แนะแนวทางเพื่อช่วยให้บุคคลสามารถป้องกันตนเอง อุปกรณ์ และข้อมูลของตนอีกด้วย

นอกเหนือจากคำแนะนำนี้ NCSC ยังมีการเผยแพร่เอกสารรายละเอียดทางเทคนิคฉบับเต็มพร้อมคำแนะนำที่แยกต่างหาก

ใครบ้างที่ตกอยู่ในความเสี่ยง?

หน่วยงานผู้จัดทำเอกสารนี้และพันธมิตรในอุตสาหกรรมพบว่า BADBAZAAR และ MOONSHINE มุ่งเป้าไปที่บุคคลที่เกี่ยวข้อง
โดยเฉพาะกับประเด็นที่รัฐบาลจีนพิจารณาว่าเป็นภัยคุกคามต่ออำนาจในประเทศ ความใฝ่ฝัน และชื่อเสียงของจีนในระดับโลก
กลุ่มที่ตกอยู่ในความเสี่ยงสูงสุด ได้แก่ แต่ไม่จำกัดเฉพาะผู้ที่มีความเกี่ยวข้องกับ

- **เอกราชของไต้หวัน**
- **สิทธิของชาวทิเบต**
- **ชาวมุสลิมอุยกูร์และชนกลุ่มน้อยทางชาติพันธุ์อื่น ๆ**
  ภายในหรือมาจากเขตปกครองตนเองซินเจียงอุยกูร์ของจีน
- **การสนับสนุนประชาธิปไตย (รวมถึงฮ่องกง)**
- **การเคลื่อนไหวทางจิตวิญญาณของฝ่าหลุนกง**

ซึ่งรวมถึงองค์กรนอกภาครัฐ (Non-governmental organisations - NGOs) นักข่าว ธุรกิจ และบุคคลที่สนับสนุน เกี่ยวข้องกับ
หรือเป็นตัวแทนของบุคคลในกลุ่มเหล่านี้ วิธีที่สปายแวร์นี้แพร่กระจายทางออนไลน์แบบไม่เลือกปฏิบัติ
ยังหมายความว่าสปายแวร์
มีความเสี่ยงที่อาจแพร่กระจายไปไกลกว่าเหยื่อที่ตั้งเป้าจะบุกรุกไว้ด้วย

คำแนะนำนี้มุ่งหวังที่จะช่วยให้ผู้ที่ตกอยู่ในความเสี่ยงสามารถตอบสนองต่อภัยคุกคามเฉพาะจากสปายแวร์ BADBAZAAR และ
MOONSHINE ได้อย่างมีประสิทธิภาพ
มาตรการบรรเทาปัญหาที่แนะนำนั้นเป็นส่วนเสริมความแข็งแกร่งให้กับคำแนะนำด้านการรักษา
ความปลอดภัยทางไซเบอร์ในภาพรวม และไม่ควรพิจารณาแยกจากกันโดยลำพัง

โดยการปฏิบัติตามคำแนะนำที่อ้างอิงในคำแนะนำนี้
ผู้ใช้สามารถลดความเสี่ยงของการติดมัลแวร์บนอุปกรณ์เคลื่อนที่และข้อมูลของตนได้

ภัยคุกคาม

MOONSHINE และ BADBAZAAR เป็นตัวอย่างของโทรจัน
ซึ่งเป็นมัลแวร์ที่มีฟังก์ชันการทำงานอันตรายซ่อนอยู่ภายในแอปที่ดูเหมือน
จะทำงานได้ตามปกติ และสามารถดาวน์โหลดได้จากแอปสโตร์ (App stores) หรือบริการแชร์ไฟล์ออนไลน์

แอปพวกนี้ออกแบบมาเพื่อหลอกล่อให้ผู้ใช้ดาวน์โหลดและติดตั้งลงในอุปกรณ์ เมื่อติดตั้งแล้ว แอปจะใช้ช่องโหว่บนอุปกรณ์
เพื่อดำเนินการที่ไม่ได้รับอนุญาต หรืออาจอาศัยการที่ผู้ใช้อนุญาตการเข้าถึงแอปและดาวน์โหลดข้อมูลจากอุปกรณ์ ซึ่งรวมถึง

- **ข้อมูลตำแหน่ง รวมถึงการติดตามแบบเรียลไทม์หรือตามเวลาจริง**
- **การเข้าถึงไมโครโฟนและกล้อง**
- **ข้อความ รูปภาพ และไฟล์อื่น ๆ ที่จัดเก็บไว้ในอุปกรณ์**
- **ข้อมูลอุปกรณ์ และอื่น ๆ**

จากนั้นผู้ไม่ประสงค์ดีจะฉวยโอกาสจากความสนใจที่แท้จริงของกลุ่มที่ตกอยู่ในความเสี่ยง
เพื่อตรวจจับและแพร่กระจายมัลแวร์ไปยัง
ผู้เสียหายให้ได้มากที่สุดเท่าที่จะทำได้ และเข้าถึงข้อมูลของเหยื่อเหล่านั้น
วิธีหนึ่งที่พวกเขาทำคือการออกแบบแอปที่รู้ว่าจะดึงดูด
เหยื่อได้ เช่น แอปที่รองรับภาษาพื้นเมืองของผู้เสียหาย หรือมีเนื้อหาเฉพาะของสถานที่ เช่น ภูมิภาคทิเบตของจีนหรือซินเจียง

กรณีศึกษาในคำแนะนำนี้ยกตัวอย่างให้เห็นภาพบางส่วน ได้แก่ แอป TibetOne และ Uyghur Quran

ผู้ไม่ประสงค์ดีเหล่านี้มีการเคลื่อนไหวในฟอรัมออนไลน์ ซึ่งมีฐานผู้ใช้ที่เป็นเหยื่อเป้าหมายของพวกเขา เพื่อเพิ่มโอกาสในการ
แพร่กระจายมัลแวร์ให้เหยื่อได้มากที่สุด มีการสังเกตพบว่าผู้ไม่ประสงค์ดีจงใจแชร์สปายแวร์ในช่อง Telegram
ที่เกี่ยวข้องกับทิเบต
และฟอรัม Reddit กรณีศึกษาในคำแนะนำนี้ยังให้ตัวอย่างของวิธีการเหล่านี้ด้วย

แอปที่เป็นอันตรายมักถูกแชร์เป็นไฟล์เดี่ยว ๆ แยกต่างหาก เช่น ไฟล์ APK ใน Android ซึ่งผู้ใช้จำเป็นต้องดาวน์โหลดและติดตั้ง
ผู้ไม่ประสงค์ดีพยายามทำให้สปายแวร์ของพวกเขาดูน่าเชื่อถือมากขึ้นโดยอัปโหลดไปยังแอปสโตร์ทางการ เช่น Google Play
Store
และ Apple App Store หรือโดยการเพิ่มโค้ดที่เป็นอันตรายลงในแอปที่เคยปลอดภัยมาก่อน อย่างไรก็ตาม แอปสโตร์ทางการ
มีคุณลักษณะด้านการรักษาความปลอดภัยและกระบวนการตรวจสอบที่ทำให้กลวิธีนี้ประสบความสำเร็จน้อยลง
ซึ่งทำให้แอปจาก
แอปสโตร์ทางการปลอดภัยกว่า แต่จากที่แสดงให้เห็นในกรณีศึกษาและรายงานภัยคุกคามแอปสโตร์ที่ชื่อว่า App Store Threat
Report ของ NCSC กระบวนการเหล่านี้ก็ไม่ได้สมบูรณ์แบบ

การปฏิบัติตามเคล็ดลับ 4 ข้อนี้อาจช่วยปกป้องคุณจากภัยคุกคามที่ระบุไว้ในคำแนะนำนี้ได้

สำหรับคำแนะนำเพิ่มเติมโดยละเอียด โปรดดูหัวข้อมาตรการบรรเทาปัญหา

กรณีศึกษา

กรณีศึกษาทั้งสองกรณีนี้แสดงให้เห็นว่า MOONSHINE และ BADBAZAAR ทำงานอย่างไร
และผู้ไม่ประสงค์ดีทางไซเบอร์กำลังมุ่งเป้า
ไปหาผู้ที่มีความเสี่ยงมากที่สุดอย่างไร

กรณีศึกษากรณีที่หนึ่ง: MOONSHINE

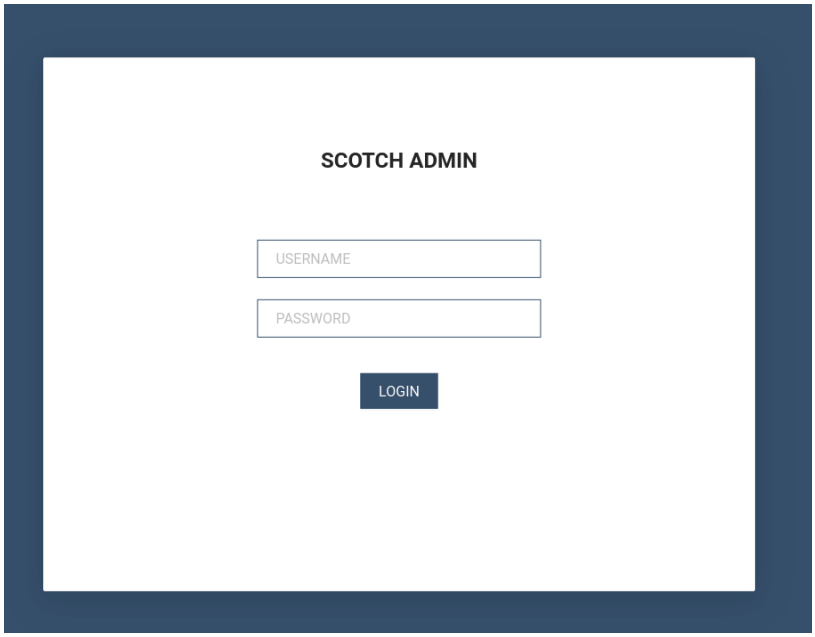
MOONSHINE เป็นสปายแวร์ระบบปฏิบัติการ Android ที่ Citizen Lab รายงานในปี 2019 ว่ามีกลุ่มเป้าหมายเป็นชาวทิเบต
MOONSHINE ปลอมตัวเป็นแอปที่ถูกต้องตามกฎหมายเพื่อล่อลวงเหยื่อให้ติดตั้งแอปนี้ ซึ่งมีการแชร์ผ่านช่อง Telegram
และลิงก์
ที่ส่งผ่าน WhatsApp ด้วย

MOONSHINE มีความสามารถในการสอดแนมอย่างครอบคลุม เช่น

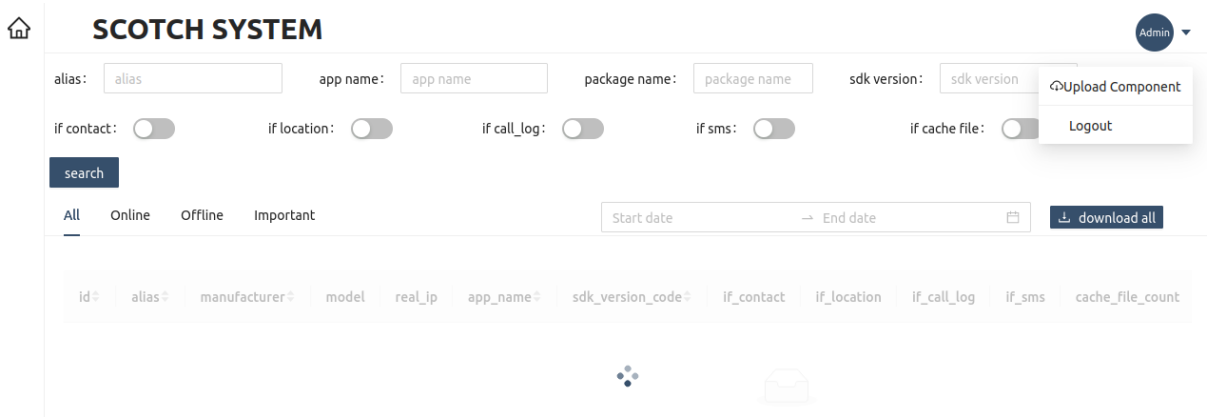
- **ข้อมูลตำแหน่ง รวมถึงการติดตามแบบเรียลไทม์หรือตามเวลาจริง**
- **การบันทึกเสียงและถ่ายภาพสด**
- **การดาวน์โหลดไฟล์จากอุปกรณ์**
- **การดึงข้อมูลจากอุปกรณ์**
- **การเล่นไฟล์เสียงบนอุปกรณ์**

แอปพลิเคชันที่ชื่อว่า '**ئاۋازلىق قۇرئان.apk**' ซึ่งแปลว่า '**Audio Quran.apk**' เป็นตัวอย่างของการใช้ MOONSHINE
เพื่อเจาะจงมุ่งเป้า
ไปที่ชาวอุยกูร์ การใช้ภาษาอุยกูร์ในชื่อไฟล์ ซึ่งบ่งชี้ว่าเป็นแอปพลิเคชันคัมภีร์กุรอานนั้น
น่าจะออกแบบมาเพื่อดึงดูดชาวมุสลิมอุยกูร์

เมื่อติดตั้งแล้ว ผู้ไม่ประสงค์ดีทางไซเบอร์สามารถรวบรวมข้อมูลจากอุปกรณ์ของเหยื่อได้ ข้อมูลนี้
เข้าถึงได้ผ่านแผงควบคุมที่เรียกว่า
'SCOTCH ADMIN'



เมื่อเข้าสู่ระบบแล้ว ผู้ไม่ประสงค์ดีสามารถเข้าถึงเพจที่แสดงในภาพหน้าจอด้านล่างได้ หน้าเพจนี้แสดงรายละเอียดของอุปกรณ์ที่ติดมัลแวร์ และระดับการเข้าถึงที่ผู้ไม่ประสงค์ดีมีต่ออุปกรณ์เหล่านั้น



แผงควบคุมที่จัดการมัลแวร์จะแสดงข้อมูลที่ผู้ไม่ประสงค์ดีรวบรวมไว้ รวมถึง

- **ระดับการเข้าถึงอุปกรณ์**
- **ข้อความ SMS**
- **บันทึกการโทร**
- **ข้อมูลตำแหน่ง**
- **ข้อมูลอุปกรณ์**

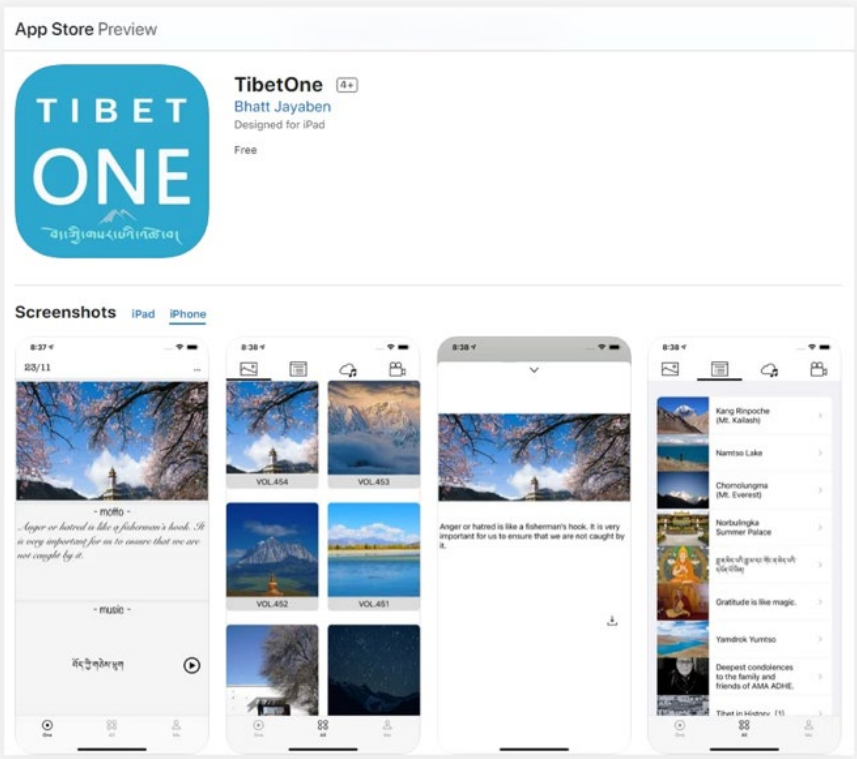
NCSC ร่วมกับ Cyber League ได้ใช้รายงานจากอุตสาหกรรมที่ชื่อว่า reporting from Trend Micro มาต่อยอดเพื่อค้นหาความเชื่อมโยงระหว่างชุดเครื่องมือแสวงหาประโยชน์จาก MOONSHINE และแผงควบคุมการเข้าสู่ระบบที่มีคำว่า 'UPSEC' ในชื่อ HTML รายละเอียดทั้งหมดอยู่ในคำแนะนำทางเทคนิคที่แนบมา

จากการรายงานของ Intelligence Online UPSEC นั้นหมายถึง ‘Sichuan Dianke Network Security Technology Co. Ltd’ อย่างไรก็ตาม หน่วยงานผู้จัดทำเอกสารนี้ยังไม่ได้ตรวจสอบยืนยันข้อความดังกล่าว

กรณีศึกษา กรณีที่สอง: BADBAZAAR

BADBAZAAR เป็นมัลแวร์บนอุปกรณ์เคลื่อนที่ที่มีทั้งเวอร์ชัน iOS และ Android ซึ่งมุ่งเป้าไปที่ชาวอุยกูร์ ชาวทิเบต และชาวไต้หวัน
มัลแวร์นี้แพร่กระจายผ่านแพลตฟอร์มโซเชียลมีเดียและแอปสโตร์ทางการ

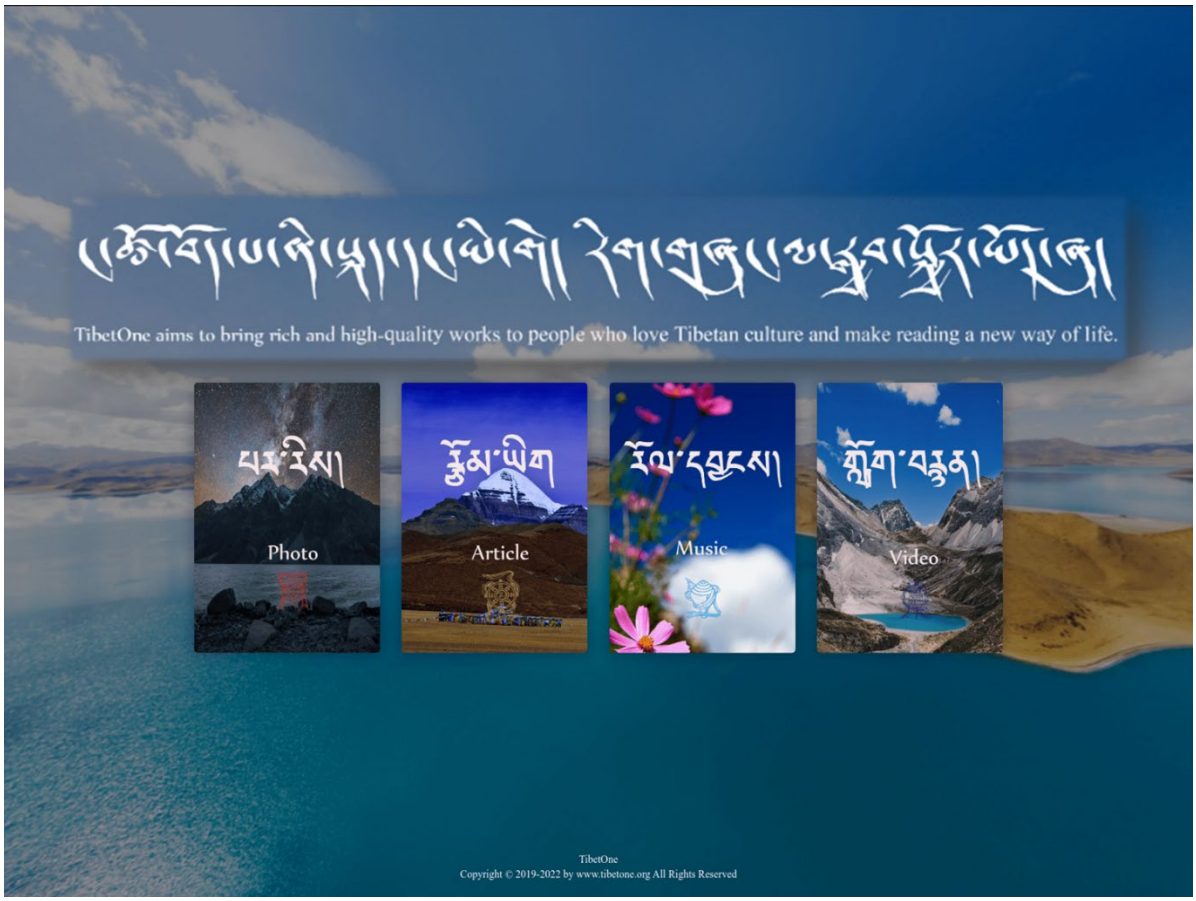
BADBAZAAR ถูกใช้เพื่อมุ่งเป้าไปที่ชาวทิเบตผ่านแอป ‘**TibetOne**’ ตามการรายงานของ Lookout และ Volexity **TibetOne** เป็นแอป iOS ที่สร้างขึ้นโดยผู้ไม่ประสงค์ดี ซึ่งมีความสามารถในการเข้าถึงข้อมูลอุปกรณ์และข้อมูลตำแหน่ง
แอปนี้ถูกอัปโหลดไปยัง
Apple App Store ในเดือนธันวาคม 2021 แต่ปัจจุบันไม่มีให้บริการอีกแล้ว เพื่อแพร่กระจายมัลแวร์ต่อไป
ผู้ไม่ประสงค์ดียังโฆษณา
แอปนี้ในช่อง Telegram ที่เรียกว่า ‘**tibetanphone**’ อีกด้วย



ภาพที่ 1: หน้าแอป TibetOne ที่ปรากฏใน Apple App Store แอปดังกล่าวถูกลบไปแล้ว

ภาพที่ 2: TibetOne ดังที่มีการแชร์ทางช่อง Telegram

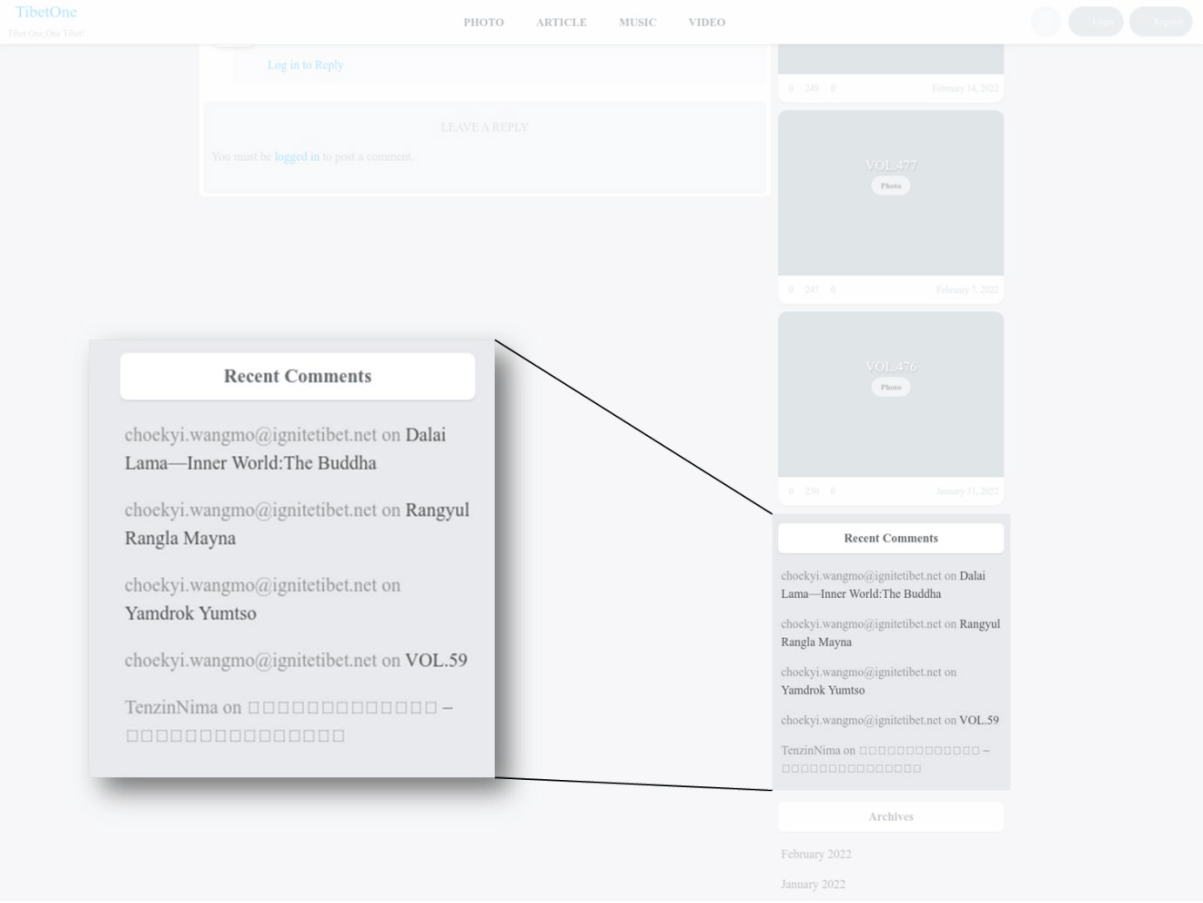
เพื่อเพิ่มความน่าเชื่อถือให้กับแอป ผู้ไม่ประสงค์ดียังได้พัฒนาเว็บไซต์ที่ชื่อ '**tibetone[.]org**' ซึ่งให้คำจำกัดความถึงตนเองว่าเป็นผู้ *'นำเสนอผลงานคุณภาพสูงและหลากหลายแก่ผู้ที่รักวัฒนธรรมทิเบต และทำให้การอ่านเป็นวิถีชีวิตใหม่'*



ภาพที่ 3: โฮมเพจของ 'tibetone\[.]org'.

รูปภาพนี้ได้รับการแก้ไขเพื่อให้ส่วนที่เกี่ยวข้องชัดเจนยิ่งขึ้น

เว็บไซต์นี้มีหน้าเพจสำหรับบทความที่อนุญาตให้ผู้ใช้แสดงความคิดเห็นได้ ความคิดเห็นที่แสดงโดยผ่าน ที่อยู่อีเมล '**choekyi.wangmo@ignitetibet.net**' เชื่อว่าเป็นอีเมลที่ถูกควบคุมโดยผู้ไม่ประสงค์ดี และน่าจะแอบอ้างตัวเป็น '**Choekyi Wangmo**' ซึ่งเป็นชื่อผู้ประท้วงที่สนับสนุนทิเบตในนามศูนย์สิทธิมนุษยชนและประชาธิปไตยแห่งทิเบต (Tibetan Centre of Human Rights and Democracy) นี่อาจเป็นความพยายามอีกอย่างหนึ่งในการทำให้ดูเหมือนว่าว่าแอปนี้สนับสนุนเอกราชของชาวทิเบตอย่างแท้จริง

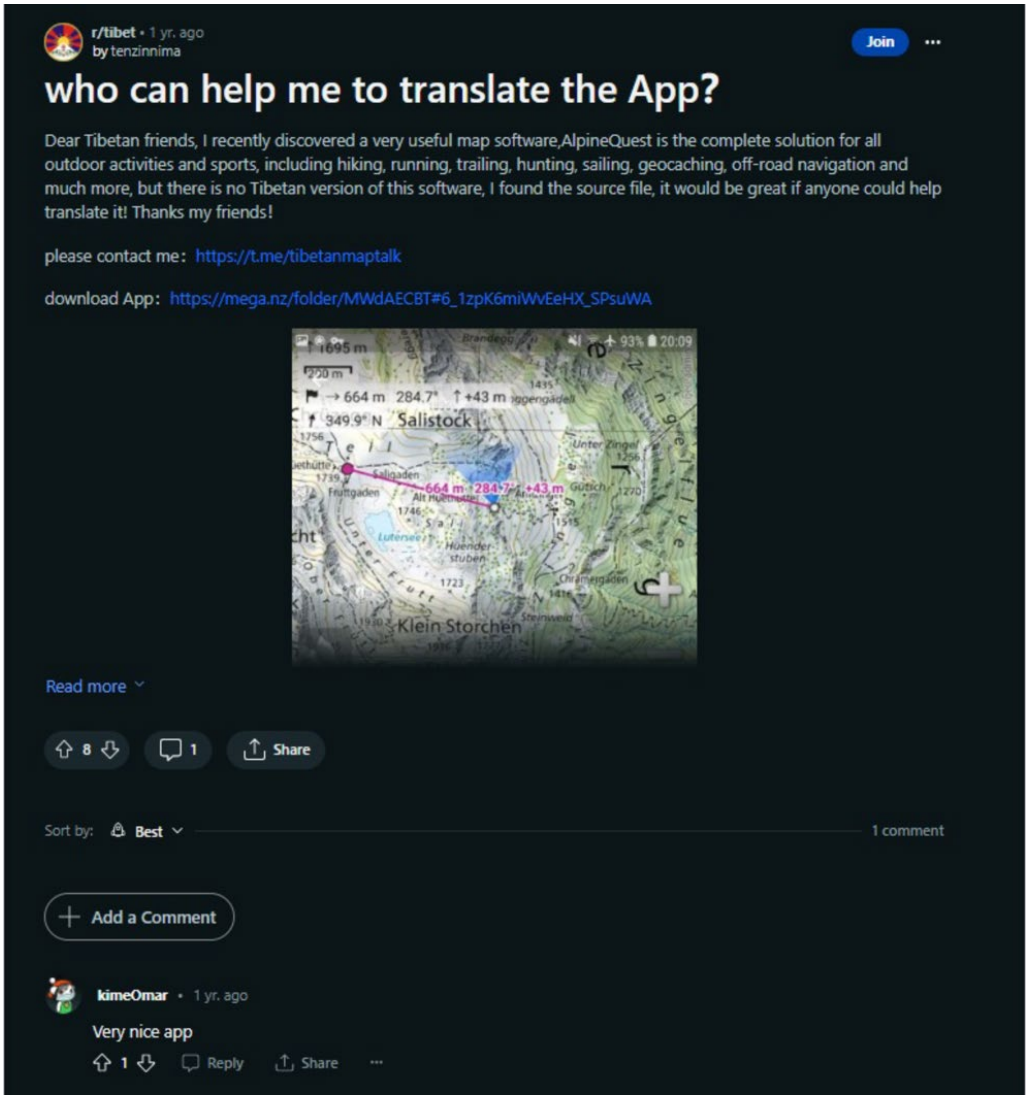


ภาพที่ 4: หน้าเว็บ 'tibetone\[.]org' แสดงความคิดเห็นจากผู้ใช้ที่เชื่อว่าถูกควบคุมโดยผู้ไม่ประสงค์ดี

รูปภาพนี้ได้รับการแก้ไขเพื่อให้ส่วนที่เกี่ยวข้องชัดเจนยิ่งขึ้น

'**TenzinNima'** เป็นชื่อผู้ใช้อีกชื่อหนึ่งที่เพิ่มความคิดเห็นในไซต์นี้ Volexity ได้รายงานว่า ชื่อผู้ใช้นี้ยังถูกใช้บน Reddit เพื่อโฆษณา

ช่อง Telegram ที่ชื่อ '**Tibetanmaptalk**' ซึ่งรวมลิงก์สำหรับดาวน์โหลดตัวอย่างที่เป็นอันตรายของ '**AlpineQuest**' ซึ่งเป็นแอปนำทางที่มีให้ใช้งานบนอุปกรณ์ Android ลิงก์ดาวน์โหลดที่ให้มานั้นเป็นบริการแชร์ไฟล์ของบุคคลที่สามที่ชื่อว่า Mega



ภาพที่ 5: โพสต์ Reddit โฆษณาแอปพลิเคชันที่เป็นอันตรายโดยบัญชีที่เชื่อว่าถูกควบคุมโดยผู้ไม่ประสงค์ดี

Volexity ยังตั้งข้อสังเกตอีกว่าผู้ใช้ที่รู้จักกันในชื่อ '**KimeOmar**' ซึ่งแสดงความคิดเห็นในโพสต์ดังกล่าว ก็เคยถูกพบว่าแชร์แอปที่เป็นอันตรายใน sub-Reddit อีกฟอรัมหนึ่งด้วย
ซึ่งอาจบ่งชี้ได้ว่าผู้ไม่ประสงค์ดีใช้โปรไฟล์โซเชียลมีเดียหลายบัญชีเพื่อให้โพสต์ของตน
ดูน่าเชื่อถือ

การประเมินผล

BADBAZAAR และ MOONSHINE ใช้กลวิธีทางวิศวกรรมสังคมหลายวิธีเพื่อมุ่งเป้าไปที่ชุมชนอุยกูร์ ชาวทิเบต และชาวไต้หวันโดยเฉพาะ
ซึ่งได้แก่

- การฝังโทรจันไว้ในแอปที่กลุ่มเป้าหมายให้ความสนใจ เช่น แอปคัมภีร์กุรอานในภาษาอุยกูร์
  ซึ่งเกือบจะแน่นอนว่าได้รับการ
  ปรับแต่งให้เหมาะกับกลุ่มเหยื่อเป้าหมายที่ต้องการโจมตีโดยเฉพาะ
- การเพิ่มแอปที่ฝังโทรจันเหล่านี้ลงไปยังแอปสโตร์ทางการ มีแนวโน้มสูงที่จะช่วยสร้างความรู้สึกว่าแอปมีความน่าเชื่อถือ และการแชร์แอปเหล่านี้ในกลุ่มแชตก็มีความเป็นไปได้สูงว่ามีจุดประสงค์เพื่อแสวงหาประโยชน์จากความสัมพันธ์ที่ไว้วางใจกัน
  ภายในชุมชนเหล่านี้

BADBAZAAR และ MOONSHINE รวบรวมข้อมูล ซึ่งแทบจะแน่นอนว่าจะเป็นประโยชน์กับรัฐบาลจีน แม้ว่า BADBAZAAR และ MOONSHINE จะถูกพบว่ามุ่งเป้าไปที่ชาวอุยกูร์ ชาวทิเบต และชาวไต้หวัน แต่ก็ยังมีมัลแวร์อื่น ๆ ที่มุ่งเป้าไปที่ชนกลุ่มน้อยอื่น ๆ ในจีนด้วย
พลเมืองจากประเทศพันธมิตรทั้งในจีนและต่างประเทศที่ถูกมองว่าสนับสนุนกิจกรรมที่คุกคามเสถียรภาพของระบอบการปกครอง แทบจะ
แน่นอนว่าตกอยู่ภายใต้การคุกคามจากมัลแวร์บนอุปกรณ์เคลื่อนที่ เช่น BADBAZAAR และ MOONSHINE
ความสามารถในการเก็บข้อมูล
ตำแหน่ง เสียง และภาพถ่าย
เกือบจะแน่นอนว่าเปิดโอกาสให้สามารถนำข้อมูลไปใช้ในการแจ้งปฏิบัติการเฝ้าระวังและการคุกคามในอนาคต
โดยให้ข้อมูลตามเวลาจริงเกี่ยวกับกิจกรรมของเป้าหมาย

มาตรการบรรเทาปัญหาสำหรับผู้ใช้แอปบนอุปกรณ์เคลื่อนที่

หน่วยงานผู้จัดทำเอกสารนี้ขอสนับสนุนให้ใช้แนวทางปฏิบัติการรักษาความปลอดภัยต่อไปนี้เพื่อป้องกันภัยคุกคามตามที่อธิบายไว้ใน
กรณีศึกษา คำแนะนำเหล่านี้อ้างอิงตามแนวปฏิบัติที่ดีที่สุดของ NCSC โปรดดูหัวข้อในส่วน 'อ่านเพิ่มเติม'
สำหรับลิงก์ไปยังคำแนะนำ
ตามแนวทางปฏิบัติที่ดีที่สุดสำหรับผู้อ่านในออสเตรเลียและสหรัฐอเมริกา

รักษาอุปกรณ์ของคุณให้ปลอดภัย

- **ดาวน์โหลดเฉพาะแอปจากแอปสโตร์ทางการ เช่น Play Store ของ Google หรือ App Store ของ Apple** Play Store ของ Google และ App Store ของ Apple สแกนซอฟต์แวร์ตรวจหาไวรัสก่อนที่จะนำไปใช้งาน
  เพื่อให้คุณมั่นใจได้
  มากขึ้นว่าสิ่งที่คุณดาวน์โหลดนั้นปลอดภัย แอปจากแอปสโตร์ที่เชื่อถือได้ก็อาจยังมีความเสี่ยงอยู่บ้าง
  แต่การดาวน์โหลดจาก
  แหล่งอื่นอาจไม่มีการป้องกันใด ๆ เลย NCSC มีรายงานภัยคุกคามเกี่ยวกับแอปสโตร์ ดูได้ที่
  https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

- **อัปเดตอุปกรณ์และแอปของคุณให้เป็นปัจจุบันอยู่เสมอ**
  ติดตั้งการอัปเดตแอปและซอฟต์แวร์อุปกรณ์ของคุณทันทีที่มี
  ให้ใช้งาน เปิดการใช้งาน 'การอัปเดตอัตโนมัติ' ในการตั้งค่าอุปกรณ์ของคุณ หากมีตัวเลือกนี้
  เพื่อที่คุณจะได้ไม่ต้องคอยเตือน
  ตัวเองให้อัปเดตอุปกรณ์ทุกครั้ง โปรดดูคำแนะนำของ NCSC เกี่ยวกับการรักษาความปลอดภัยออนไลน์
  เพื่อป้องกันไวรัส
  ที่รู้จักและมัลแวร์ประเภทอื่น การอัปเดตมักจะรวมการปรับปรุงและคุณสมบัติใหม่ ๆ ดูได้ที่
  https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

- **อย่า 'เจลเบรค' (jailbreak) หรือ 'รูท' (root) อุปกรณ์ของคุณ**
  เนื่องจากการกระทำดังกล่าวเป็นการใช้ช่องโหว่ที่ยังไม่ได้
  รับการแก้ไขเพื่อข้ามการควบคุมด้านการรักษาความปลอดภัยที่ตั้งไว้
  ซึ่งจะทำให้อุปกรณ์เสี่ยงต่อการถูกโจมตีมากขึ้น
  โปรดดูคำแนะนำของ NCSC ที่ https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

จัดการแอปต่าง ๆ ของคุณ

- **ตรวจสอบแอปของคุณและสิทธิ์การเข้าถึงของแต่ละแอป** หากคุณไม่จำเป็นต้องใช้แอปใดแล้ว ให้ลบออกไปหากทำได้
  ให้จำกัดสิทธิ์การเข้าถึงของแอปเพื่อลดการเปิดเผยข้อมูล
  เนื่องจากมัลแวร์มักถูกออกแบบมาเพื่อเข้าถึงไฟล์ที่ได้รับการ
  ป้องกันหรืออุปกรณ์ต่อพ่วง เช่น กล้องและไมโครโฟน
  - วิธีตรวจสอบสิทธิ์การเข้าถึงแอปสำหรับผู้ใช้ Apple ดูได้ที่ https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios
  - วิธีตรวจสอบสิทธิ์การเข้าถึงแอปสำหรับผู้ใช้ Android ดูได้ที่ https://support.google.com/android/answer/9431959?hl=en-GB

- **ส่งแอปที่ไม่รู้จักไปยัง Google โดยอัตโนมัติ** หากคุณเป็นผู้ใช้ Android และได้ดาวน์โหลดแอปที่ไม่ได้มาจาก Play Store
  ของ Google คุณสามารถส่งแอปดังกล่าวไปยัง Google ได้โดยเปิดใช้งาน ‘ปรับปรุงการตรวจจับแอปที่เป็นอันตราย (Improve harmful app detection)’ ในการตั้งค่าแอป Play Store ของ Google ภายใต้หัวข้อ ‘Play Protect’
  การทำเช่นนี้จะเป็นการสแกนแอปเพื่อตรวจจับมัลแวร์ ซึ่งช่วยปกป้องผู้ใช้งาน ข้อมูลเกี่ยวกับวิธีการตั้งค่านี้ ดูได้ที่ https://support.google.com/android/answer/2812853?hl=en-GB

ใช้ประโยชน์จากบริการทางไซเบอร์

- **ใช้บริการตรวจสอบความน่าเชื่อถือของ URL ก่อนคลิกลิงก์** คุณสามารถตรวจสอบได้ว่าลิงก์จากอีเมล ข้อความ หรือแหล่งอื่น ๆ ปลอดภัยหรือไม่ โดยการสแกนลิงก์นั้นก่อนล่วงหน้าด้วยบริการต่าง ๆ เช่น Google Transparency Report หรือ Virus Total คุณยังสามารถอัปโหลดไฟล์และแอปที่น่าสงสัยไปยังเครื่องวิเคราะห์มัลแวร์ เช่น Virus Total
  ซึ่งสามารถช่วยตรวจจับได้ว่าไฟล์นั้นเป็นอันตรายหรือไม่ พึงระวังว่าบริการสแกนอาจให้ผลลบปลอมได้

- **ลงทะเบียนในโปรแกรมการป้องกันขั้นสูงของ Google (Google Advanced Protection programme)**
  โปรแกรมนี้เป็นบริการฟรีที่ออกแบบมาเพื่อปกป้องบุคคลที่ใช้บริการของ Google (Gmail, Play Store เป็นต้น) ซึ่งมีความเสี่ยงที่จะตกเป็นเป้าหมายของมัลแวร์ บริการนี้เพิ่มความปลอดภัยเมื่อใช้บริการของ Google ให้มากขึ้น
  https://landing.google.com/advancedprotection/

- **ลงทะเบียนใช้บริการเสริมความยืดหยุ่น (Resilience) หากมีให้บริการ** ตัวอย่างเช่น
  บุคคลที่มีความเสี่ยงสูงในสหราช
  อาณาจักรอาจมีสิทธิ์ได้รับบริการป้องกันเพิ่มเติมเพื่อช่วยในด้านการรักษาความปลอดภัยทางไซเบอร์ของตน ตรวจสอบ
  คุณสมบัติและดูข้อมูลเพิ่มเติมได้ที่ https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e

รายงานภัยคุกคาม

- **การระบุและรายงานบัญชีปลอม**
  ผู้ไม่ประสงค์ดีทางไซเบอร์สร้างบัญชีปลอมหรือแฮ็กเข้าบัญชีจริงเพื่อบรรลุเป้าหมาย
  ของตน หากคุณสงสัยว่าบัญชีใดเป็นของปลอมหรือถูกบุกรุก
  ให้รายงานไปยังแพลตฟอร์มนั้นและบล็อกบัญชีดังกล่าวไปเสีย
  บริการจำนวนมากมีกระบวนการในการยืนยันบัญชี เช่น 'เครื่องหมายยืนยัน' (Verified badges) สำหรับ Instagram และ Facebook ซึ่งสามารถช่วยระบุได้ว่าบัญชีนั้นเป็นของจริงหรือไม่ NCSC
  มีคำแนะนำเกี่ยวกับการใช้โซเชียลมีเดีย
  อย่างปลอดภัย ซึ่งรวมถึงรายละเอียดวิธีการยืนยันและรายงานบัญชีที่ถูกบุกรุก ดูได้ที่
  https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- **ฟิชชิ่งโดยใช้อีเมล SMS และลิงก์เพื่อการหลอกลวง** NCSC
  สามารถตรวจสอบที่อยู่อีเมลและเว็บไซต์ที่น่าสงสัยได้
  หากคุณคิดว่าเว็บไซต์ อีเมล หรือข้อความใดน่าสงสัย คุณสามารถรายงานได้ที่
  https://www.ncsc.gov.uk/collection/phishing-scams

อภิธานศัพท์ NCSC

Android

ระบบปฏิบัติการเคลื่อนที่ของ Google ซึ่งใช้งานโดยผู้ผลิตสมาร์ทโฟนและแท็บเล็ตหลายราย

แอป

แอปพลิเคชันหรือแอป คือชุดซอฟต์แวร์ที่ผู้ใช้สามารถติดตั้งเองหรือมีการติดตั้งไว้ล่วงหน้าบนอุปกรณ์
เพื่อเพิ่มฟังก์ชันการทำงาน
หรือเนื้อหาให้กับอุปกรณ์ของตน

ความปลอดภัยทางไซเบอร์

การปกป้องอุปกรณ์ บริการ และเครือข่าย รวมถึงข้อมูลที่อยู่บนสิ่งเหล่านั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม หรือความเสียหาย

อุปกรณ์

ฮาร์ดแวร์คอมพิวเตอร์ที่มีอยู่จริงจับต้องได้ เช่น คอมพิวเตอร์เดสก์ท็อป สมาร์ทโฟน หรือแท็บเล็ต

iOS

ระบบปฏิบัติการเคลื่อนที่ของ Apple ที่ใช้กับอุปกรณ์เคลื่อนที่ต่าง ๆ ของ Apple

มัลแวร์ (Malware)

มัลแวร์มาจากคำว่า ‘ซอฟต์แวร์ที่เป็นอันตราย (Malicious software)’
คือซอฟต์แวร์ทุกประเภทที่สามารถสร้างความเสียหายให้กับ
ระบบคอมพิวเตอร์ เครือข่าย หรืออุปกรณ์ต่าง ๆ ซึ่งรวมถึงไวรัส แรนซัมแวร์ และโทรจัน

ระบบปฏิบัติการ

ซอฟต์แวร์พื้นฐานที่ทำงานบนคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟน
ซึ่งจำเป็นสำหรับการใช้งานแอปพลิเคชันและฮาร์ดแวร์เพิ่มเติม

ฟิชชิ่ง (Phishing)

อีเมลหรือข้อความหลอกลวงที่มีลิงก์ไปยังเว็บไซต์ซึ่งอาจมีมัลแวร์ หรืออาจหลอกล่อผู้ใช้ให้เปิดเผยข้อมูลที่ละเอียดอ่อน (เช่น รหัสผ่าน)
หรือโอนเงิน

สปายแวร์ (Spyware)

มัลแวร์ประเภทหนึ่งที่ติดตั้งบนอุปกรณ์โดยไม่ได้รับความยินยอมจากผู้ใช้
ซึ่งจะรวบรวมข้อมูลแล้วส่งข้อมูลดังกล่าวไปยังบุคคลที่สาม

- **โซเชียลมีเดีย**

เว็บไซต์และแอป เช่น Facebook, X และ Instagram ที่อนญาตให้ผู้คนสามารถแบ่งปันและตอบสนองต่อเนื้อหาที่ผู้ใช้สร้างขึ้น (โพสต์ข้อความ รูปภาพ และวิดีโอ)

- **สมาร์ทโฟน**

โทรศัพท์มือถือยุคใหม่ที่มีฟังก์ชันการทำงานที่ซับซ้อน รวมถึงโทรศัพท์ที่ใช้ระบบปฏิบัติการ Android และ iOS

- **โทรจัน (Trojan)**

มัลแวร์ประเภทหนึ่งที่ปลอมตัวเป็นซอฟต์แวร์ที่ถูกต้องตามกฎหมาย ซึ่งใช้ในการเข้าถึงอุปกรณ์ของเหยื่อโดยไม่ได้รับอนุญาต

- **URL**

รูปแบบมาตรฐานในการเข้าถึงข้อมูลบนอินเทอร์เน็ต (Uniform Resource Locator) ที่อยู่บนเวิลด์ไวด์เว็บ เช่น ชื่อโดเมน (ตัวอย่างเช่น
www.bbc.co.uk)

- **ไวรัส (Virus)**

มัลแวร์ประเภทหนึ่งที่ออกแบบมาเพื่อฝังตัวในโปรแกรมซอฟต์แวร์ที่ถูกต้องตามกฎหมาย
และสามารถแพร่กระจายไปตามเครือข่ายได้
เมื่อเปิดใช้งานโปรแกรมเหล่านั้น

อ่านเพิ่มเติม

คำแนะนำจากศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย (Australian Cyber Security Centre)

- รายงานอาชญากรรมไซเบอร์ เหตุการณ์ หรือช่องโหว่
- วิธีรักษาความปลอดภัยอุปกรณ์ของคุณ
- รักษาความปลอดภัยโทรศัพท์มือถือของคุณ
- ฟิชชิ่ง
- การหลอกลวง
- รักษาความปลอดภัยโซเชียลมีเดียของคุณ
- เคล็ดลับการรักษาความปลอดภัยสำหรับโซเชียลมีเดียและแอปส่งข้อความ

คำแนะนำจาก NCSC ของสหราชอาณาจักร และ NPSA

- การปกป้องประชาธิปไตย
- โซเชียลมีเดีย: ใช้อย่างไรให้ปลอดภัย
- คำแนะนำด้านการรักษาความปลอดภัยของอุปกรณ์สำหรับองค์กร รวมถึงอุปกรณ์เคลื่อนที่
- รายงานภัยคุกคามที่เกี่ยวกับแอปสโตร์
- ความปลอดภัยส่วนบุคคลและการรักษาความปลอดภัยสำหรับบุคคลที่มีความเสี่ยงสูง

คำแนะนำจาก NSA ของสหรัฐอเมริกา

- แนวปฏิบัติที่ดีที่สุดสำหรับอุปกรณ์เคลื่อนที่

ข้อจำกัดความรับผิดชอบ (Disclaimer)

โปรดทราบว่า คำแนะนำฉบับนี้ให้ข้อมูลที่ได้รับการตรวจสอบความถูกต้องแล้ว ณ เวลาที่เผยแพร่

รายงานฉบับนี้อ้างอิงข้อมูลจากหน่วยงานผู้จัดทำและแหล่งข้อมูลจากภาคอุตสาหกรรม ข้อค้นพบและคำแนะนำใด ๆ ที่จัดทำขึ้นนี้
ไม่ได้มีจุดมุ่งหมายเพื่อหลีกเลี่ยงความเสี่ยงทั้งหมด และแม้จะปฏิบัติตามคำแนะนำแล้ว
ก็ไม่อาจขจัดความเสี่ยงทั้งหมดดังกล่าวได้
ความรับผิดชอบเกี่ยวกับความเสี่ยงด้านข้อมูลยังคงเป็นของเจ้าของระบบที่เกี่ยวข้องเสมอ

ในสหราชอาณาจักร ข้อมูลนี้ได้รับการยกเว้นตามพระราชบัญญัติเสรีภาพในการเข้าถึงข้อมูลปี 2000 (Freedom of Information Act
2000 - FOIA) และอาจได้รับการยกเว้นตามกฎหมายว่าด้วยข้อมูลอื่น ๆ ของสหราชอาณาจักรด้วย

อ้างอิงคำถาม FOIA ใด ๆ ไปที่ ncscinfoleg@ncsc.gov.uk

ภาคผนวก ตัวอย่างของ MOONSHINE และ BADBAZAAR ที่ตรวจพบ

ตารางนี้แสดงรายการแอปที่ใช้ในการโจมตีของ MOONSHINE และ BADBAZAAR ในช่วงสองปีที่ผ่านมา

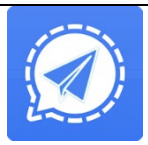
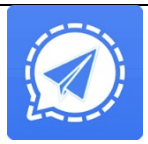
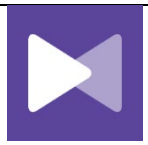
แอปเหล่านี้หลายตัวแสดงให้เห็นความคล้ายคลึงกับแอปที่มีชื่อเสียงได้รับการยอมรับอยู่แล้วอย่างชัดเจน ซึ่งอาจจะเป็นเทคนิคที่ผู้ไม่ประสงค์ดีตั้งใจใช้เพื่อ ‘เลียนแบบ’ แบรนด์ที่มีชื่อเสียงเป็นที่รู้จัก

สิ่งสำคัญที่ควรทราบคือ ชื่อแอป ชื่อแพ็กเกจ และไอคอน อาจเลียนแบบหรือเหมือนกับแอปพลิเคชันจริงได้ทั้งหมด ดังนั้นจึงไม่ควร
ใช้เพียงสิ่งเหล่านี้เท่านั้นในการระบุว่าอุปกรณ์ติดมัลแวร์หรือไม่

ตามที่แสดงอยู่ในหัวข้อมาตรการบรรเทาปัญหา คุณสามารถส่งแอปบนอุปกรณ์ Android ของคุณไปยัง Google ได้โดยเปิดใช้งาน
ฟังก์ชัน ‘ปรับปรุงการตรวจจับแอปที่เป็นอันตราย (Improve harmful app detection)’ ซึ่งจะสแกนแอปที่ติดตั้งจากภายนอก Play Store บนอุปกรณ์ของคุณ

ชื่อแอป	ชื่อแพ็กเกจ	ไอคอนแอป
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	

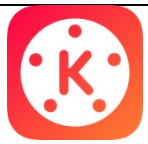
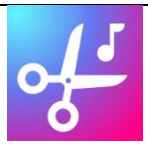
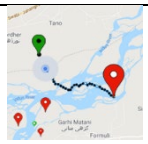
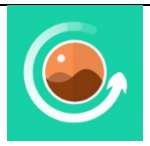
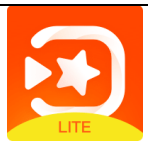
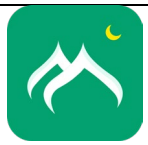
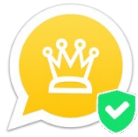
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

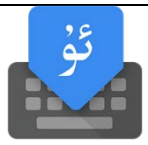
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

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

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

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

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

ئاۋازلىق ئەسەرلەر	com.ewlat.eserler	
ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى ئۇيغۇرچە APK	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