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:

การวิเคราะห์ทางเทคนิค

และการบรรเทาปัญหา

9 เมษายน 2025

BADBAZAAR และ MOONSHINE:
การวิเคราะห์ทางเทคนิคและการบรรเทาปัญหา

บทสรุป

ด้วยการสนับสนุนจาก Cyber League ของสหราชอาณาจักร
คำแนะนำนี้จัดทำขึ้นโดยความร่วมมือระหว่างศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาติของสหราชอาณาจักร (National Cyber Security Centre - NCSC UK) และพันธมิตรสากล ดังต่อไปนี้

- **ศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย ซึ่งเป็นส่วนหนึ่งของหน่วยข่าวกรองสัญญาณออสเตรเลีย**
- **ศูนย์รักษาความปลอดภัยทางไซเบอร์แคนาดา**
  ส่วนหนึ่งของหน่วยงานการรักษาความปลอดภัยทางการสื่อสาร
- **สำนักงานข่าวกรองกลางแห่งสหพันธรัฐเยอรมัน**
- **สำนักงานสหพันธรัฐเยอรมันเพื่อการปกป้องรัฐธรรมนูญ**
- **ศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาตินิวซีแลนด์ ซึ่งเป็นส่วนหนึ่งของสำนักการรักษาความปลอดภัยทางการสื่อสารของรัฐบาล**
- **สำนักงานสอบสวนกลางสหรัฐอเมริกา**
- **หน่วยงานรักษาความปลอดภัยแห่งชาติสหรัฐอเมริกา**

คำแนะนำนี้ให้ข้อมูลข่าวกรองด้านภัยคุกคามใหม่และที่มีการรวบรวมไว้เกี่ยวกับสปายแวร์ 2 รูปแบบที่รู้จักกันในชื่อ BADBAZAAR และ MOONSHINE พร้อมทั้งให้คำแนะนำแก่ผู้ให้บริการแอปสโตร์ นักพัฒนาแอป และบริษัทโซเชียลมีเดียเพื่อช่วยให้ผู้ใช้ของตน ปลอดภัย

คำแนะนำฉบับนี้เผยแพร่ควบคู่ไปกับคำแนะนำสำหรับผู้ที่ตกเป็นเหยื่อของมัลแวร์เหล่านี้

เอกสารนี้ใช้คำจำกัดความตามอภิธานศัพท์ของ NCSC สำหรับคำว่า สปายแวร์ นั่นคือ “มัลแวร์ ประเภทหนึ่งที่ติดตั้งบนอุปกรณ์โดยไม่ได้รับความยินยอมจากผู้ใช้ ซึ่งจะรวบรวมข้อมูลแล้วส่งข้อมูลดังกล่าวไปยังบุคคลที่สาม”

กรณีศึกษากรณีที่หนึ่ง: MOONSHINE

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

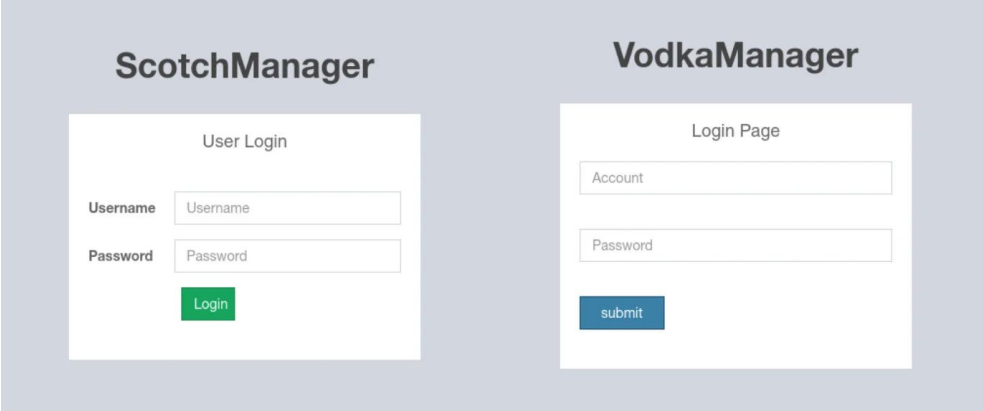
การวิจัยของ NCSC เกี่ยวกับ MOONSHINE ระบุดังนี้

- MOONSHINE ใช้อินเทอร์เฟซการจัดการที่มีการเปลี่ยนแปลงไปจากเดิมนับตั้งแต่มีการรายงานครั้งแรก
- อินเทอร์เฟซการจัดการแสดงให้เห็นถึงความสามารถในการสอดแนมอย่างกว้างขวาง
  รวมไปถึงความสามารถในการดึงข้อมูลไฟล์
  ออกจากอุปกรณ์ ตลอดจนการบันทึกเสียงและบันทึกหน้าจอในเวลาจริง
- มีการค้นพบชุดอินเทอร์เฟซการจัดการของ MOONSHINE ที่เป็นโฮสต์แบบเสมือนจริง
  อินเทอร์เฟซเหล่านี้มีโครงสร้างพื้นฐาน
  ที่ทับซ้อนกับแผงควบคุมเข้าสู่ระบบที่เชื่อมโยงกับ UPSEC ซึ่งตามรายงานของ Intelligence Online หมายถึงบริษัท
  'Sichuan Dianke Network Security Technology Co., Ltd.'

อินเทอร์เฟซการจัดการ

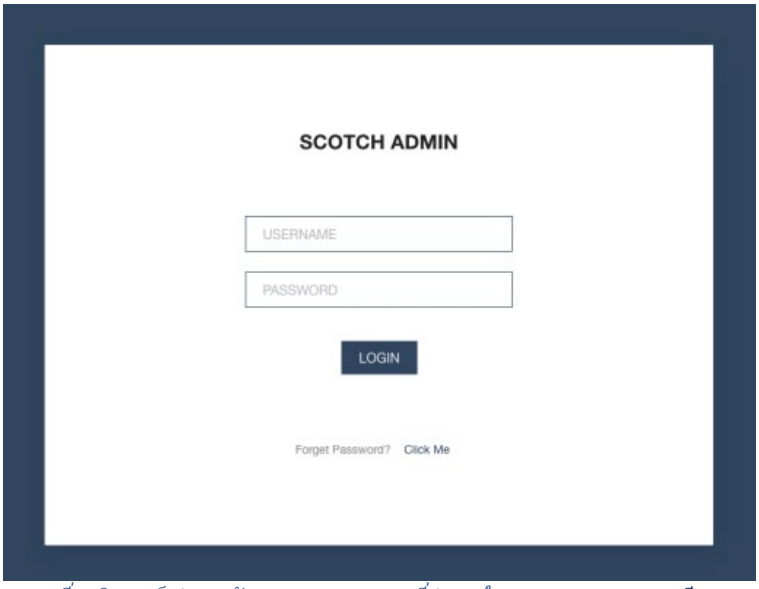
การรายงานก่อนหน้านี้เกี่ยวกับอินเทอร์เฟซการจัดการ MOONSHINE ระบุว่ามีการเปลี่ยนแปลงเกิดขึ้น
ซึ่งบ่งชี้ถึงการพัฒนาอย่างต่อเนื่อง

ตัวอย่างแรกของอินเทอร์เฟซการจัดการพบได้ในรายงานของ Citizen Lab เมื่อปี 2019



ภาพที่ 1: อินเทอร์เฟซการจัดการ MOONSHINE ที่ปรากฏในรายงานของ Citizen Lab เมื่อปี 2019
เรื่อง 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'

เมื่อต้นปี 2022 Lookout มีการรายงานว่าอินเทอร์เฟซการจัดการรูปแบบใหม่ถูกออกแบบขึ้น เพื่อให้มีหน้าตาดังภาพด้านล่างนี้ (แทนที่อินเทอร์เฟซก่อนหน้าในภาพที่ 1)

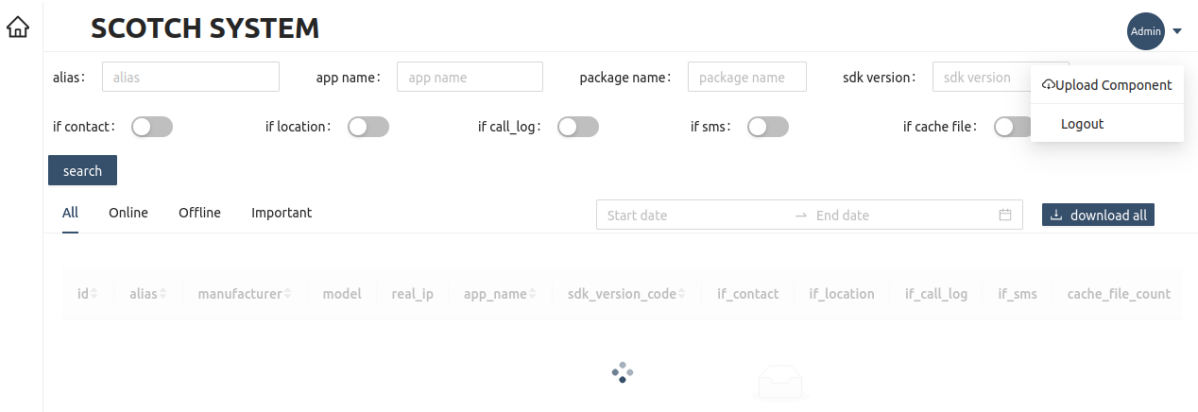


ภาพที่ 2: อินเทอร์เฟซการจัดการ MOONSHINE ที่ปรากฏในรายงานของ Lookout ปี 2022 ที่ชื่อว่า 'MOONSHINE: Evolving Android Surveillanceware by Chinese APT POISON CARP To Target Tibetans and Uyghurs'.

ในเดือนสิงหาคม 2023 การสแกนระบบสั่งการและควบคุม (C2) ของ MOONSHINE เผยให้เห็นอินเทอร์เฟซมีลักษณะคล้ายกับอินเทอร์เฟซในปี 2022 โดยไม่มีฟังก์ชันการทำงาน '**ลืมรหัสผ่าน**' อีกต่อไปตามที่แสดงในภาพที่ 2

ภาพที่ 3: อินเทอร์เฟซการจัดการ MOONSHINE ที่พบในเดือนสิงหาคมปี 2023 ซึ่งไม่มีข้อความแจ้งเตือน 'ลืมรหัสผ่าน' อีกต่อไป

การตรวจสอบเพิ่มเติมของอินเทอร์เฟซการจัดการแสดงให้เห็นเนื้อหาภายในแผงควบคุม
ซึ่งเปิดเผยว่ารายละเอียดของอุปกรณ์ที่ถูกบุกรุก จะถูกจัดเก็บไว้อย่างไร



ภาพที่ 4: หน้าเว็บที่อยู่ด้านหลังหน้าเข้าสู่ระบบ (LOGIN) ของอินเทอร์เฟซการจัดการ MOONSHINE

งานวิจัยของ Lookout พบว่ามีการส่งผ่านค่า **'คะแนน'** จากอุปกรณ์ของเหยื่อไปยังเซิร์ฟเวอร์ระบบสั่งการและควบคุม (C2) ของ MOONSHINE ค่าของ 'คะแนน' จะขึ้นอยู่กับสิทธิ์การเข้าถึงของตัวอย่างมัลแวร์ ซึ่งเป็นอันตรายบนอุปกรณ์ของเหยื่อ

คอลัมน์ 'if_contact', 'if_location', 'if_call_log' และ 'if_sms' ภายในหน้าเพจดังกล่าวบ่งชี้ว่าไม่ใช่ตัวอย่างมัลแวร์ MOONSHINE ทุกตัวสามารถเข้าถึงอุปกรณ์ที่ถูกบุกรุกได้อย่างสมบูรณ์ ความรู้เกี่ยวกับคอลัมน์เหล่านี้ และ "คะแนน"
ที่ส่งจากอุปกรณ์ไปยังระบบ C2
บ่งชี้ว่าผู้ก่อภัยคุกคามใช้คะแนนดังกล่าวเพื่อสื่อสารระดับการเข้าถึงของมัลแวร์ที่มีต่ออุปกรณ์ที่ถูกบุกรุกไปยังบุคคลที่เข้าถึงอินเทอร์เฟซ การจัดการ

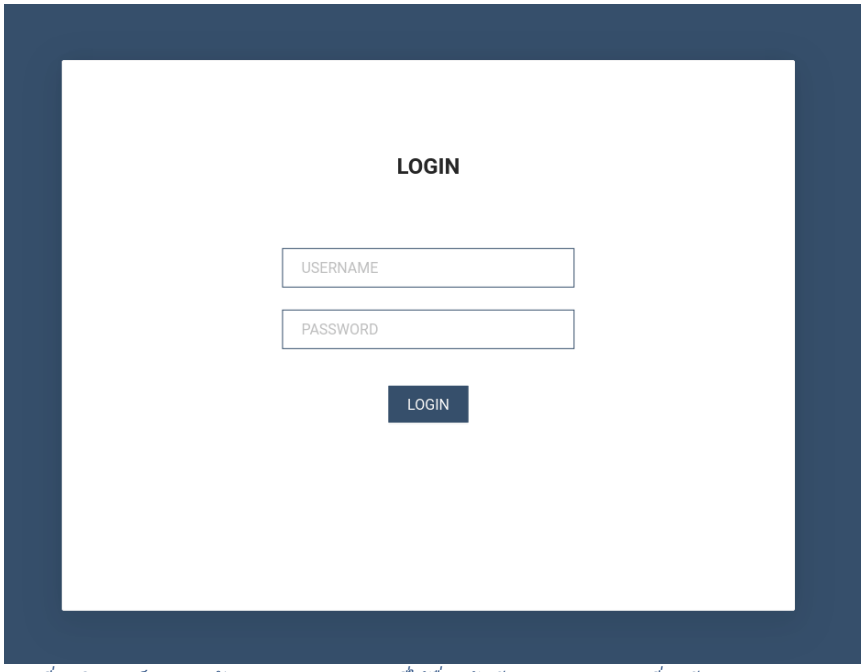
โดยทั่วไป คำแนะนำแนวปฏิบัติที่ดีที่สุดในการป้องกันไม่ให้แอปเก็บข้อมูลจากอุปกรณ์ คือ การตรวจสอบสิทธิ์การเข้าถึงของแอป เพื่อดูว่ามีสิ่งผิดปกติหรือไม่ ก่อนทำการดาวน์โหลด อย่างไรก็ตาม ตัวอย่างมัลแวร์ MOONSHINE จะขอสิทธิ์การเข้าถึง
ซึ่งสอดคล้องกับ ฟังก์ชันการทำงานของแอป ดังนั้นจึงอาจดูไม่น่าสงสัย
แต่ยังใช้การขอสิทธิ์เหล่านี้เพื่อเก็บข้อมูลจากอุปกรณ์อีกด้วย

MOONSHINE ยังมีอินเทอร์เฟซโปรแกรมประยุกต์ (Application Programming Interface - API)
ที่เผยให้เห็นขอบเขตความสามารถ ที่กว้างขวางของมัน เอกสาร API เวอร์ชันแรก ๆ มีการใช้ชื่อ API เป็นภาษาจีนกลาง

โฮสต์แบบเสมือนจริง

ในการค้นหาแผงควบคุมของ MOONSHINE มีการพบกรณีโฮสต์แบบเสมือนจริงอยู่ด้วย การทำโฮสต์แบบเสมือนจริง คือ เมื่อที่อยู่ IP เดียว สามารถโฮสต์เว็บไซต์ได้หลายเว็บไซต์พร้อมกัน ไม่มีการพบที่อยู่ IP ของกรณีโฮสต์แบบเสมือนจริงเหล่านี้ และโดเมนที่โฮสต์ในตัวอย่าง มัลแวร์ที่รู้จัก

กรณีของอินเทอร์เฟซการจัดการเหล่านี้มีความแตกต่างกัน เนื่องจากชื่อของหน้าเว็บถูกระบุว่า '**ลอกอิน**' แทนที่จะเป็น '**สก็อตช์แอดมิน**' อย่างที่เคยพบก่อนหน้านี้



ภาพที่ 5: อินเทอร์เฟซการจัดการ MOONSHINE ที่ใช้ชื่อหน้าเว็บว่า LOGIN แทนที่จะเป็น SCOTCH ADMIN

นอกจากนี้ เนื้อหาบนแผงควบคุมยังแตกต่างจากภาพที่ 4 อีกด้วย ดังที่เห็นในภาพที่ 6

ภาพที่ 6: หน้าเว็บที่อยู่ด้านหลังหน้าเข้าสู่ระบบ (LOGIN) ของอินเทอร์เฟซการจัดการ MOONSHINE ที่เป็นโฮสต์แบบเสมือนจริง

แผงควบคุมในภาพที่ 6 ดูเหมือนจะเป็นเวอร์ชันที่ตัดทอนลงของแผงควบคุมในภาพที่ 4 ลักษณะที่ทับซ้อนกันของแผงควบคุม คือ ชื่อคอลัมน์ 'id', 'manufacturer' และ 'model' ในตาราง

กรณีของ MOONSHINE ที่เป็นโฮสต์แบบเสมือนจริง ซึ่งถูกค้นพบ ได้แก่

โดเมน	ที่อยู่
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

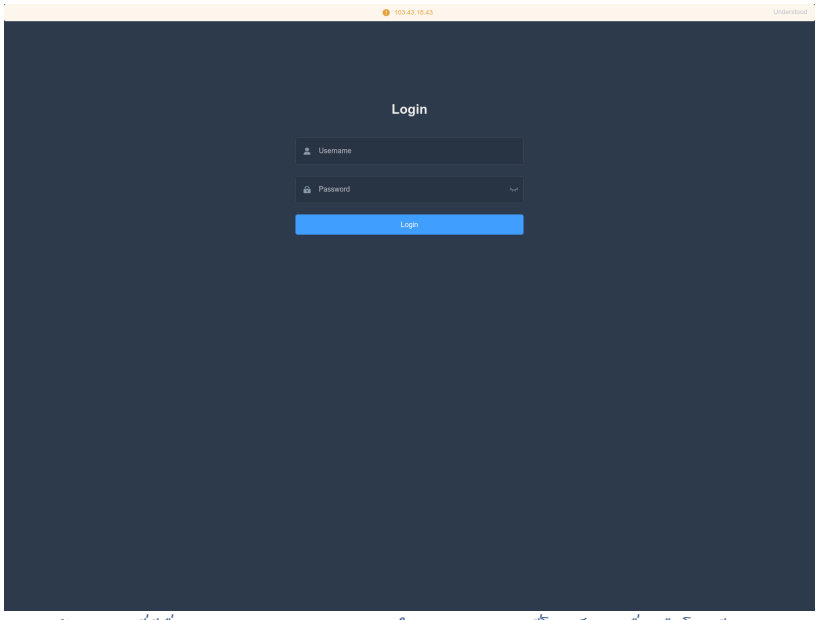
โดเมนเหล่านี้ถูกระบุโดย Trend Micro ว่าเป็นชุดเครื่องมือโจมตี (Exploit kits) ของ MOONSHINE
ซึ่งมีหน้าที่ในการแสวงหาประโยชน์ จากช่องโหว่ของเบราว์เซอร์เพื่อติดตั้งมัลแวร์บนอุปกรณ์เคลื่อนที่ Trend Micro
ให้ชื่อมัลแวร์นี้ว่า 'Dark Nimbus'

เพื่อความชัดเจน อินเทอร์เฟซการจัดการของ MOONSHINE คือ สิ่งที่ตัวอย่างมัลแวร์ MOONSHINE ใช้สื่อสารด้วย
และเป็นจุดที่ข้อมูล ของเหยื่อถูกส่งออกไปถึง ชุดเครื่องมือโจมตีของ MOONSHINE ที่ Trend Micro รายงานนั้น
เป็นความสามารถแยกต่างหากที่แสวงหา ประโยชน์จากช่องโหว่ของเบราว์เซอร์ในการติดตั้งมัลแวร์ที่ชื่อ Dark Nimbus
บนอุปกรณ์เคลื่อนที่ นอกจากนี้ Dark Nimbus และ MOONSHINE ยังเป็นมัลแวร์ที่แตกต่างกันอย่างสิ้นเชิง

ทั้งอินเทอร์เฟซการจัดการ MOONSHINE และชุดเครื่องมือโจมตี MOONSHINE นั้นมีโค้ดที่ทับซ้อนกัน
จึงทำให้มีข้อความแจ้งให้เข้าสู่ ระบบที่คล้ายคลึงกันในภาพที่ 3 และ 5 เช่นเดียวกับเนื้อหาของหน้าเพจในภาพที่ 4 และ 6
ทั้งสองยังมีสตริง 'webpackJsonpreact-scotchui' ในซอร์สโค้ด (source code) ด้วย

ผู้ก่อภัยคุกคามสร้างลิงก์ URL ที่เชื่อมต่อกับชุดเครื่องมือโจมตี MOONSHINE
จากนั้นเปลี่ยนเส้นทางไปยังวิดีโอที่เกี่ยวข้องกับชาวทิเบต และชาวอุยกูร์ ซึ่งทับซ้อนกับเป้าหมายของ MOONSHINE

จากบรรดาที่อยู่ IP จำนวนมากที่โฮสต์โดเมนของชุดเครื่องมือโจมตี MOONSHINE พบหน้าเข้าสู่ระบบหรือหน้าล็อกอินที่มีชื่อว่า
‘VLiteUI’ บนพอร์ต 444 หน้าเว็บนี้ไม่เป็นที่สังเกตเห็นโดยทั่วไป และการที่มันปรากฏอยู่บนหมายเลข IP
เหล่านี้บ่งชี้ถึงความเป็นไปได้ว่า เชื่อมโยงกับการปฏิบัติการของผู้ไม่ประสงค์ดี



ภาพที่ 7: แผงควบคุมเข้าสู่ระบบที่มีชื่อ HTML ว่า 'VLiteUI' ถูกพบในหมายเลข IP ที่โฮสต์ชุดเครื่องมือโจมตี MOONSHINE ด้วยเช่นกัน

การวิเคราะห์มัลแวร์ Dark Nimbus ของ Trend Micro เปิดเผยว่ามัลแวร์นี้สามารถรวบรวมข้อมูลจากอุปกรณ์ได้อย่างครอบคลุม และยังสื่อสารกับระบบ C2 โดยใช้โปรโตคอล XMPP ด้วย

นอกจากนี้ Trend Micro ระบุด้วยว่าในมัลแวร์ Dark Nimbus บางเวอร์ชัน ยังพบการแพร่หลายของสตริง 'DKNS'

‘**ansec[.]com**’ (ซึ่งถูกจัดให้อยู่ในฐานะระบบ C2 ของ Dark Nimbus โดย TrendMicro) ยังพบในบริการ XMPP สำหรับที่อยู่ IP อื่น ๆ ที่ให้บริการหน้าเว็บ ซึ่งมีคำว่า DKNS ในชื่อเรื่องดังต่อไปนี้ด้วย

- DKNS Android远程取证系统 (ระบบพิสูจน์หลักฐานระยะไกลสำหรับแอนดรอยด์ DKNS)
- DKNS云网侦控平台 (แพลตฟอร์มการสอบสวนและควบคุมเครือข่ายคลาวด์ DKNS)
- DKNS 云网侦控平台 (แพลตฟอร์มการสอบสวนและควบคุมเครือข่ายคลาวด์ DKNS)
- DKNS远程控制侦查系统 (ระบบสอบสวนควบคุมระยะไกล DKNS)

ที่อยู่ IP อีกชุดหนึ่งที่มี ‘**ansec[.]com**’ ในบริการ XMPP มีหน้าเว็บที่มีชื่อเรื่องดังนี้

- UPSEC互联网控制指挥系统 (ระบบสั่งการควบคุมอินเทอร์เน็ต UPSEC)
- UPSEC无线侦控系统 (ระบบเฝ้าระวังและควบคุมแบบไร้สาย UPSEC)
- UPSEC重点人数据还原系统 (ระบบกู้คืนข้อมูลที่สำคัญสำหรับบุคคล)

จากรายงานของ Intelligence Online การอ้างอิงถึง ‘UPSEC’ ที่ปรากฏในชื่อของหน้า HTML นั้นหมายถึงบริษัท ‘Sichuan Dianke Network Security Technology Co., Ltd’

กรณีศึกษากรณีที่สอง: BADBAZAAR

BADBAZAAR เป็นมัลแวร์บนอุปกรณ์เคลื่อนที่ที่มีทั้งเวอร์ชัน iOS และ Android ซึ่งมุ่งเป้าไปที่ชาวอุยกูร์ ชาวทิเบต และชาวไต้หวัน 1 สปายแวร์นี้แพร่กระจายผ่านแพลตฟอร์มโซเชียลมีเดียและแอปสโตร์ทางการ รายงานล่าสุดจาก Volexity แสดงให้เห็นมัลแวร์ BADBAZAAR ในหลากหลายรูปแบบ ซึ่งแยกเป็น BadSolar, BADBAZAAR และ BadSignal ทั้งสามรูปแบบเชื่อมโยงกันด้วยฟังก์ชั่น การทำงานที่ทับซ้อนกัน ซึ่งใช้ในการเก็บข้อมูลอุปกรณ์และข้อมูลผู้ปฏิบัติงาน

การวิจัยของ NCSC เกี่ยวกับ BADBAZAAR เปิดเผยข้อมูลดังนี้

- การจัดคลัสเตอร์โดเมนระบบ C2
  เผยให้เห็นความเชื่อมโยงเพิ่มเติมกับโดเมนที่รายงานในข่าวกรองด้านภัยคุกคามในอดีต
- เซิร์ฟเวอร์ระบบ C2 และตัวอย่างมัลแวร์เปิดเผยชื่อโฮสต์ที่เชื่อมโยงกับโครงสร้างพื้นฐานของกลุ่มผู้ไม่ประสงค์ดี
- โปรไฟล์เพิ่มเติมที่ผู้ก่อภัยคุกคามใช้วิธีการทางวิศวกรรมสังคม (Social engineering)
  เพื่อแพร่กระจายมัลแวร์ของตนออกไป
  นอกเหนือจากแอปสโตร์ทางการ

การจัดกลุ่มคลัสเตอร์ WHOIS/โบรกเกอร์โดเมน

'UJYJYUJ'

การวิเคราะห์บันทึก WHOIS สำหรับโดเมน BADBAZAAR '**signalplus[.]org**' (รายงานโดย ESET) แสดงให้เห็นค่า '**UJYJYUJ**' ในช่อง '**State**'

การค้นหาโดเมนอื่นที่มีค่าเดียวกันเผยให้เห็นโดเมนที่อยู่ในความสนใจดังต่อไปนี้

- thetubeplus[.]com
- tubevideoplus[.]org
- pmumail[.]com
- signalplus[.]org

(ดูภาคผนวก A รูปภาพที่ 1)

โดเมน **signalplus[.]org, tubevideoplus[.]org** และ thetubeplus[.]com ได้รับการรายงานว่าเป็นโดเมนระบบ C2 ของ BADBAZAAR ในขณะที่ ESET รายงานว่าซับโดเมน **mail.pmumail[.]com** เป็นพร็อกซีเซิร์ฟเวอร์ของ FlyGram FlyGram เป็นแอป BADBAZAAR ที่พัฒนาโดยกลุ่มผู้ไม่ประสงค์ดีทางไซเบอร์ (ดูภาคผนวกสำหรับรายชื่อแอป BADBAZAAR อื่น ๆ)

ค่าการเดินแป้นพิมพ์ (Keyboard walking values)

NCSC ยังพบรูปแบบการเดินแป้นพิมพ์ที่คล้ายกันในโดเมนระบบ C2 ของ BADBAZAAR ที่จดทะเบียนไว้กับโดเมนอื่นด้วย

ตัวอย่างเช่น โดเมนทั้งหมดต่อไปนี้มีค่า **'REWR'** ที่พบในช่อง **'State'** (ดังที่ใช้ก่อนหน้านี้) ได้แก่

- yumoftion[.]com
- fvbyavgyea[.]com
- jkiohreh[.]com
- pmstwocqn[.]com

(ดูภาคผนวก A รูปภาพที่ 2)

โดเมนที่มีค่าช่อง State เป็น 'FSDF'

อีกชุดหนึ่งของโดเมนระบบ C2 ของ BADBAZAAR ที่มีค่าช่อง '**State**' เป็น '**FSDF**' ได้แก่

- tryhrwserf[.]com
- tibetone[.]org
- comeflxyr[.]com

(ดูภาคผนวก A รูปภาพที่ 3)

รายงานในอดีตเกี่ยวกับค่าการเดินแป้นพิมพ์ (Keyboard walking values)

การใช้ค่าการเดินแป้นพิมพ์ในบันทึก WHOIS ของโดเมน BADBAZAAR
ยังสามารถพบเห็นได้ในการมุ่งเป้าสู่องค์กรชาวทิเบตโดยกลุ่ม TA413 ที่มีการรายงานในอดีต Recorded Future
ได้สังเกตเห็นโดเมนที่ควบคุมโดยผู้ไม่ประสงค์ดี ซึ่งแอบอ้างตัวเป็นองค์กรชาวทิเบต รวมถึงการใช้ค่าชื่อองค์กรผู้จดทะเบียนเป็น "**asfasf**"

clublogs[.]com

ตัวอย่าง BADBAZAAR ที่ได้รับจาก Lookout มีโดเมนระบบ C2 เป็น '**xle.clublogs[.]com**' โดเมนหลัก **'clublogs[.]com'**
ถูกโฮสต์บนที่อยู่ IP **'95.179.210[.]85'** และมีใบรับรอง SSL ที่มีค่า subject และ issuer เป็น '**CN=WIN-50QO3EIRQVP**'
ค่านี้ตรงกับใบรับรอง SSL ที่พบในตัวอย่าง BADBAZAAR ซึ่งใช้เทคนิคการปักหมุด SSL (SSL pinning)
เพื่อหลีกเลี่ยงการดักจับ การสื่อสาร

ประวัติการโฮสต์ของที่อยู่ IP **95.179.210[.]85** แสดงโดเมนที่อยู่ในความสนใจดังต่อไปนี้

- actuallys[.]com
- bre.myloughborough[.]com
- rewrwer[.]com
- www.voiceoftibet[.]net
- clublogs[.]com

(ดูภาคผนวก A รูปภาพที่ 4)

www.voiceoftibet[.]net

โดเมน '**www.voiceoftibet[.]net**' ดูเหมือนจะแอบอ้างเป็นสถานีวิทยุ 'Voice of Tibet' ซึ่งคล้ายกับ TTP (กลยุทธ์ เทคนิค และขั้นตอนปฏิบัติ) ที่กลุ่ม TA413 เคยใช้

โดเมน '**rewrwer[.]com**' มีลักษณะคล้ายคลึงกับค่าช่อง '**State**' ที่ระบุไว้ก่อนหน้านี้เป็น '**REWR**' ซึ่งพบในบันทึก WHOIS ของโดเมน BADBAZAAR

โดเมน '**clublogs[.]com', 'rewrwer[.]com**', '**voiceoftibet[.]net**' และ '**myloughborough[.]com**' ทั้งหมดถูกจดทะเบียนโดยใช้ที่อยู่อีเมล '**tplutalova@list[.]ru**'

actuallys[.]com

บันทึก WHOIS สำหรับโดเมน '**actuallys[.]com**' แสดงให้เห็นกรณีที่ที่อยู่อีเมลสำหรับฝ่ายเทคนิคและผู้ดูแลระบบ คือ '**tplutalova@list[.]ru**' แต่อีเมลของผู้จดทะเบียนคือ '**ivan_s81@mail[.]ru**'

ข้อมูล WHOIS ในอดีตของโดเมน '**actuallys[.]com**' เปิดเผยว่าอีเมลที่ใช้จดทะเบียนคือ '**wangminghua6@gmail[.]com**' ซึ่งปรากฏเมื่อวันที่ 24 กุมภาพันธ์ 2016 เมื่อวันที่ 11 มีนาคม 2016 อีเมลดังกล่าวถูกเปลี่ยนไปเป็น '**ivan_s81@mail.ru**' แต่วันที่หมดอายุของการจดทะเบียนกับผู้ให้บริการยังคงเดิม

wangminghua6@gmail[.]com

ที่อยู่อีเมล '**wangminghua6@gmail[.]com**'
ถูกใช้ในการจดทะเบียนโดเมนที่ปรากฏอยู่ในรายงานข่าวกรองด้านภัยคุกคามในอดีต ในปี 2015 Palo Alto ได้ระบุว่าอีเมลนี้ใช้ในการจดทะเบียนโดเมนระบบ C2 สำหรับมัลแวร์ Cmstar ในปี 2014 อีเมลดังกล่าวยังถูกใช้ในการจดทะเบียนโดเมนที่ Mandiant ระบุว่าเกี่ยวข้องกับการโจมตีแบบฟิชชิ่งที่ดำเนินการโดย APT3 ในปี 2013 อีเมลดังกล่าวถูกใช้ ในการจดทะเบียนโดเมนที่ CrowdStrike ตรวจพบในมัลแวร์ดรอปเปอร์ ซึ่งมีเส้นทางฐานข้อมูลโปรแกรม (Program Database - PDB) ที่มีตัวอักษรจีนประกอบอยู่ด้วย ซึ่งบ่งชี้ว่ามีการรวบรวมข้อมูล (Compilation) บนระบบภาษาจีน

taoyujun@gmail[.]com

โดเมน '**hcjbtt[.]com**' ถูกจดทะเบียนด้วยที่อยู่อีเมล '**taoyujun@gmail[.]com**' แต่อีเมลผู้ดูแลระบบที่จดทะเบียนเป็น '**wangminghua6@gmail[.]com**'

ไม่มีกิจกรรมที่เป็นอันตรายเชื่อมโยงกับโดเมน '**hcjbtt[.]com**' อย่างไรก็ตาม มีการพบที่อยู่อีเมล '**taoyujun@gmail[.]com**' ในรายงานข่าวกรองด้านภัยคุกคามในอดีต ในปี 2014 อีเมลดังกล่าวถูกใช้ในการจดทะเบียนโดเมนที่ Mandiant ตรวจพบในตัวอย่าง '**Cueisfry Trojan**' ซึ่งใช้ในการโจมตีเป้าหมายองค์กรของญี่ปุ่น

ที่อยู่อีเมลดังกล่าวยังได้จดทะเบียนโดเมนต่าง ๆ เช่น '**iaea-international[.]org**' งดูเหมือนจะแอบอ้างเป็น**ทบวงการพลังงานปรมาณูระหว่างประเทศ** และ '**idc-ctbto[.]org**'
ซึ่งแอบอ้างเป็น**ศูนย์ข้อมูลระหว่างประเทศที่องค์การสนธิสัญญาว่าด้วยการ ห้ามทดลองนิวเคลียร์โดยสมบูรณ์ (CTBTO).**

บันทึก Whois ก่อนหน้านี้สำหรับโดเมน '**iaea-international[.]org**' แสดงให้เห็นว่าอีเมลผู้จดทะเบียน คือ '**wangminghua6@gmail[.]com**'

udtglobals[.]com

โดเมน '**udtglobals[.]com**' ถูกพบว่าใช้อีเมล '**wangminghua6@gmail[.]com**' เป็นอีเมลผู้ดูแลระบบ และ '**ocean.nio@rediffmail[.]com**' เป็นอยู่อีเมลผู้จดทะเบียน บันทึก WHOIS อื่น ๆ สำหรับโดเมนนี้ แสดงอีเมลผู้จดทะเบียนคนเดียวกัน แต่มีที่อยู่อีเมลผู้ดูแลระบบเป็น '**taoyujun@gmail[.]com**'

'**udtglobals[.]com**' ดูเหมือนว่าจะแอบอ้างเป็น '**UDT Global**' ซึ่งเป็นงานระดับโลกสำหรับบริษัทด้านการป้องกันและการรักษาความปลอดภัยใต้ทะเล ชื่อผู้ใช้ '**ocean.nio**' ในที่อยู่อีเมล อาจเลียนแบบ**สถาบันสมุทรศาสตร์แห่งชาติ (NIO)**
ซึ่งมีอยู่ในหลายประเทศ แม้ว่าการใช้บริการอีเมล '**Rediff**' (ซึ่งมีฐานอยู่ในอินเดีย)
อาจบ่งชี้ถึงการเลียนแบบ**สถาบันสมุทรศาสตร์แห่งชาติของอินเดีย**

Djibdiplomatie[.]com

โดเมน '**djibdiplomatie[.]com**' ดูเหมือนจะแอบอ้างเป็นบริการการทูตของประเทศจิบูตี (Djibouti diplomacy services) ซึ่งมีบันทึก WHOIS ที่คล้ายกับ '**utdglobals[.]com**' บันทึกหนึ่งดูเหมือนจะแสดงผู้จดทะเบียนเป็น '**ocean.nio@rediffmail[.]com**' และผู้ดูแลระบบเป็น '**taoyujun@gmail[.]com**' ในขณะที่บันทึกอื่นแสดง '**wangminghua6@gmail[.]com**'
เป็นที่อยู่อีเมลผู้ดูแล ระบบ โดยมี '**ocean.nio@rediffmail[.]com**' เป็นอีเมลผู้จดทะเบียน

โดเมนทั้งสองนี้ยังมีค่าประเภทการเดินแป้นพิมพ์ในบันทึก WHOIS อีกด้วย ตัวอย่างเช่น '**udtglobals[.]com**' มีค่า '**ASDF**' เป็นเมืองที่จดทะเบียนและ '**djibdiplomatie[.]com**' มีค่า '**DAF DAGF**' เป็นค่าชื่อผู้จดทะเบียน ซึ่งมีความคล้ายคลึงกับค่าที่พบในโดเมน BADBAZAAR อื่น ๆ

ถึงแม้ว่าจะพบที่อยู่อีเมล '**wangminghua6@gmail[.]com**' และ '**taoyujun@gmail[.]com**' ในบันทึก WHOIS สำหรับโดเมนที่แอบอ้างว่าเป็น**งานด้านการป้องกันใต้น้ำระดับโลก บริการทางการทูตของจิบูตี**
และ**ทบวงการพลังงานปรมาณูระหว่างประเทศ** แต่ทั้งสองอีเมลนี้ก็ยังพบในบันทึก WHOIS
ของโดเมนที่ไม่มีพฤติกรรมเป็นอันตรายจำนวนมากด้วยเช่นกัน

การผสมผสานกันระหว่างโดเมนที่แอบอ้างและโดเมนที่ไม่เป็นอันตรายอาจบ่งชี้ถึงการมีอยู่ของหน่วยงานหนึ่งที่จัดหาโครงสร้างพื้นฐานในการสนับสนุนการปฏิบัติการของผู้ไม่ประสงค์ดีทางไซเบอร์

ที่อยู่อีเมล '**ocean.nio@rediffmail[.]com**' พบได้เฉพาะในโดเมนแอบอ้างที่อธิบายไว้ข้างต้นเท่านั้น '**ivan_s81@mail[.]ru**' และ '**tplutalova@list[.]ru**' ได้จดทะเบียนโดเมนจำนวนเล็กน้อยตามลำดับ และโดเมนบางส่วนเหล่านี้ได้ถูกโฮสต์บนโครงสร้างพื้นฐานของ BADBAZAAR ด้วย
เชื่อกันว่าที่อยู่อีเมลทั้งสามนี้มีความเชื่อมโยงอย่างใกล้ชิดกับการปฏิบัติการของผู้ไม่ประสงค์ดีทางไซเบอร์ ทั้งนี้ เป็นเพราะโดเมนจำนวนมากที่เกี่ยวข้องมีการเชื่อมโยงกับกิจกรรมที่เป็นอันตราย เมื่อเทียบกับอีเมล '**wangminghua6@gmail[.]com**' และ '**taoyujun@gmail[.]com**'

(ดูภาคผนวก A รูปภาพที่ 5)

ลิงก์สู่ผู้ก่อภัยคุกคามรายอื่น

ลักษณะร่วมอีกประการหนึ่งของโดเมนที่เชื่อมโยงกับ BADBAZAAR ได้แก่ '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**' และ '**voiceoftibet[.]net**' ก็คือ ทั้งหมดได้จดทะเบียนผ่าน eNom และถูก 'จอดพัก (Parked)' ไว้ที่หมายเลข IP '**255.255.255[.]254**'.

จากการตรวจสอบของ NCSC ก่อนหน้านี้ โดเมนอื่นที่มีลักษณะดังกล่าวเผยให้เห็นกิจกรรมที่เชื่อมโยงกับ **APT5** ในปี 2019 และ **APT14** ระหว่างปี 2009 ถึง 2011

โดเมนที่เชื่อมโยงกับ APT5 มีบันทึก WHOIS ในอดีตที่ระบุว่า '**taoyujun@gmail[.]com**' เป็นที่อยู่อีเมลของผู้จดทะเบียน

โดเมนที่เชื่อมโยงกับ APT14 มีซับโดเมนสามตัวอักษร
ซึ่งดูเหมือนว่าจะแสดงถึงเป้าหมายที่ตั้งใจไว้ของการปฏิบัติการที่เป็นอันตราย ของพวกเขา ตัวอย่างหนึ่งคือ '**bae.cisconline[.]net**' ซึ่งบ่งชี้ถึงการมุ่งเป้าไปที่ BAE Systems และถูกพบในตัวอย่าง '**Poison Ivy**'

ลักษณะที่คล้ายกันนี้พบได้ในโดเมน BADBAZAAR ที่ซับโดเมนมีความเกี่ยวข้องกับชื่อแอปที่ถูกฝังโทรจัน ได้แก่

ชื่อแอป	URL ของระบบ C2
Muslim Pro	**mpp**.pmstwocqn[.]com
Video Player for Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Radio Afghanistan	**afg**.collinformations[.]com
EN-UG Dictionary Free	**eud**.titeperformance[.]com
Disk Video Recovery	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

สิ่งสำคัญคือ ต้องทราบว่ากิจกรรมที่เกี่ยวข้องกับ APT5 และ APT14 เป็นเหตุการณ์ในอดีต และยังมีโดเมนอื่น ๆ ที่จดทะเบียนกับ eNom และชี้ไปยัง '**255.255.255.254**' ซึ่งไม่สามารถเชื่อมโยงกับกิจกรรมที่เป็นอันตรายได้ ดังนั้น จึงไม่แน่ชัดว่ากลุ่มผู้ไม่ประสงค์ดี ที่อยู่เบื้องหลังการโจมตีเหล่านี้จะเป็นกลุ่มเดียวกันหรือติดต่อเชื่อมโยงกันหรือไม่

ชื่อเครื่อง

การวิเคราะห์ระบบ C2 และตัวอย่างของ BADBAZAAR เผยให้เห็นชื่อโฮสต์ที่ใช้เป็นค่า 'ชื่อทั่วไป' ในใบรับรอง SSL การตรวจสอบของ NCSC เกี่ยวกับชื่อโฮสต์ที่พบในตัวอย่างและโครงสร้างพื้นฐานของ BADBAZAAR แสดงให้เห็นว่าชื่อโฮสต์เหล่านี้ถูกใช้ในที่อยู่ IP หลายแห่ง ซึ่งที่อยู่ IP เหล่านี้เป็นโฮสต์สำหรับโดเมนที่พบในตัวอย่างของ BADBAZAAR มีรายละเอียดเพิ่มเติมเกี่ยวกับชื่อโฮสต์และที่อยู่ IP ที่มีชื่อโฮสต์ ซึ่งโฮสต์โดเมนระบบ C2 ของ BADBAZAAR อยู่ในส่วนด้านล่างนี้

ในเกือบทุกกรณี การมีอยู่ของใบรับรองที่มีค่าชื่อโฮสต์จะทับซ้อนกับการแก้ไข IP สำหรับชื่อโดเมนที่เป็นอันตรายที่ระบุไว้ โดยมีเพียง ไม่กี่กรณีที่ไม่สอดคล้องกัน ซึ่งได้มีการชี้แจงไว้แล้ว

WIN-EU0VLBL7TUJ

มีการตรวจพบชื่อโฮสต์ '**WIN-EU0VLBL7TUJ**' บนที่อยู่ IP ที่อยู่ในความสนใจดังต่อไปนี้

- '**116.203.53[.]21**' เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ '**uyapkfinder[.]com**' และ '**thewestuniverse[.]com**'.
- '**95.216.169[.]27**' เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ '**adysfunction[.]com**' และซับโดเมน '**download.apkbazar[.]biz**' ซึ่งถูกพบว่าเป็นลิงก์ดาวน์โหลดตัวอย่างมัลแวร์ BADBAZAAR

(ดูภาคผนวก A รูปภาพที่ 6)

WIN-70E59JVOB9G

มีการตรวจพบชื่อโฮสต์ '**WIN-70E59JVOB9G**' ในที่อยู่ IP ที่อยู่ในความสนใจดังต่อไปนี้

- '**23.88.28[.]220**' เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ '**aua.rondwsign[.]com**', '**nal.tokenmajorp[.]com**', '**pep.rondwsign[.]com**' '**doa.rondwsign[.]com**' และ '**pls.rondwsign[.]com**' มีช่วงเวลาสองวันระหว่างวันที่ตรวจพบใบรับรองที่มีชื่อเครื่องครั้งล่าสุดกับวันที่พบโดเมนที่เป็นอันตรายว่าเริ่มชี้ไปยังที่อยู่ IP ดังกล่าวเป็นครั้งแรก
- '**23.88.28[.]221**' เป็นโฮสต์ BADBAZAAR ที่เชื่อมโยงกับซับโดเมน '**bt.bhvghg[.]com**'
- '**23.88.28[.]222**' เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ '**tubevideoplus[.]org**' และ '**cde.mpoxcases[.]com**'
- '**65.21.92[.]67**' เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ '**bat.androidupdated[.]net**' นอกจากนี้ ซับโดเมน '**apps.androidupdated[.]net**' ยังเป็นระบบ C2 ของมัลแวร์ DoubleAgent อีกด้วย

- ‘**65.21.92[.]77**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ และ ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**upd.whoscaller.net**’ และ ‘**ggl.whoscaller[.]net**’

- ‘**142.132.131[.]15**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**bvn.lookincategory[.]com**’ และ ‘**edr.lookincategory[.]com**’
  มีช่วงเวลาสิบเอ็ดวันระหว่างวันที่ตรวจพบใบรับรองที่มีชื่อเครื่องครั้งล่าสุดกับวันที่พบโดเมน ที่เป็นอันตรายว่าเริ่มชี้ไปยังที่อยู่ IP ดังกล่าวเป็นครั้งแรก

- ‘**142.132.131[.]20**’ เป็นโฮสต์ของซับโดเมน ‘**son.onlinegamersgroup[.]com**’ และ ‘**system.onlinegamersgroup[.]com**’ เชื่อว่าเป็นระบบ C2 ของ BADBAZAAR เนื่องจากมีการโฮสต์อยู่ในช่วงเวลาที่ตรวจพบใบรับรอง SSL ที่เชื่อมโยงกับ BADBAZAAR บน IP ดังกล่าว

- ‘**142.132.131[.]28**’ เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**goldplusapp[.]net**’ และซับโดเมนของ ‘**who.goldplusapp[.]net**’ และ ‘**cgf.goldplusapp[.]net**’

- ‘**162.55.103[.]211**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net**’, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’ และ‘**aar.alpinemap[.]net**’

- ‘**162.55.103[.]212**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**pep.rondwsign[.]com**’, ‘**ckp.jkiohreh[.]com**’, ‘**aar.tokenmajorp[.]com**’, ‘**nal.tokenmajorp[.]com**’, ‘**pls.rondwsign[.]com**’ และ ‘**aua.rondwsign[.]com**’

- ‘**195.154.47[.]99**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**ggl.whoscaller[.]net**’ และ ‘**upd.whoscaller.net**’ มีช่วงเวลาสามวันระหว่างวันที่ตรวจพบใบรับรองที่มีชื่อเครื่องครั้งแรกกับวันที่พบโดเมน ที่เป็นอันตรายว่าเริ่มชี้ไปยังที่อยู่ IP ดังกล่าวเป็นครั้งล่าสุด

- ‘**195.154.60[.]3**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**upd.whoscaller[.]net**’ **‘ggl.whoscaller\[.]net’.**

- ‘**212.83.189[.]89**’ เป็นโฮสต์ของซับโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ และ ‘**afg.collinformations[.]com**’

- ‘**212.129.21[.]168**’ เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ และ ‘**bvn.lookincategory[.]com**’

(ดูภาคผนวก A รูปภาพที่ 7)

WIN-50QO3EIRQVP

มีการตรวจพบชื่อโฮสต์ ‘**WIN-50QO3EIRQVP**’ ในที่อยู่ IP ที่อยู่ในความสนใจดังต่อไปนี้

- ’**45.76.132[.]91**’ เป็นโฮสต์ของโดเมน ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’ โดเมนทั้งสองเชื่อมโยงกับ BADBAZAAR เนื่องจากซับโดเมน ‘**fow.yumoftion[.]com**’ และ ‘**bat.androidupdated[.]net**’ เป็นโดเมนระบบ C2 ของ BADBAZAAR นอกจากนี้ ซับโดเมน ‘**apps.androidupdated[.]net**’ ยังเป็นโดเมนระบบ C2 ของ DoubleAgent อีกด้วย มันยังโฮสต์โดเมน ‘**pmstwocqn[.]com**’ ซึ่งเชื่อมโยงกับ BADBAZAAR ผ่านบันทึก WHOIS อีกด้วย

- ‘**95.179.210[.]85**’ เคยเป็นที่ตั้งของโฮสต์ ‘**clublogs[.]com**’ ซึ่งมี ‘**xle.clublogs[.]com**’ เป็นโดเมนระบบ C2 ของ BADBAZAAR และยังเป็นที่ตั้งของโดเมนที่เชื่อมโยงกับ BADBAZAAR อื่น ๆ เช่น ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, '**www.voiceoftibet[.]net**' และ ‘**actuallys[.]com**’

- ‘**199.247.21[.]34**’ เป็นโฮสต์ของ ‘**titeperformance[.]com**’ และ ‘**collinformations[.]com**’ ซึ่งซับโดเมนของทั้งสองเป็นโดเมนระบบ C2 ของ BADBAZAAR

- ‘**217.69.10[.]128**’ เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**uyghurdict[.]com**’

(ดูภาคผนวก A รูปภาพที่ 8)

WMSvc-WIN-50QO3EIRQVP

มีการตรวจพบชื่อโฮสต์ ‘**WMSvc-WIN-50QO3EIRQVP**’ บนที่อยู่ IP ที่อยู่ในความสนใจต่อไปนี้

- ’**78.46.185[.]251**’ เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ ‘**groupgram[.]org**’ ซึ่ง Volexity รายงานว่า มีการใช้พอร์ต 4432 สำหรับการเชื่อมต่อที่เป็นอันตราย

- ‘**65.21.92[.]69**’ และ ‘**163.172.205[.]207**’ เป็นโฮสต์ของโดเมน ‘**widelygram[.]org**’ ซึ่งเชื่อว่าเป็นโดเมนระบบ C2 ของ BADBAZAAR เนื่องจากในขณะที่โฮสต์อยู่บน IP ทั้งสอง พอร์ต 4432 ยังเปิดใช้งานอยู่

- ‘**163.172.198[.]206**’ เป็นโฮสต์ของโดเมน ‘**maxgram[.]org**’ ซึ่งเชื่อว่าเป็นโดเมนระบบ C2 ของ BADBAZAAR เนื่องจากในขณะที่โดเมนนี้โฮสต์อยู่นั้น พอร์ต 4432 ยังคงเปิดอยู่

(ดูภาคผนวก A รูปภาพที่ 9)

WMSvc-WIN-50QO3EIRQVP และ WIN-7LSBB9R0F1L

มีการตรวจพบชื่อโฮสต์ '**WMSvc-WIN-50QO3EIRQVP**' และ '**WIN-7LSBB9R0F1L**' บนที่อยู่ IP ที่อยู่ในความสนใจต่อไปนี้

- '**148.251.87[.]245**' เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ '**flygram[.]org**' และ '**groupgram[.]org**'.

(ดูภาคผนวก A รูปภาพที่ 10)

WIN-N8H8S9BG2P0

มีการตรวจพบชื่อโฮสต์ '**WIN-N8H8S9BG2P0**' บนที่อยู่ IP ที่อยู่ในความสนใจต่อไปนี้

- '**148.251.87[.]247**' เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ '**omarwhatsapp[.]org**' และ '**flygram[.]org**'

(ดูภาคผนวก A รูปภาพที่ 11)

WIN-I6VBN8MR92A

มีการตรวจพบชื่อโฮสต์ '**WIN-I6VBN8MR92A**' บนที่อยู่ IP ที่อยู่ในความสนใจต่อไปนี้

- '**148.251.87[.]197**' เป็นโฮสต์ของโดเมนระบบ C2 ของ BADBAZAAR คือ '**tryhrwserf[.]com**'

(ดูภาคผนวก A รูปภาพที่ 12)

จากข้อมูลเชิงพาณิชย์ที่มีอยู่ในปัจจุบัน พบว่าชื่อเครื่องเหล่านี้มีการใช้งานแพร่หลายบนอินเทอร์เน็ตในหลากหลายชื่อ
โดยมีบางชื่อ ปรากฏบนที่อยู่ IP หลายรายการในเวลากัน ซึ่งบ่งชี้ว่าการสร้างเครื่องแบบเสมือนจริง (Virtual Machine - VM)
ถูกสร้างมาจากแม่แบบ เทมเพลตเดียวกัน สิ่งสำคัญคือต้องทราบว่าสำหรับชื่อโฮสต์บางชื่อ ไม่ใช่ทุกที่อยู่ IP
ที่ตรวจพบนั้นจะเชื่อมโยงกับกิจกรรมที่เป็นอันตราย เสมอไป
ซึ่งอาจหมายความว่าการใช้ชื่อโฮสต์เหล่านี้ไม่ได้จำกัดอยู่แค่กลุ่มผู้ก่อภัยคุกคามเหล่านี้เท่านั้น

อย่างไรก็ตาม การแพร่หลายของชื่อเครื่องเหล่านี้บนที่อยู่ IP บางแห่งที่เคยโฮสต์โดเมนระบบ C2 ของ BADBAZAAR
อาจบ่งชี้ได้ว่า
มีหน่วยงานหนึ่งที่จัดหาโครงสร้างพื้นฐานเพื่อใช้กำหนดค่าระบบของเครื่องในการสนับสนุนการปฏิบัติการของผู้ไม่ประสงค์ดีทางไซเบอร์

สถานะบนโซเชียลมีเดีย

การรายงานก่อนหน้านี้โดย Volexity แสดงให้เห็นว่าวิดีโอบน YouTube (ที่ส่งเสริมให้ใช้งานแอปพลิเคชันที่เป็นอันตราย) ถูกสร้างขึ้นโดย กลุ่มผู้ไม่ประสงค์ดีทางไซเบอร์ วิดีโอเหล่านี้มีบทแนะนำวิธีการใช้งานแอปพลิเคชันที่พัฒนาขึ้น

NCSC ค้นพบช่อง YouTube เพิ่มเติมอีกสองช่องที่เกี่ยวกับการปฏิบัติการของผู้ก่อภัยคุกคาม YouTube ช่องที่ใช้ URL handle ว่า '**@josephjoey3499**' ดูเหมือนจะส่งเสริมการใช้งาน '**Maxgram**' และอีกช่องหนึ่งที่จดทะเบียนด้วยชื่อ '**@uyghurapks3096**' ส่งเสริมการใช้งาน '**Uyghur APK Finder**'

นอกจากนี้ วิดีโอ YouTube ที่ส่งเสริมการใช้งาน '**Flygram**' และ '**Signal Plus**' ยังแสดงให้เห็นว่าผู้ก่อภัยคุกคามใช้หมายเลขโทรศัพท์ที่สามารถมองเห็นได้อย่างชัดเจน ในวิดีโอ '**Flygram**' ที่นาที 0:36 หมายเลขโทรศัพท์ **'+1 (570) 378-7250**' ปรากฏให้เห็น อย่างชัดเจนและระหว่างวีดิโอ '**Signal Plus**' มีการเปิดเผยหมายเลขโทรศัพท์ '**+1 (267) 298 4259**' เช่นกัน

Volexity รายงานว่าพบเว็บไซต์ข่าวปลอมเกี่ยวกับธิเบตชื่อ '**ignitetibet[.]net**' ซึ่งพวกเขาพบในช่อง Telegram ที่เชื่อว่าอยู่ภายใต้ การควบคุมของผู้ก่อภัยคุกคามเหล่านี้ มีการพบที่อยู่อีเมล **'choekyi.wangmo@ignitetibet[.]net'** แสดงความคิดเห็นในโพสต์ บนเพจ **'tibetone.org'** ซึ่ง Lookout เคยรายงานต่อสาธารณะว่าเป็นเพจระบบ C2 ที่ใช้สำหรับมัลแวร์ BADBAZAAR เวอร์ชั่น iOS

เชื่อว่าที่อยู่อีเมลนี้ถูกควบคุมโดยกลุ่มผู้ไม่ประสงค์ดี โดยใช้ตัวตนปลอมในชื่อ '**Choekyi Wangmo**'.

การประเมินผล

BADBAZAAR และ MOONSHINE
ใช้วิธีการทางวิศวกรรมสังคมหลากหลายรูปแบบในการมุ่งเป้าเฉพาะไปที่ชุมชนชาวอุยกูร์
ชาวทิเบต และชาวไต้หวัน อันได้แก่

- การฝังโทรจันลงในแอปที่ชุมชนเหล่านี้สนใจ เช่น แอปคัมภีร์กุรอานภาษาอุยกูร์
  ซึ่งเกือบจะแน่นอนว่าถูกปรับแต่ง
  ให้เหมาะกับฐานกลุ่มเหยื่อเป้าหมาย
- การเพิ่มแอปที่ฝังโทรจันเหล่านี้เข้าสู่แอปสโตร์ทางการ ซึ่งมีแนวโน้มสูงว่าจะช่วยเพิ่มความน่าเชื่อถือ
  และการแชร์
  ในกลุ่มแชตต่าง ๆ
  ก็มีความเป็นไปได้สูงที่มีจุดประสงค์เพื่อแสวงหาผลประโยชน์จากความสัมพันธ์ที่ไว้วางใจกัน
  ภายในชุมชนเหล่านี้

BADBAZAAR และ MOONSHINE รวบรวมข้อมูล ซึ่งเกือบจะแน่นอนว่ามีค่าต่อรัฐบาลจีน แม้ BADBAZAAR และ MOONSHINE
จะถูกพบว่ามุ่งเป้าไปที่บุคคลชาวอุยกูร์ ชาวทิเบต และชาวไต้หวัน ยังมีมัลแวร์อื่น ๆ ที่มุ่งเป้าไปที่กลุ่มชนกลุ่มน้อยอื่น ๆ ในจีนอีก
พลเมืองจากประเทศที่ร่วมลงนามผนึกกัน (Co-sealing nations) ทั้งภายในจีนและต่างประเทศ
ซึ่งถูกมองว่าสนับสนุนกิจกรรม
ที่เป็นภัยคุกคามต่อเสถียรภาพของระบอบการปกครอง
ก็แทบจะแน่นอนว่าตกอยู่ภายใต้การคุกคามจากมัลแวร์ในอุปกรณ์เคลื่อนที่
อย่างเช่น BADBAZAAR และ MOONSHINE ความสามารถของมัลแวร์ในการบันทึกข้อมูลตำแหน่งที่ตั้ง เสียง และภาพถ่าย
เกือบจะแน่นอนว่าเปิดโอกาสให้ผู้อยู่เบื้องหลังสามารถสอดแนมและคุกคามในอนาคตได้
โดยให้ข้อมูลแบบตามเวลาจริงเกี่ยวกับ
กิจกรรมของเป้าหมาย

MITRE ATT&CK®

รายงานฉบับนี้จัดทำขึ้นโดยคำนึงถึงกรอบการทำงานของ MITRE ATT&CK®
ซึ่งเป็นคลังความรู้ที่เข้าถึงได้ทั่วโลกเกี่ยวกับ
กลยุทธ์และเทคนิคของผู้ไม่ประสงค์ดี โดยอ้างอิงจากการสังเกตการณ์ในโลกแห่งความเป็นจริง

กลยุทธ์	รหัส (ID)	เทคนิค	ขั้นตอนปฏิบัติ
การสำรวจ	T1593.001	ค้นหาเว็บไซต์/โดเมนสาธารณะ: โซเชียลมีเดีย	ผู้ไม่ประสงค์ดีค้นหากลุ่มและฟอรัมออนไลน์ ที่ตรงกับกลุ่มเป้าหมายที่ต้องการ เพื่อใช้ในการเผยแพร่มัลแวร์
การพัฒนาทรัพยากร	T1583.001	จัดหาโครงสร้างพื้นฐาน: โดเมนต่าง ๆ	ผู้ไม่ประสงค์ดีลงทะเบียนโดเมนสำหรับเซิร์ฟเวอร์ ระบบสั่งการและควบคุมของตน
การพัฒนาทรัพยากร	T1587.001	พัฒนาความสามารถ: มัลแวร์	มีการเขียนโค้ดที่เป็นอันตรายสำหรับฝังลงในแอป ที่ถูกดัดแปลงให้เป็นโทรจัน
การพัฒนาทรัพยากร	T1608.001	ความสามารถในการเตรียมการ: อัปโหลดมัลแวร์	แอปที่ถูกฝังโทรจันถูกอัปโหลดไปยังแพลตฟอร์ม ออนไลน์ รวมถึงแอปสโตร์ต่าง ๆ
การพัฒนาทรัพยากร	T1585.001	สร้างบัญชี: บัญชีโซเชียลมีเดีย	ผู้ไม่ประสงค์ดีสร้างบัญชีบนเว็บไซต์และโซเชียล มีเดียเพื่อเผยแพร่และโฆษณามัลแวร์
การพัฒนาทรัพยากร	T1585.002	สร้างบัญชี: บัญชีอีเมล	ผู้ไม่ประสงค์ดีใช้บัญชีอีเมลที่โฮสต์แบบส่วนตัว และแบบเชิงพาณิชย์สำหรับการโฮสต์และเผยแพร่ มัลแวร์
การเข้าถึงในขั้นต้น	T1189	การบุกรุกแบบ Drive-by	สคริปต์ที่เป็นอันตรายถูกซ่อนไว้ในแอปที่ดูเหมือน ถูกต้องตามกฎหมายและถูกอัปโหลดขึ้นสู่แอปสโตร์
การเข้าถึงในขั้นต้น	T1566.003	ฟิชชิ่ง: การโจมตีแบบสเปียร์ฟิชชิ่ง (Spearphishing) ผ่านบริการ	ผู้ไม่ประสงค์ดีส่งแอปที่ถูกฝังโทรจันไปยังกลุ่มเป้าหมายผ่านโซเชียลมีเดียรวมถึง Telegram
การดำเนินการ	T1204.002	การดำเนินการโดยผู้ใช้: ไฟล์ที่เป็นอันตราย	เหยื่อต้องติดตั้งแอปที่ถูกฝังโทรจันเพื่อให้โค้ดอันตรายทำงาน
การหลบเลี่ยงการป้องกัน	T1027.009	ไฟล์หรือข้อมูลที่ซ่อนเร้น: เพย์โหลดที่ฝังตัว	เพย์โหลดอันตรายถูกซ่อนอยู่ภายในแอปพลิเคชัน ที่ดูเหมือนถูกต้องตามกฎหมาย
การหลบเลี่ยงการป้องกัน	T1036.005	การแอบอ้าง: ใช้ชื่อหรือที่อยู่ที่ดูเหมือน ถูกต้องต้องกฎหมาย	ไฟล์ที่ถูกฝังโทรจันมีชื่อ รูปลักษณ์ และการทำงาน ที่เหมือนกับแอปที่ถูกต้องตามกฎหมาย

การหลบเลี่ยงการป้องกัน	T1656	การปลอมตัว	ผู้ไม่ประสงค์ดีปลอมตัวเป็นบุคคลที่น่าเชื่อถือโดยสร้างเว็บไซต์ปลอมและใช้ชื่อผู้ใช้ที่เกี่ยวข้อง กับกลุ่มเป้าหมาย
การรวบรวมข้อมูล	T1123	การบันทึกเสียง	แอปที่ถูกฝังโทรจันอาจร้องขอสิทธิ์ที่ไม่จำเป็น รวมถึงการเข้าถึงไมโครโฟน
การรวบรวมข้อมูล	T1125	การบันทึกวิดีโอ	แอปที่ถูกฝังโทรจันอาจร้องขอสิทธิ์ที่ไม่จำเป็น รวมถึงการเข้าถึงกล้อง
การรวบรวมข้อมูล	T1005	ข้อมูลจากระบบภายในเครื่อง	แอปที่ถูกฝังโทรจันอาจร้องขอสิทธิ์ที่ไม่จำเป็น รวมถึงการเข้าถึงไฟล์ภายในเครื่อง
ระบบสั่งการและควบคุม	T1071.001	โปรโตคอลชั้นแอปพลิเคชัน: โปรโตคอลเว็บ	มัลแวร์เชื่อมต่อกับระบบ C2 โดยใช้ HTTPS และ WebSocket
ระบบสั่งการและควบคุม	T1509	พอร์ตที่ไม่ได้มาตรฐาน	ใช้พอร์ตที่ไม่ได้มาตรฐาน เช่น พอร์ต 4432 และ 2333
การขโมยข้อมูล	T1041	การขโมยข้อมูลออกผ่านช่องทางระบบ C2	มัลแวร์ขโมยข้อมูลออกโดยใช้การเชื่อมต่อ ผ่าน HTTPS และ WebSocket
ผลกระทบ	T1565.002	การจัดการข้อมูล: การดัดแปลงข้อมูล ที่ส่งผ่าน	ผู้ไม่ประสงค์ดีดึงข้อมูลจากเหยื่อโดยเปิดใช้งาน การรับส่งข้อมูลเว็บของแอปที่ไม่จำเป็นต่อ การทำงานของแอป

ตัวบ่งชี้

MOONSHINE:

- เมื่อวันที่ 1 เมษายน 2025 การค้นหาแผงควบคุม VLiteUI พบผลลัพธ์ดังต่อไปนี้

ที่อยู่ IP	พอร์ต	พบครั้งแรก	พบครั้งล่าสุด
103.254.108[.]87	888	17 ตุลาคม 2024	14 กุมภาพันธ์ 2025
43.159.192[.]7	444	21 พฤศจิกายน 2024	13 กุมภาพันธ์ 2025
103.27.109[.]109	444	11 กรกฎาคม 2024	7 กุมภาพันธ์ 2025
45.119.99[.]83	444	26 ธันวาคม 2024	24 มกราคม 2025
103.254.108[.]76	444	12 กันยายน 2024	5 ธันวาคม 2024
194.71.107[.]160	444	10 ธันวาคม 2023	1 พฤศจิกายน 2024
103.254.108[.]108	444	12 พฤศจิกายน 2023	25 กันยายน 2024
103.56.17[.]194	444	3 เมษายน 2024	23 สิงหาคม 2024
103.254.108[.]87	444	14 พฤศจิกายน 2023	15 สิงหาคม 2024
62.72.58[.]168	444	29 มกราคม 2024	7 สิงหาคม 2024
103.43.18[.]43	444	12 กุมภาพันธ์ 2024	19 กรกฎาคม 2024
77.91.123[.]208	444	4 กุมภาพันธ์ 2024	9 เมษายน 2024
46.246.98[.]229	444	7 มีนาคม 2024	26 มีนาคม 2024
2.58.15[.]101	444	23 กุมภาพันธ์ 2024	27 กุมภาพันธ์ 2024
46.246.98[.]209	444	8 มกราคม 2024	14 กุมภาพันธ์ 2024
103.254.108[.]87	8000	17 ตุลาคม 2023	17 ตุลาคม 2023
103.254.108[.]87	8080	15 เมษายน 2023	16 ตุลาคม 2023
103.254.108[.]108	9090	13 เมษายน 2023	16 ตุลาคม 2023
103.45.66[.]123	9090	2 มีนาคม 2023	8 เมษายน 2023
103.45.66[.]32	8080	29 กรกฎาคม 2022	6 เมษายน 2023
27.124.20[.]23	9090	28 พฤษภาคม 2022	24 มีนาคม 2023
27.124.20[.]22	9090	28 พฤษภาคม 2022	23 มีนาคม 2023
27.124.20[.]24	9090	27 พฤษภาคม 2022	17 มีนาคม 2023
69.176.94[.]148	9090	4 มีนาคม 2023	10 มีนาคม 2023
69.176.94[.]228	9090	24 ธันวาคม 2022	25 กุมภาพันธ์ 2023
103.253.40[.]137	8000	24 มิถุนายน 2022	2 กันยายน 2022
27.124.4[.]80	8080	25 กุมภาพันธ์ 2022	23 มิถุนายน 2022
27.124.4[.]81	8080	25 กุมภาพันธ์ 2022	23 มิถุนายน 2022
47.242.46[.]79	8080	3 พฤษภาคม 2021	17 มิถุนายน 2022
27.124.4[.]82	8080	24 กุมภาพันธ์ 2022	15 มิถุนายน 2022
27.124.4[.]165	9090	14 พฤษภาคม 2022	28 พฤษภาคม 2022
27.124.4[.]184	9090	14 พฤษภาคม 2022	27 พฤษภาคม 2022
27.124.4[.]178	9090	13 พฤษภาคม 2022	26 พฤษภาคม 2022
103.15.28[.]165	8080	5 มีนาคม 2022	25 พฤษภาคม 2022
69.176.94[.]226	8080	5 มีนาคม 2022	22 เมษายน 2022

27.124.4[.]3	8080	11 มีนาคม 2022	2 เมษายน 2022
103.140.238[.]235	8080	4 มีนาคม 2022	1 เมษายน 2022
27.124.4[.]2	8080	12 มีนาคม 2022	1 เมษายน 2022
165.84.180[.]107	8000	25 กุมภาพันธ์ 2022	19 มีนาคม 2022
69.176.94[.]156	8000	25 กุมภาพันธ์ 2022	5 มีนาคม 2022
141.98.212[.]70	9090	5 ตุลาคม 2021	4 มีนาคม 2022
5.188.33[.]50	8000	15 กุมภาพันธ์ 2022	4 มีนาคม 2022
5.188.70[.]193	8000	15 กุมภาพันธ์ 2022	4 มีนาคม 2022
69.176.94[.]140	8080	24 กุมภาพันธ์ 2022	24 กุมภาพันธ์ 2022
27.124.20[.]83	8000	14 กุมภาพันธ์ 2022	18 กุมภาพันธ์ 2022
208.87.200[.]106	8000	2 มกราคม 2022	2 มกราคม 2022
121.127.241[.]37	8000	8 ธันวาคม 2021	8 ธันวาคม 2021
156.255.2[.]211	443	5 ตุลาคม 2021	5 ตุลาคม 2021
156.255.2[.]211	8000	4 ตุลาคม 2021	4 ตุลาคม 2021
156.255.2[.]203	8000	3 ตุลาคม 2021	3 ตุลาคม 2021
47.243.43[.]248	8000	5 กรกฎาคม 2021	5 กรกฎาคม 2021
45.115.236[.]6	8080	3 พฤษภาคม 2021	1 มิถุนายน 2021
43.251.118[.]97	8000	3 มกราคม 2021	1 มีนาคม 2021
185.243.43[.]138	8000	4 มกราคม 2021	2 กุมภาพันธ์ 2021
47.245.59[.]33	8000	5 พฤษภาคม 2021	5 พฤษภาคม 2021

- เมื่อวันที่ 1 เมษายน 2025 การค้นหาแผงควบคุม SCOTCH ADMIN พบผลลัพธ์ดังต่อไปนี้

ที่อยู่ IP	พอร์ต	พบครั้งแรก	พบครั้งล่าสุด
104.194.152[.]24	2333	6 กุมภาพันธ์ 2025	27 กุมภาพันธ์ 2025
172.86.80[.]126	2333	7 กุมภาพันธ์ 2025	27 กุมภาพันธ์ 2025
154.90.59[.]62	2333	20 มิถุนายน 2024	20 กันยายน 2024
154.90.59[.]88	2333	21 มิถุนายน 2024	20 กันยายน 2024
154.90.58[.]210	2333	16 พฤษภาคม 2024	14 มิถุนายน 2024
154.90.59[.]225	2333	17 พฤษภาคม 2024	13 มิถุนายน 2024
38.60.199[.]208	2333	26 พฤศจิกายน 2023	9 มกราคม 2024
38.60.199[.]254	2333	28 พฤศจิกายน 2023	9 มกราคม 2024
38.60.199[.]99	2333	26 สิงหาคม 2023	21 พฤศจิกายน 2023
38.60.199[.]44	2333	20 กรกฎาคม 2023	11 กันยายน 2023
194.163.34[.]23	443	30 กันยายน 2022	14 เมษายน 2023
45.32.125[.]112	10443	1 ตุลาคม 2022	17 มีนาคม 2023

- เมื่อวันที่ 14 มีนาคม 2024 การค้นหาแผงควบคุม SCOTCH ADMIN เสมือน พบผลลัพธ์ดังต่อไปนี้

โดเมน	ที่อยู่ IP
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

BADBAZAAR

คำอธิบาย	ตรวจพบใบรับรอง SSL บนระบบ C2 ของ BADBAZAAR
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- เมื่อวันที่ 1 เมษายน 2025 การค้นหาใบรับรอง BADBAZAAR ที่อยู่ด้านบนพบผลลัพธ์ดังนี้

ที่อยู่ IP	พอร์ต	พบครั้งแรก	พบครั้งล่าสุด
65.108.192[.]173	31237	14 มีนาคม 2025	28 มีนาคม 2025
65.108.192[.]173	31236	14 มีนาคม 2025	28 มีนาคม 2025
65.108.192[.]173	31235	14 มีนาคม 2025	28 มีนาคม 2025
157.90.129[.]73	31236	27 มีนาคม 2025	27 มีนาคม 2025
142.132.131[.]15	31236	24 กรกฎาคม 2024	27 มีนาคม 2025
142.132.131[.]15	31235	26 กรกฎาคม 2024	27 มีนาคม 2025
142.132.131[.]20	31237	11 สิงหาคม 2023	27 มีนาคม 2025
142.132.131[.]15	31237	24 กรกฎาคม 2024	27 มีนาคม 2025
142.132.131[.]20	31236	27 กันยายน 2023	26 มีนาคม 2025
142.132.131[.]20	31235	18 ตุลาคม 2023	26 มีนาคม 2025
65.108.192[.]155	31236	5 ธันวาคม 2023	20 กุมภาพันธ์ 2025
65.108.192[.]155	31237	5 ธันวาคม 2024	20 กุมภาพันธ์ 2025
65.108.192[.]155	31235	5 ธันวาคม 2024	19 กุมภาพันธ์ 2025
23.88.28[.]222	31237	25 เมษายน 2024	29 พฤศจิกายน 2024
23.88.28[.]222	31235	2 พฤษภาคม 2024	28 พฤศจิกายน 2024
23.88.28[.]222	31236	1 พฤษภาคม 2024	28 พฤศจิกายน 2024
212.129.21[.]168	31235	16 ตุลาคม 2023	17 มีนาคม 2024
212.129.21[.]168	31237	24 สิงหาคม 2023	17 มีนาคม 2024

212.129.21[.]168	31236	26 กันยายน 2023	14 มีนาคม 2024

คำอธิบาย	ตรวจพบใบรับรอง SSL บนระบบ C2 ของ BADBAZAAR
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- เมื่อวันที่ 1 เมษายน 2025 การค้นหาใบรับรอง BADBAZAAR ที่อยู่ด้านบนพบผลลัพธ์ดังนี้

ที่อยู่ IP	พอร์ต	พบครั้งแรก	พบครั้งล่าสุด
162.55.103[.]211	20122	12 มกราคม 2023	28 มีนาคม 2025
162.55.103[.]212	20121	30 มิถุนายน 2022	28 มีนาคม 2025
162.55.103[.]212	20122	14 กรกฎาคม 2023	28 มีนาคม 2025
162.55.103[.]211	20121	3 มิถุนายน 2022	28 มีนาคม 2025
162.55.103[.]211	20123	22 กรกฎาคม 2023	27 มีนาคม 2025
162.55.103[.]212	20123	22 กรกฎาคม 2023	27 มีนาคม 2025
212.83.162[.]152	9090	13 ตุลาคม 2022	27 มีนาคม 2025
23.88.28[.]221	20422	28 กรกฎาคม 2023	30 กันยายน 2023
23.88.28[.]221	20421	18 พฤษภาคม 2023	28 กันยายน 2023
23.88.28[.]221	20423	28 กรกฎาคม 2023	28 กันยายน 2023
162.55.103[.]210	20121	30 กันยายน 2022	23 กุมภาพันธ์ 2023
65.21.92[.]67	20121	2 พฤศจิกายน 2021	13 ตุลาคม 2022
65.21.92[.]67	20122	10 สิงหาคม 2022	13 ตุลาคม 2022
23.88.28[.]220	20121	8 ธันวาคม 2021	13 พฤษภาคม 2022
94.130.92[.]230	20121	4 มกราคม 2021	5 ตุลาคม 2021
88.99.150[.]246	20121	6 เมษายน 2021	8 กันยายน 2021
45.76.132[.]91	20121	2 กุมภาพันธ์ 2021	1 มีนาคม 2021

โดเมน WHOIS

ด้านล่างนี้คือรายการโดเมนที่ปัจจุบันหรือในอดีตมีบันทึก WHOIS ซึ่งมีค่าตรงกับที่พบในโดเมนระบบ C2 ของ BADBAZAAR

ค่า WHOIS	โดเมนต่าง ๆ
ภูมิภาค ที่จดทะเบียน: UJYJYUJ **ประเทศผู้จดทะเบียน: โบลิเวีย** **ผู้รับจดทะเบียน: eNom**	• ntc-mobile[.]com • microtik[.]net • ntc-ftth[.]net • axisupdating[.]com • axisupdate[.]com • telegramrouter[.]org • telegramtor[.]com • fufijxgkg[.]com

	• jindjjdtc[.]com • tubevideoplus[.]org • thetubeplus[.]com • tbgram[.]org • signalplus[.]org • pmumail[.]com
ภูมิภาค ที่จดทะเบียน: **REWR** ประเทศผู้จดทะเบียน: **CF** ผู้รับจดทะเบียน: **eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
ภูมิภาค ที่จดทะเบียน: **FSDF** ประเทศผู้จดทะเบียน: **AL** ผู้รับจดทะเบียน: **eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

ที่อยู่อีเมลต่าง ๆ
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

ช่องต่าง ๆ บน YouTube
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

ลิงก์ต่อไปนี้เป็นตัวบ่งชี้ภัยคุกคาม (IoCs) อื่น ๆ ที่เชื่อมโยงกับ BADBAZAAR และ MOONSHINE NCSC ไม่สามารถยืนยันความถูกต้อง
ของข้อมูลทั้งหมดในลิงก์เหล่านี้ได้ และขอแนะนำให้ผู้อ่านตรวจสอบความถูกต้องและความเกี่ยวข้องด้วยตนเอง

- ESET
- Trend Micro
- Lookout
- Lookout
- Volexity
- Citizen Lab

การบรรเทาปัญหา

NCSC สนับสนุนให้มีการนำข้อเสนอแนะด้านล่างนี้ไปปรับใช้เพื่อป้องกันภัยคุกคามตามที่อธิบายไว้ในกรณีศึกษา

- **ผู้ประกอบการแอปสโตร์ รวมถึงแอปสโตร์ของบุคคลที่สาม และนักพัฒนาแอป ควรตรวจสอบให้แน่ใจว่าแอป บนแพลตฟอร์มของตนมีความปลอดภัย และเป็นไปตามหลักจรรยาบรรณปฏิบัติ (Code of Practice) ของหน่วยงาน ภาครัฐ** โปรดดูคำแนะนำที่ https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version

- **การสนับสนุนในหลายภาษา**
  นักพัฒนาแอปควรลงทุนแปลแอปยอดนิยมให้เป็นภาษาท้องถิ่นที่เหมาะสำหรับผู้ใช้ที่พูดภาษาชนกลุ่มน้อยในกลุ่มเป้าหมาย ซึ่งรวมถึงภาษาอุยกูร์ ภาษาทิเบต ภาษาฮกเกี้ยนแบบไต้หวัน และภาษากวางตุ้ง ดูคำแนะนำของ Apple สำหรับการแปลแอปให้รองรับภาษาท้องถิ่นได้ที่ https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. ดูคำแนะนำของ Google สำหรับการแปลแอปให้รองรับภาษาท้องถิ่นได้ที่ https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **การรักษาความปลอดภัยแพลตฟอร์มโซเชียลมีเดียของคุณ**
  บริษัทโซเชียลมีเดียสามารถทำให้เป็นเรื่องที่ยากขึ้นได้สำหรับผู้ไม่ประสงค์ดีทางไซเบอร์ที่จะสร้างบัญชีปลอม และแชร์ไฟล์หรือลิงก์ที่เป็นอันตรายบนแพลตฟอร์มของตนในชุมชนออนไลน์ที่ถูกต้องตามกฎหมาย หากเป็นไปได้ บริษัทต่าง ๆ ควรแบ่งปันตัวบ่งชี้ภัยอันตรายกับอุตสาหกรรมในวงกว้าง เพื่อเพิ่มความเข้าใจร่วมกันเกี่ยวกับภัยคุกคามและเพื่อช่วยในการหามาตรการป้องกัน

- **แผนการแก้ไขปัญหาสำหรับลูกค้า** องค์กรต่าง ๆ ควรมีขั้นตอนปฏิบัติในการแจ้งเตือนลูกค้าที่ได้ติดตั้งแอปที่เป็นอันตราย ผ่านการใช้บริการของตน การแจ้งเตือนเหล่านี้ควรเป็นที่ดึงดูดความสนใจและให้ข้อมูลที่เป็นประโยชน์ ในกรณีที่เหมาะสม องค์กรควรให้คำแนะนำเกี่ยวกับวิธีการลบซอฟต์แวร์

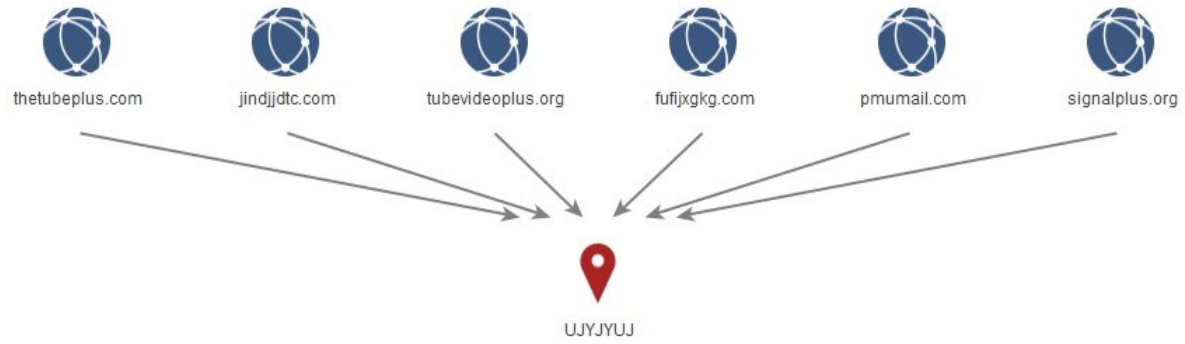
และสนับสนุนให้เหยื่อผู้เสียหายรายงานต่อเจ้าหน้าที่ผู้มีอำนาจของตน
เช่น NCSC ในสหราชอาณาจักร
ดูข้อมูลเพิ่มเติมเรื่องจรรยาบรรณปฏิบัติของแอปสโตร์ได้ที่
https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **กลุ่มการทำงานเพื่อความร่วมมือ** บริษัทโซเชียลมีเดียต่าง ๆ สามารถจัดตั้งกลุ่มการทำงานขึ้น
  โดยให้ทีมงานรักษาความ
  ปลอดภัยของแต่ละฝ่ายสามารถแชร์ตัวบ่งชี้ภัยอันตราย TTP และการสังเกตการณ์ต่าง ๆ ได้
  ซึ่งจะทำให้เป็นเรื่องยากขึ้น
  สำหรับที่ผู้ไม่ประสงค์ดีในการใช้แพลตฟอร์มของตนในการสนับสนุนการโจมตีที่เป็นอันตราย

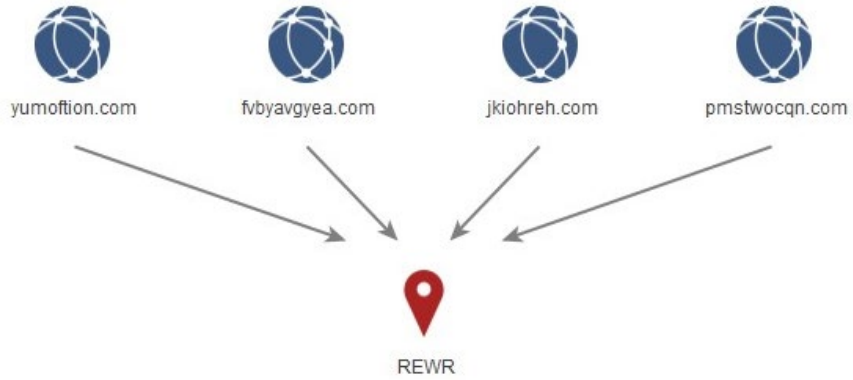
- **การตรวจจับแอปที่ถูกดัดแปลง** หากเป็นไปได้
  นักพัฒนาแอปควรเพิ่มฟังก์ชันการทำงานที่แจ้งให้ผู้ใช้ทราบหากผู้ใช้ดาวน์โหลดแอปเวอร์ชัน 'ที่ไม่เป็นทางการ'
  เพื่อช่วยป้องกันการใช้แอปปลอมที่เป็นอันตราย

ภาคผนวก A: กราฟการจัดกลุ่มคลัสเตอร์ WHOIS ของ BADBAZAAR/ ข้อมูลโบรกเกอร์โดเมน

รูปภาพที่ 1 - ‘UKYJYUJ’

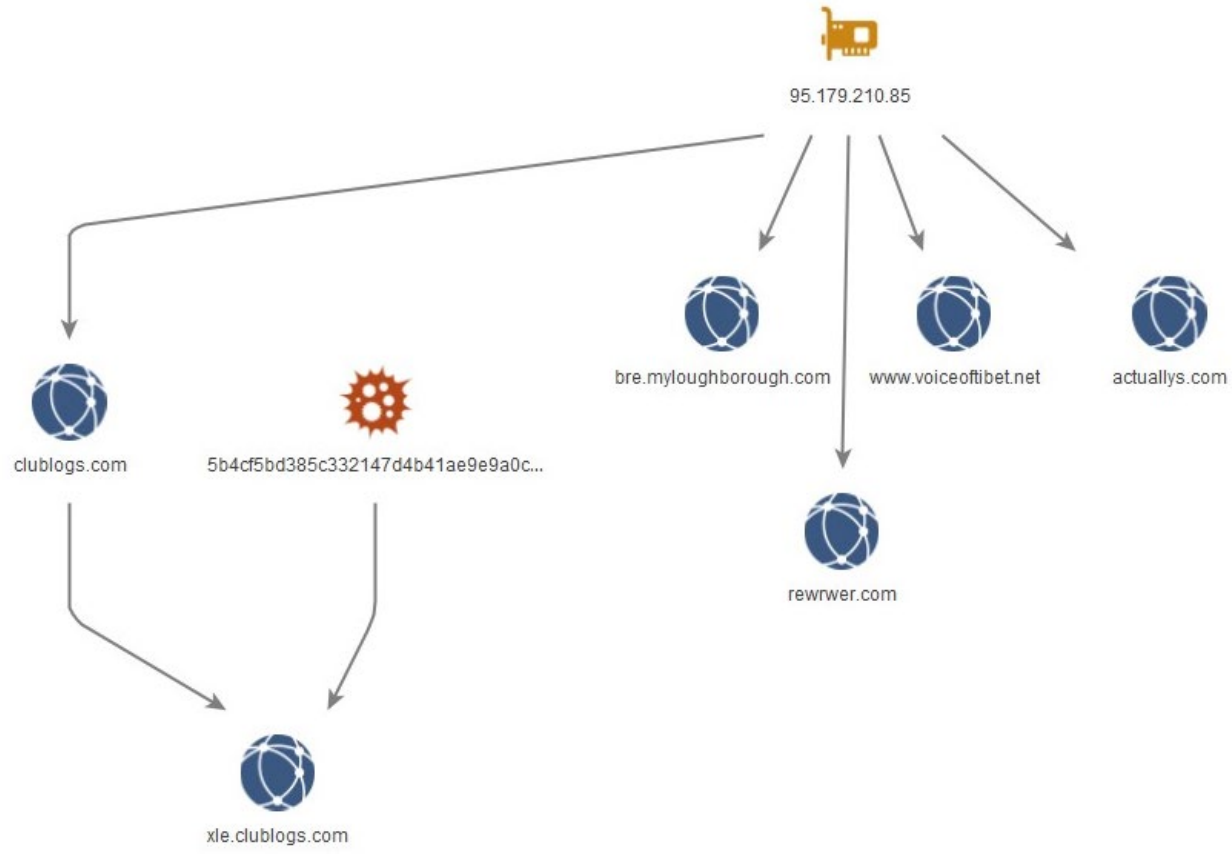


รูปภาพที่ 2 – ค่าการเดินแป้นพิมพ์

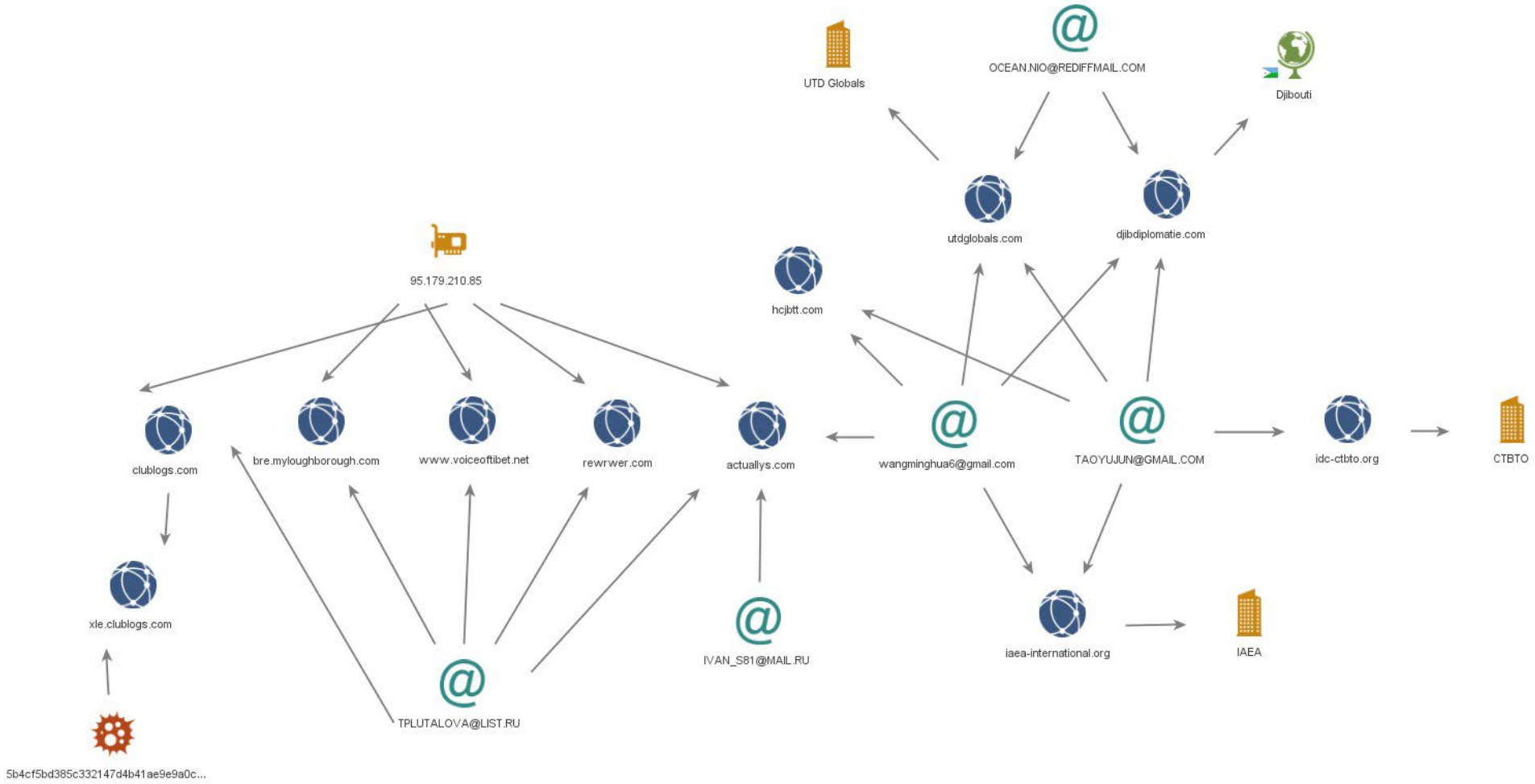


รูปภาพที่ 3 – โดเมนเพิ่มเติมที่มีค่าในช่อง State เป็น ‘FSDF’

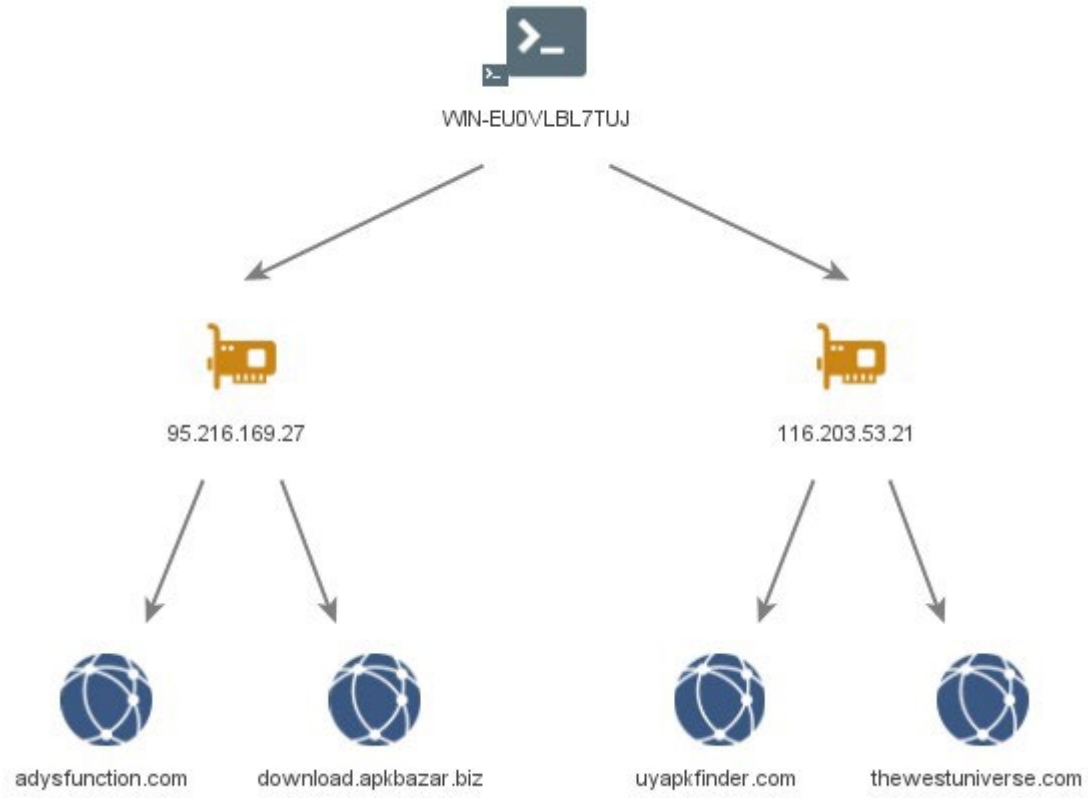
รูปภาพที่ 4 – **95.179.210[.]85**



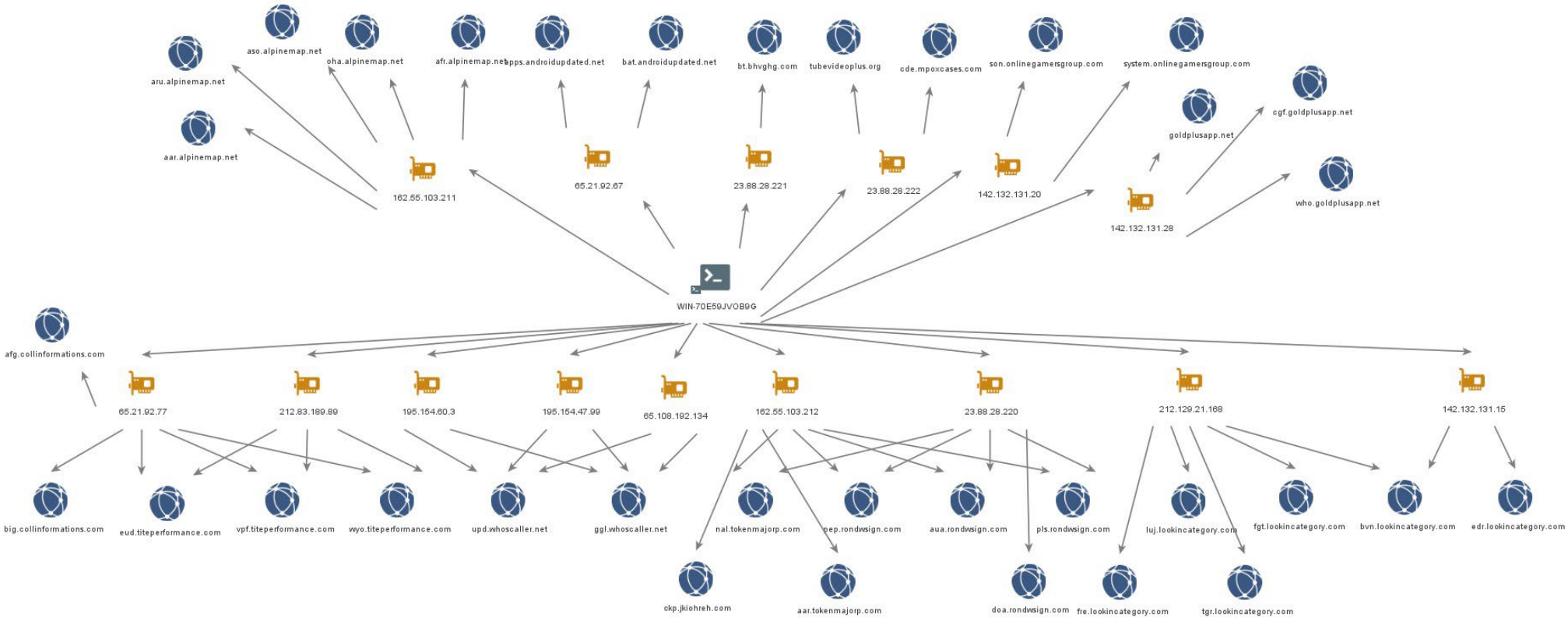
รูปภาพที่ 5 – ลิงก์ WHOIS



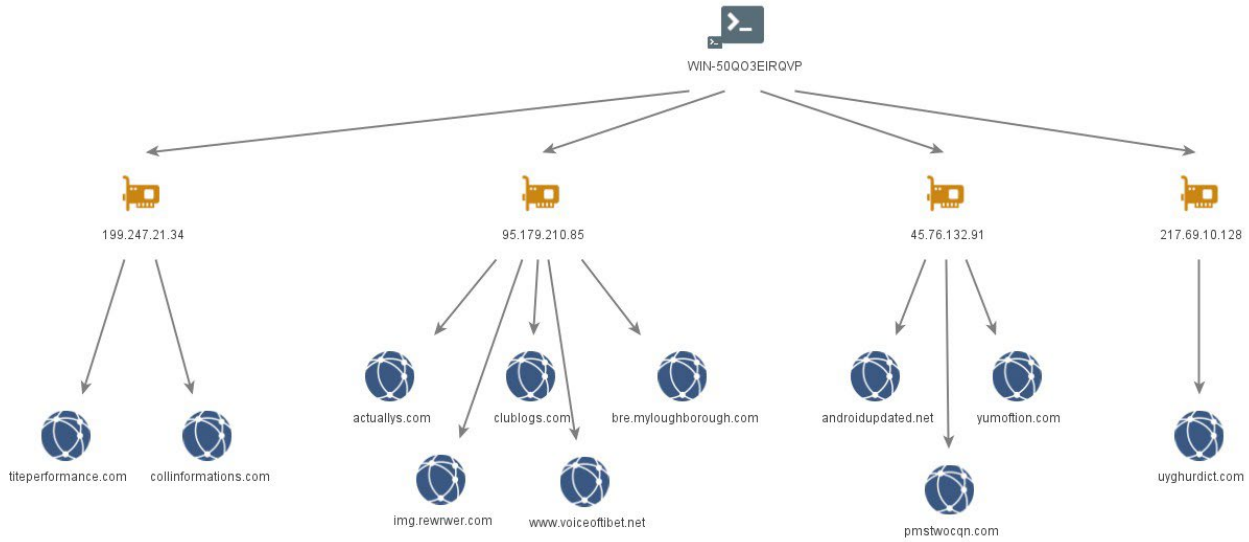
รูปภาพที่ 6 – **WIN-EU0VLBL7TUJ**



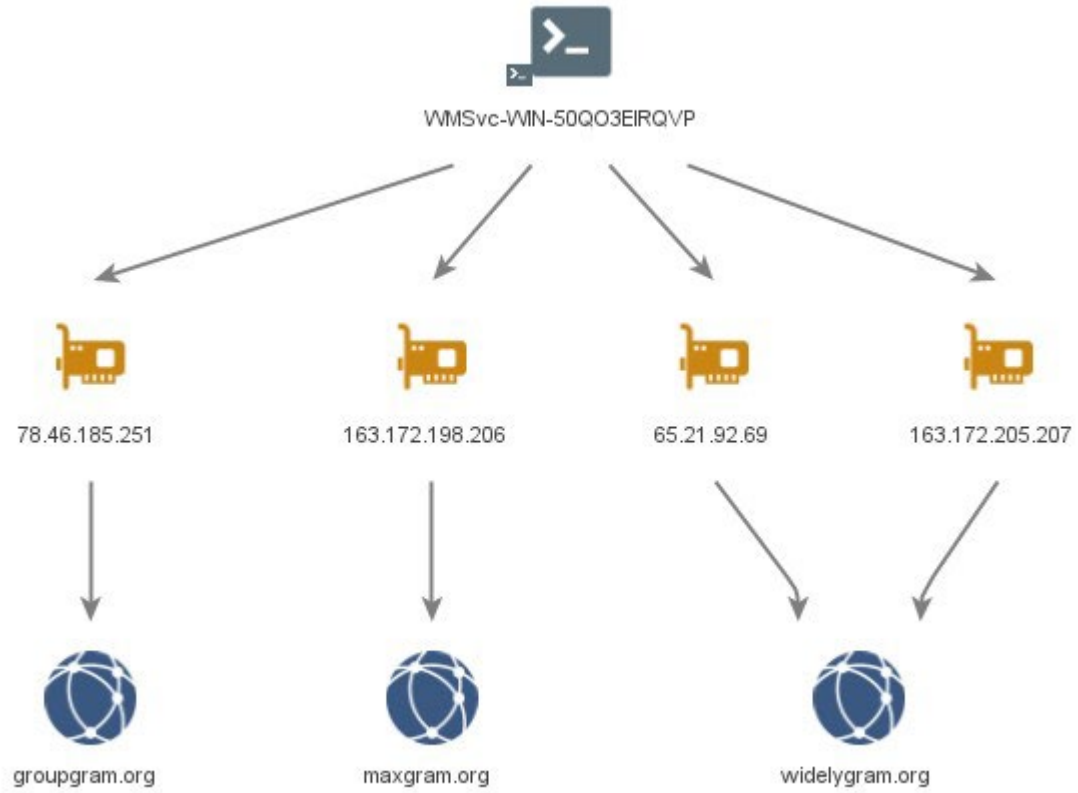
รูปภาพที่ 7 – **WIN-70E59JVOB9G**



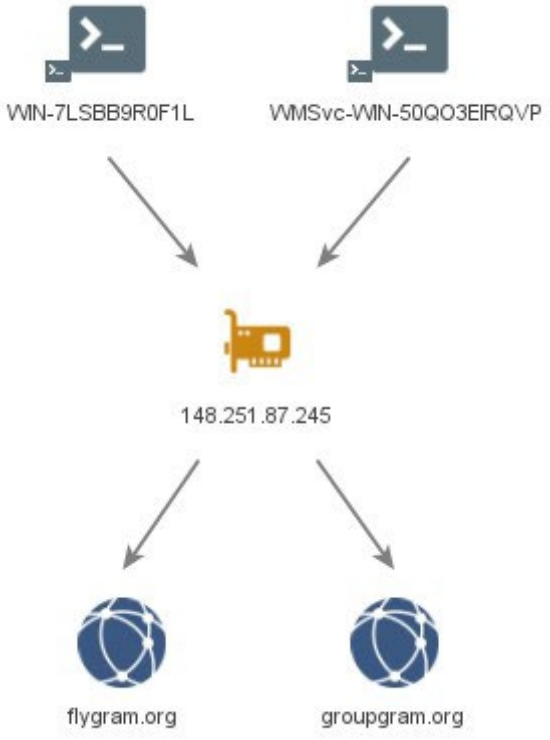
รูปภาพที่ 8 - **WIN-50QO3EIRQVP**



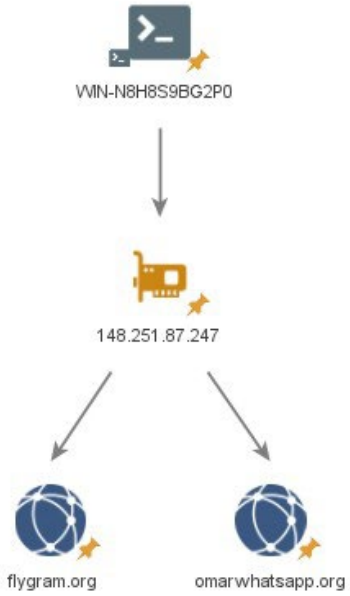
รูปภาพที่ 9 - **VMSvc-WIN-50QO3EIRQVP**



รูปภาพที่ 10 – **VMSvc-WIN-50QO3EIRQVP** และ **WIN-7LSBB9R0F1L**



รูปภาพที่ 11 - **WIN-N8H8S9BG2P0**



รูปภาพที่ 12 – **WIN-I6VBN8MR92A**

ภาคผนวก B: ตัวอย่างของ MOONSHINE และ BADBAZAAR ที่ตรวจพบ

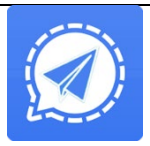
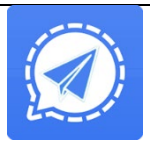
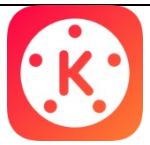
ตารางด้านล่างนี้แสดงรายการแอปที่ใช้ในการโจมตีของ MOONSHINE และ BADBAZAAR ในช่วงสองปีที่ผ่านมา

แอปเหล่านี้หลายตัวแสดงให้เห็นความคล้ายคลึงกับแอปที่มีชื่อเสียงได้รับการยอมรับอยู่แล้วอย่างชัดเจน ซึ่งอาจจะเป็นเทคนิคที่ผู้ไม่ประสงค์ดีตั้งใจใช้เพื่อ ‘เลียนแบบ’ แบรนด์ที่มีชื่อเสียงเป็นที่รู้จัก

สิ่งสำคัญที่ควรทราบคือ ชื่อแอป ชื่อแพ็กเกจ และไอคอน อาจเลียนแบบหรือเหมือนกับแอปพลิเคชันจริงได้ทั้งหมด ดังนั้นจึงไม่ควรใช้เพียงสิ่งเหล่านี้เท่านั้นในการระบุว่าอุปกรณ์ติดมัลแวร์หรือไม่

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	

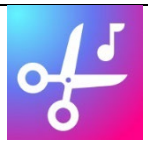
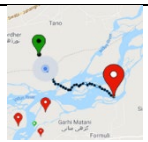
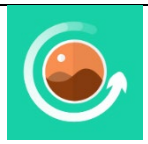
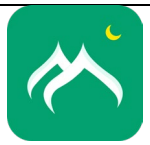
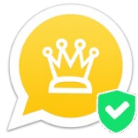
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra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

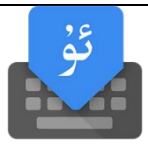
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video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

อ่านเพิ่มเติม

คำแนะนำจากศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย

- 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

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