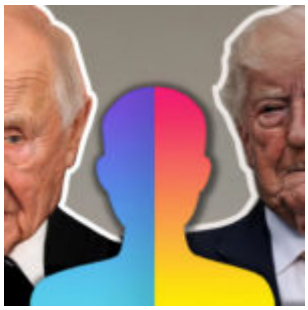
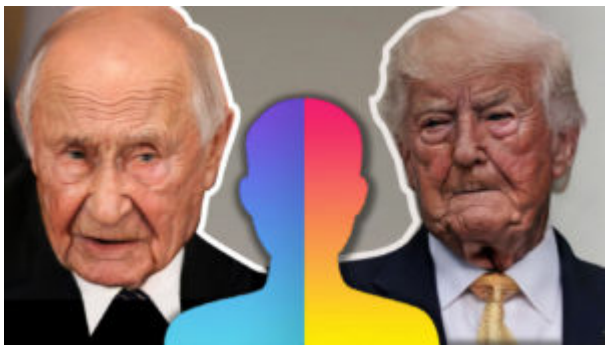
FaceApp ปลอมแพร่เชื้อไปยังเหยื่อด้วยโมดูลแอดแวร์





Kaspersky เผยว่า ได้พบแอปปลอมที่ออกแบบมาเพื่อให้ผู้ใช้หลงเชื่อว่าเป็น FaceApp ที่ถูกต้อง
แต่จะแพร่เชื้อบนอุปกรณ์ของเหยื่อด้วยโมดูลแอดแวร์ที่ชื่อว่า MobiDash
เมื่อดาวน์โหลดแอปจากแหล่งที่ไม่รู้จักหรือไม่เป็นทางการนี้ มันจะแกล้งทำเป็นล้มเหลวและถูกลบออกไปภายหลัง
หลังจากนั้นโมดูลที่เป็นอันตรายจะแฝงตัวอยู่ในอุปกรณ์ของผู้ใช้ โดยแสดงเป็นโฆษณา
ซึ่งข้อมูลของ Kaspersky รายงานว่า ขณะนี้มีผู้ใช้ที่ประสบปัญหาดังกล่าวแล้วประมาณ 500 ราย เมื่อ 2
วันที่ผ่านมา โดยตรวจจับได้ครั้งแรกเมื่อวันที่ 7 กรกฎาคม ซึ่งระบุได้ว่ามีโมดูลที่แตกต่างกันกว่า 800 โมดูลด้วยกัน
“กลุ่มคนที่อยู่เบื้องหลัง MobiDash
มักจะซ่อนโมดูลแอดแวร์ภายใต้หน้ากากของแอปและบริการที่กำลังได้รับความนิยม
ซึ่งหมายถึงกิจกรรมของแอปปลอมอาจเพิ่มความรุนแรงได้
โดยเฉพาะอย่างยิ่งที่เรากล่าวถึงไปว่ามีเหยื่อหหลายร้อยเพียงแค่ไม่กี่วัน
ดังนั้นเราขอแนะนำให้ผู้ใช้ไม่ดาวน์โหลดแอปพลิเคชั่นจากแหล่งไม่น่าเชื่อถือ
และควรติดตั้งโซลูชั่นรักษาความปลอดภัยบนอุปกรณ์ต่าง ๆ เพื่อหลีกเลี่ยงจากความเสียหายที่อาจจะเกิดขึ้นได้”
ไอกอร์ โกโลวิน นักวิจัยด้านความปบอดภัย Kaspersky กล่าว
ผลิตภัณฑ์ต่าง ๆ ของ Kaspersky สามารถตรวจจับและบล็อกภัยคุกคามที่ไม่ได้เป็นไวรัสอย่าง
HEUR:AdWare.AndroidOS.Mobidash ได้
เซียง เทียง (Yeo Siang Tiong) ผู้จัดการทั่วไปของแคสเปอร์สกี ได้ให้ความเห็นว่า

อีกหนึ่งแอปที่กำลังนิยมและเป็นไวรัลในขณะนี้ ที่กำลังกลายเป็นปรากฏการณ์ที่เห็นในทุกโซเชียลมีเดีย ซึ่งในยุคนี้ผู้ใช้ต่างร่วมใช้บริการเพราะสนุกและอยู่ในกระแส ซึ่งอาจเรียกได้ว่า FOMO ที่แปลว่า กลัวที่จะตกเทรนด์ โดยที่ไม่คำนึงถึงความปลอดภัย หรือระมัดระวังต่อการอนุญาตการเข้าถึงของแอปนั้น ๆ จากผลการวิจัยก่อนหน้านี้ของเรา ที่ได้เปิดเผยว่า ผู้บริโภคส่วนใหญ่ 63% ไม่อ่านข้อตกลงหรือสัญญาใด ๆ และ 43% ก็จะเลือกตกลงในทุกเงื่อนไขของข้อตกลงของแอปนั้น ก่อนที่จะดาวน์โหลดแอปต่าง ๆ

โดยการสำรวจนี้ได้จัดทำขึ้นมาเมื่อ 3 ปีก่อน
เราเชื่อว่าผลการวสำรวจนี้ยังคงเป็นจริงต่อพฤติกรรมด้านดิจิทัลของผู้บริโภคในปัจจุบันเช่นกัน
โดยทั่วไปการดาวน์โหลดแอปใหม่ไม่ได้อันตรายแต่อย่างใด
อันตรายจะเกิดขึ้นก็ต่อเมื่อผู้ใช้อนุญาตให้แอปเหล่านี้เข้าถึงข้อมูลต่าง ๆ ของผู้ใช้ ไม่ว่าจะเป็น ข้อมูลติดต่อ รูปภาพ ข้อความส่วนตัว และอื่น ๆ ซึ่งการกระทำเหล่านี้ถือเป็นการกระทำที่ถูกกฎหมายที่ผู้ผลิตแอปสามารถทำได้ แม้แต่การเข้าถึงข้อมูลที่เป็นความลับก็ตาม เมื่อข้อมูลที่สำคัญเหล่านี้ได้ถูกเข้าถึงหรือโดนขโมย แอปไวรัลเหล่านี้จะกลายเป็นแหล่งหลบซ่อนหรือทางหนีที่พวกแฮกเกอร์สามารถแพร่กระจายไวรัสที่เป็นอันตรายได้นั่นเอง
ถือเป็นสถานการณ์หนึ่งที่พวกเรา Kaspersky ต้องหลักเลี่ยง เราแนะนำให้ผู้ใช้ออนไลน์ทั้งหลาย ควรจะระมัดระวังและรอบคอบกับทุกอย่างที่กำลังทำในกิจกรรมบนอินเตอร์เน็ต รวมถึงอุปกรณ์ต่าง ๆ โดยมีข้อพึงกระทำพื้นฐาน ดังนี้

· ดาวน์โหลดเฉพาะแอปจากแหล่งที่น่าเชื่อถือได้เท่านั้น อ่านรีวิวและการจัดอันดับ (ratings) ของแอปนั้น ๆ ด้วย
· เลือกดาวน์โหลดแอปเพื่อติดตั้งบนอุปกรณ์ของคุณอย่างรอบคอบ
· อ่านรายละเอียดของข้อตกลงอย่างละเอียด
· ระมัดระวังต่อรายการการขออนุญาตการเข้าถึง ที่แอปนั้น ๆ ร้องขอ
· หลีกเลี่ยงการกด next หรือ ถัดไป ในระหว่างการติดตั้งแอป
· เพื่อมั่นใจถึงความปลอดภัยขั้นสูง ควรติดตั้งโซลูชั่นรักษาความปลอดภัยบนอุปกรณ์ต่าง ๆ ของคุณ