แอปตกแต่งภาพปลอมบน Google Play มีมัลแวร์แบคดอร์ที่มีพลังอันตรายมากแฝงอยู่

ผู้เชี่ยวชาญของ Kaspersky เปิดเผยว่ามัลแวร์ที่ขโมยเงินที่เรียกว่า MobOk มักจะซ่อนอยู่กับแอปพลิเคชั่นแต่งรูปถูกกฎหมายที่สามารถดาวน์โหลดได้ผ่าน Google Play store ในช่วงเวลาที่ตรวจจับนั้น แอปพลิเคชั่นที่ชื่อว่า Pink Camera และ Pink Camera 2 ได้ถูกติดตั้งกว่า 10,000 ครั้ง แอปพลิเคชั่นนี้ได้ถูกออกแบบมาเพื่อขโมยข้อมูลส่วนตัวของเหยื่อและนำไปใช้ในการลงทะเบียนในบริการเสียเงินต่าง ๆ เหยื่อจะทราบว่ามีการหักเงินไปเมื่อเห็นใบแจ้งหนี้เท่านั้น ซึ่งตอนนี้แอปพลิเคชั่นนี้ได้ถูกถอดออกจาก Google Play store และไม่สามารถดาวน์โหลดได้อีกแล้ว มัลแวร์ MobOk เป็นแบคดอร์ จัดอยู่ในมัลแวร์ประเภทอันตรายรูปแบบหนึ่ง เพราะมัลแวร์นี้สามารถทำให้ผู้โจมตีควบคุมอุปกรณ์ที่ติดเชื้อได้อย่างเต็มที่ ถึงแม้ว่าเนื้อหาของแอปพลิเคชั่นที่อัปโหลดผ่าน Google Play นั้นจะได้รับการคัดกรองเป็นอย่างดี แต่นี่ไม่ใช่เป็นครั้งแรกที่ภัยคุกคามจะสามารถหาช่องทางในการเข้าถึงอุปกรณ์ของผู้ใช้ได้ในหลายกรณี ที่มัลแวร์แบบแบคดอร์ได้มาพร้อมกับแอปแบบกึ่งใช้งานได้ ซึ่งปรากฏตัวอย่างรวดเร็วและดูไม่ออก โดยทำให้ดูว่าเป็นแอปที่ถูกกฎหมายอย่างแนบเนียน ด้วยเหตุผลนี้ทำให้แอป Pink Camera ดูไม่น่าสงสัย เพราะพวกเขาได้จัดทำฟังก์ชั่นสำหรับการตกแต่งภาพอย่างถูกต้องและที่สำคัญได้รับการดาวน์โหลดผ่านช่องทางที่น่าเชื่อถือได้อย่าง Google Pay store อีกด้วย

อย่างไรก็ตามเมื่อผู้ใช่เริ่มใช้งานตกแต่งรูปภาพด้วยแอป Pink Camera แอปจะร้องขอการแจ้งเตือนซึ่งเป็นการเริ่มให้มัลแวร์เริ่มทำงานนั่นเอง โดยกิจกรรมนี้มีวัตถุประสงค์เพื่อต้องการข้อมูลของผู้ใช้เพื่อนำไปลงทะเบียนในบริการที่จ่ายเงินผ่านมือถือ ซึ่งจะเป็นเว็บไซต์ที่นำเสนอบริการที่ชำระเงินทุกวันโดยตัดจากบิลโทรศัพท์มือถือ ซึ่งเริ่มแรกการจ่ายเงินรูปแบบนี้ถูกออกแบบขึ้นโดยผู้ให้บริการโทรศัพท์มือถือ แต่ปัจจุบันพวกหลอกลวงใช้เป็นช่องทางในการโจมทางทางไซเบอร์

เมื่อเหยื่อได้รับมัลแวร์นั้นมาในเครื่อง มัลแวร์ MobOk จะเริ่มทำงานโดยงานเก็บข้อมูลในเครื่อง ได้แก่ หมายเลขโทรศัพท์มือถือ เพื่อนำไปใช้ประโยชน์ในการโจมตีขั้นต่อไป จากนั้นผู้โจมตีจะส่งรายละเอียดหน้าเว็บไซต์ของการลงทะเบียนในบริการที่ต้องชำระเงินมายังเครื่องที่โดนมัลแวร์ และมัลแวร์จะเปิดเว็บไซต์นั้นโดยผู้ใช้ไม่รู้ตัวเพราะพวกขาจะทำเป็นความลับ การใช้หมายเลขโทรศัพท์นั้น มัลแวร์สามารถใช้ในการลงทะเบียนและยืนยันการสั่งซื้อ เนื่องจากมัลแวร์สามารถควบคุมเครื่องที่ติดเชื่อได้อย่างเต็มที่ และสามารถตรวจสอบการแจ้งเตือนได้อีกด้วย มัลแวร์จึงสามารถเข้ารหัสจากรหัสผ่านยืนยันที่ส่งมายังเครื่องได้อีกด้วย โดยที่ผู้ใช้ไม่รู้ตัวแต่อย่างใด ซึ่งเหยื่อจะไม่ทราบจนกว่าจะเห็นใบแจ้งหนี้ของโทรศัพท์มือถือว่ามีการจ่ายเงินไปในการบริการอะไรบ้างนั่นเอง

“ ถึงแม้ว่าประสิทธิภาพในการใช้งานตกแต่งภาพของแอปพลิเคชั่น Pink Cameras จะดูธรรมดาไม่น่าประทับใจ แต่

การทำงานหลังบ้านที่แอบอยู่น่ากลัวมาก ซึ่งสามารถทำให้ผู้ใช้ได้รับความเสียหาย จากบริการที่ทำให้เสียเงิน ที่มีทั้งการใช้งานภาษารัสเซีย อังกฤษ และไทยในการตรวจสอบข้อความ sms และการกรอกรหัส Capcha ซึ่งเป็นรหัสที่ต้องกรอกเพื่อยืนยันว่าคุณไม่ใช่หุ่นยนต์ ผ่านการให้บริการออนไลน์ นั่นหมายความว่าพวกเขาสามารถขโมยข้อมูลสำคัญที่เกี่ยวข้องกับการเงินของเหยื่อ โดยเฉพาะอย่างยิ่งบัญชีธนาคารได้ด้วย โดยพวกโจมตีที่อยู่เบื้องหลังแอปนี้ได้ออกแบบบริการที่ต้องมีการลงทะเบียนจ่ายเงิน ซึ่งไม่ใช่ของจริง และมัลแวร์จะทำหน้าที่ดึงข้อมูลสมาชิก ที่สำคัญออกแบบให้พวกเขาสามารถเข้าถึงกลุ่มเป้าหมายระหว่างประเทศได้อีกด้วย” ไอกอร์ โกโลฟวิน นักวิจัยด้านความปลอดภัย Kaspersky

Kaspersky ได้ตรวจจับมัลแวร์ MobOk ที่ใช้ชื่อว่า HEUR:Trojan.AndroidOS.MobOk.a

เพื่อหลักเลี่ยงการตกเป็นเหยื่อของแอปที่เป็นอันตราย นักวิจัย Kaspersky แนะนำให้ผู้ใช้ปฏิบัติดังนี้

• ควรจำไว้ว่า ถึงแม้ว่าแหล่งที่น่าเชื่อถือได้อย่าง app store ที่เป็นทางการ ก็สามารถมีแอปที่เป็นอันตรายได้เช่นกัน ดังนั้นควรระมัดระวังและตรวจสอบสิทธิ์ของแอปนั้น ๆ ว่าอนุญาตให้ทำอะไรบ้าง ตรวจสอบเรตติ้งของแอปและอ่านรีวิวของผู้ใช้ หรือคำเตือนของความเสี่ยงในการติดมัลแวร์ เมื่อคุณกำลังติดตั้งแอปควรให้ความสนใจเป็นพิเศษกับคำขออนุญาต

• Install system and application updates as soon as they are available — they patch vulnerabilities and keep devices protected.

• ติดตั้งการอัปเดตของแอปพลิเคชั่นทันทีเมื่อมีการอัปเดต เพื่อเป็นการลดช่องโหว่และปกป้องอุปกรณ์จากการโจมตี

• ใช้โซลูชั่นด้านความปลอดภัยที่น่าเชื่อถือได้ เพื่อเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามที่หลากหลาย อย่างเช่น Kaspersky Security Cloud

ติดตามรายงานฉบับเต็มได้ที่ Securelist.com

เกี่ยวกับ Kaspersky

Kaspersky เป็นบริษัทด้านความปลอดภัยบนอินเทอร์เน็ตระดับโลก ที่ก่อตั้งในปี 1997 ด้วยความเชี่ยวชาญด้านความปลอดภัยที่ได้พัฒนามาอย่างต่อเนื่อง จนปัจจุบันเปลี่ยนเป็นโซลูชั่นความปลอดภัยยุคใหม่ ที่ให้บริการในการป้องกันสำหรับธุรกิจ โครงสร้างพื้นฐาน รัฐบาลและลูกค้าทั่วโลก การให้บริการของบริษัทประกอบด้วย การป้องกันปลายทาง โซลูชั่นการป้องกันความปลอดภัยแบบพิเศษจำนวนมาก และบริการเพื่อป้องกันภัยคุกคามดิจิทัล ซึ่ง Kaspersky ได้ป้องกันความปลอดภัยให้แก่ผู้ใช้กว่า 400 ล้านคน และอีกกว่า 270,000 องค์กร ที่ป้องกันความปลอดภัยให้กับทุกส่วนที่สำคัญสำหรับลูกค้า ศึกษาข้อมูลเพิ่มเติมได้ที่ www.kaspersky.com