แคสเปอร์สกี้ แลป เผย โทรจัน Faketoken เวอร์ชั่นใหม่ จ้องโจมตีผู้ใช้แอพบริการเรียกรถแท็กซี่บนแอนดรอยด์

นักวิจัยแคสเปอร์สกี้ แลป ค้นพบโมบายแบงกิ้งโทรจัน Faketoken ในฉบับที่ได้รับการปรับแต่ง พัฒนาต่อยอดมาจนกระทั่งสามารถขโมยข้อมูลสำคัญจากแอพพลิเคชั่นเรียกรถแท็กซี่

ตลาดโมบายแอพเติบโตและมีแอพให้บริการมากมายที่ต้องใช้ข้อมูลทางการเงิน แม้กระทั่งแอพบริการเรียกแท็กซี่ รถบริการสาธารณะ หรือแอพเพื่อนร่วมเดินทาง (ride-sharing apps) ก็ต้องใช้ข้อมูลบัตรธนาคารของผู้โดยสาร จะพบว่ามีแอพเหล่านี้ติดตั้งอยู่บนอุปกรณ์แอนดรอยด์นับเป็นล้านๆ ตัวทั่วโลก ทำให้กลายมาเป็นเป้าหมายของอาชญากรไซเบอร์ที่ได้พัฒนาเพิ่มฟังก์ชั่นให้มัลแวร์บุกโจมตีโมบายแบงกิ้งกันอย่างเป็นล่ำเป็นสัน

มัลแวร์ Faketoken เวอร์ชั่นใหม่นี้สามารถตามสะกดรอยแอพได้ทันที (live) ที่แอพที่กำหนดไว้มีการใช้งาน และจะสร้างหน้าต่างฟิชชิ่ง (phishing window) ของมัลแวร์ซ้อนทับทันที เพื่อขโมยรายละเอียดบัตรธนาคารของเหยื่อ โดยโทรจันมีอินเทอร์เฟซที่มีหน้าตาเลียนแบบแอพได้แนบเนียน ไม่ว่าจะเป็นโทนสีหรือโลโก้ จึงสามารถสร้างหน้าต่างฟิชชิ่งมาซ้อนทับลงบนแอพที่ถูกต้องได้เร็วและจับผิดแทบไม่ได้เลย จากผลการวิจัยของแคสเปอร์สกี้ แลป อาชญากรมีเป้าหมายที่แอพบริการเรียกรถสาธารณะหรือหาเพื่อนร่วมเดินทางที่เป็นที่นิยมในระดับนานาชาติ

ยิ่งไปกว่านั้น โทรจันจะแอบอ่านข้อความขาเข้าทั้งหมด จากนั้น ส่งต่อไปยังคอมมานด์และคอนโทรลเซิร์ฟเวอร์ ทำให้อาชญากรเข้าถึงรหัสผ่านแบบใช้ได้ครั้งเดียวที่ทางธนาคารได้ส่งมาให้เจ้าของ หรือข้อความอื่นๆ ที่ส่งมาจากบริการเรียกแท็กซี่หรือเพื่อนร่วมเดินทาง และยิ่งไปกว่านั้น ตัวขยายของมัลแวร์ Faketoken นี้สามารถที่จะเฝ้าดูสายเรียกเข้าออกของเจ้าของเครื่อง แอบบันทึกและส่งข้อมูลไปยังเซิร์ฟเวอร์คอมมานด์และคอนโทรล

การวางทับซ้อน หรือ Overlaying นั้นเป็นวิธีการธรรมดาทั่วไปที่ใช้กับโมบายแอพพลิเคชั่นหลายตัวด้วยกัน เมื่อปีที่แล้ว แคสเปอร์สกี้ แลป รายงาน เกี่ยวกับส่วนที่ปรับเพิ่มฟังก์ชั่นของมัลแวร์ Faketoken นี้ ซึ่งตอนนั้นกำลังอาละวาดโจมตีเหยื่อถึงกว่า 2,000 แอพด้านการเงินทั่วโลก ด้วยการปลอมแปลงตัวเองเป็นโปรแกรมและเกมหลากหลายประเภท โดยมากมักปลอมเป็น Adobe Flash Player ตั้งแต่นั้นเป็นต้นมา มัลแวร์ Faketoken ก็ได้มีพัฒนาการเรื่อยมา และขยายพื้นที่ในการก่ออาชญากรรมอีกด้วย

วิกเตอร์ เชบีเชฟ ผู้เชี่ยวชาญด้านความปลอดภัย แคสเปอร์สกี้ แลป กล่าวว่า “ความจริงที่ว่าอาชญากรไซเบอร์ได้ขยายรูปแบบอาชญากรรม จากแอพพลิเคชั่นด้านการเงินไปยังธุรกิจอื่นๆ รวมทั้ง บริการเรียกรถสาธารณะ หมายความว่าคนที่พัฒนาแอพพลิเคชั่นสำหรับบริการเหล่านี้ควรที่จะต้องให้ความสำคัญใส่ใจกับการป้องกันผู้ที่ใช้แอพของตนเพิ่มขึ้น อุตสาหกรรมการธนาคารการเงินนั้นมีความคุ้นเคยอยู่แล้วกับการฉ้อโกง กลก่อการร้ายรูปแบบต่างๆ และที่เคยกระทำกันมาโดยตลอดเพื่อลดความเสี่ยงของการขโมยข้อมูลที่มีความสำคัญทงการเงินคือการติดตั้งเทคโนโลยีเพื่อความปลอดภัยในแอพพลิเคชั่น และก็น่าที่จะถึงเวลาของบริการด้านอื่นๆ บ้างแล้วที่มีการใช้ข้อมูลสำคัญทารการเงิน ที่จะต้องพิจารณาเดินตามรอยนี้บ้าง เวอร์ชั่นล่าสุดของมัลแวร์ Faketoken มีเป้าหมายที่ผู้ใช้ชาวรัสเซียส่วนใหญ่ อย่างไรก็ตาม ก็เป็นไปได้ว่าจะได้มีการขยายพื้นที่เป้าหมายออกไป ซึ่งเราเคยได้พบเห็นรูปการณ์เช่นนั้นมากแล้วจากมัลแวร์ Faketoken ในเวอร์ชั่นเก่า รวมไปถึงแบงกิ้งมัลแวร์ตัวอื่นๆ ด้วย”

เหล่านักวิจัยก็ยังได้ตรวจพบการโจมตีของ Faketoken กับโมบายแอพพลิเคชั่นที่เป็นที่นิยมตัวอื่น เช่น แอพจองโรงแรมที่พัก แอพชำระค่าปรับจราจร แอนดรอยด์เพย์ และกูเกิ้ลเพย์ เป็นต้น

ซิลเวีย อึง ผู้จัดการทั่วไป แคสเปอร์สกี้ แลป เอเชียตะวันออกเฉียงใต้ กล่าวเสริมว่า “เราพบปัญหาด้านความปลอดภัยของแอนดรอยด์เกิดขึ้นอยู่เป็นประจำ แม้ว่าทางกูเกิ้ลเองจะได้มีความพยายามอย่างต่อเนื่องในการยกระดับความปลอดภัยของตน นักพัฒนาซอฟต์แวร์ผลักดันเวอร์ชั่นใหม่ที่มีความปลอดภัยมากขึ้นออกมา แต่ก็ยังไม่เป็นที่ใช้แพร่หลายเท่าใดนัก การนำมาใช้ถือว่าตามหลังการใช้แอพอยู่มากๆ”

เพื่อป้องกันตนเองให้พ้นจากโทรจัน Faketoken และภัยมัลแวร์อื่นๆ ที่มุ่งร้ายต่อแอนดรอยด์ แคสเปอร์สกี้ แลปแนะนำให้ผู้ใช้เพิ่มความระมัดระวังอย่าได้ดาวน์โหลดแอพจากแหล่งที่ไม่รู้จัก และควรที่จะติดตั้งโซลูชั่นเพื่อความปลอดภัยที่เสถียร ไว้วางใจได้ เช่น โซลูชั่นของแคสเปอร์สกี้ แลป Kaspersky Mobile Antivirus: Web Security & Applock บนดีไวซ์ของตนเอง