เทรนด์ไมโครเตือน มัลแวร์เรียกค่าไถ่ Pokemon Go สร้างช่องโหว่ให้กับ Windows

เทรนด์ไมโครเตือน มัลแวร์เรียกค่าไถ่ Pokemon Go สร้างช่องโหว่ให้กับ Windows

ท่ามกลางความคลั่งไคล้ในโมบายล์เกมโปเกมอน โก (Pokemon GO) คนร้ายเตรียมที่จะใช้ประโยชน์จากความแพร่หลายของเกมดังกล่าวเพื่อแพร่กระจายมัลแวร์เรียกค่าไถ่ (Ransomware) โดยมัลแวร์ชนิดใหม่ที่ตรวจพบเมื่อไม่นานมานี้ปลอมแปลงเป็นเกม Pokemon GO สำหรับ Windows โดยเทรนด์ไมโครได้ตรวจพบมัลแวร์ชนิดนี้มีชื่อว่า Ransom_POGOTEAR.A มีลักษณะคล้ายคลึงกับมัลแวร์เรียกค่าไถ่อื่นๆ อย่างไรก็ตาม หลังจากที่ตรวจสอบอย่างละเอียด พบว่าผู้สร้างพัฒนาต่อยอดจาก Hidden Tear ซึ่งเป็นมัลแวร์เรียกค่าไถ่แบบโอเพ่นซอร์สที่ถูกเผยแพร่เมื่อเดือนสิงหาคม ปีที่แล้ว โดยมีจุดมุ่งหมายเพื่อให้ความรู้แก่บุคคลทั่วไป

มัลแวร์เรียกค่าไถ่ Pokemon GO ได้รับการออกแบบให้สร้างบัญชีผู้ใช้ที่เป็นช่องโหว่ภายใต้ชื่อ “Hack3r” ในระบบปฏิบัติการ Windows และถูกเพิ่มไปยังกลุ่มผู้ดูแลระบบ (Administrator) นอกจากนี้ ยังมีการปรับเปลี่ยนการลงทะเบียน (registry) เพื่อซ่อนบัญชี Hack3r จากหน้าจอล็อกอินของ Windows และยังมีอีกฟีเจอร์ที่สร้างการใช้งานเครือข่ายร่วมกันบนคอมพิวเตอร์ของเหยื่อ เพื่อให้มัลแวร์เรียกค่าไถ่สามารถแพร่กระจาย ด้วยการคัดลอกไฟล์มัลแวร์ไปยังไดรฟ์ทั้งหมด และเมื่อไฟล์มัลแวร์ถูกคัดลอกไปยังไดรฟ์ที่ถอดออกได้ ก็จะสร้างไฟล์รันอัตโนมัติ (Autorun) เพื่อให้มัลแวร์ทำงานทุกครั้งที่มีใครบางคนเข้าถึงไดรฟ์ที่ถอดออกได้ นอกจากนี้ไฟล์มัลแวร์ยังถูกคัดลอกไปยังส่วนรูท (Root) ของไดรฟ์แบบติดตั้งถาวรอื่นๆ วิธีนี้จะทำให้มัลแวร์เรียกค่าไถ่ Pokemon GO เริ่มทำงานเมื่อเหยื่อล็อกอินเข้าสู่ Windows

นักวิจัยระบุว่า มีตัวบ่งชี้มากมายที่ทำให้ทราบว่ามัลแวร์เรียกค่าไถ่ดังกล่าวยังคงอยู่ระหว่างการพัฒนา เช่น มีการใช้คีย์เข้ารหัส AES แบบคงที่ “123vivalalgerie” นอกจากนี้ เซิร์ฟเวอร์สั่งการและควบคุม (C&C) ใช้ไอพีแอดเดรสแบบส่วนตัว ซึ่งนั่นหมายความว่ามัลแวร์ไม่สามารถเชื่อมต่อผ่านอินเทอร์เน็ตได้

จากภาษาที่ใช้ในข้อความเรียกค่าไถ่ เชื่อว่ามัลแวร์ Pokemon GO น่าจะพุ่งเป้าหมายไปที่ผู้ใช้ที่พูดภาษาอาหรับ โดยหน้าจอเรียกค่าไถ่ที่แนบมาเป็นรูปตัวการ์ตูนปิกาจู (Pikachu) นอกจากนั้น ไฟล์สกรีนเซฟเวอร์ยังประกอบด้วยรูปภาพที่มีข้อความว่า “Sans Titre” ซึ่งเป็นภาษาฝรั่งเศสที่ตรงกับคำว่า “Untitled” นับเป็นเบาะแสหนึ่งที่บ่งบอกถึงแหล่งที่มาของผู้พัฒนา

มัลแวร์เรียกค่าไถ่ Hidden Tear ไม่ใช่สิ่งใหม่ โดยเมื่อเดือนมกราคม 2558 เทรนด์ไมโครได้ตรวจพบเว็บไซต์ที่ถูกแฮ็กในประเทศปารากวัย ซึ่งแพร่กระจายมัลแวร์เรียกค่าไถ่ที่มีชื่อว่า RANSOM_CRYPTEAR.B ทั้งนี้ ข้อมูลวิเคราะห์ชี้ว่า เว็บไซต์ดังกล่าวถูกเจาะระบบโดยแฮ็กเกอร์ชาวบราซิล และมัลแวร์เรียกค่าไถ่ดังกล่าวถูกสร้างขึ้นโดยใช้โค้ด Hidden Tear ที่มีการดัดแปลง ก่อนหน้าที่จะมีการตรวจพบ เมื่อซอร์สโค้ดของ Hidden Tear ถูกเผยแพร่แก่สาธารณชนเพื่อจุดประสงค์ด้านการให้ความรู้ ผู้สร้างได้ระบุอย่างชัดเจนว่าไม่ควรนำเอา Hidden Tear ไปใช้เป็นมัลแวร์เรียกค่าไถ่ แต่ปรากฏว่า การค้นพบมัลแวร์ Ransom_CRYPTEAR.B และ Pokemon Go นี้แสดงให้เห็นว่าถึงแม้จะมีเจตนาที่ดี แต่การเปิดเผยข้อมูลสำคัญในลักษณะที่ไม่เหมาะสมอาจก่อให้เกิดปัญหาในบางสถานการณ์ดังเช่นที่กล่าวมาแล้ว

เพื่อหลีกเลี่ยงปัญหาจากมัลแวร์เรียกค่าไถ่ ผู้ใช้ควรแบ็คอัพข้อมูลอย่างสม่ำเสมอ และติดตั้งโซลูชั่นการรักษาความปลอดภัยที่ทันสมัย โซลูชั่นของเทรนด์ไมโครสามารถปกป้องผู้ใช้จากมัลแวร์เรียกค่าไถ่ Pokemon Go ขณะที่เกมดังกล่าวได้รับการเปิดตัวในประเทศต่างๆ เพิ่มเติม ความคลั่งไคล้ในเกม Pokemon GO จะดึงดูดให้อาชญากรไซเบอร์พยายามมองหาหนทางที่จะใช้ประโยชน์จากเกมดังกล่าวนี้ ที่จริงแล้วลำพังเพียงแค่ในช่วงเดือนกรกฎาคม มีการตรวจพบแอพ Pokemon Go จำนวนมากที่มีอันตราย ซึ่งหลอกล่อให้ผู้ใช้ดาวน์โหลดแอพเข้าสู่อุปกรณ์ สถานการณ์ดังกล่าวนับเป็นเครื่องเตือนภัยว่าผู้ใช้ควรระมัดระวังภัยคุกคามที่อาจมาพร้อมกับเกมยอดนิยม