วันที่ 6 สิงหาคม 2569

แพ็กเกจ npm ที่ถูกฝังโทรจันใช้เทคนิค NullReceiver เพื่อถอดรหัสที่อยู่ IP ของเซิร์ฟเวอร์ควบคุม (C2)

นักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ตรวจพบการพัฒนารูปแบบใหม่ของเทคนิคควบคุมและสั่งการ (C2) บนบล็อกเชนที่เรียกว่า EtherHiding โดยเทคนิคใหม่นี้ซ่อนที่อยู่ IP ของเซิร์ฟเวอร์ C2 ไว้ภายในที่อยู่ปลายทางที่ถูกสร้างขึ้นมาเองของธุรกรรมโอน Ethereum ที่ว่างเปล่าโดยสมบูรณ์ แนวทางใหม่ที่เรียกว่า dead drop resolver ซึ่งถูกพบในแพ็กเกจ npm ที่ถูกดัดแปลงให้เป็นอันตราย 2 รายการ ได้แก่ "bianira-ui" และ "fluid-type-ui" ได้รับชื่อรหัสว่า NullReceiver โดย OpenSourceMalware ซึ่งอธิบายว่าเป็น "การพัฒนาต่อยอดจาก EtherHiding อย่างตั้งใจ" ทั้งยังเชื่อมโยงกิจกรรมนี้กับเกาหลีเหนือ ปัจจุบันแพ็กเกจทั้งสองถูกนำออกจาก npm แล้ว อย่างไรก็ตาม สถิติแสดงให้เห็นว่าตั้งแต่เผยแพร่ครั้งแรกเมื่อวันที่ 28 กรกฎาคม 2026 มีผู้ดาวน์โหลดไปแล้วหลายร้อยครั้ง ดังนี้

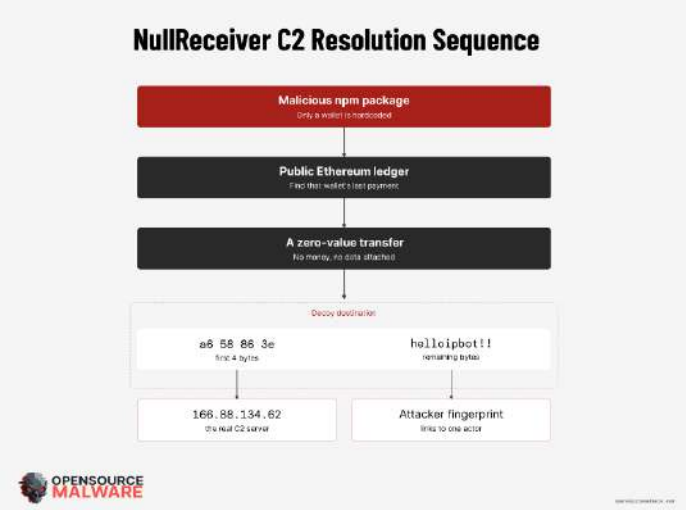
- bianira-ui (ดาวน์โหลด 109 ครั้ง) อัปโหลดโดยผู้ใช้ npm ชื่อ "npmuser1101"
- fluid-type-ui (ดาวน์โหลด 587 ครั้ง) อัปโหลดโดยผู้ใช้ npm ชื่อ "npmuser3002"

EtherHiding ถูกเปิดเผยต่อสาธารณะครั้งแรกโดย Guardio Labs ในเดือนตุลาคม 2023 ในฐานะเทคนิคที่ใช้ซ่อนโค้ดอันตรายไว้ภายในสมาร์ตคอนแทรกต์บนบล็อกเชนสาธารณะ เช่น BNB Smart Chain (BSC) หรือ Ethereum เทคนิคนี้ถูกมองว่าเป็น "ก้าวต่อไปของการโฮสต์ที่ทนต่อการปิดกั้น" เนื่องจากช่วยให้โครงสร้างการโจมตีมีความยืดหยุ่นมากขึ้น แม้จะถูกพยายามปิดหรือถอดออกจากระบบ

การที่กลุ่มแฮกเกอร์จากเกาหลีเหนือนำ EtherHiding มาใช้นั้น ถูกเปิดเผยโดย Google Threat Intelligence Group (GTIG) ในช่วงปลายปีที่ผ่านมา โดยเชื่อมโยงกับปฏิบัติการ Contagious Interview ซึ่งเป็นแคมเปญที่ดำเนินมานาน มีเป้าหมายหลอกล่อเหยื่อผ่าน LinkedIn ด้วยข้อเสนองานที่ให้ผลตอบแทนสูง ก่อนขอให้ทำแบบทดสอบ ซึ่งสุดท้ายจะนำไปสู่การติดตั้งมัลแวร์ ความเคลื่อนไหวล่าสุดแสดงให้เห็นว่าผู้โจมตีกำลังปรับปรุงเทคนิคของตนอย่างต่อเนื่อง และทำให้ผู้ป้องกันตรวจจับได้ยากยิ่งขึ้น แทนที่จะฝังที่อยู่ C2 ไว้ในโค้ดโดยตรง หรือซ่อนไว้ในข้อมูล calldata ของธุรกรรมเหมือน EtherHiding นั้น

NullReceiver จะเข้ารหัส IP ของ C2 ลงในข้อมูลไบต์ของที่อยู่ผู้รับของธุรกรรมโอน Ethereum ที่ไม่มีการโอนมูลค่าและไม่มีข้อมูลใดๆ Paul McCarty นักวิจัยด้านความปลอดภัยกล่าว

มัลแวร์จะตรวจสอบกระเป๋าเงินของผู้โจมตี อ่านที่อยู่ปลายทางของธุรกรรมขาออกล่าสุด แล้วถอดรหัส IP ของ C2 ออกจากข้อมูลไบต์ของที่อยู่นั้นโดยตรง โดยไม่ต้องใช้สมาร์ตคอนแทรกต์ และไม่ต้องใช้ช่องข้อมูล payload แต่อย่างใด



การฝังที่อยู่ IP ของ C2 ด้วยวิธีนี้มีเป้าหมายเพื่อแก้ข้อจำกัดสำคัญของ EtherHiding ซึ่งจำเป็นต้องใช้ที่อยู่ปลายทางแบบคงที่และเปิดเผยต่อสาธารณะ ทำให้ผู้ป้องกันสามารถติดตามธุรกรรมใหม่ที่มี payload, ที่อยู่ IP ของ C2 หรือสคริปต์อันตรายได้ แม้ว่าจะต้องเสียค่าธรรมเนียมธุรกรรม (Gas Fee) ก็ตาม

ในทางกลับกัน NullReceiver ใช้ที่อยู่ปลายทางที่ไม่มีอยู่จริง ที่อยู่นี้ มีอยู่เพียงเพื่อใช้เป็นพื้นที่สำหรับเข้ารหัส IP ของ C2 เท่านั้น ส่งผลให้การระบุความเชื่อมโยงของการโจมตีทำได้ยากขึ้น เพราะไม่มีที่อยู่ปลายทางแบบคงที่ที่สามารถเฝ้าติดตามได้

แพ็กเกจ npm ที่ค้นพบใหม่ทั้งสองรายการ ได้แก่ bianira-ui และ fluid-type-ui ไม่ได้เรียกใช้สมาร์ตคอนแทรกต์ และไม่ได้ฝังข้อมูลใด ๆ ไว้ในช่อง calldata ของธุรกรรม แต่ไลบรารี JavaScript เหล่านี้ใช้เทคนิคใหม่ในการดึงที่อยู่ IP แล้วเชื่อมต่อไปยังปลายทางดังกล่าว โดยลำดับการทำงานทั้งหมดบนเครื่องของเหยื่อมีดังนี้

- ตรวจสอบกระเป๋าเงินของผู้โจมตีที่ถูกกำหนดไว้ล่วงหน้า (0xa322e5f3d311d3080e6f0121063e9adc2490ef1 a")
- ค้นหาธุรกรรมขาออกล่าสุดของกระเป๋าเงินดังกล่าว
- อ่านที่อยู่ปลายทางของธุรกรรมนั้น
- ถอดรหัสที่อยู่ IP ของ C2 จากข้อมูลไบต์ของที่อยู่ โดยแปลงข้อมูล 4 ไบต์แรกจากเลขฐานสิบหก (Hexadecimal) ให้เป็นตัวเลข
- เชื่อมต่อไปยังที่อยู่ IP ดังกล่าว ("166.88.134[.]62")

จากการตรวจสอบธุรกรรมของกระเป๋าเงินดังกล่าว พบว่าที่อยู่ปลายทาง ของทุกธุรกรรมเป็นค่าเดียวกัน คือ "0xa658863ea658863e68656c6c6f6970626f742121" โดยค่า "a658863e" เมื่อนำมาแปลงจะได้ "166.88.134[.]62" ส่วนข้อมูลต่อท้าย "68656c6c6f6970626f742121" เมื่อนำมาแปลงเป็นข้อความ ASCII จะได้คำว่า "helloipbot!!"

ณ เวลาที่เขียนบทความนี้ มีธุรกรรมเกิดขึ้นทั้งหมด 68 รายการ นับตั้งแต่วันที่ 27 กรกฎาคม 2026 ซึ่งเป็นหนึ่งวันก่อนที่แพ็กเกจทั้งสองจะถูกเผยแพร่ สิ่งที่ทำให้ NullReceiver แอบแฝงได้มากกว่าคือ การไม่มีเป้าหมายแบบคงที่และไม่มีรูปแบบเฉพาะที่ใช้ระบุตัวตน อีกทั้งธุรกรรมยังมีต้นทุนต่ำกว่าเดิม ความแตกต่างสำคัญระหว่างสองเทคนิคนี้คือ EtherHiding สามารถซ่อน URL หรือสคริปต์ได้ทั้งชุด ขณะที่ NullReceiver สามารถเข้ารหัสข้อมูลได้เพียงไม่กี่ไบต์เท่านั้น

NullReceiver จะไม่ใช้ที่อยู่ปลายทางเดิมซ้ำเลย OpenSourceMalware ระบุทุกครั้งที่มีการค้นหา จะใช้ที่อยู่ใหม่ที่สร้างขึ้นเพื่อใช้งานครั้งเดียวและไม่เคยปรากฏมาก่อน ธุรกรรมของ NullReceiver ไม่มีข้อมูลเพิ่มเติมใดๆ จึงไม่มีช่องข้อมูลที่สามารถใช้เป็นลายนิ้วมือในการตรวจจับได้ เพราะไม่มีช่องข้อมูลนั้นตั้งแต่แรก

ข้อมูล calldata มีค่าใช้จ่ายตามจำนวนไบต์ที่ใช้ ซึ่ง EtherHiding ต้องเสียค่าใช้จ่ายในส่วนนี้ แต่ธุรกรรมของ NullReceiver ว่างเปล่าโดยสมบูรณ์ ทำให้เป็นรูปแบบธุรกรรมที่มีต้นทุนต่ำที่สุดและสังเกตเห็นได้ยากที่สุดบนเครือข่าย

ข้อมูลอ้างอิง

Aug 05, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/trojanized-npm-packages-decode-c2-ip.html