ประจำวันพฤหัสบดีที่ 2 มิถุนายน 2565

เครื่องมือ YODA ตรวจสอบพบ Plugins WordPress ที่เป็นอันตรายถูกติดตั้งบนเว็บไซต์กว่า 24,000 เว็บไซต์

Plugins ที่เป็นอันตรายจำนวน 47,337 รายการถูกค้นพบในเว็บไซต์ที่ไม่ซ้ำกันจำนวน 24,931 เว็บไซต์ โดยในจำนวนนั้นมี 3,685 รายการ ที่ Plugins ถูกนำไปขายในตลาดการซื้อขายที่ถูกกฎหมาย ซึ่งทำให้ผู้โจมตีนั้นมีรายได้ที่ผิดกฎหมายมากถึง 41,500 ดอลลาร์ ซึ่งการค้นพบมาจากเครื่องมือใหม่ที่เรียกว่า YODA ซึ่งมีจุดมุ่งหมายเพื่อตรวจจับ Plugins WordPress โดยการดำเนินการของกลุ่มนักวิจัยจากสถาบันเทคโนโลยีจอร์เจีย

นักวิจัยกล่าวในบทความใหม่ชื่อ " Mistrust Plugins You Must " โดยผู้โจมตีได้ปลอมตัวเป็นผู้เขียน Plugins ที่ไม่เป็นอันตรายและแพร่กระจายมัลแวร์โดยแจกจ่าย Plugins ที่ละเมิดลิขสิทธิ์ ซึ่งจำนวน Plugins ที่เป็นอันตรายบนเว็บไซต์เพิ่มขึ้นอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา และมีกิจกรรมที่เป็นอันตรายสูงสุดในเดือนมีนาคม 2020 ซึ่ง 94% ของ Plugins ที่เป็นอันตรายที่ถูกติดตั้งในช่วง 8 ปีที่ผ่านมายังคงทำงานอยู่ในปัจจุบัน

เครื่องมือ YODAสามารถรวมเข้ากับเว็บไซต์และผู้ให้บริการโฮสต์เว็บเซิร์ฟเวอร์โดยตรง นอกจากการตรวจจับส่วนเสริมที่ซ่อนอยู่และมัลแวร์แล้วยังสามารถใช้เพื่อระบุที่มาของ Plugins และความเป็นเจ้าของได้ ซึ่งทำได้โดยการวิเคราะห์ไฟล์โค้ดฝั่งเซิร์ฟเวอร์และข้อมูลเมตาที่เกี่ยวข้องเพื่อตรวจหา Pluginsตามด้วยการวิเคราะห์วากยสัมพันธ์และความหมายเพื่อระบุพฤติกรรมที่เป็นอันตราย

โดยการค้นพบ มีดังนี้
- มี Plugins3,452 รายการในตลาด Plugins ที่ถูกกฎหมาย อำนวยความสะดวกในการ injectionspam
- Plugins 40,533 รายการ ถูกพบติดไวรัสหลังการติดตั้งทั่วทั้ง 18,034 เว็บไซต์
- Plugins WordPress หรือธีมที่ถูกดัดแปลงเพื่อดาวน์โหลดโค้ดที่เป็นอันตรายบนเซิร์ฟเวอร์ คิดเป็น 8,525 ของส่วนเสริมที่เป็นอันตรายทั้งหมด โดย 75% ของปลั๊กอินละเมิดลิขสิทธิ์

การใช้เครื่องมือ YODA ทำให้เจ้าของเว็บไซต์และผู้ให้บริการโฮสติ้งสามารถระบุ Plugins ที่เป็นอันตรายบนเว็บเซิร์ฟเวอร์ นักพัฒนา Plugins และตลาดกลางสามารถตรวจสอบ Plugins ก่อนที่จะทำการเผยแพร่

ที่มาของข่าว: https://thehackernews.com/2022/06/yoda-tool-found-47000-malicious.html