ประจำวันจันทร์ที่ 11 กรกฎาคม 2565

แฮกเกอร์ใช้ประโยชน์จากช่องโหว่ของ Follina Bug เพื่อใช้ Rozena Backdoor

Cara Lin นักวิจัยของ Fortinet FortiGuard Labs กล่าวในรายงานว่ามีแคมเปญฟิชชิ่งใหม่กำลังใช้ช่องโหว่ด้านความปลอดภัย Follina ที่เพิ่งถูกเปิดเผยเมื่อเร็ว ๆ นี้ เพื่อแจกแบ็คดอร์ที่ระบบ Windows โดย Rozena เป็นมัลแวร์แบ็คดอร์ที่สามารถ injecting ระยะไกลด้วย remote shell กลับไปยังเครื่องของผู้โจมตี

ช่องโหว่หมายเลข CVE-2022-30190 เป็นช่องโหว่การเรียกใช้โค้ดจากระยะไกลของ Microsoft Windows Support Diagnostic Tool (MSDT) ที่ได้รับการปรับปรุงแก้ไขขณะนี้ และถูกใช้หาผลประโยชน์อย่างหนักในช่วงไม่กี่สัปดาห์ที่ผ่านมานับตั้งแต่มีการเปิดเผยในปลายเดือนพฤษภาคม 2565

การใช้ประโยชน์จากช่องโหว่ของ Follina เพื่อการแจกจ่ายมัลแวร์ผ่านเอกสาร Word ที่เป็นอันตรายนั้นมาจากการโจมตีทางวิศวกรรมสังคม ที่ ใช้ Microsoft Excel ทางลัดของ Windows (LNK) และไฟล์อิมเมจ ISO เป็นตัวหยด เพื่อปรับใช้มัลแวร์ เช่นEmotet , QBot , IcedID และ Bumblebee อุปกรณ์ของเหยื่อ แม้ว่าการโจมตีที่ตรวจพบในช่วงต้นเดือนเมษายนจะแสดงให้เห็นไฟล์ Excel ที่มีมาโคร XLM อย่างเด่นชัด การตัดสินใจของ Microsoft ในการบล็อกมาโครโดยค่าเริ่มต้นในช่วงเวลาเดียวกันนั้น กันว่าได้บังคับให้ผู้โจมตีเปลี่ยนไปใช้วิธีการอื่น เช่น HTML smuggling รวมถึงไฟล์ .LNK และ .ISO

เมื่อเดือนที่แล้ว Cyble ได้เปิดเผยรายละเอียดของเครื่องมือมัลแวร์ที่เรียกว่า Quantum ซึ่งขายในฟอรัมใต้ดิน เพื่อให้อาชญากรไซเบอร์มีความสามารถในการสร้างไฟล์ .LNK และ .ISO ที่เป็นอันตราย และเป็นที่น่าสังเกตว่ามาโคร ซึ่งเป็นการโจมตีที่ทดลองและทดสอบแล้วสำหรับคู่ต่อสู้ที่ต้องการปล่อยแรนซัมแวร์และมัลแวร์อื่นๆ ในระบบ Windows ไม่ว่าจะผ่านอีเมลฟิชชิ่งหรือวิธีการอื่น ๆ โดยต่อมา Microsoft ได้หยุดแผนการปิดการใช้งานมาโครของ Office ในไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตชั่วคราว โดยทางบริษัทแจ้งกับ The Hacker News ว่ากำลังใช้เวลาในการทำการเปลี่ยนแปลงเพิ่มเติมเพื่อเพิ่มความสามารถในการใช้งาน

ที่มาของข่าว : https://thehackernews.com/2022/07/hackers-exploiting-follina-bug-to.html