WinRAR (CVE-2023-38831) and Fudshell

อาจารย์ : ศ.ดร.จักรชัย โสอินทร์

SC362006

Information and Communication Tecnology Security

หลักการและเหตุผล

CVE-2023-38831 เป็นช่องโหว่ Zero day ที่เกิดขึ้นใน WinRAR เวอร์ชันก่อนหน้า 6.23 การทำงานของมันคือ เมื่อเหยื่อทำการเปิดไฟล์ .ZIP ทำให้ผู้โจมตีสามารถเข้าไปรันคำสั่งในเครื่องผ่านทาง Windows ShellExecute ได้ ซึ่งใช้หลักการ Spoof Extension เป็นการหลอกว่าไฟล์ข้างในเป็นไฟล์ปกติ และเมื่อคลิกเข้าไปจะทำการเปิดไฟล์mareware ของผู้โจมตี ซึ่งสามารถใช้ช่องโหว่นี้ได้ตั้งแต่WinRAR เวอร์ที่ต่ำกว่า 6.23

ขอบเขตการทำงาน

1.ทำการทดลองการทำงานของของช่องโหว่ Zeroday : WinRaR CVE-2023-38831
2.เพื่อศึกษาการทำงานของ Fudshell ที่ใช้หลักการ Reverse shell ฟนการเข้ายึดเครื่อง
3.การทดลองทำงานอยู่ใน VM เท่านั้นเพื่อความปลอดภัยของผู้ทดลอง

วัตถุประสงค์

1. เพื่อทำความเข้าใจเกี่ยวกับช่องโหว่ Zeroday ใน WinRAR (CVE-2023-38831) โดยละเอียดและวิเคราะห์แนวทางการโจมตีที่สามารถใช้งานช่องโหว่นี้ได้

2. พัฒนาการทดสอบและการจำลองเพื่อยืนยันช่องโหว่สร้างตัวอย่างการโจมตีเพื่อแสดงถึงความเสี่ยงที่เกิดจากช่องโหว่ เพื่อการศึกษา

3. พัฒนามาตรการป้องกันที่เข้มงวดเพื่อลดความเสี่ยงจากช่องโหว่ จัดทำแผนการปรับปรุงที่ชัดเจนเพื่อแก้ไขปัญหาและปรับปรุงความปลอดภัยของ WinRAR ในรุ่นที่มีช่องโหว่

วิธีการใช้งาน

1.เปิด Kali OS ขึ้นมา จากนั้นทำการเปิด port โดยใช้ nc -nvls 1337
2.จากนั้นทำการเปิด Server http เพื่อให้เหยื่อสามารถ download payload ได้โดยใช้คำสั่ง sudo python -m http.server 3000
3.สร้างPayload stub.ps1 จากโปรแกรม Fubshell และทำการ craft payload โดยใช้ช่องโหว่ WinRaR
4.วิธีการ Craft payload อย่างแรกเริ่มหาไฟล์ที่เราจะหลอกก่อนคือเราจะใช้ไฟล์ pdf
5.จากนั้นทำการสร้างสคลิปที่เป็น Payload
6.ทำการคลิกขวาที่ไฟล์ pdf จากนั้นกดที่ add to archive จากนั้นเลือกเป็นไฟล์ Zip
7.เลือกFiles และกดที่ append จากนั้นเลือก และกด OK
8.จากนั้นเข้าไปในไฟล์ของเราและกดคลิกขวาที่folder และกดrename จากนั้นเพิ่ม space ด้านหลังมา 1 ตัว และ Enter
9.ให้เหยื่อ Download จากเว็ปไซต์หลอก และเปิดไฟล์ pdf ผ่าน WinRaR โดยตรง
10.รอดู connection จากเหยื่อที่port 1337 ที่เราได้ทำการเปิดไว้จากนั้นเราจะสามารถ เข้าควบคุม cmd shell ของเครื่องเหยื่อได้

เครื่องมือที่ใช้งาน

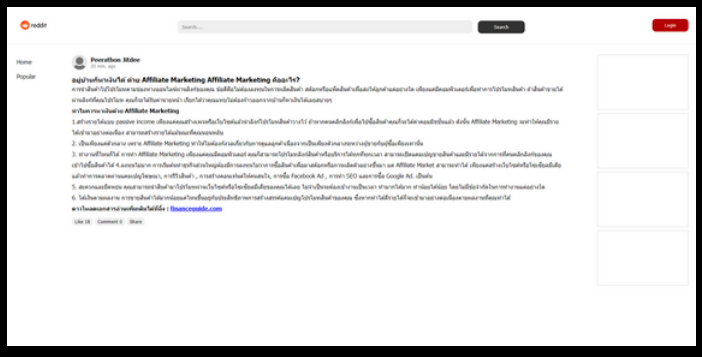
- Kali Linux
- Cloudflare
- Fudshell
- WinRaR
- virtualbox

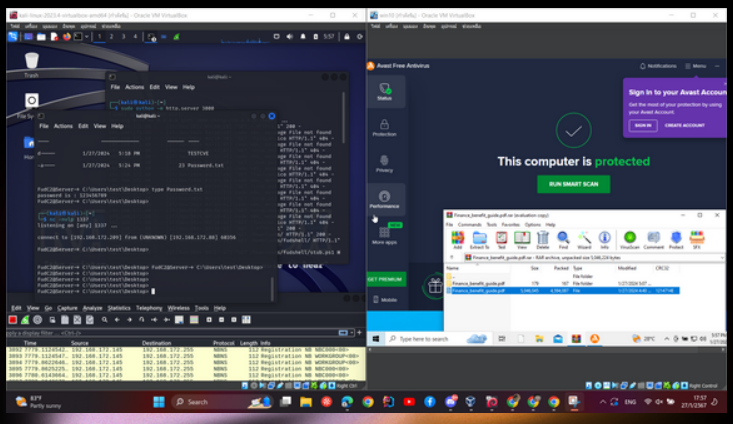
สรุปผลการดำเนินงาน

จากการทดลองเราสามารถเข้าควบคุมเครื่องเหยื่อจากช่องโหว่ cve-2023-38831 ของโปรแกรม WinRaR ได้ และเราได้ทำการโหลดตัว antivirus ชื่อ Avast มาและ Avast ไม่สามารถจับหาตัว Virus ของเราได้

สมาชิก

1. นางสาวชญาดา ภูสีดิน 653380004-4
2. นางสาวณัฐริกา โสมิตร 653380005-2
3. นายพีระพงศ์ เต้าประจิม. 653380008-6
4. นางสาวณัฐิยา แสนนา 653380090-5
5. นายพัชรพงษ์ พูนทรัพย์อมร 653380104-0
6. นายพิสิษฐ์ จินานิกร 653380105-8





อ้างอิง : https://github.com/machine1337/fudshell
https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/