Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính nâng cao

Kỳ báo cáo: Buổi 02 (Session 02)

Tên chủ đề: Malware

GV: Nguyễn Duy

Ngày báo cáo: 26/04/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT534.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
3	Nguyễn Bình Thục Trâm	20520815	20520815@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Kịch bản 01: Malware: theZoo	100%	
2	Kịch bản 02: Capa: Mal analysis	100%	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Cấu hình máy thực hiện:

Intel core i5 8250U 8th gen

SSD 500GB

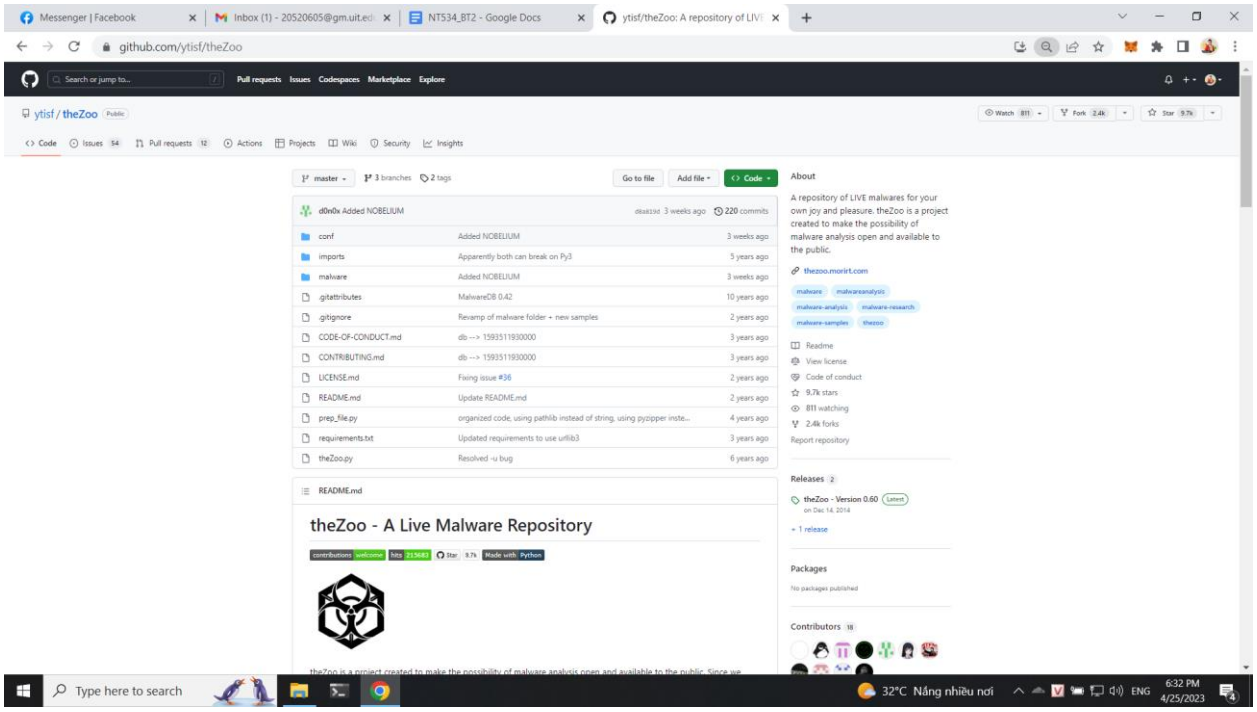
HDD 1000GB

RAM 16GB DDR3L

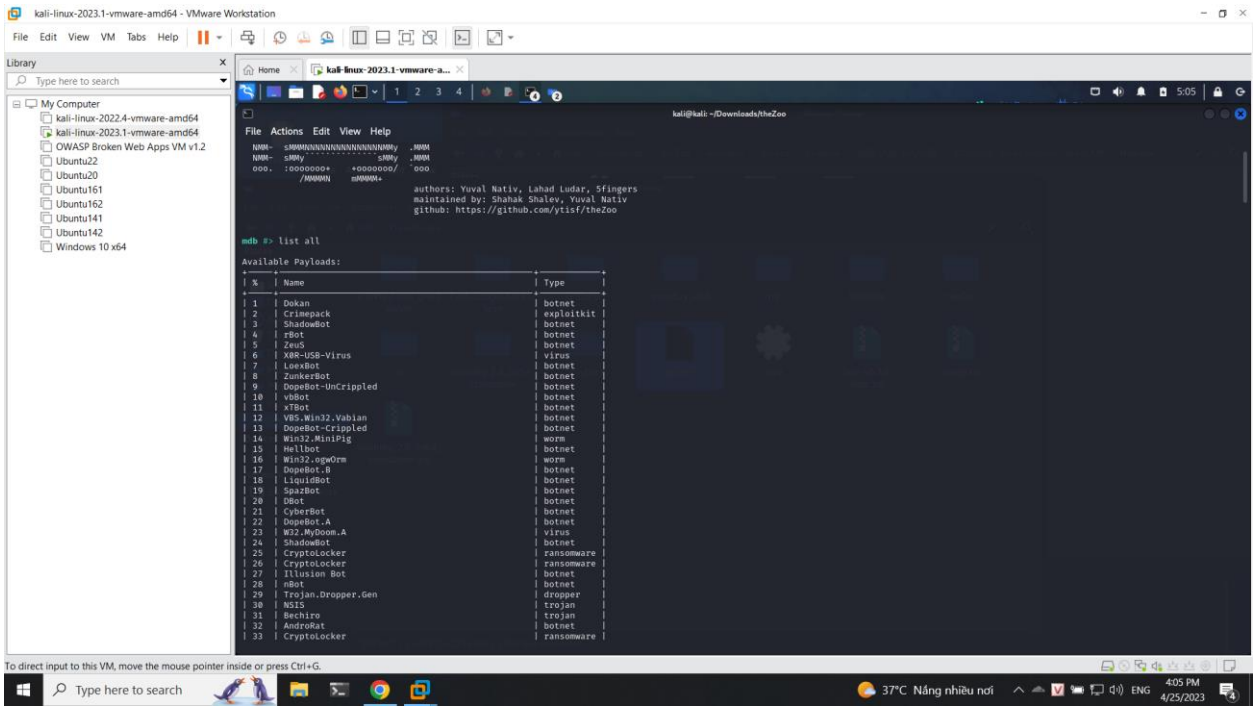
OS Kali Linux 2023.1

2. Kịch bản 1

Đầu tiên thực hiện clone repo theZoo để lấy mã độc



Tiếp theo thực hiện list các mã độc ra để xem

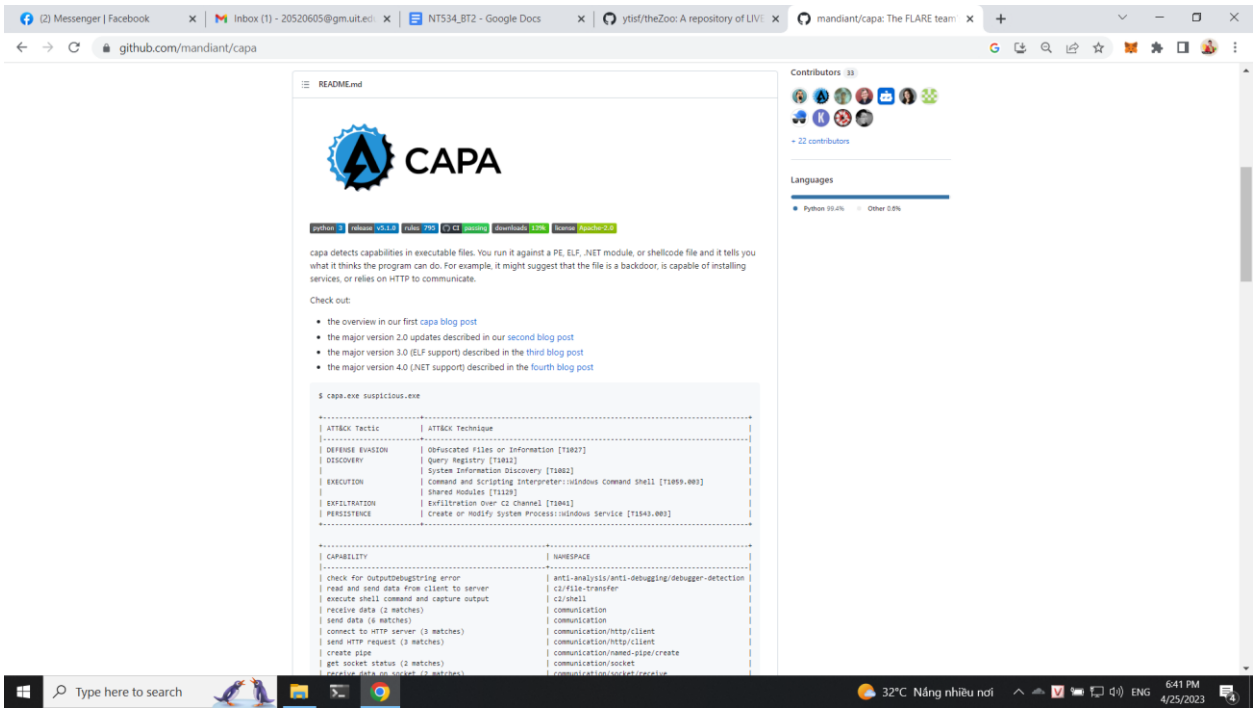


Với yêu cầu virus ta sẽ thực hiện 5 trường hợp virus bao gồm:

- Xor USB
- Viking Horde
- Anthrax
- Relock
- Whore

3. Kịch bản 2

Tool thực hiện kiểm tra, phân tích mã độc: Capa



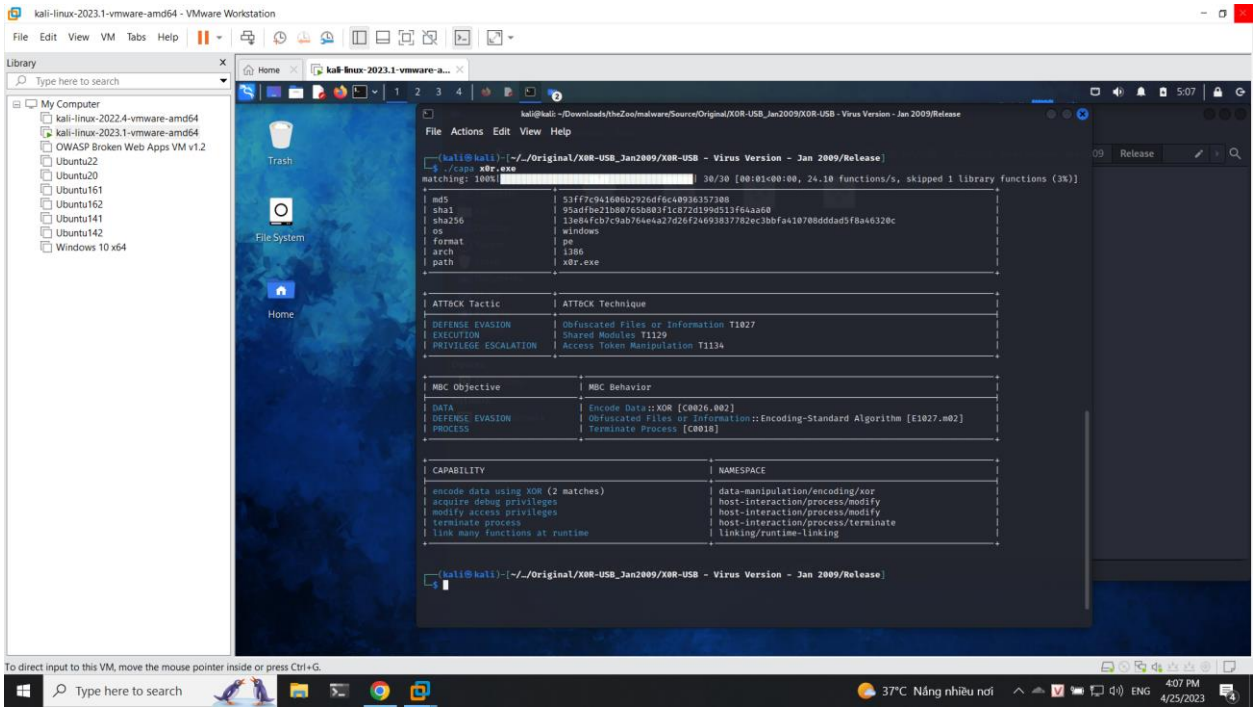
Đầu tiên ta sẽ tải Capa phiên bản standalone cho linux để thực hiện

Sau đó thực hiện quét

Với xor usb virus ta thấy được thông tin về kỹ thuật tấn công như obfuscate file, information, share module, access token manipulation. Ta thấy được các behavior như encode bằng xor, obfuscate file và terminal process

Cuối cùng ta thấy được các khả năng của virus:

- encode data using XOR (2 matches)
- acquire debug privileges
- modify access privileges
- terminate process
- link many functions at runtime



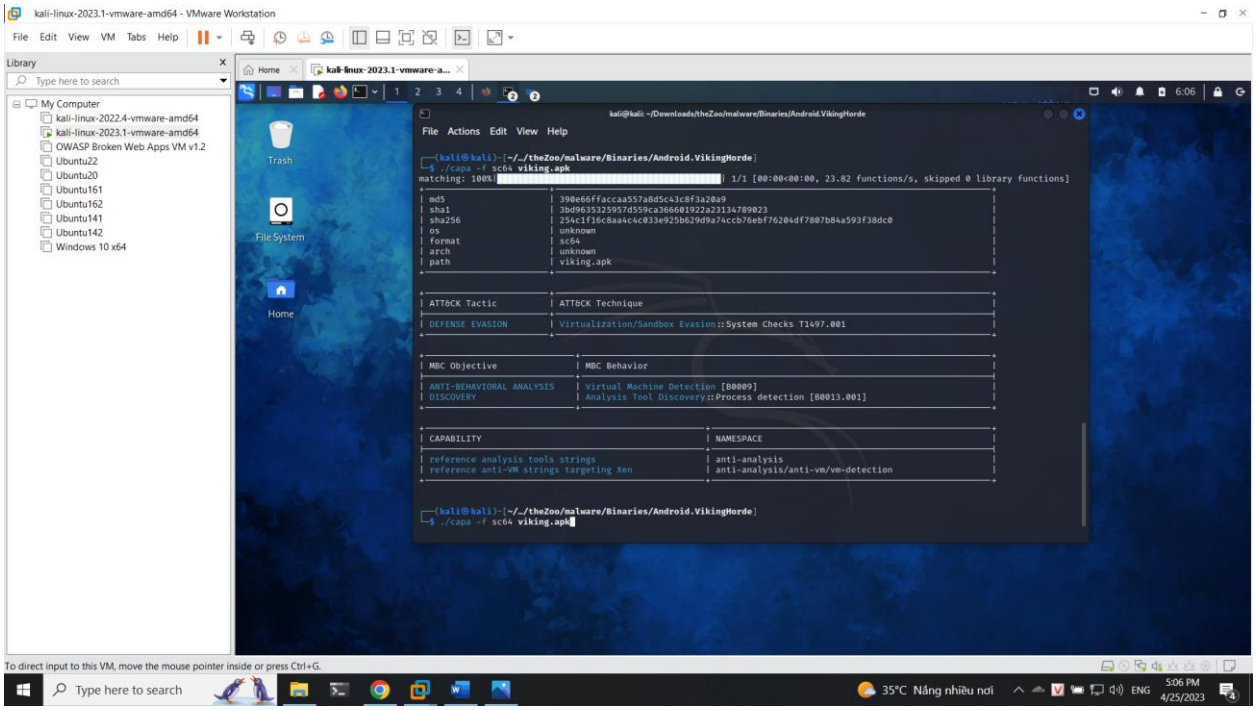
Ta có thể sử dụng thêm flag -vv để xem thêm thông tin

```
encode data using XOR (2 matches)
namespace  data-manipulation/encoding/xor
author     moritz.raabe@mandiant.com
scope      basic block
att&ck     Defense Evasion::Obfuscated Files or Information [T1027]
mbc        Defense Evasion::Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02], Data::Encode Data::XOR
[C0026.002]
basic block @ 0x4013B8 in function 0x401385
  and:
    characteristic: tight loop @ 0x4013B8
    characteristic: nzxor @ 0x4013C5
    not: = filter for potential false positives
      or:
        or: = unsigned bitwise negation operation (~i)
          number: 0xFFFFFFFF = bitwise negation for unsigned 32 bits
          number: 0xFFFFFFFFFFFFFFFF = bitwise negation for unsigned 64 bits
        or: = signed bitwise negation operation (~i)
          number: 0xFFFFFFF = bitwise negation for signed 32 bits
          number: 0xFFFFFFFFFFFFFFF = bitwise negation for signed 64 bits
        or: = Magic constants used in the implementation of strings functions.
          number: 0x7EFEFEFF = optimized string constant for 32 bits
          number: 0x81010101 = -0x81010101 = 0x7EFEFEFF
          number: 0x81010100 = 0x81010100 = ~0x7EFEFEFF
          number: 0x7EFEFEFEFEFEFEFF = optimized string constant for 64 bits
          number: 0x8101010101010101 = -0x8101010101010101 = 0x7EFEFEFEFEFEFEFF
          number: 0x8101010101010100 = 0x8101010101010100 = ~0x7EFEFEFEFEFEFEFF
basic block @ 0x402C5B in function 0x402C2B
  and:
    characteristic: tight loop @ 0x402C5B
    characteristic: nzxor @ 0x402C67
    not: = filter for potential false positives
      or:
        or: = unsigned bitwise negation operation (~i)
          number: 0xFFFFFFFF = bitwise negation for unsigned 32 bits
          number: 0xFFFFFFFFFFFFFFFF = bitwise negation for unsigned 64 bits
        or: = signed bitwise negation operation (~i)
          number: 0xFFFFFFF = bitwise negation for signed 32 bits
          number: 0xFFFFFFFFFFFFFFF = bitwise negation for signed 64 bits
        or: = Magic constants used in the implementation of strings functions.
          number: 0x7EFEFEFF = optimized string constant for 32 bits
          number: 0x81010101 = -0x81010101 = 0x7EFEFEFF
          number: 0x81010100 = 0x81010100 = ~0x7EFEFEFF
```

Tiếp tục với virus Viking Horde thì ta thấy được virus này có các hành vi:

- Phát hiện máy ảo
- Phát hiện các công cụ phân tích mã độc

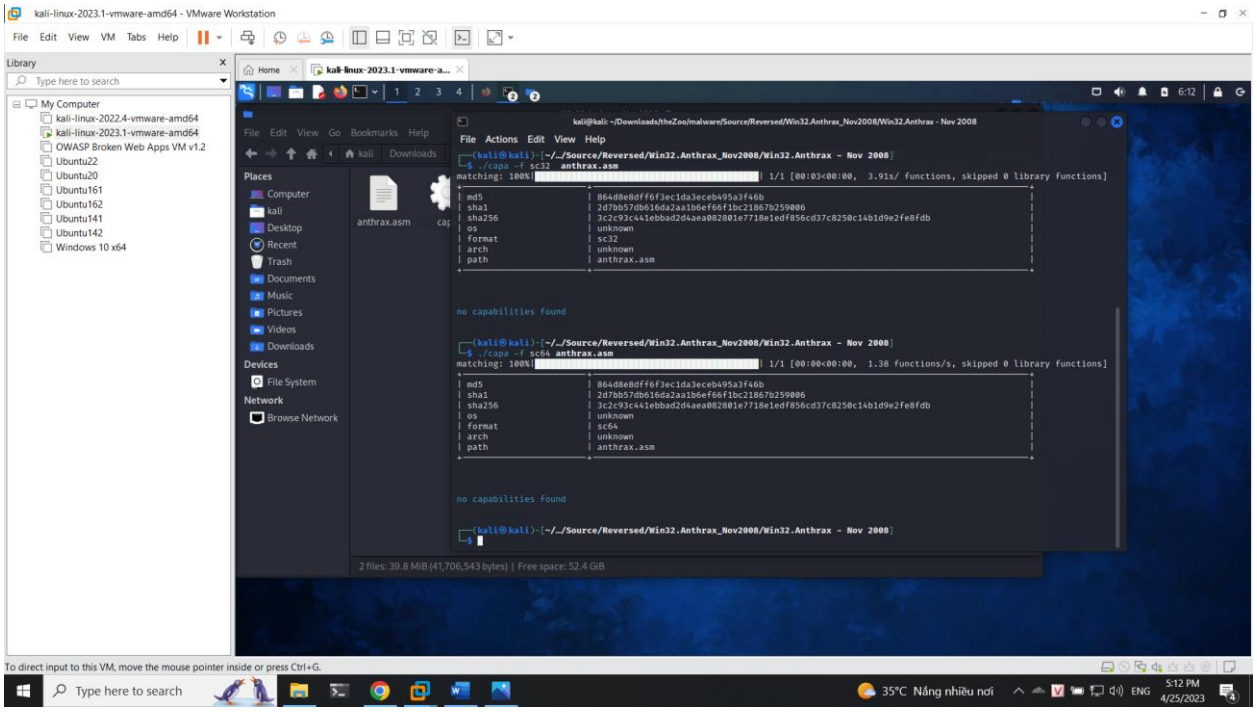
Ngoài ra cũng có các kỹ thuật tấn công được cung cấp là sandbox evasion



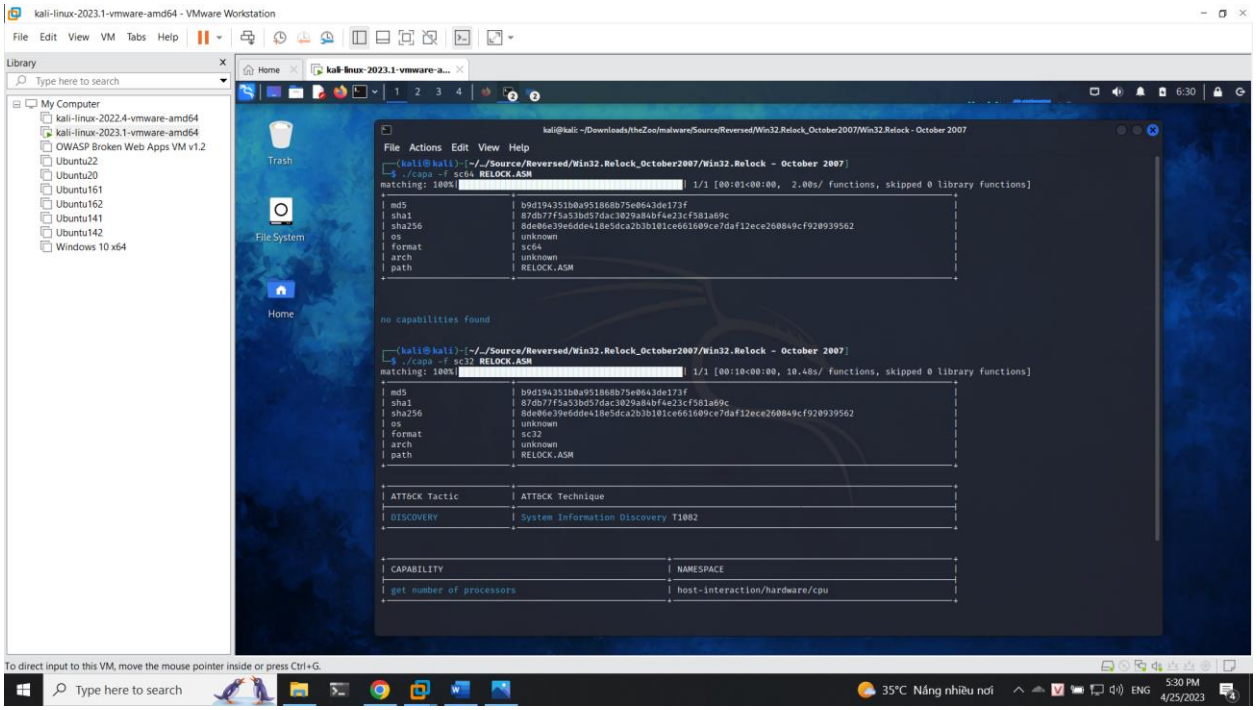
Sử dụng thêm flag -vv

```
contain loop (library rule)
author  moritz.raabe@mandiant.com
scope   function
function @ 0x690000
  or:
    characteristic: loop @ 0x690000

reference analysis tools strings
namespace   anti-analysis
author      michael.hunhoff@mandiant.com
scope       file
mbc         Discovery::Analysis Tool Discovery::Process detection [B0013.001]
references  https://github.com/LordNoteworthy/al-khaser/blob/master/al-khaser/AntiAnalysis/process.cpp
or:
  regex: /ida[gqtuw]?(\.exe)?$/i
    - " klaida" @ file+0x34A100
    - "$8IDAT" @ file+0x705226
    - ".8IDAT" @ file+0x2A89B6
    - "IDAT" @ file+0x13B939, file+0x13D945, file+0x13F951, file+0x143969, and 7 more ...
    - "RIDAT" @ file+0x2C86C0
    - "Tinklo klaida" @ file+0x34A12A
    - "gIDAT" @ file+0x203E78
    - "lida" @ file+0x349359, file+0x34A75F, file+0x35F130

reference anti-VM strings targeting Xen
namespace   anti-analysis/anti-vm/vm-detection
author      michael.hunhoff@mandiant.com
scope       file
attck       Defense Evasion::Virtualization/Sandbox Evasion::System Checks [T1497.001]
mbc         Anti-Behavioral Analysis::Virtual Machine Detection [B0009]
references  https://github.com/LordNoteworthy/al-khaser/blob/master/al-khaser/AntiVM/Xen.cpp
or:
  regex: /^Xen/i
    - "XENV@" @ file+0x4DC390
```

Tiếp tục với virus Anthrax thì ta không thấy có thông tin được cung cấp



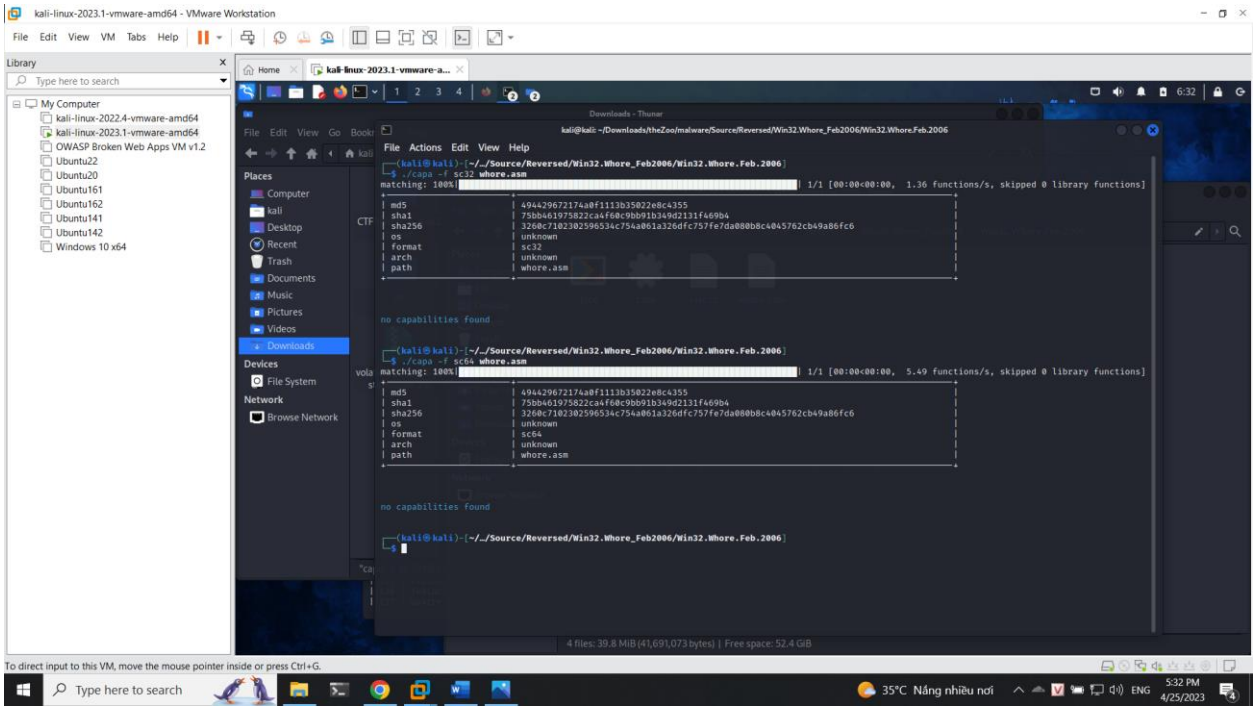
Tiếp tục với virus relock thì ta thấy được thông tin chính là virus có khả năng thực hiện get number of processor và kỹ thuật tấn công được cung cấp là System Info Discovery



Thêm flag -vv để xem

```
PEB access (library rule)
author      michael.hunhoff@mandiant.com
scope       basic block
mbc         Anti-Behavioral Analysis::Debugger Detection::Process Environment Block [B0001.019]
references  https://github.com/LordNoteworthy/al-khaser/blob/master/al-khaser/AntiDebug/NtGlobalFlag.cpp
basic block @ 0x69948A in function 0x690000
  or:
    and:
      arch: i386
      characteristic: fs access @ 0x69948A
      or:
        offset: 0x30 @ 0x6994A9

get number of processors
namespace   host-interaction/hardware/cpu
author      michael.hunhoff@mandiant.com, anushka.virgaonkar@mandiant.com
scope       function
att&ck      Discovery::System Information Discovery [T1082]
references  https://github.com/LordNoteworthy/al-khaser/blob/bed03d2f849d9060c68f8d5905bd204d0cb3f593/al-khaser/AntiVM/Generi
c.cpp#L361
function @ 0x690000
  or:
    and:
      match: PEB access @ 0x69948A
        or:
          and:
            arch: i386
            characteristic: fs access @ 0x69948A
            or:
              offset: 0x30 @ 0x6994A9
      or:
        and:
          arch: i386
          number: 0x64 = PEB->NumberOfProcessors @ 0x69111F, 0x698165, 0x69826A, 0x698345, and 8 more ...
```

Cuối cùng với virus whore thì ta thấy được thông tin không được cung cấp như virus Anthrax



Kết luận

theZoo cung cấp được một lượng lớn malware cho phép thực hiện công việc học tập nghiên cứu

Capa là một ứng dụng hỗ trợ một phần công việc cho việc phân tích mã độc nhằm phục vụ học tập nghiên cứu

Hạn chế:

theZoo chỉ cung cấp known mal và unknown mal chưa cung cấp được advanced mal

Capa vẫn còn nhiều hạn chế trong việc phân tích mã độc (do kết quả thực nghiệm đã không cung cấp được một số trường hợp, hoặc chạy ra kết quả sai ở một số trường hợp)

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT