BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC

THÀNH PHỐ HỒ CHÍ MINH

ĐỒ ÁN MÔN HỌC

PHÂN TÍCH MALWARE

Nguyễn Công Khang - 21DH110770

Phạm Đức Thiên Phúc - 21DH112813

GVGD: Th.S Phạm Đình Thắng

LỜI MỞ ĐẦU

Hiện nay khoa học kỹ thuật ngày càng phát triển, an toàn thông tin là yếu tố quan trọng được đặt lên hàng đầu trong thời điểm hiện nay. Điển hình trong năm 2023, Việt Nam đã chịu ảnh hưởng nặng nề bởi 59837 vụ tấn công dữ liệu.

Môn học Phân tích Malware này đã giúp chúng em nắm vững kiến thức và kỹ năng cơ bản trong hoạt động của Malware, cách nhận diện, phân loại và kỹ thuật Malware lây nhiễm vào hệ thống.

Chúng em rất cảm ơn thầy Th.S Phạm Đình Thắng đã giúp em hoàn thành báo cáo này.

MỤC LỤC

Chương 1: Cơ sở lí thuyết

I. Warzone RAT là gì?

Warzone RAT (hay còn gọi là Ave Maria) là một trojan truy cập từ xa (RAT) được bán dưới dạng phần mềm độc hại dịch vụ (MaaS) lần đầu tiên được phát hiện vào tháng 1 năm 2019 và nhanh chóng trở nên phổ biến để trở thành một loại phần mềm độc hại hàng đầu vào năm 2020. Tải trọng của Warzone bao gồm nhiều chức năng, nhưng mục đích chính của nó là đánh cắp thông tin. Nó có khả năng ẩn náu và chống phân tích tiên tiến và đã được triển khai bằng cách sử dụng một loạt các kỹ thuật thả rộng.

Warzone ngụy trang thành một công cụ quản trị IT thương mại hợp pháp được bán và duy trì bởi một nhân vật trực tuyến tên là Solmyr. Trang web chính thức của nó là nơi các gói cơ bản được bán với giá 37,95 đô la mỗi tháng - rẻ hơn nhiều so với các loại MaaS hàng đầu khác. Warzone có sẵn dưới dạng giấy phép 1 tháng, 3 tháng và 12 tháng với dịch vụ Dynamic Domain Name System (DDNS) tùy chọn và có phiên bản "Poison" bao gồm mô-đun cài đặt rootkit. DDNS được sử dụng trong các cuộc tấn công mạng để ẩn vị trí của các máy chủ command-and-control (C2) được sử dụng bởi các nhà vận hành phần mềm độc hại. Các phiên bản Warzone bị crack cũng có thể được tìm thấy trên các diễn đàn darknet, và loại này có các video hướng dẫn trên YouTube để học cách triển khai cơ bản và quản trị command-and-control (C2).

Một số chiến dịch tác động nhất của Warzone bao gồm các mục tiêu địa chính trị như xâm phạm nhân viên chính phủ và quân đội của Trung tâm Tin học Quốc gia (NIC) của Ấn Độ và việc nó được nhóm Confucius APT sử dụng chống lại chính phủ Trung Quốc đại lục và các quốc gia Nam Á khác. Warzone cũng đã được sử dụng trong một chiến dịch lừa đảo tinh vi giả mạo thông tin liên lạc chính thức của chính phủ để phân phối phần mềm độc hại ở Hungary.

II. Phạm vi tấn công

Truy cập máy tính từ xa qua VNC, shell từ xa và quản lý tệp từ xa

Truy cập máy tính từ xa ẩn qua RDPWrap và máy tính mạng ảo ẩn (hVNC)

Giám sát các tiến trình hệ thống

Khai thác leo thang đặc quyền thông qua bỏ qua UAC

Ghi lại webcam của hệ thống bị nhiễm

Đánh cắp thông tin đăng nhập từ các trình duyệt và ứng dụng email phổ biến, bao gồm Chrome, Firefox, IE, Edge, Outlook, Thunderbird, Foxmail

Nhập và thực thi các tải trọng phần mềm độc hại bổ sung

Ghi nhật ký bàn phím thời gian thực

Bỏ qua Windows Defender

III. Phương thức hoạt động

Warzone đã được phân phối qua một số lượng gần như vô tận các vector lây nhiễm ban đầu nhưng được bán chính thức dưới hai cấu hình giai đoạn đầu khác biệt; dưới dạng một macro nhúng trong Microsoft Office hoặc được đóng gói dưới dạng tải trọng được nén và mã hóa để vượt qua sự phát hiện của phần mềm chống vi-rút. Tuy nhiên, ngoài các chế độ chính thức, Warzone được triển khai qua cả malspam và các chiến dịch lừa đảo nhắm mục tiêu sử dụng:

- Các trang web WordPress bị hack và các dịch vụ lưu trữ tệp phổ biến như archive.org và discord.com để lưu trữ tải trọng
- Các tệp tự giải nén (SFX) định dạng .rar và .zip, và .iso với các biểu tượng tệp giả được thiết kế giống như các ứng dụng phần mềm phổ biến
- Macro Microsoft Office sử dụng kỹ thuật VBA-stomping biên dịch macro nhúng thành mã P để tránh sự phát hiện của các sản phẩm chống vi-rút
- Một trình tải .net viết bằng C# sử dụng RunPE.dll để chiếm đoạt, làm rỗng và tiêm Warzone vào quy trình InstallUtil.exe
- Sử dụng ngôn ngữ kịch bản Windows AutoIt để triển khai tải trọng Warzone
- Các lỗ hổng đã biết như CVE-2017-11882 và CVE-2018-0802

Warzone duy trì sự tồn tại trên máy chủ mục tiêu bằng cách tạo ra một khóa registry Windows—thường có tên là HKLM\SOFTWARE Wow6432Node\Microsoft Windows\CurrentVersion\Run—và thiết lập giá trị của nó thành vị trí của tệp thực thi Warzone. Cuối cùng, Warzone có thể khai thác leo thang đặc quyền bằng cách sử dụng kỹ thuật chiếm đoạt DLL cũ để bỏ qua UAC.

IV. Dấu hiện nhận biết các cuộc tấn công

Các nhà nghiên cứu mối đe dọa đã công bố các quy tắc YARA và Sigma để xác định các trình thả được sử dụng trong các cuộc tấn công Warzone. Tuy nhiên, các chỉ báo thỏa hiệp (IOCs) đáng tin cậy nhất liên quan đến Warzone liên quan đến cách phần mềm độc hại này thiết lập kết nối với các điểm cuối C2 và tạo ra

các khóa registry riêng biệt để duy trì sự tồn tại. Các nhà nghiên cứu mối đe dọa đã công bố các quy tắc YARA và Sigma để xác định các trình thả được sử dụng trong các cuộc tấn công Warzone. Tuy nhiên, các chỉ báo thỏa hiệp (IOCs) đáng tin cậy nhất liên quan đến Warzone liên quan đến cách phần mềm độc hại này thiết lập kết nối với các điểm cuối C2 và tạo ra các khóa registry riêng biệt để duy trì sự tồn tại.

Chương 2: Phân tích Malware

I. Phân tích cơ bản

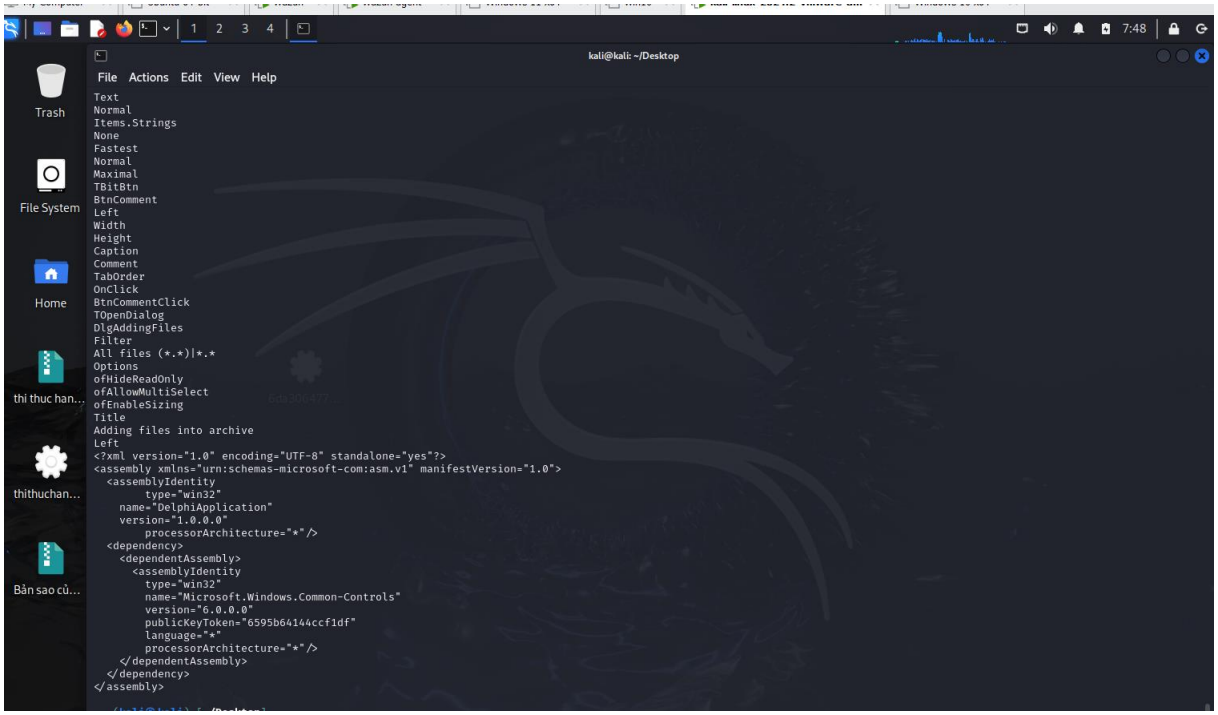
SHA256(đảm bảo tính toàn vẹn và bảo mật của dữ liệu, do tính chất không thể đảo ngược và tính duy nhất của nó) của nó là :

6da3064773edf094f014b7aa13f2e3f74634f62552a91f88bf306f962bbf0563

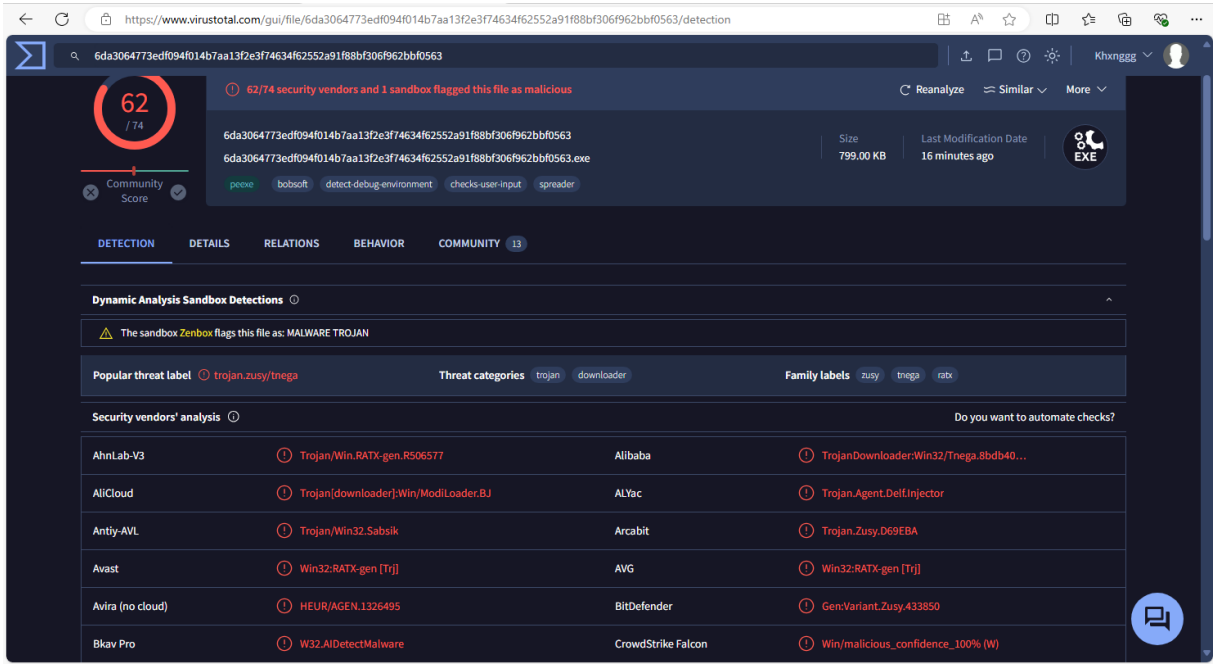
Ta có thể phân tích dễ dàng bằng lệnh:

malwoverview.py -b 5 -B 6da3064773edf094f014b7aa13f2e3f74634f62552a91f88bf306f962bbf0563 -o 0

Tiến hành kiểm tra strings của file malware



Ta cũng có thể có được thông tin của nó bằng cách kiểm tra thông tin trên VirusTotal:



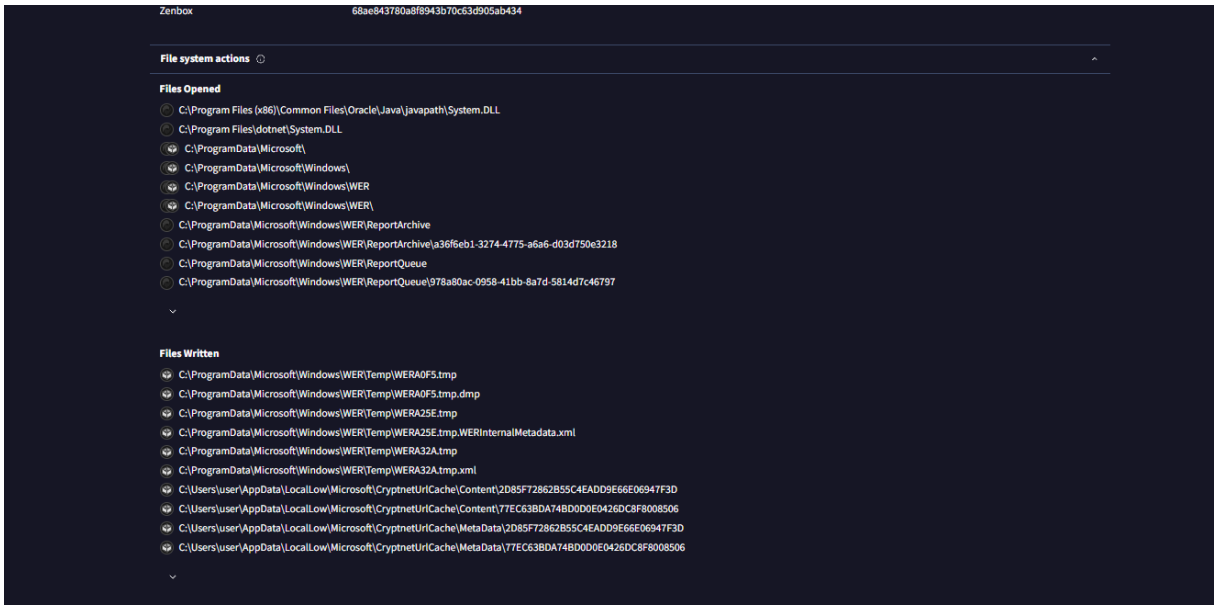
Dưới đây là tổng hợp chi tiết hành vi của tệp tin từ trang VirusTotal:

- **Hoạt động mạng**:

Tệp tin đã cố gắng kết nối với nhiều miền và địa chỉ IP, bao gồm các miền độc hại và IP không xác định(bao gồm cả c2 server)

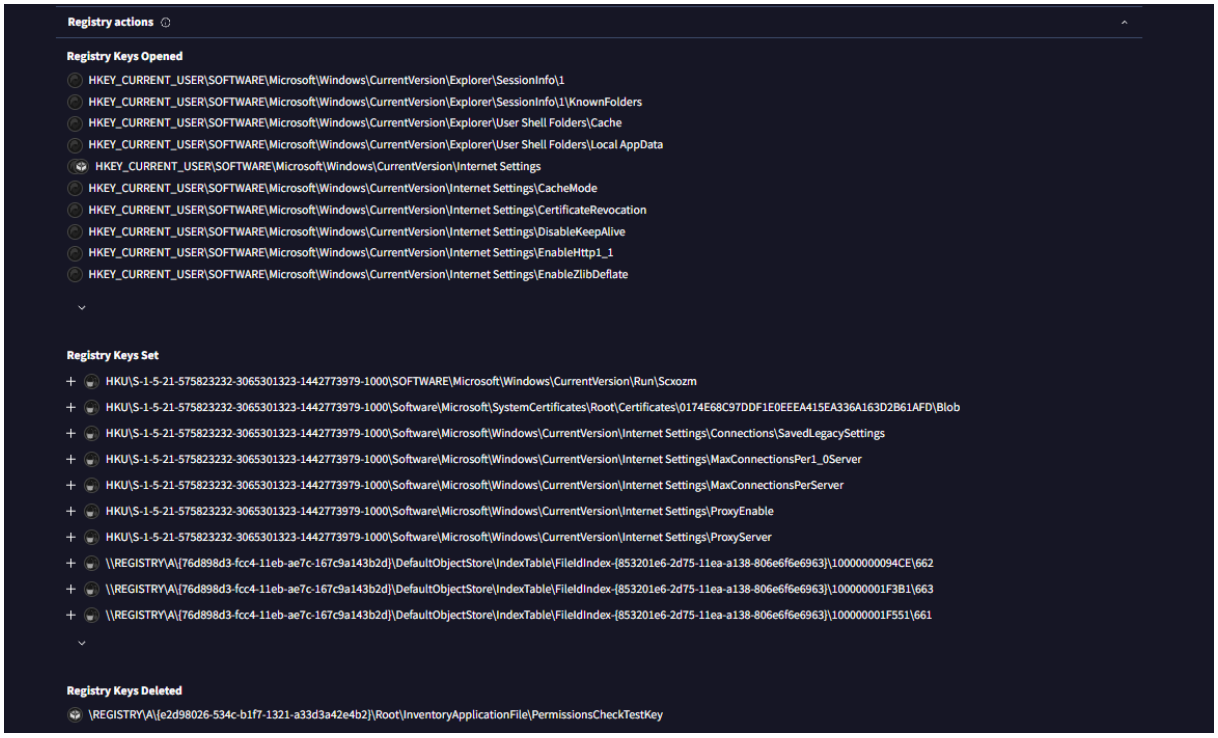
- **Hoạt động hệ thống tệp**:

Tạo, đọc, viết và xóa file trong các thư mục tạm thời của hệ điều hành, cũng như can thiệp vào registry để thiết lập sự hiện diện của nó.

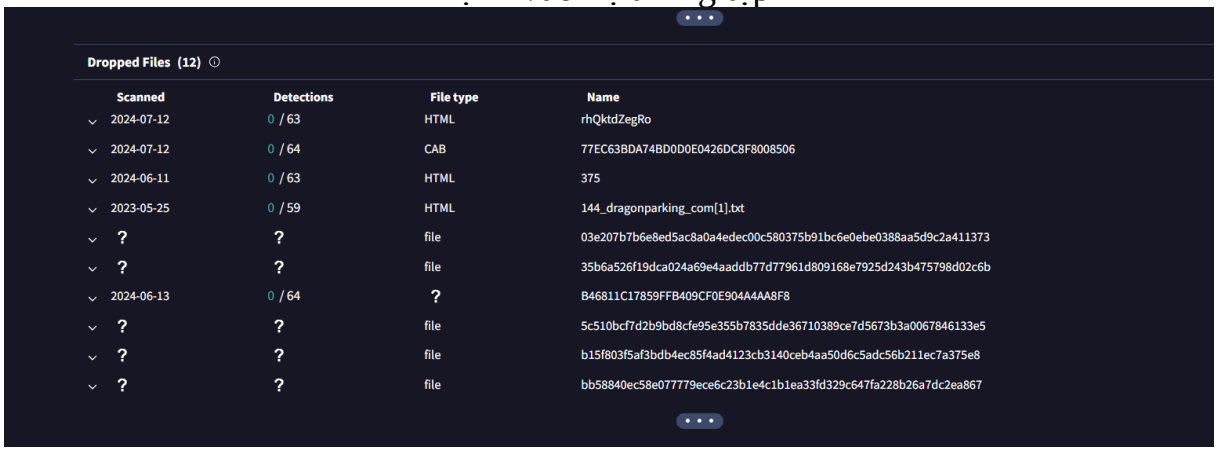


- **Hoạt động registry**:

Tệp tin đã thực hiện thay đổi trong registry của hệ thống, bao gồm việc thêm, sửa đổi hoặc xóa các khóa registry.

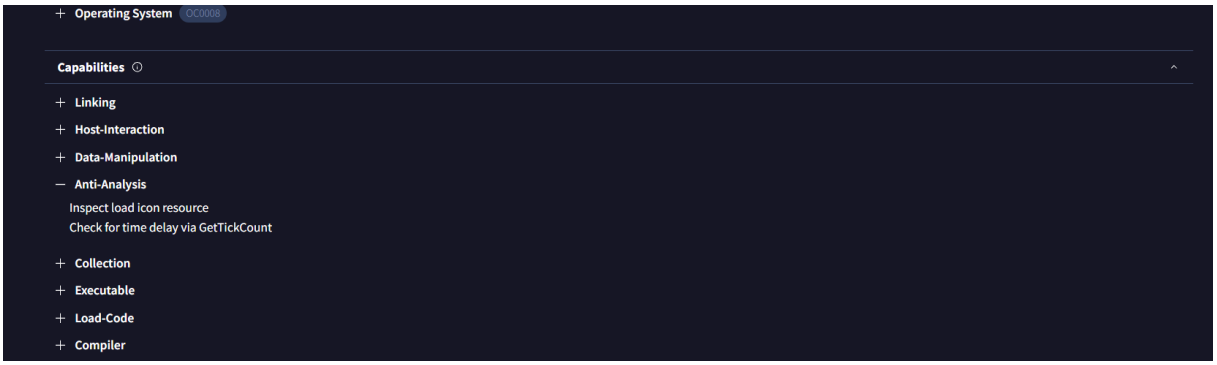


Nó có thể có chức năng tải xuống và cuối cùng, thả tệp nhị phân hoặc thậm chí tập lệnh vào hệ thống tệp



- **Chống phân tích (Anti-Analysis)**

Malware có khả năng phát hiện và tránh bị phân tích, ví dụ như kiểm tra xem nó có đang chạy trong môi trường debug hay không.



Khi ta bỏ malware vào cuckoo sanbox thì dựa vào behavior analysis

Ta có thể thấy port kết nối của malware hoạt động từ khoảng 49240 -> 49250

getsockname July 21, 2024, 9:25 p.m.	s: 952 ip_address: 192.168.168.220 port: 49240	1	0	0
getsockname July 21, 2024, 9:25 p.m.	s: 780 ip_address: 192.168.168.220 port: 49241	1	0	0
getsockname July 21, 2024, 9:25 p.m.	s: 784 ip_address: 192.168.168.220 port: 49244	1	0	0
getsockname July 21, 2024, 9:25 p.m.	s: 1540 ip_address: 192.168.168.220 port: 49247	1	0	0
getsockname July 21, 2024, 9:25 p.m.	s: 1488 ip_address: 192.168.168.220 port: 49248	1	0	0
setsockopt July 21, 2024, 9:25 p.m.	buffer: optname: 28688 socket: 1564 level: 65535	1	0	0
getsockname July 21, 2024, 9:25 p.m.	s: 1564 ip_address: 192.168.168.220 port: 49249	1	0	0

Network analysis cho ta thấy phân tích sau:

Network Analysis

Download pcap

Hosts 0 | DNS 0 | TCP 0 | UDP 0 | HTTP 0 | ICMP 0 | IRC 0 | Suricata | Snort

Suricata Alerts

Flow	SID	Signature	Category
TCP 192.168.168.220:49248 -> 172.67.168.124:80	2850263	ETPRO MALWARE MalDoc Downloader User-Agent	A Network Trojan was detected
TCP 192.168.168.220:49249 -> 188.114.96.1:80	2850263	ETPRO MALWARE MalDoc Downloader User-Agent	A Network Trojan was detected
TCP 38.150.25.58:443 -> 192.168.168.220:49250	2025194	ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.xyz)	Potentially Bad Traffic
TCP 192.168.168.220:49248 -> 172.67.168.124:80	2850263	ETPRO MALWARE MalDoc Downloader User-Agent	A Network Trojan was detected
TCP 192.168.168.220:49252 -> 172.67.168.124:80	2037828	ET USER_AGENTS Suspicious User-Agent (56)	A Network Trojan was detected

Suricata TLS

Flow	Issuer	Subject	Fingerprint
TLS 1.2 192.168.168.220:49240 172.67.168.124:443	C=US, O=Google Trust Services, CN=WE1	CN=morientlines.com	33:61:2a:33:07:5a:18:1f:4c:c3:b6:92:5e:de:24:0e:04:4e:66:95
TLS 1.2 192.168.168.220:49250 38.150.25.58:443	C=US, O=Let's Encrypt, CN=R10	CN=hemnz.xyz	79:27:6e:12:a0:09:2c:bb:0f:2d:62:42:d6:70:2c:fd:f5:27:c8:23

Start

Ý Nghĩa và Giải Thích:

Kết nối tới morientlines.com và **hemnz.xyz**:

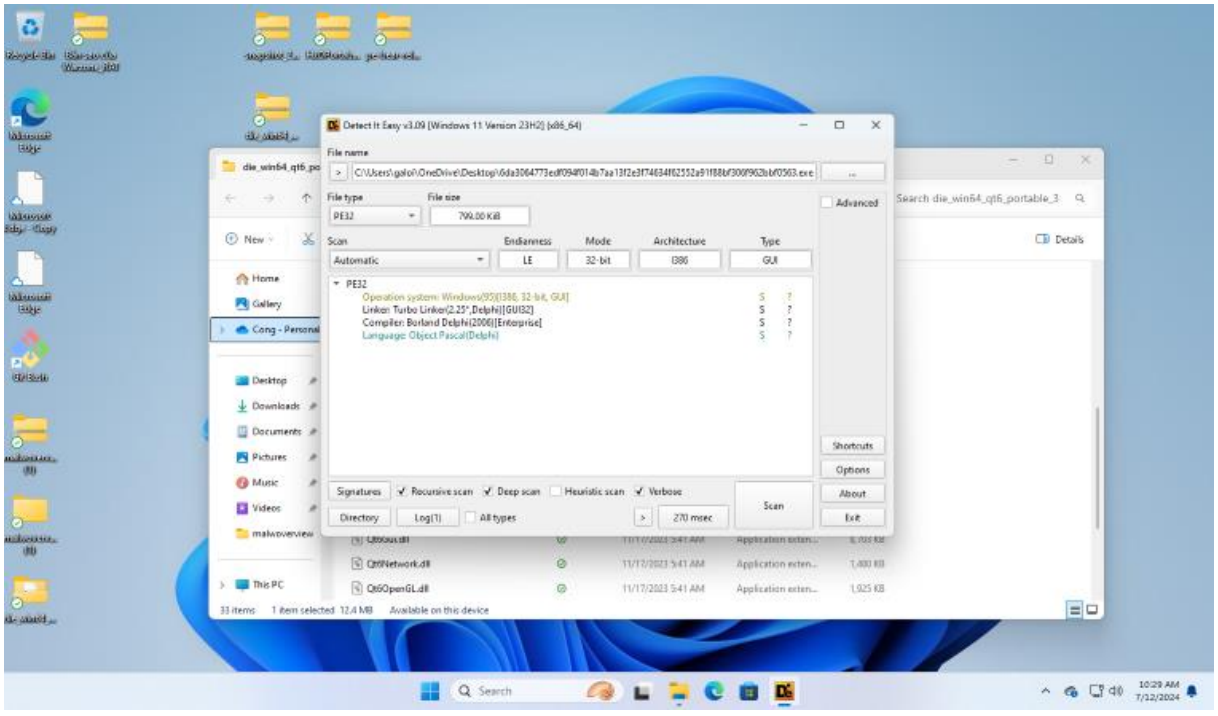
- Đảm bảo rằng các tên miền này không liên quan đến hoạt động độc hại hoặc phần mềm độc hại. Các tên miền này có thể là các máy chủ điều khiển(C2 Server) hoặc các máy chủ tấn công mà phần mềm độc hại kết nối tới.

Các kết nối khác nhau: Các cổng kết nối (49240, 49250) và địa chỉ IP nguồn (192.168.168.220) cho thấy rằng phần mềm độc hại có thể đang thực hiện nhiều kết nối tới các máy chủ khác nhau, có thể để gửi dữ liệu hoặc nhận lệnh từ các máy chủ điều khiển.

Chứng chỉ SSL/TLS khác nhau: Việc sử dụng chứng chỉ từ các nhà cung cấp khác nhau (Google Trust Services và Let's Encrypt) có thể cho thấy phần mềm độc hại đang cố gắng che giấu hoặc làm cho các kết nối của nó trông hợp pháp hơn.

II. Tiến hành giải nén và phân tích

Đầu tiên, chúng ta phải giải nén phần mềm độc hại. Trước khi thực hiện giải nén, bạn nên kiểm tra nó bằng DiE:



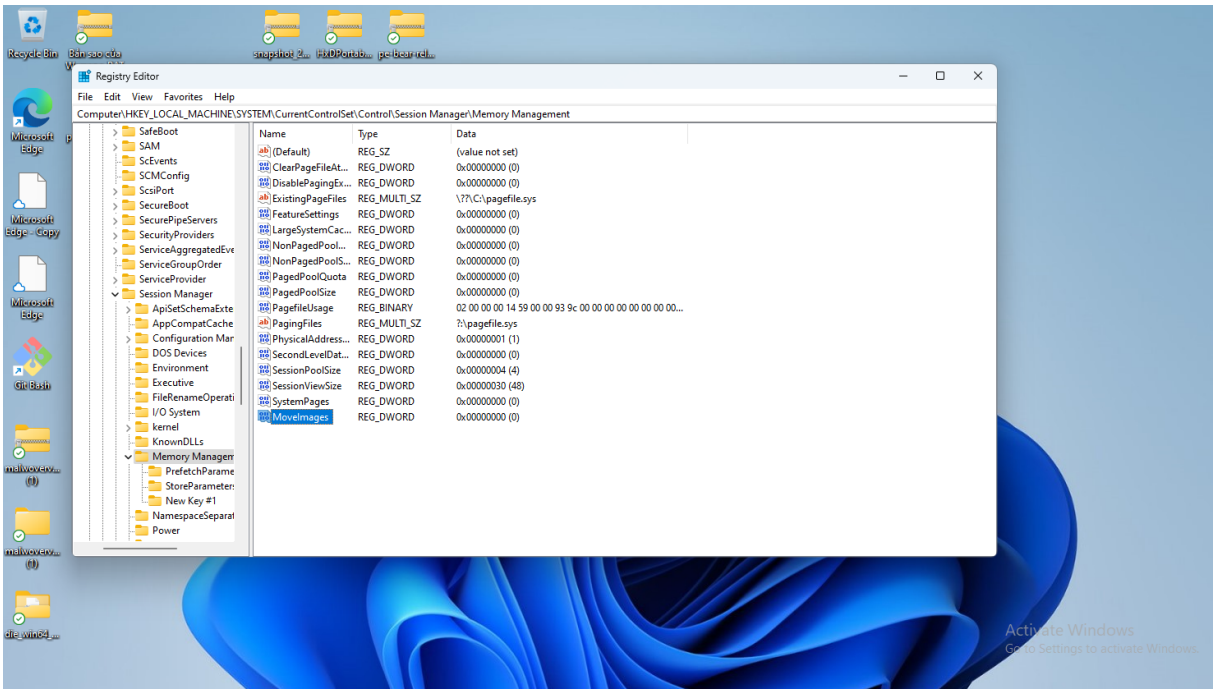
Theo kết quả đầu ra ở trên, nó là tệp nhị phân 32 bit có thể thực thi được và được biên dịch bằng Borland Dephi. Có những trình đóng gói phần mềm độc hại sử dụng trình biên dịch Borland Dephi để che giấu phần mềm độc hại thực sự bên trong mẫu ban đầu và có thể trường hợp này là như vậy.

Borland Delphi là một môi trường phát triển tích hợp (IDE) được sử dụng để lập trình ứng dụng, chủ yếu bằng ngôn ngữ lập trình Object Pascal. Borland Delphi có thể có một số ứng dụng trong việc phát triển malware:

- **Tích hợp hệ thống**: Với khả năng truy cập vào API của Windows, Delphi có thể tương tác trực tiếp với hệ điều hành, cho phép thực hiện các hoạt động ẩn danh.
- **Biên dịch thành mã máy**: Mã được biên dịch từ Delphi có thể tạo ra các executable nhỏ gọn và có thể được tối ưu hóa để tránh bị phát hiện bởi phần mềm diệt virus.
- **Thư viện phong phú**: Delphi cung cấp nhiều thư viện hỗ trợ việc phát triển các tính năng như mã hóa, mạng, và xử lý file, hữu ích cho việc xây dựng các chức năng của malware.

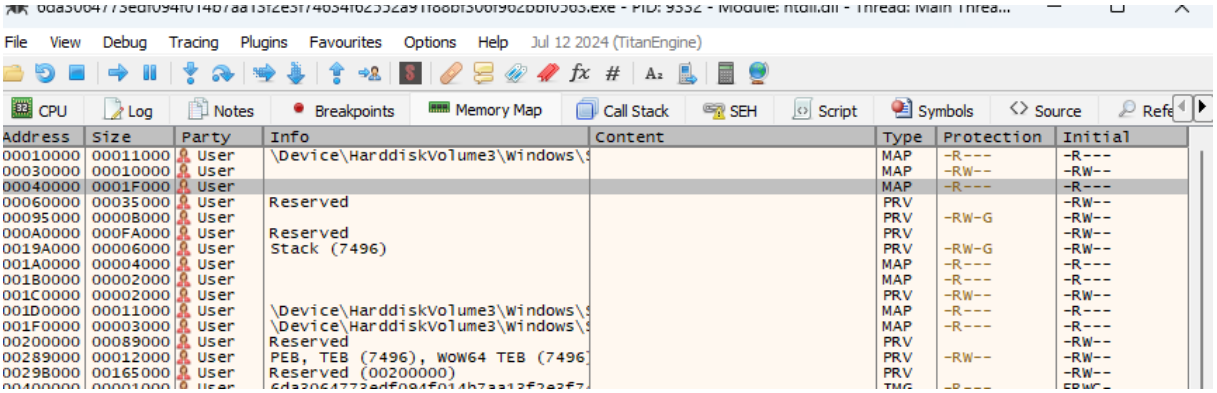
Bước tiếp theo là vô hiệu hóa ASLR cho toàn bộ hệ thống hoặc thậm chí đối với nhị phân cụ thể.

ASLR (Address Space Layout Randomization) là một kỹ thuật bảo mật được sử dụng để ngăn chặn các cuộc tấn công lợi dụng lỗi phần mềm bằng cách ngẫu nhiên hóa các địa chỉ không gian bộ nhớ của tiến trình.



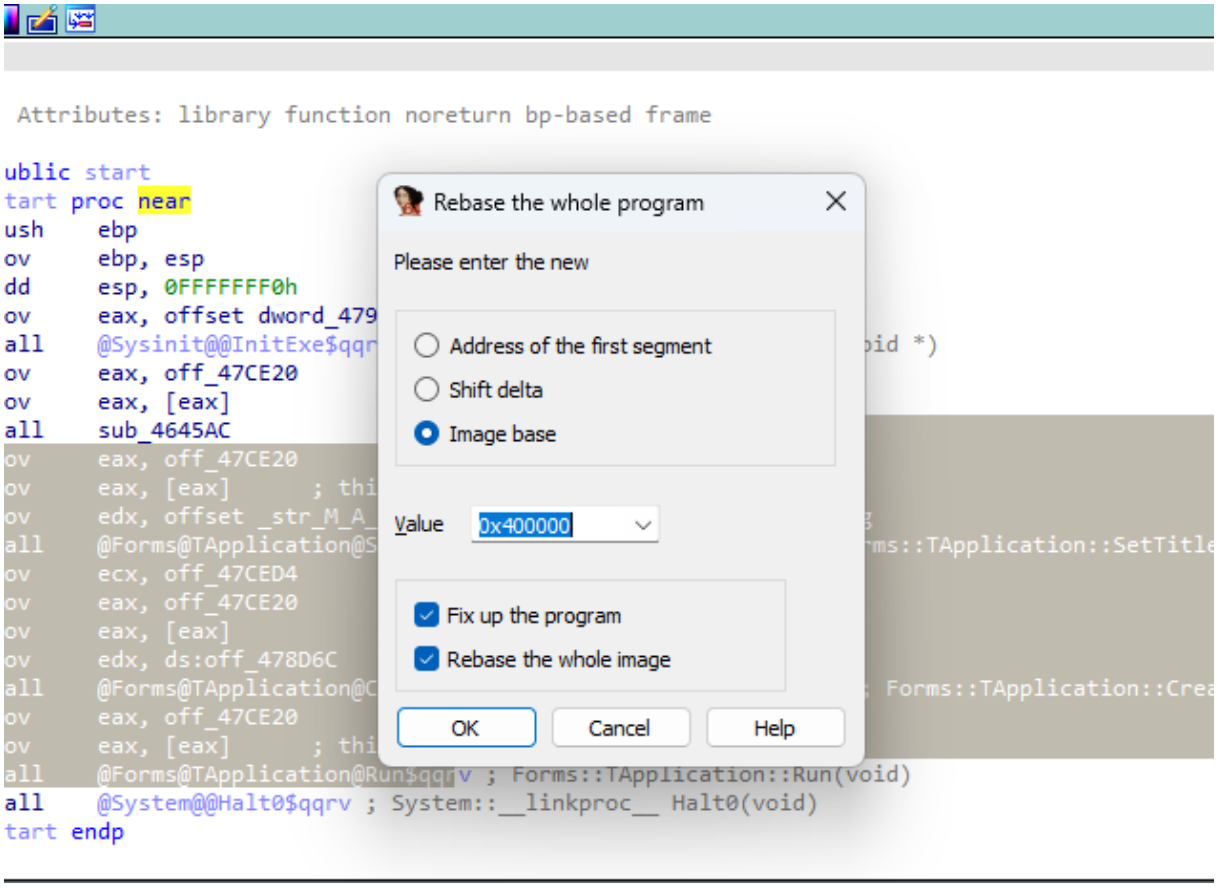
Vô hiệu hóa ASLR cho toàn bộ hệ thống

Tất cả các địa chỉ đều khớp với nhau. Nếu như bạn không biết cách tắt ASLR ,thì địa chỉ cơ sở của nhị phân đang chạy có thể được lấy từ trình gỡ lỗi, như minh họa bên dưới:



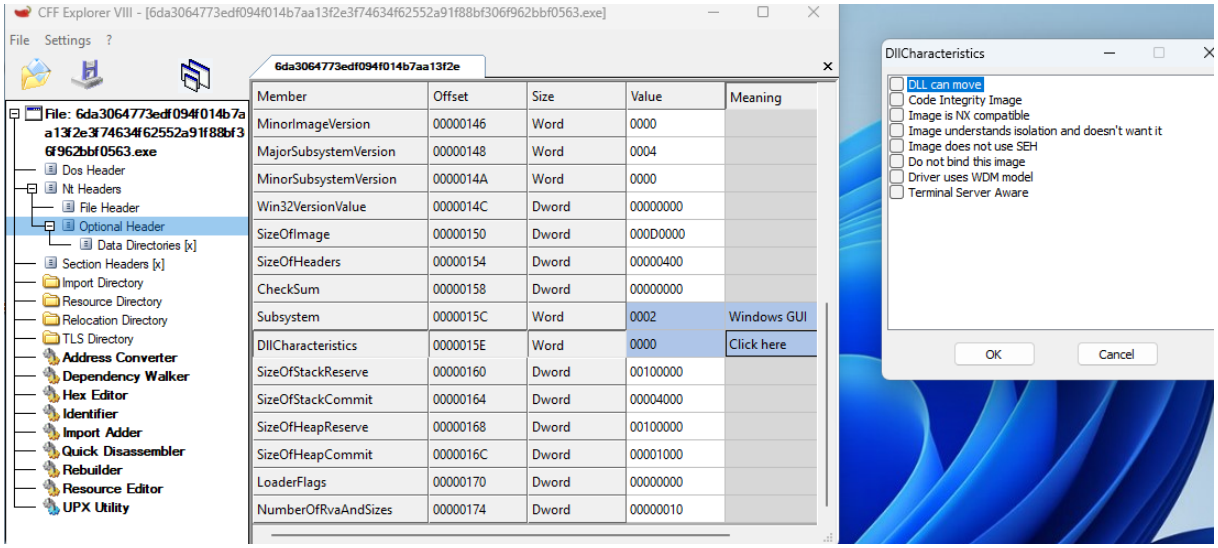
x32dbg: hiển thị địa chỉ cơ sở

Có địa chỉ cơ sở, vì vậy hãy mở IDA Pro: Edit -> Segments -> Rebase Program

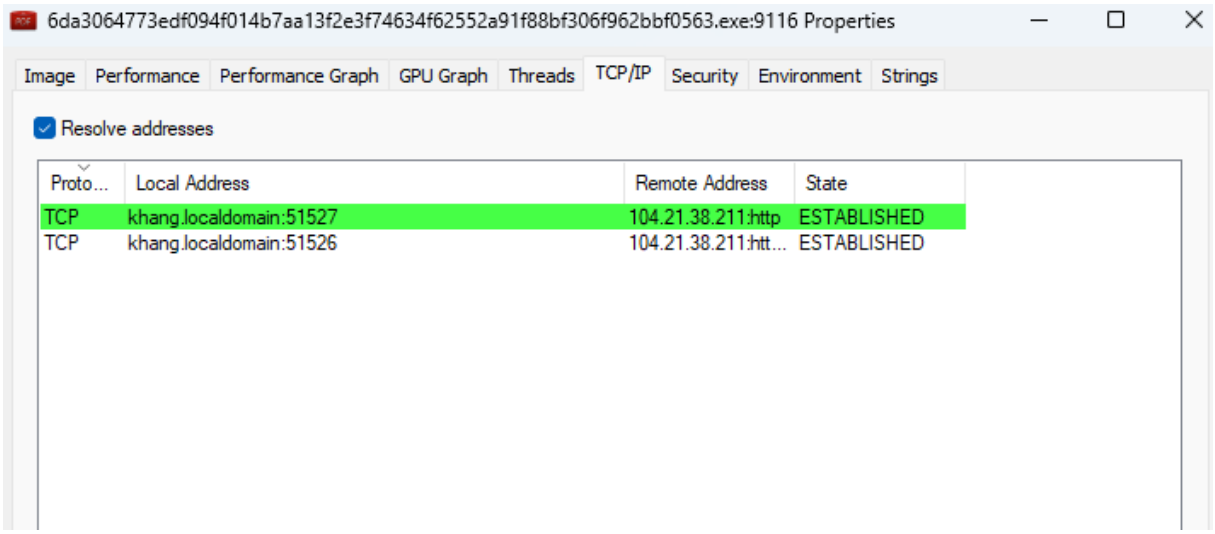


]IDA Pro rebasing

Ta cũng có thể chọn sử dụng CFF Explorer và "loại bỏ" đặc tính ASLR, như hiển thị bên dưới



] CFF Explorer: ASLR manipulation



Process Explorer hiển thị kết nối đã thiết lập với máy chủ sau khi tiến hành chạy thử file, Kiểm tra các thẻ điều khiển liên quan đến quy trình là một hành động được đề xuất khác và không có gì đáng ngạc nhiên khi ta tìm thấy bằng chứng về giao tiếp mạng của tải trọng đã được giải nén.