1. **CƠ SỞ LÝ THUYẾT**
2. **Tổng quan về mã độc**
3. **Mã độc là gì?**

* Mã độc (Malware) là phần mềm độc hại được thiết kế để xâm nhập vào hệ thống máy tính mà không có sự đồng ý của người dùng. Mục đích của mã độc có thể là gây hại cho hệ thống, đánh cắp dữ liệu cá nhân hoặc làm gián đoạn hoạt động của máy tính.
* Mã độc có thể tồn tại dưới nhiều hình thức, như tập tin thực thi, script hoặc mã nguồn. Kẻ tấn công sử dụng mã độc để thu thập thông tin nhạy cảm, theo dõi hành vi người dùng hoặc chiếm quyền điều khiển máy tính.
* Thông thường, mã độc xâm nhập qua email lừa đảo, trang web độc hại hoặc thiết bị lưu trữ USB. Các mục tiêu chính của mã độc bao gồm:
  + Gây rối hoạt động hệ thống: Làm giảm hiệu suất hoặc ngăn chặn hoạt động.
  + Đánh cắp thông tin cá nhân: Lấy cắp dữ liệu nhạy cảm.
  + Truy cập trái phép: Chiếm quyền kiểm soát tài khoản hoặc hệ thống.
  + Gián điệp và gửi thư rác: Theo dõi và thu thập thông tin.
  + Tấn công DDoS: Làm tê liệt dịch vụ khác.
  + Ransomware: Khóa tệp tin và yêu cầu tiền chuộc.

1. **Phân loại mã độc**

**Bom logic** (Logic bombs): mã độc này thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể. Khi “phát nổ” bom logic có thể xoá dữ liệu, files, tắt cả hệ thống…

**Trojan Horses**: Đây là loại mã độc ngụy trang dưới vỏ bọc phần mềm vô hại và thậm chí có thể hoạt động. Như một chương trình hợp pháp trong hệ thống trước khi thực hiện các hành vi độc hại được chỉ định Các đoạn mã của Trojan được “che giấu” trong các phần mềm máy tính bình thường để bí mật xâm nhập vào máy tính. Tới thời điểm thuận lợi, chúng sẽ đánh cắp thông tin cá nhân và chiếm quyền điều khiển máy tính…

**Backdoor (cửa hậu/ cửa sau)** là một dạng Trojan. Khi xâm nhập vào máy tính, backdoor sẽ mở ra một cổng dịch vụ cho phép tin tặc điều khiển máy tính nạn nhân. Tin tặc có thể cài phần mềm backdoor lên nhiều máy tính khác nhau thành một mạng lưới các máy bị điều khiển – Botnet. Từ đó, thực hiện các vụ tấn công từ chối dịch vụ DDoS.

**Rootkit**: Là một loại phần mềm độc hại được thiết kế để ẩn danh trên hệ thống máy tính và cho phép kẻ tấn công có quyền truy cập cao nhất vào hệ thống mà không bị phát hiện. Rootkit thường được sử dụng để giấu các hoạt động độc hại khác trên hệ thống, như truy cập trái phép, sao chép dữ liệu hoặc thực hiện các cuộc tấn công khác.

**Adware** (tên đầy đủ là advertising supported software): Là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm. Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm hoặc một dịch vụ miễn phí.

**Spyware:** là một loại phần mềm độc hại được thiết kế để bí mật quan sát hoạt động trên thiết bị và gửi những quan sát đó cho kẻ theo dõi. Dữ liệu đó có thể được sử dụng để theo dõi hoạt động của bạn trực tuyến và thông tin đó có thể được bán cho các nhà tiếp thị. Spyware cũng có thể được sử dụng để lấy cắp thông tin cá nhân, chẳng hạn như mật khẩu tài khoản và số thẻ tín dụng, việc này có thể dẫn đến hành vi đánh cắp danh tính và gian lận.

**Ransomware** là một loại mã độc được dùng để ngăn chặn người dùng truy cập dữ liệu và sử dụng máy tính. Để lấy lại dữ liệu và quyền kiểm soát máy tính, nạn nhân cần chuyển tiền cho tin tặc. Vì thế mà nó được gọi là mã độc tống tiền. Ransomware thường xâm nhập qua email rác hoặc trang web lừa đảo. Trong vài trường hợp, Ransomware được cài đặt cùng với Trojan để có thể kiểm soát nhiều hơn trên thiết bị của nạn nhân.

**Vi rút** (Virus): Là một chương trình có thể “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì virus sẽ tiếp tục “lây nhiễm” sang các chương trình khác. Vi rút máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email…

**Worm:** là một loại chương trình phần mềm độc hại có chức năng chính là lây nhiễm sang các máy tính khác trong khi vẫn hoạt động trên những hệ thống bị nhiễm.Worm máy tính là phần mềm độc hại tự sao chép để lây lan sang các máy tính chưa bị nhiễm. Worm thường sử dụng các phần tự động và vô hình đối với người dùng của hệ điều hành. Thông thường, worm chỉ được chú ý khi sự sao chép không kiểm soát của chúng tiêu tốn tài nguyên hệ thống, làm chậm hoặc tạm dừng các tác vụ khác.

**Zombie/Bot:** Là một chương trình được thiết kế để giành quyền kiểm soát một máy tính, hoặc thiết bị tính toán có kết nối Internet và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác, hoặc gửi thư rác. Botnet (mạng máy tính ma) là một tập hợp các máy tính bot dưới sự kiểm soát của một, hoặc một nhóm kẻ tấn công.

1. **Nguyên tắc hoạt động của mã độc**

**a. 5 nguyên tắc hoạt động chung của mã độc bao gồm:**

**· Xâm nhập vào hệ thống:** Mã độc thường khai thác các lỗ hổng bảo mật hoặc sử dụng các phương pháp xâm nhập khác như email lừa đảo, tải phần mềm từ nguồn không đáng tin cậy, hoặc sử dụng thiết bị lưu trữ ngoại vi để xâm nhập vào hệ thống máy tính hoặc thiết bị khác.

**· Điều khiển và kiểm soát hệ thống:** Sau khi xâm nhập thành công, mã độc tìm cách chiếm quyền điều khiển và kiểm soát hệ thống. Điều này cho phép kẻ tấn công thực hiện các hoạt động độc hại trên hệ thống mà không bị phát hiện, như theo dõi hành động của người dùng hoặc thay đổi các cài đặt hệ thống.

**· Mở cửa hậu cho kẻ tấn công:** Mã độc thường tạo ra các lỗ hổng hoặc cửa sau (backdoor) trên hệ thống, cho phép kẻ tấn công tiếp tục truy cập và kiểm soát hệ thống trong tương lai mà không cần phải thực hiện lại quá trình xâm nhập ban đầu.

**· Thực hiện các hoạt động độc hại:** Mã độc tiến hành các hoạt động gây hại như tạo ra các file giả mạo, thay đổi các cài đặt hệ thống, mã hóa các tệp tin quan trọng để đòi tiền chuộc, đánh cắp thông tin cá nhân hoặc dữ liệu quan trọng, và thậm chí điều khiển các thiết bị khác trong mạng của nạn nhân.

**· Che dấu hoạt động:** Mã độc sử dụng nhiều kỹ thuật để giấu kín sự hiện diện của mình nhằm tránh bị phát hiện và loại bỏ. Các phương pháp bao gồm mã hóa các tệp tin, tránh bị phát hiện bởi phần mềm diệt virus, và thay đổi các cài đặt hệ thống để làm khó việc nhận diện và loại bỏ mã độc.

**b. Hình thức phát tán:**

● Phát tán qua email

● Phát tán qua usb

● Phát tán qua lỗ hổng

● Phát tán qua điểm yếu hệ thống

● Phát tán qua các file nguồn không an toàn: crack, keygen, free, social

1. **Các định dạng dữ liệu nhiễm mã độc**

* **Tập tin văn bản**
  + Loại virus: File virus, Worm, Trojan
  + Các định dạng:
* Tập tin lô (BAT)
* Tập tin script (VBS, JS)
* Tập tin registry (REG)
* Tập tin siêu văn bản (HTT, HTA)

**· Tập tin chương trình**

* Loại virus: File virus, Worm, Trojan
* Các định dạng:
* Tập tin lệnh (COM)
* Tập tin thi hành (EXE, SCR)
* Tập tin thư viện (DLL, CPL, SYS, VXD)
* Tập tin tư liệu (DOC, DOT)

**· Tập tin MS Office**

* Loại virus: Macro virus
* Các định dạng:
* Tập tin bảng tính (XLS, XLT)
* Tập tin trình diễn (PPT, POT)

**· Mã khởi động**

* Loại virus: Boot virus
* Các định dạng:
* Mẫu tin khởi động hệ điều hành đĩa mềm
* Mẫu tin khởi động hệ điều hành đĩa cứng
* Mẫu tin khởi tạo phân khu đĩa cứng

**5. Các hành vi & kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc**

**a. *Thành phần của mã độc***

Window:

● File

● Registry

● Keys

● Processes memory

● Folder

Linux:

● File

● Processes memory

● Folder

***b. Kỹ thuật ẩn mình***

* Che giấu: Sử dụng các kỹ thuật mã hóa, ẩn file.
* File có thuộc tính ẩn (hidden file, system file): Theo mặc định, windows thiết lập
* không hiển thị các tệp có thuộc tính ẩn hoặc thuộc tính tệp hệ thống (system files)
* Mã độc thường lợi dụng cơ chế này để ẩn các file độc hại.
* Giả mạo icon: Mã độc có thể giả mạo icon của thư mục file nén phần mềm chuẩn.
* Giả mạo shortcut.
* Giả mạo file.
* Rootkit: Mã độc ẩn đi các thành phần của chính nó.
* Fileless: Mã độc Fileless không tồn tại dạng file trong hệ thống.
* Chèn mã, system call: Mã độc thực thi qua các lời gọi hệ thống hoặc chèn mã
* vào các tiến trình có sẵn.
* Mã độc có thể lợi dụng các tiến trình, service hệ thống để ẩn mình.
* Khai báo lỗ hổng:Mã độc sử dụng các kỹ thuật và lỗ hổng mới
* Virus lây file: mã độc ẩn mình bằng cách lây nhiễm vào các chương trình thực
* thi.
* Chèn mã và gọi hệ thống (System Call):
* Mã độc có thể chèn mã của nó vào các tiến trình hợp pháp đang chạy trên hệ thống. Điều này cho phép mã độc thực thi từ bên trong các tiến trình hợp pháp, giúp nó tránh bị phát hiện.
* Kỹ thuật này thường đi kèm với việc thực hiện các lời gọi hệ thống (system call) để thực thi mã độc mà không cần tạo ra các tiến trình mới hoặc các hoạt động dễ bị phát hiện.
* Khai thác lỗ hổng:
* Mã độc thường sử dụng các kỹ thuật khai thác lỗ hổng bảo mật trong hệ điều hành, phần mềm hoặc ứng dụng để xâm nhập vào hệ thống.
* Bằng cách khai thác các lỗ hổng mới chưa được vá (zero-day), mã độc có thể lây nhiễm vào hệ thống mà không gặp phải sự chống trả từ các công cụ bảo mật.

***Dấu hiệu nhận biết:***

● Máy tính chạy chậm bất thường, chậm kết nối mạng

● Máy tính bị khóa hoặc không trả lời (stop responding) liên tục, không cho chạy các chương trình hệ thống (cmd, regedit, task manager, gpedit, run,..)

● Máy tính tự động khởi động lại hoặc bị lỗi (crashes).

● Khi chạy một chương trình thường thông báo lỗi, chạy các file \*.exe, \*.com,...

đều bị thay thế bởi các chương trình khác.

● Ẩn file, thư mục, tạo các thư mục lạ, các biểu tượng lạ. Xuất hiện icon mới hoặc icon cũ tự mất.

● Xuất hiện các cửa sổ pop-up hoặc thông báo lạ, những tin nhắn báo lỗi không bình thường.

● Hiển thị hoặc file in ra bị biến dạng.

● Xuất hiện cặp đôi phần mở rộng của file. Ví dụ: vbs.txt...

● Phần mềm diệt virus không chạy hoặc không thể cài đặt.

● Tệp bị lỗi hoặc thư mục được tạo ra một cách tự động hoặc bị thay đổi, bị xóa, bị mã hóa.

● Hệ thống bị thay đổi cài đặt hay bị kiểm soát từ xa

**6. Các công cụ rà quét mã độc và các phương pháp phòng chống mã độc**

Công cụ rà quét

* File: Explorer, cmd…
* Process: Task manager, Process Explorer, Process Hacker…
* Network: TcpView, Wireshark…
* Startup: Regedit, AutoRuns…
* Rootkit: PC Hunter, Rootkit Remover…
* Logs: Event Viewer, Process Monitor…
* Scanner: KVRT, TDSSKiller, Norton Power Eraser, ClamAV…

Phương pháp phòng chống

* Cập nhật phần mềm và hệ điều hành thường xuyên:
* Sử dụng tường lửa (Firewall):
* Thiết lập quyền truy cập an toàn:
* Hạn chế quyền truy cập vào các tập tin và thư mục quan trọng:
* Sử dụng phần mềm chống mã độc và tường lửa cá nhân:
* Tránh tải xuống và cài đặt phần mềm từ các nguồn không đáng tin cậy:
* Cảnh giác với email và liên kết đáng ngờ:
* Sao lưu dữ liệu thường xuyên:
* Sử dụng mật khẩu mạnh và xác thực hai yếu tố:
* Giám sát hệ thống liên tục

1. **Tổng quan về phân tích mã độc**
2. **Phân tích mã độc là gì?**

* Phân tích mã độc là việc sử dụng các công cụ, kỹ thuật phân tích nhằm xác định hành vi “độc hại” của mã độc đến hệ thống máy tình.
* Phân tích mã độc có mục tiêu nữa là từ kết quả của việc phần tích đưa ra cách để gỡ bỏ và phòng tránh mã độc đó.
* Về phương pháp phân tích, có hai phương pháp phân tích mã độc là phân tích tĩnh và phân tích động.

1. **Vai trò của phân tích mã độc**

* Phân tích mã độc (malware analysis) đóng một vai trò rất quan trọng trong lĩnh vực an ninh mạng, nhằm xác định, hiểu rõ và khắc phục các mối đe dọa từ các phần mềm độc hại.
* Ngoài ra phân tích mã độc cũng làm nguồn cung cấp, xác định mẫu mã độc để hỗ trợ việc phát hiện và ngăn chặn trong tương lai.
* Dưới đây là những vai trò chính của phân tích mã độc:
  + **Phát hiện và hiểu rõ mã độc**: Phân tích mã độc giúp các chuyên gia an ninh mạng phát hiện và hiểu cách hoạt động của phần mềm độc hại, từ đó tìm ra cách khắc phục hoặc bảo vệ hệ thống trước các cuộc tấn công tương tự.
  + **Xác định mức độ thiệt hại**: Phân tích mã độc giúp xác định những dữ liệu hoặc hệ thống nào bị ảnh hưởng, từ đó giúp đánh giá được mức độ thiệt hại của cuộc tấn công.
  + **Phòng ngừa và ngăn chặn**: Qua việc phân tích, các chuyên gia có thể phát triển các giải pháp ngăn chặn mã độc trước khi nó gây ra những hậu quả nghiêm trọng. Điều này bao gồm việc cập nhật các chữ ký mã độc và cải tiến phần mềm bảo mật.
  + **Tăng cường các biện pháp an ninh**: Khi hiểu rõ cách mã độc lây nhiễm và hoạt động, các tổ chức có thể cải thiện các biện pháp an ninh hiện tại, vá các lỗ hổng và giảm thiểu nguy cơ bị tấn công trong tương lai.
  + **Phát triển công cụ chống mã độc**: Từ những phân tích về cách thức hoạt động của mã độc, các công ty bảo mật có thể phát triển các công cụ phát hiện và loại bỏ mã độc hiệu quả hơn.

1. **Phân loại kỹ thuật phân tích mã độc**

* **Phân tích tĩnh**
* Phân tích tĩnh là một kỹ thuật phân tích mã độc mà không cần thực thi mã nguồn hoặc chương trình.
* Phân tích này được thực hiện trên mã độc để hiểu cấu trúc, chức năng và hành vi của nó mà không cần chạy mã.
* Phương pháp này thường được sử dụng trong giai đoạn đầu của việc phân tích mã độc và có thể cung cấp cái nhìn tổng quan ban đầu về mã độc.
* Lợi ích:
  + **Nhanh chóng và an toàn**: Vì không cần thực thi mã, quá trình này an toàn và không làm lây nhiễm mã độc vào hệ thống phân tích.
  + **Cung cấp cái nhìn tổng quan ban đầu**: Phân tích tĩnh thường giúp các chuyên gia có cái nhìn tổng quan ban đầu trước khi thực hiện phân tích động (dynamic analysis).
* Hạn chế:
  + **Không phân tích được hành vi thực sự**: Phân tích tĩnh không cho thấy các hành vi của mã độc khi nó được thực thi trong một môi trường thực tế.
  + **Bị giới hạn bởi các kỹ thuật làm rối mã (obfuscation)**: Nhiều mã độc hiện đại sử dụng các kỹ thuật làm rối để che giấu mục đích thực sự, khiến việc phân tích tĩnh trở nên khó khăn.
* Phân loại:
  + Phân tích tĩnh cơ bản: tìm cách hiểu mã độc bằng cách phân tích chính file, cấu trúc file, các chức năng được sử dụng bởi mã độc ...
  + Phân tích tĩnh nâng cao: phân tích sâu hơn và tìm cách hiểu được mã độc dựa trên dịch ngược (disassembled).
* **Phân tích động**
* là một kỹ thuật phân tích mã độc mà trong đó mã độc được thực thi trong một môi trường kiểm soát để quan sát và nghiên cứu hành vi của nó khi hoạt động.
* Phân tích động thường được thực hiện sau phân tích tĩnh, giúp các nhà nghiên cứu hiểu rõ hơn về cách mã độc tương tác với hệ thống và ảnh hưởng của nó.
* Lợi ích
  + **Xác định hành vi thực sự của mã độc**: Phân tích động cung cấp cái nhìn toàn diện về cách mã độc hoạt động trong thực tế, bao gồm những thay đổi cụ thể mà nó gây ra cho hệ thống.
  + **Hiểu rõ hơn về các cuộc tấn công nâng cao**: Một số mã độc có hành vi phức tạp chỉ kích hoạt khi gặp điều kiện nhất định. Phân tích động giúp phát hiện những hành vi này.
  + **Khắc phục hạn chế của phân tích tĩnh**: Phân tích động giúp vượt qua những kỹ thuật làm rối mã và mã hóa mà phân tích tĩnh không thể phát hiện.
* Hạn chế
  + **Nguy cơ làm lây nhiễm hệ thống**: Mặc dù được thực hiện trong môi trường cách ly, nếu không cẩn thận, mã độc có thể thoát ra và gây thiệt hại cho hệ thống thật.
  + **Yêu cầu thiết lập phức tạp**: Cần có một môi trường phân tích an toàn và được kiểm soát để đảm bảo việc thực thi mã độc không gây ra rủi ro.
  + **Khó khăn với mã độc có tính năng chống phân tích**: Một số mã độc tiên tiến có cơ chế phát hiện khi chúng đang bị theo dõi hoặc phân tích, từ đó thay đổi hành vi hoặc không hoạt động.
* Phân loại
  + Phân tích động cơ bản: Chạy mã độc trong môi trường cô lập có trang bị sẵn các công cụ giám sát khác nhau và cố gắng hiểu mã độc đang làm gì dựa trên đầu ra của các công cụ đó.
  + Phân tích động nâng cao: nếu phân tích cơ bản không đem lại kết quả hoặc muốn tìm hiểu kỹ hơn thì cần thực hiện phân tích nâng cao mã đ bằng cách sử dụng một bộ gỡ lỗi (debugger). Bằng cách này, chuyên gia có nhiều quyền kiểm soát hơn về cách mã độc được thực thi.

1. **CÀI ĐẶT VÀ CẤU HÌNH**
2. **Một số công cụ**

* PEStudio: <https://pestudio.en.lo4d.com/download/mirror-ls1>

*+ PEStudio* là một công cụ dùng để phân tích tĩnh các tệp tin Portable Executable (PE), cung cấp thông tin về cấu trúc của tệp, mã băm, chuỗi, thư viện liên kết động (DLL), và các chỉ số liên quan đến khả năng độc hại.

+ Ở đây nhóm e sử dụng công cụ này để phân tích file nghi ngờ

* **Cutter**: <https://cutter.re/>

+ *Cutter* là một giao diện đồ họa nguồn mở được xây dựng trên nền tảng Radare2, hỗ trợ phân tích tĩnh và phân tích động mã nguồn, giúp bạn hiểu rõ hơn về cách phần mềm hoạt động hoặc mã độc thực thi.

* **Capa**: <https://github.com/mandiant/capa/releases>

+ *Capa* là một công cụ giúp xác định các khả năng và hành vi của mã độc thông qua phân tích nhị phân. Nó phát hiện các chức năng cụ thể như mã hóa, tự sao chép, hay giao tiếp mạng.

* **CFF Explorer**: <https://ntcore.com/?page_id=388>

+ *CFF Explorer* cung cấp khả năng chỉnh sửa tệp PE, giúp bạn truy cập và thay đổi các phần bên trong của tệp tin thực thi, chẳng hạn như sửa đổi tài nguyên, bảng nhập (Import), bảng xuất (Export), và nhiều yếu tố khác.

1. **Cấu hình cài đặt**

* Sau khi tải về PEStudio, Cutter, và CFF Explorer, tiến hành giải nén các tệp đã tải xuống và chạy trực tiếp các công cụ từ các tệp này mà không cần cài đặt thêm.
* Đối với Cmder, sau khi giải nén, bạn có thể chạy trực tiếp công cụ này. Sau đó, bắt đầu cấu hình Capa và Floss bằng cách cài đặt chúng vào môi trường làm việc thông qua các đường dẫn tương ứng. Capa và Floss sẽ giúp bạn thực hiện phân tích mã độc, phát hiện các hành vi nguy hiểm và trích xuất thông tin từ tệp mã độc.

1. **TROJAN ZEUS BANKING**

* Virus **trojan Zeus** được tạo ra lần đầu tiên vào năm 2007, khi tin tặc ở Đông Âu sử dụng nó để nhắm vào Bộ Giao thông Vận tải Hoa Kỳ.
* Mặc dù khó có thể nói chắc chắn ai đã tạo ra nó, nhưng cuộc tấn công thực sự bùng nổ khi mã độc của nó bị công khai vào năm 2011.
* Kể từ đó, nó đã tạo ra hàng chục biến thể khiến các chuyên gia bảo mật internet và cơ quan thực thi pháp luật bận rộn.
* Có hai vectơ tấn công phổ biến mở máy tính Windows cho các cuộc tấn công của phần mềm độc hại trojan Zeus.
  + Tải xuống tự động yêu cầu người dùng truy cập trang web có mã trojan cửa sau trên đó. Sau đó, chúng tải xuống các tệp vào máy tính của người dùng mà người dùng không biết. Các trình duyệt hiện đại như Google Chrome thường chặn các lượt tải xuống này và các trang web mà chúng được tìm thấy, nhưng tin tặc liên tục triển khai các giải pháp thay thế mới cho việc này. Trong khi đó, các trình duyệt web cũ hơn như Internet Explorer có thể không chặn được các lượt tải xuống tự động.
  + Phương thức lây nhiễm chính khác của Zeus là thông qua các cuộc tấn công lừa đảo, trong đó người dùng nghĩ rằng họ đang tải xuống phần mềm lành tính từ các liên kết trong email lừa đảo hoặc bài đăng trên phương tiện truyền thông xã hội.
* Zeus Banking Trojan hay còn gọi là ZueS hoặc Zbot, là một gói phần mềm mãi độc dạng Trojan, nó phổ biến và đáng ngại trong lĩnh vực tài chính trên internet. Nó được thiết kế để đánh cắp thông tin đăng nhập của người dùng, cho phép kẻ tấn công truy cập và lừa đảo trong quá trình giao dịch tài khoản trực tuyến.
* Mã độc này hoạt động như một phần mềm độc hại có khả năng đánh cắp thông tin và hoạt động trong các môi trường trực tuyến, chủ yếu là tập trung vào việc tấn công hệ thống ngân hàng và tài chính. Nó có thể ghi lại thông tin đăng nhập, số thẻ tín dụng, mật khẩu và các thông tin nhạy cảm từ máy tính của nạn nhân.
* Nó gây ra nguy cơ lớn đối với người dùng và tổ chức tài chính. Nó có thể gây ra mất cắp tài sản, mất thông tin cá nhân, và tiềm tàng nguy cơ cho sự riêng tư và an ninh tài chính của người dùng. Nó cũng có thể gây ra thiệt hại danh tiếng và kinh tế đối với các tổ chức bị tấn công.
* **Link tải**:

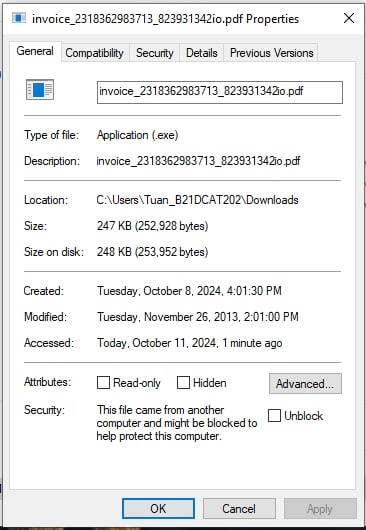
**TrojanBankingMalware**: https://github.com/ytisf/theZoo/tree/master/malware/Binarie s/ZeusBankingVersion\_26Nov2013

1. **PHÂN TÍCH - THỰC NGHIỆM**
2. **Xác định loại của tệp**

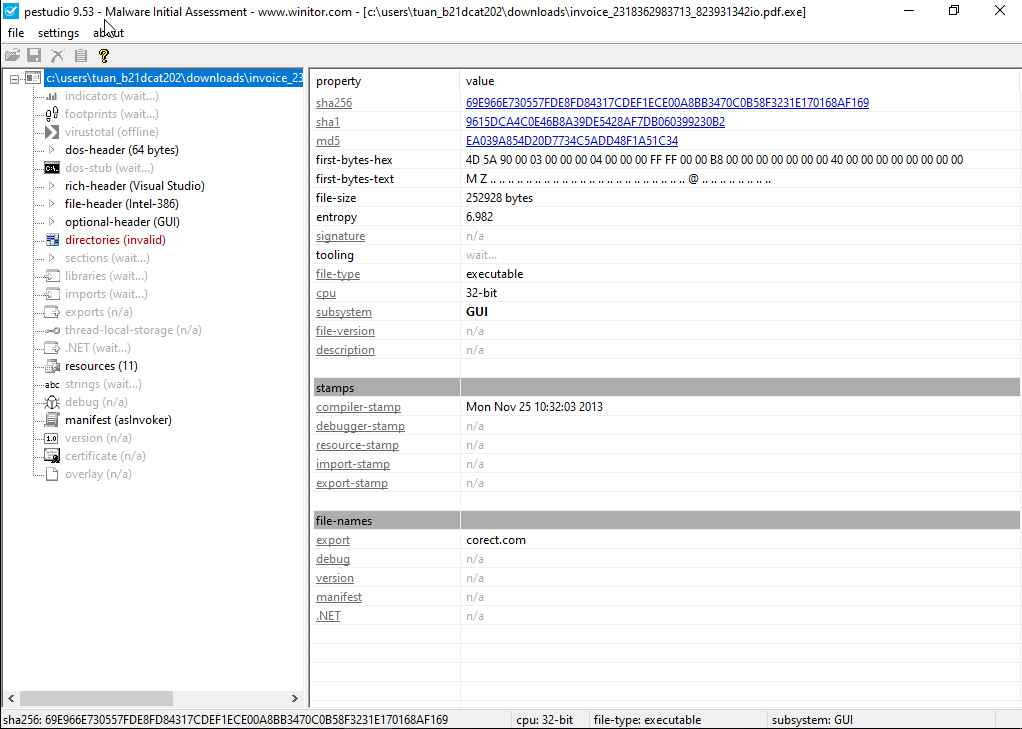
* Phát hiện một tệp đáng ngờ trong máy với đuôi file là .pdf



* Ta xem thông tin của file



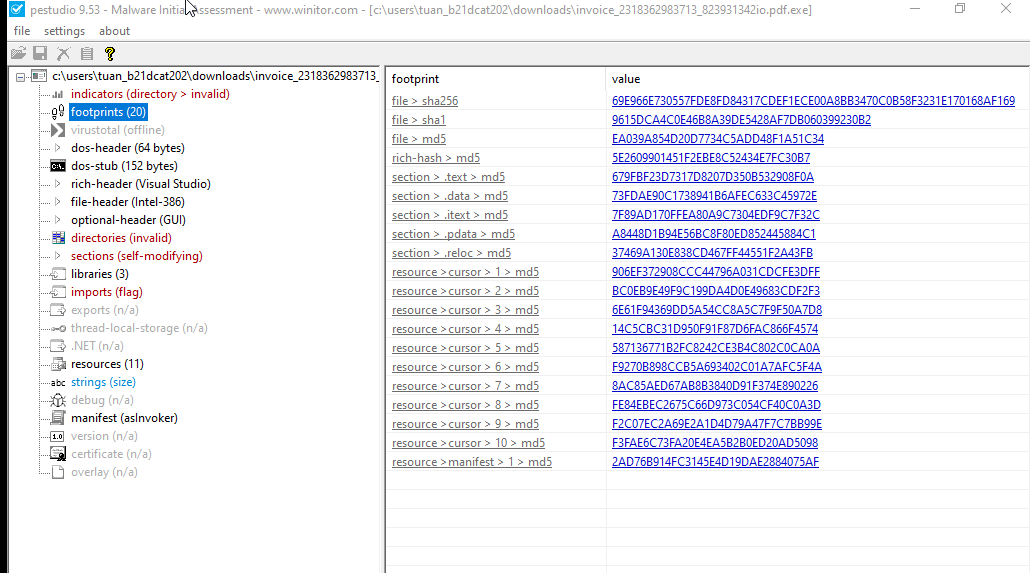
* Có thể thấy file quá nặng khi là một file pdf
* Sử dụng PE studio để xem kĩ file nghi ngờ



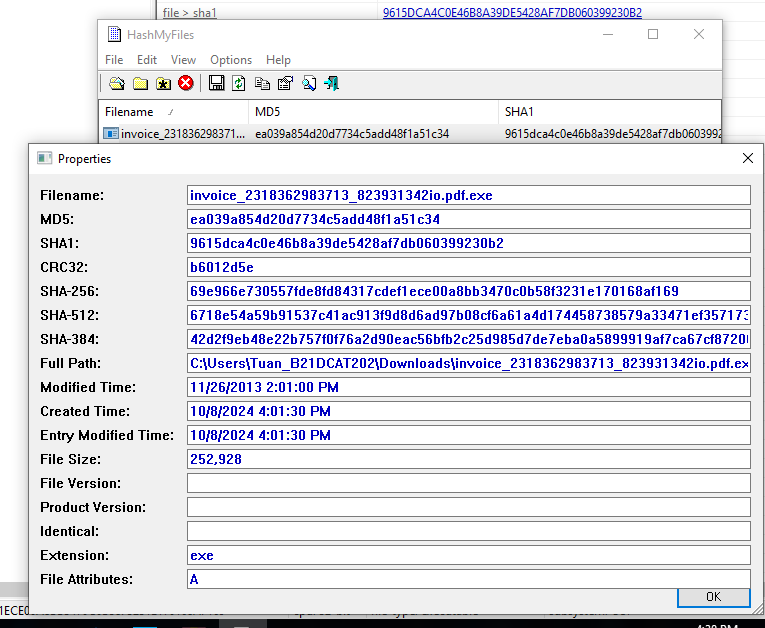
**Hình 1.1:** Sử dụng PEStudio để phân tích tệp đáng ngờ

* Khi sử dụng PEStudio để phân tích một tệp đáng ngờ, tại mục "first-byte > text", chúng ta phát hiện chữ ký của tệp là MZ.
* Kích thước tệp được xác định là **252928 byte.**
* Loại tệp hiển thị là Portable Executable 32-bit, cho thấy đây là tệp được phát triển nhằm mục tiêu tấn công hệ điều hành Windows.
* Trong phần "Stamps", chúng ta có thể xác định rằng tệp này lần đầu tiên được biên dịch vào ngày Thứ Hai, 25/11/2013 lúc 10:32:03

1. **Phân tích mã Hash**
2. **Kiểm Tra mã HASH thu được của Pestudio**



1. **Sử dụng HashMyFiles để tính toán mã Hash của File gốc**



1. **So sánh - Kiểm Tra tính toàn vẹn của file mã độc**

* Khi tiến hành phân tích mã độc bằng PEStudio, mã băm thu được là:

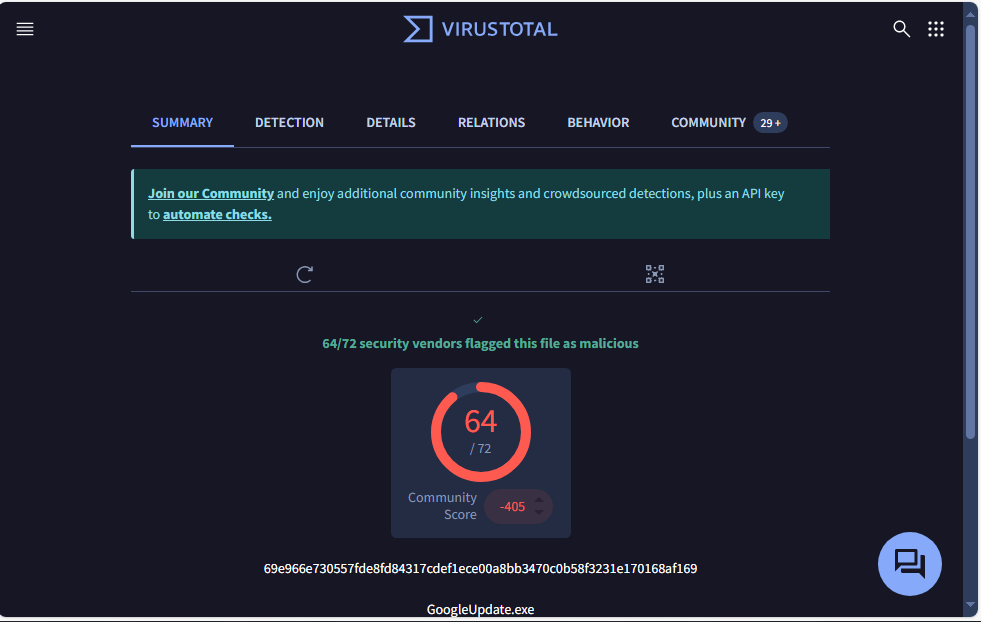
**69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169**

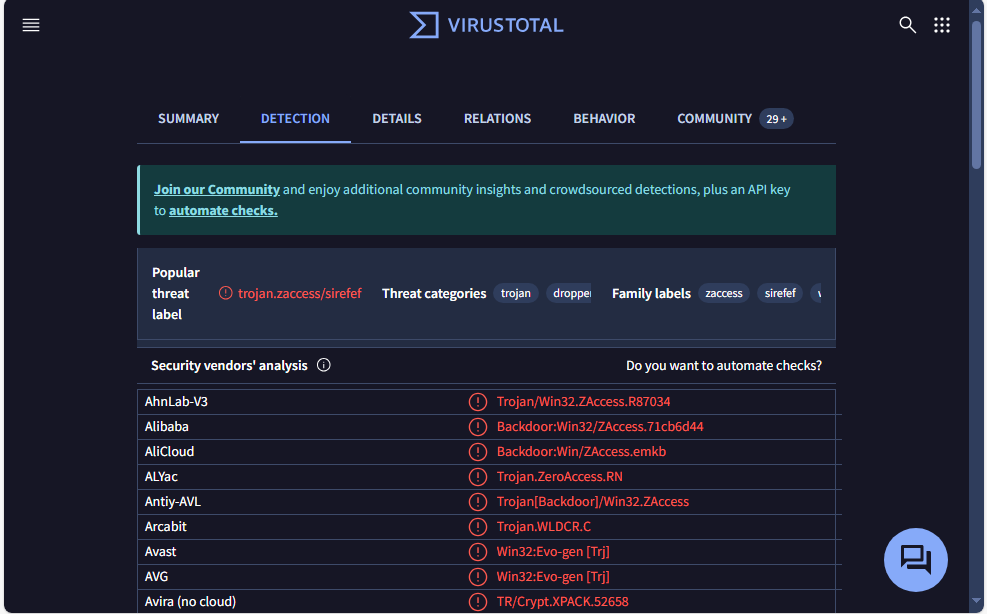
* Trong khi đó, khi sử dụng HashMyFiles, mã băm của tệp cũng được tính toán là:

**69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169**

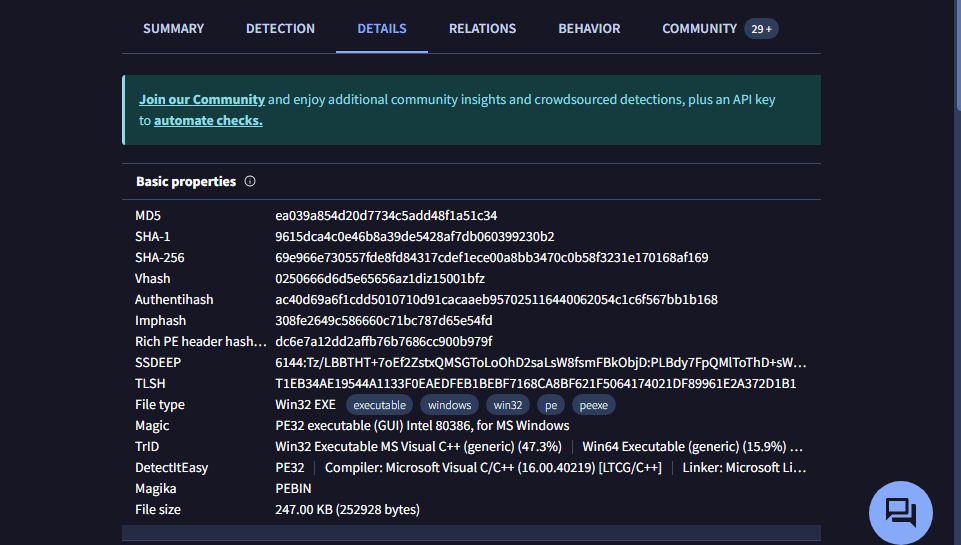
* Nhìn chung, hai mã hash này hoàn toàn trùng khớp, điều này chứng tỏ rằng tệp không bị thay đổi kể từ khi bắt đầu quá trình tính toán hash. Sự toàn vẹn của tệp vẫn được đảm bảo.
* Xác định tính toàn vẹn của một tệp là rất quan trọng, đặc biệt khi kết hợp phân tích tĩnh và phân tích động.
* Trong phân tích động, khi mã độc được thực thi, nó có thể sao chép bản thân đến một vị trí khác hoặc tạo ra một biến thể mới.
* Nhờ có mã băm, chúng ta có thể xác định xem biến thể mới có phải là một phiên bản chính xác của mẫu ban đầu hay không.
* Trong trường hợp này, việc mã hash không thay đổi cho thấy không có sự khác biệt giữa các tệp trong quá trình phân tích.
* Điều này giúp xác định rằng chỉ cần tập trung vào một mẫu duy nhất để tiến hành phân tích thay vì phải xem xét nhiều biến thể khác nhau.

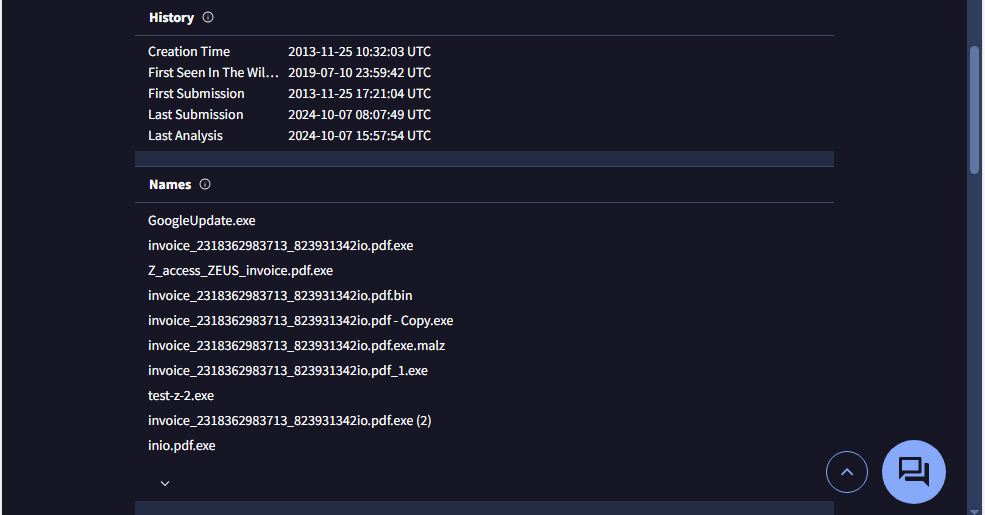
1. **Phân tích mẫu đang có sử dụng công cụ kết hợp nhiều Antivirus (AV)**



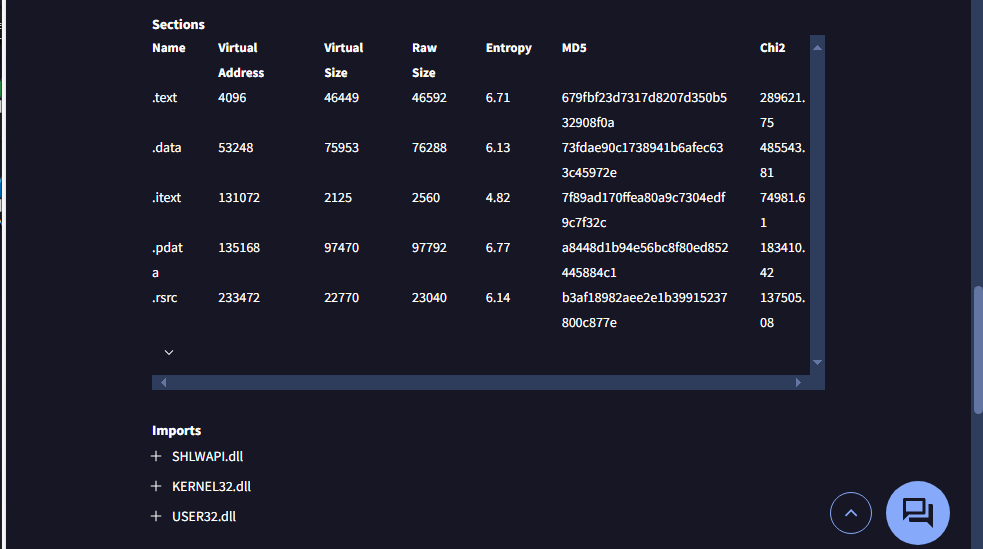


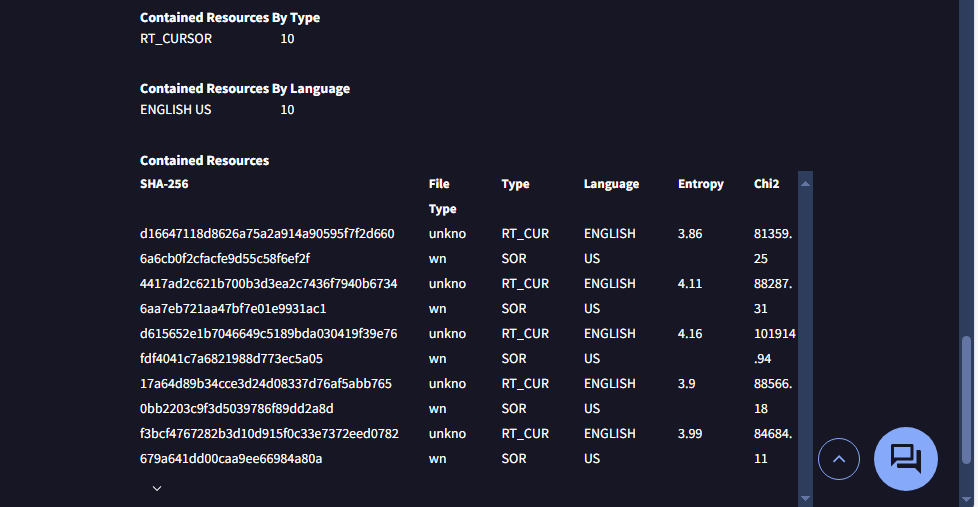
* Như ta có thể thấy các nhà cung cấp đều thông báo file có hại



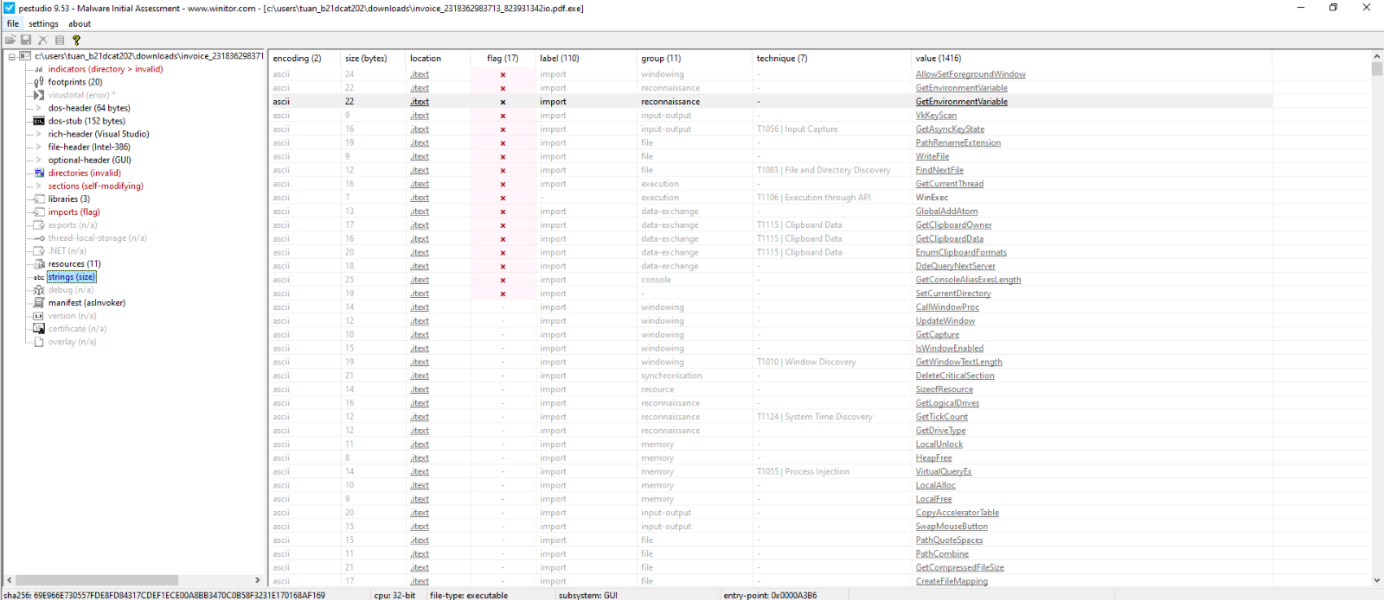








1. **Tách chuỗi từ chương trình**
2. **Sử dụng Pestudio để tách chuỗi từ chương trình**



* Khi sử dụng PEStudio để hiển thị cả chuỗi ASCII và Unicode, có thể thấy tổng cộng hơn 1416 chuỗi trong tệp tin. Tuy nhiên, do giới hạn của PEStudio, chỉ có 1416 chuỗi đầu tiên được hiển thị.
* Trong PEStudio, các chuỗi được đánh dấu bằng cờ “x” thường được coi là có khả năng liên quan đến hành vi độc hại của phần mềm mã độc. Những chuỗi này có thể bao gồm tên file, đường dẫn, lệnh hệ thống, hoặc các yếu tố khác thường được mã độc sử dụng trong quá trình hoạt động của mình

1. **Lấy chuỗi bị che dấu bằng floss**

* Sẽ có những chuỗi mà mã độc không muốn ta phát hiện ra nên đã che giấu đi và để lấy được những chuỗi được che giấu đó ta sử dụng FLOSS.

