| **BỘ GIÁO DỤC VÀ ĐÀO TẠO**  **ĐẠI HỌC FPT** |  |
| --- | --- |

**BÁO CÁO DỰ ÁN**

**A TROJAN WITH IMAGE FILE**

****

Team 1: Lê Đức Văn, Trần Công Toàn - IA1707

| Instructor: Ngô Hải Anh |
| --- |

**Hà Nội, ngày 24 tháng 2 năm 2024**

**Mục lục**

**Lời mở đầu.…………………………………………………………………. 3**

**Chương I - Tổng quan về Malware……………………………………… 4**

**1.1 Khái niệm...……………………………………………………………. 4**

**1.2 Phân loại Malware……………………………………………………. 5**

**1.3 Reverse Shell…...……………………………………………….……. 7**

***1.3.1* Khái niệm...…………………………………………………….. 7**

***1.3.2* Hình thức tấn công....….…………………………………….. 7**

***1.3.3* RCE……………………………………………………………… 8**

***1.3.4* Cách phòng tránh…………………………………………….. 9**

**Chương II - Trojan Horse Virus………………………………………….. 9**

**2.1 Giới thiệu………………………………………………………………. 9**

***2.1.1* Khái niệm………………………………………………………. 9**

***2.1.2* Phát tán và hành động………………………………………. 9**

**2.2 Trojan Horse Virus with image file……………………………….. 11**

***2.2.1* Ý tưởng…...…………………………………………………… 11**

***2.2.2* Recipe…………...…………………………………………….. 12**

***2.2.3* Quy trình thực hiện………………..…………..…………..... 12**

**Kết luận……………………………………………………………………... 18**

**Tài liệu tham khảo……………………………………………………...…. 19**

**Lời mở đầu**

Trong thời đại kỹ thuật số hiện nay, tấn công an ninh mạng đã trở thành một trong những thách thức phức tạp và đe dọa đáng kể đối với hệ thống thông tin và mạng internet toàn cầu. Các hành vi tấn công này không chỉ làm mất dữ liệu quan trọng, mà còn gây ra những hậu quả nghiêm trọng cho các tổ chức và cá nhân, bao gồm mất trắc ẩn, thất thoát tài chính, và thậm chí ảnh hưởng đến sự ổn định và an ninh quốc gia.

Tấn công an ninh mạng có thể xảy ra dưới nhiều hình thức khác nhau, từ việc tấn công trực tiếp vào cơ sở hạ tầng kỹ thuật số bằng cách tận dụng lỗ hổng bảo mật đến việc lừa đảo người dùng thông qua các kỹ thuật xã hội. Sự phát triển không ngừng của công nghệ cũng tạo ra các cơ hội mới cho các kẻ tấn công, từ việc tận dụng trí tuệ nhân tạo và máy học đến việc phát triển các công cụ tấn công tiên tiến.

An ninh mạng ngày nay đang đối mặt với nhiều thách thức lớn do sự phát triển của công nghệ. Các mối đe dọa mạng ngày càng phức tạp và tiên tiến hơn, từ các loại virus, malware thông thường đến các cuộc tấn công mạng phức tạp như tấn công mạng lưới, tấn công từ chối dịch vụ (DDoS), và các hình thức tấn công mới sử dụng trí tuệ nhân tạo (AI) và machine learning.

Các tổ chức và cá nhân ngày càng phải đối mặt với việc bảo vệ dữ liệu quan trọng trước những nguy cơ về lỗ hổng bảo mật, việc sử dụng phương thức tấn công ngày càng tinh vi và phức tạp.

Để đối phó với tình trạng này, việc nắm bắt các phương thức tấn công và triển khai các biện pháp bảo mật hiệu quả là cực kỳ quan trọng. Trong bài báo cáo này giới thiệu cho người đọc về một loại hình thức tấn công để hiểu rõ về cơ chế hoạt động cũng như tầm ảnh hưởng của nó.

Phần còn lại được tổ chức như sau:

Chương I - Tổng quan về Malware

Chương II - Trojan Horse Virus

**CHƯƠNG I: TỔNG QUAN VỀ MALWARE**

**1.1 Khái niệm**

Malware, viết tắt của malicious software (phần mềm độc hại), là một thuật ngữ chung để chỉ virus, worm, trojan và các chương trình máy tính độc hại khác mà các hacker dùng để phá hoại và giành quyền truy cập vào những thông tin nhạy cảm.

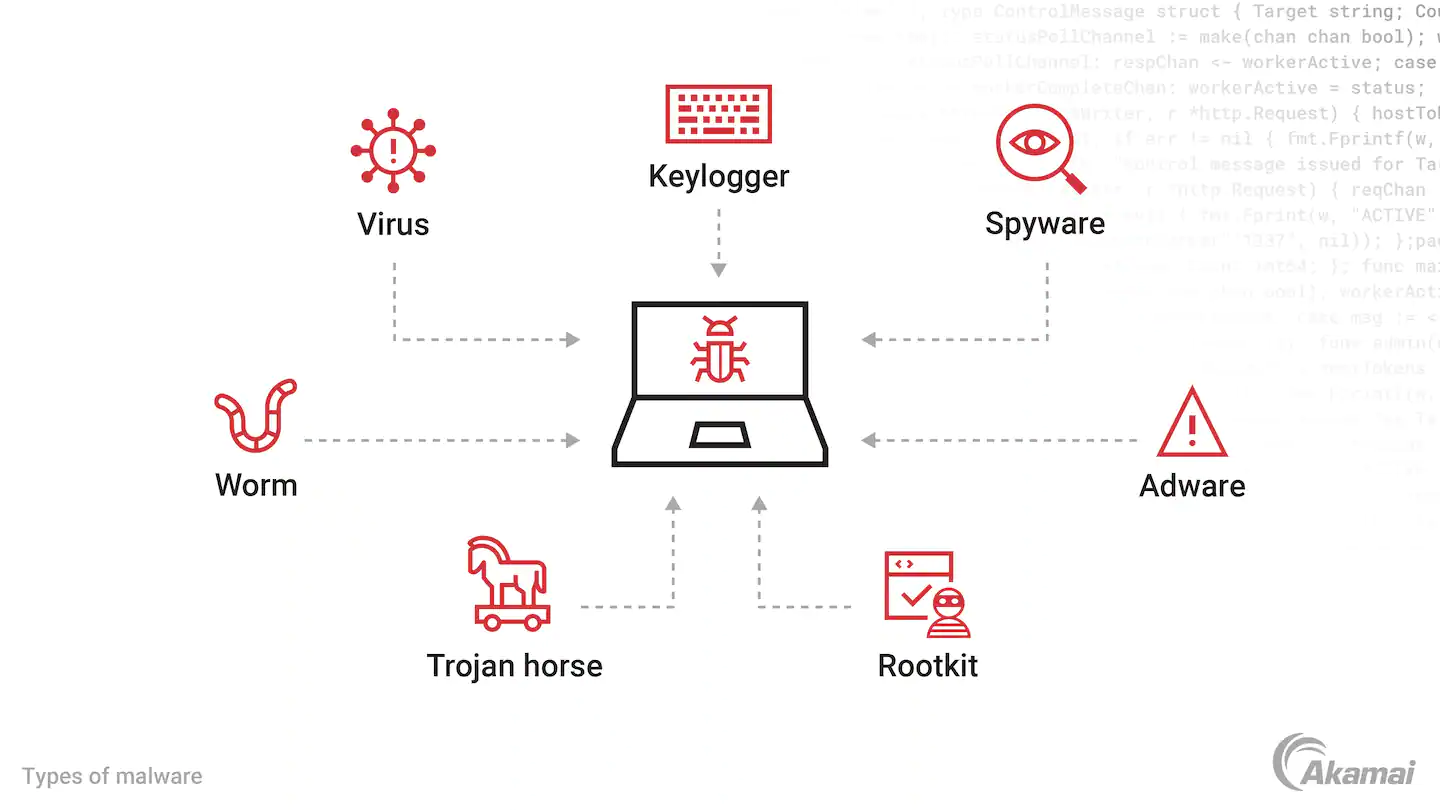


Theo Microsoft, “[malware] là một thuật ngữ chung để chỉ mọi phần mềm được thiết kế để gây ảnh hưởng xấu đến các máy tính, server hay mạng máy tính.” Nói cách khác, phần mềm sẽ được xem là một malware dựa trên mục đích sử dụng của nó, chứ không phải là một kỹ thuật hay công nghệ cụ thể dùng để build nó.

Có một số thắc mắc về sự khác biệt giữa virus và malware. Thực ra, virus chính là một loại malware, nên mọi virus đều chính là malware. Nhưng ngược lại, malware chưa chắc là virus.

Nói tóm lại Malware hay phần mềm độc hại là một thuật ngữ chung mô tả bất kỳ chương trình độc hại hoặc mã nào có hại cho hệ thống. Những phần mềm này do tin tặc tạo ra trong hệ thống máy tính của người dùng sẽ có nhiệm vụ ăn cắp, mã hóa hoặc xóa dữ liệu nhạy cảm, hay chiếm đoạt các chức năng tính toán lõi và giám sát hoạt động máy tính của người dùng mà không được sự cho phép của họ thông qua những phần mềm độc hại.

**1.2 Phân Loại Malware**

****

Để tìm hiểu sâu hơn về tấn công phát tán malware là gì, hãy cùng tìm hiểu về các loại malware phổ biến hiện nay. Có khá nhiều cách khác nhau để phân loại malware.

Đầu tiên trong đó là phân loại theo cách malware phát tán. Trong đó, virus, trojan và worm mô tả 3 cách lây nhiễm khác nhau của malware:

**Worm:** là một phần mềm malware độc lập, tự tái tạo và lây lan từ máy tính này sang máy tính khác.

**Virus:** là một đoạn code máy tính, nó tự chèn mình vào trong code của một chương trình độc lập khác. Sau đó buộc chương trình thực hiện hành động độc hại và tự phát tán.

**Trojan:** là một chương trình, dù không có khả năng tái tạo nhưng có thể giả dạng những mục tiêu mà người dùng muốn. Từ đó lừa họ kích hoạt để trojan có thể phát tán.

Virus, trojan và worm có thể chứa các Logic bomb trong chiến lược tấn công của chúng. Bên cạnh đó, malware cũng có thể được cài đặt lên máy tính bằng cách thủ công bởi các hacker. Chúng có thể giành quyền truy cập vào máy tính, hoặc chiếm quyền truy cập của quản trị viên từ xa.

Một cách khác để phân loại malware là phụ thuộc vào hành động của nó sau khi lây nhiễm thành công vào máy tính của nạn nhân. Loại này có rất nhiều ví dụ như Spyware, Rootkit, Adware, Ransomware, Cryptojacking, Malvertising,...

Sau đây là một số kỹ thuật tấn công được malware sử dụng:

**Spyware:** Theo Webroot Security, spyware là malware được sử dụng để bí mật thu thập dữ liệu về người dùng. Về bản chất, nó sẽ theo dõi các hành vi khi sử dụng máy tính, cũng như các dữ liệu được gửi và nhận. Thường thì mục đích của spyware là gửi các thông tin đến một bên thứ ba khác. Chẳng hạn, keylogger là một loại spyware, có khả năng ghi lại tất cả lần gõ phím của người dùng, giúp các hacker dễ dàng đánh cắp được mật khẩu.

**Rootkit:** Theo TechTarget, rootkit là một chương trình, thường là một tập hợp các công cụ phần mềm, cho phép hacker truy cập từ xa và kiểm soát máy tính hay hệ thống khác. Rootkit bao gồm các công cụ (thường là bất hợp pháp) có quyền truy cập root với hệ thống đích, và Rootkit cũng dùng nó để che giấu sự hiện diện của mình.

**Adware:** Là một malware buộc trình duyệt phải chuyển hướng đến các quảng cáo trên trang web. Các quảng cáo này cũng thường buộc người dùng download thêm các phần mềm độc hại khác.

**Ransomware:** Đây là một loại malware có khả năng mã hóa các file trong ổ cứng và yêu cầu thanh toán để đổi lấy key giải mã. Nếu không có được key giải mã, thì về mặt toán học, nạn nhân không thể nào lấy lại quyền truy cập vào file.

**Cryptojacking**: Cryptojacking lây nhiễm vào trong máy tính và sử dụng các chu kỳ CPU để có thể đào Bitcoin. Phần mềm này cũng có thể chạy nền trên nhiều hệ điều hành, thậm chí là dưới dạng JavaScript trong cửa sổ trình duyệt.

**Malvertising**: Loại malware này sử dụng các quảng cáo hoặc mạng quảng cáo hợp pháp, nhằm âm thầm phát tán malware đến máy tính của người dùng.

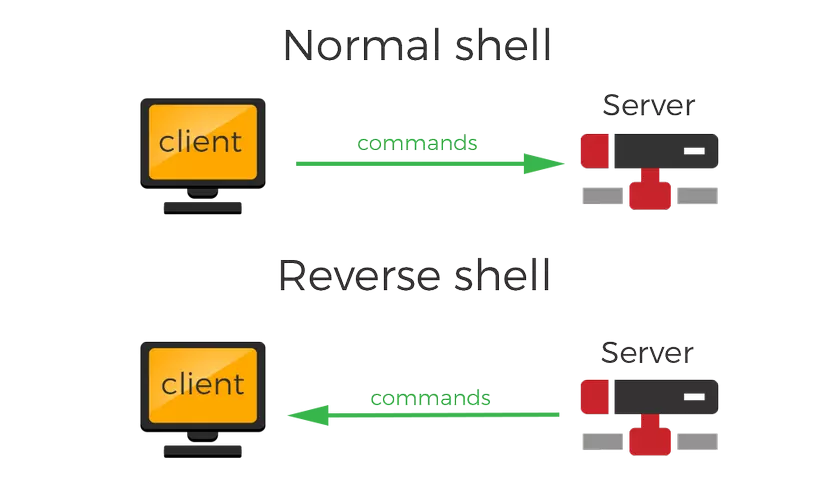
Bất kỳ malware cụ thể nào cũng đều có hai yếu tố: cách thức lây nhiễm và danh mục hành vi. Lấy ví dụ, WannaCry là một loại ransomware worm. Và một malware cụ thể cũng có thể có các dạng khác nhau, với những vector tấn công khác nhau. Chẳng hạn như Emotet banking malware có ở dạng trojan lẫn worm.

Hiện nay, vector lây nhiễm phổ biến nhất chính là qua email spam, nhằm lừa người dùng kích hoạt malware kiểu Trojan. WannaCry và Emotet chính là những malware phổ biến nhất, bên cạnh NanoCore, Gh0st – được gọi là Remote Access Trojans (RATs).

**1.3 Reverse shell**

***1.3.1 Khái niệm***

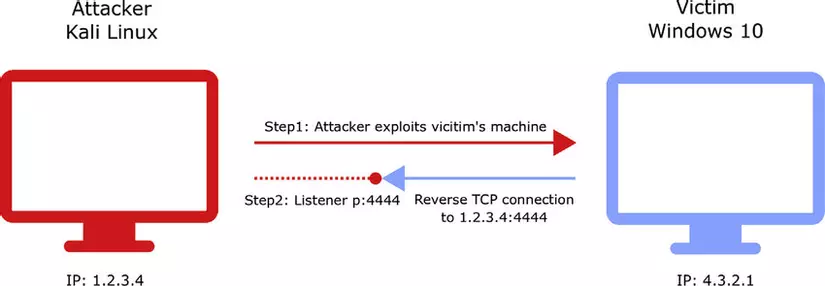
Reverse shell là 1 loại session shell (ngoài ra còn có web shell, bind shell,.. ) là shell có kết nối bắt nguồn từ 1 máy chủ đóng vai trò là target đến 1 máy chủ khác đóng vai trò host . Khi đó target sẽ tạo kết nối ra bên ngoài và host sẽ lắng nghe. Trong trường hợp Attacker mà đã khai thác được lỗ hổng có thể dẫn đến RCE có thể dùng Reverse shell để tạo kết nối đến máy attacker để hacker thao tác với máy target.



***1.3.2 Hình thức tấn công***

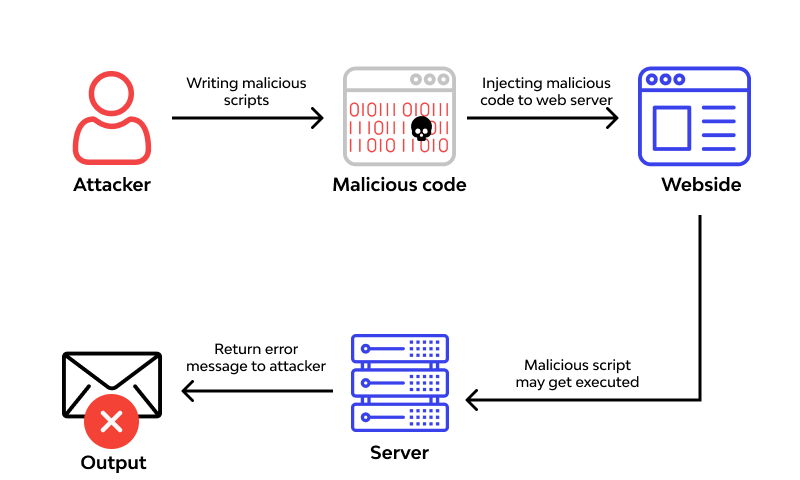
Reverse shell thường là cách duy nhất để thực hiện quản lý từ xa tới host thông qua NAT, cho nên nó cần quyền admin để sử dụng. Tuy nhiên , nó cũng có thể được tận dụng bởi tội phạm mạng để kết nối và thực thi các lệnh trên những máy chủ được bảo vệ bởi firewall hoặc hệ thống bảo mật mạng khác.

Khi thử tấn công đến server , kẻ tấn công thường thử khai thác các lỗ hổng về command injection ở trên hệ thống của mục tiêu . Các đoạn lệnh được inject thường là reverse shell script để cung cấp 1 môi trường thuận tiện cho việc sử dụng các command shell và thực thi các hành vi độc hại sau này.



***1.3.3 RCE***

RCE là viết tắt của Remote Code Execution, dịch ra tiếng Việt là Thực thi mã từ xa. RCE là [kỹ thuật tấn công mạng](https://quantrimang.com/cong-nghe/cac-kieu-tan-cong-mang-22) của hacker dựa vào lỗ hổng hoặc sơ hở nào đó của hệ thống để truy cập từ xa vào máy tính hoặc mạng máy tính của nạn nhân. Từ đó, hacker có thể thực thi các [mã độc](https://quantrimang.com/cong-nghe/10-loai-malware-dien-hinh-58733), phần mềm độc hại trên thiết bị của nạn nhân mà không cần tiếp xúc trực tiếp với thiết bị.

****

***1.3.4 Cách phòng tránh***

Để ngăn chặn các cuộc tấn công RCE, người dùng nên thường xuyên cập nhật phiên bản mới nhất cho các phần mềm của mình. Đa số các cuộc tấn công RCE đều dựa trên những lỗ hổng trong phần mềm hoặc hệ điều hành. Vì thế, việc cập nhật phiên bản phần mềm, hệ điều hành mới nhất là rất quan trọng.

Bên cạnh đó, bạn cũng nên cẩn trọng, quét virus kỹ càng trước khi nhấp vào các đường link đáng ngờ.

**Chương II - Trojan Horse Virus**

**2.1 Giới thiệu**

***2.1.1* Khái niệm**

**Trojan:** Nó thường thể hiện bản thân nó như một phần mềm hoặc gì đó hữu ích để đánh lừa người dùng.Không có khả năng tái tạo nhưng có thể giả dạng những mục tiêu mà người dùng muốn. Từ đó lừa họ kích hoạt để Trojan có thể phát tán. Cách lan truyền duy nhất là thông qua các thư điện tử hoặc thông qua các phần mềm miễn phí có đính kèm Trojan. Thông thường, tính năng chính của Trojan là nhắm đến những nhóm người dùng riêng để thu thập thông tin về hành vi và thói quen sử dụng internet của họ sau đó gửi các thông tin này về cho tin tặc. Tuy nhiên một số Trojan sẽ truy cập trái phép vào máy tính, từ đó Trojan có thể được sử dụng để đánh cắp thông tin tài chính hoặc cài đặt các dạng phần mềm độc hại khác, thường là Ransomware.

***2.1.2* Phát tán và hành động**

**Phát tán:**

- Đường dẫn và tệp tin đính kèm bên trong Email.

- Quá trình khai thác ứng dụng, cụ thể như các lỗ hổng bên trong trình duyệt web, ứng dụng hoặc phần mềm nhắn tin. Lỗ hổng này chủ yếu xuất phát từ việc khách hàng không thường xuyên cập nhật các bản vá lỗi của các nhà sản xuất.

-Vô tình tải xuống một số tệp độc hại có thể bị ẩn trong các banner hay pop-up quảng cáo, hoặc liên kết trên các trang web.

- Quá trình tải phần mềm từ những trang web lưu trữ tài nguyên hoặc các mạng chia sẻ tệp tin có chứa nhiều loại phần mềm độc hại, trong đó có cả trojan.

**Hành động:**

Trojan về nguyên lý thì giống nhau nhưng nó tồn tại một số hình thức hoạt động thường hay gặp như sau:

**Remote Access Trojans:** dịch ra có nghĩa là trojan kết nối từ xa, kẻ tấn công thực hiện phát tán trojan để kiểm soát máy tính của chúng ta từ xa.

**Data-Sending Trojans:** hình thức này sẽ sử dụng trojans để đánh cắp dữ liệu, gửi về cho kẻ tấn công.

**HTTP Trojans, FTP Trojans:** loại này sẽ khai thác lỗi của HTTP hoặc FTP server.

**Proxy Trojans**: Proxy trojan lợi dụng sơ hở để sử dụng máy tính của bạn như là một proxy server.

**Destructive Trojans:** đây là hình thức trojan có thể phá hủy hệ thống.

**Denial-of-Service Trojan:** loại này có thể vô hiệu hóa dịch vụ, sử dụng trong các cuộc tấn công DDoS.

**Security Software Disable Trojan:** trojan hoạt động theo cách này làm tắt các phần mềm bảo mật trên máy tính của bạn.

**Tổng hợp những loại Trojan phổ biến hiện nay:**

**Virus Trojan Backdoor** là một loại mã ẩn mình dưới dạng là phần mềm, để đánh lừa người dùng cài đặt vào bên trong hệ thống máy của mình. Sau khi đã thiết lập cài đặt thành công thì tin tặc sẽ có thể thực hiện được tất cả những truy xuất, xoá hoặc là truyền tải dữ liệu máy tính.

**Virus Trojan Rootkit** là một loại mã độc có chức năng che giấu và bảo vệ những loại phần mềm độc hại khác để người dùng không phát hiện được. Ưu điểm của nó chính là có thể ở lại lâu dài bên trong hệ thống máy tính và từ đó tăng thêm thời gian để thu thập thông tin, sử dụng cho mục đích xấu.

**Trình tải xuống Trojan** khá giống với các loại Virus tải tự động, nhiệm vụ của chúng sẽ giúp việc thúc đẩy phần mềm độc hại đã được cài đặt sẵn trong hệ thống máy để các kẻ xấu có thể xâm nhập nhanh hơn, tiện lợi hơn.

**Trojan-banker** là một loại mã độc được dùng cho mục đích đánh cắp các dữ liệu khách hàng lưu trữ tại các ngân hàng. Các dữ liệu mà tin tặc muốn thu thập đánh cắp chính là mã số tài khoản, số CVV, thông tin thẻ và dữ liệu cá nhân của khách hàng,…

**Trojan Zombifying** là loại mã chiếm quyền máy tính của người dùng để tạo ra được những botnet nhằm chuẩn bị có những cuộc tấn công DDoS khác.

**Download Trojan** sẽ là các phần mềm độc hại sau khi đã được cài đặt trên những ứng dụng độc hại khác như là keylogger, ransomware

**2.2 Trojan Horse Virus with image file**

***2.2.1* Ý tưởng**

Trong phần này mục tiêu chính của nhóm là thử nghiệm quá trình tạo lên 1 trojan horse loại Remote Access Trojan với mục đích nghiên cứu về quá trình tạo ra 1 trojan, và cách mà trojan sẽ hoạt động sau khi lây lan, nhằm hiểu biết hơn về cách tin tặc tạo ra trojan và phương pháp tấn công trojan để phòng vệ.



***2.2.2* Recipe**

- Kali linux (Attacker), Win 10 or win 7 (Victim), Random ảnh với đuôi .jpg + Image với đuôi .ico

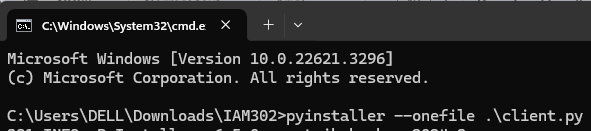
- Pyinstaller: [Install](https://pyinstaller.org/en/stable/)

- Source: [Code](https://github.com/3v01d3lu510n/IAM302)

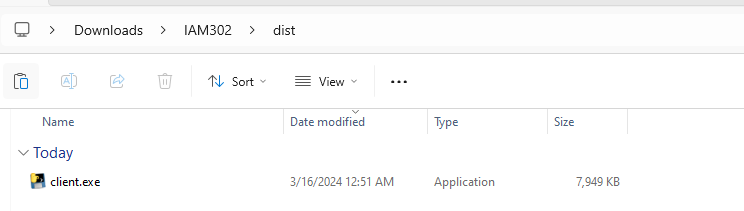
***2.2.3* Quy trình thực hiện**

Download code về máy để tiến hành giả mạo **image file** có chứa mã độc

Để code được thực thi khi nạn nhân click vào xem ảnh thì tức là chúng ta phải biến code thành 1 file **.exe**

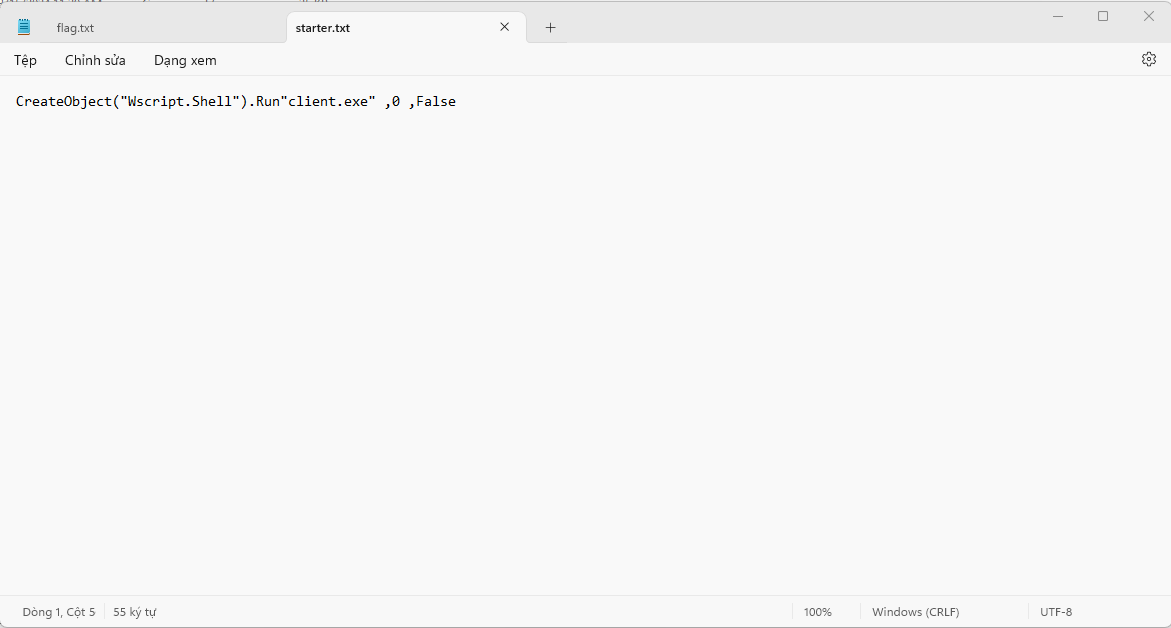


Vào folder **/dist** để lấy file **exe**

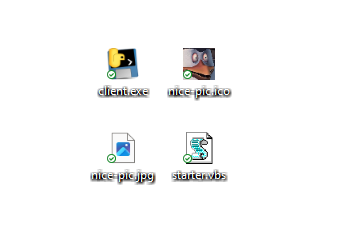
****

Sử dụng file **.ico** để làm icon cho file .**exe**

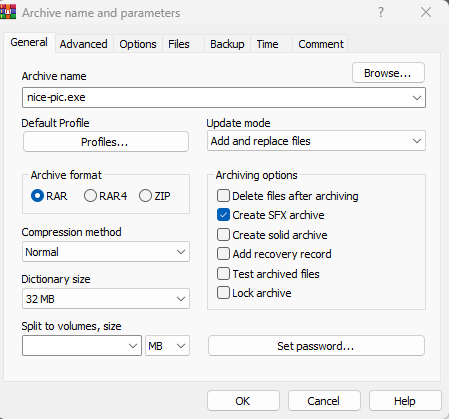
Tạo 1 shell script để chạy sau đó đổi đuôi file thành **.vbs**

****

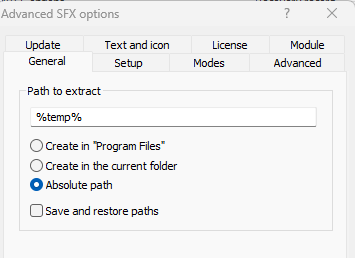
Những thứ chuẩn bị :

****

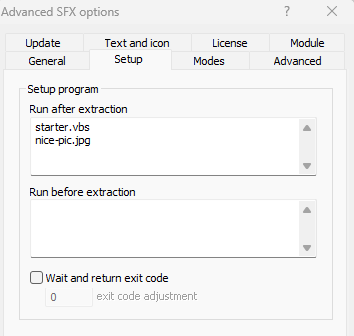
Gộp 3 file **.exe, .jpg, .vbs → Add to archive →** Archive name: **nice-pic.exe**

****

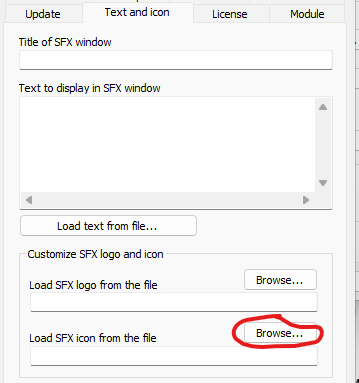
**Advance → SFX options →** **General** → %temp%



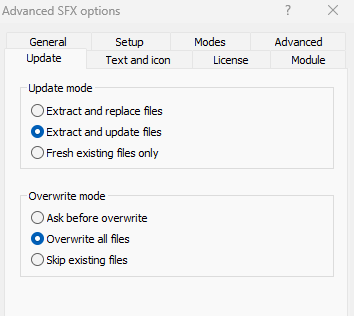
**Setup →** Run after → starter.vbs + nice-pic.jpg

****

**Text and icon →** Upload **.ico**

****

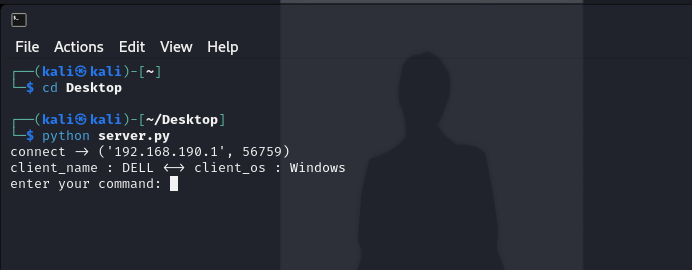
**Update →** Update all files + Overwrite

****

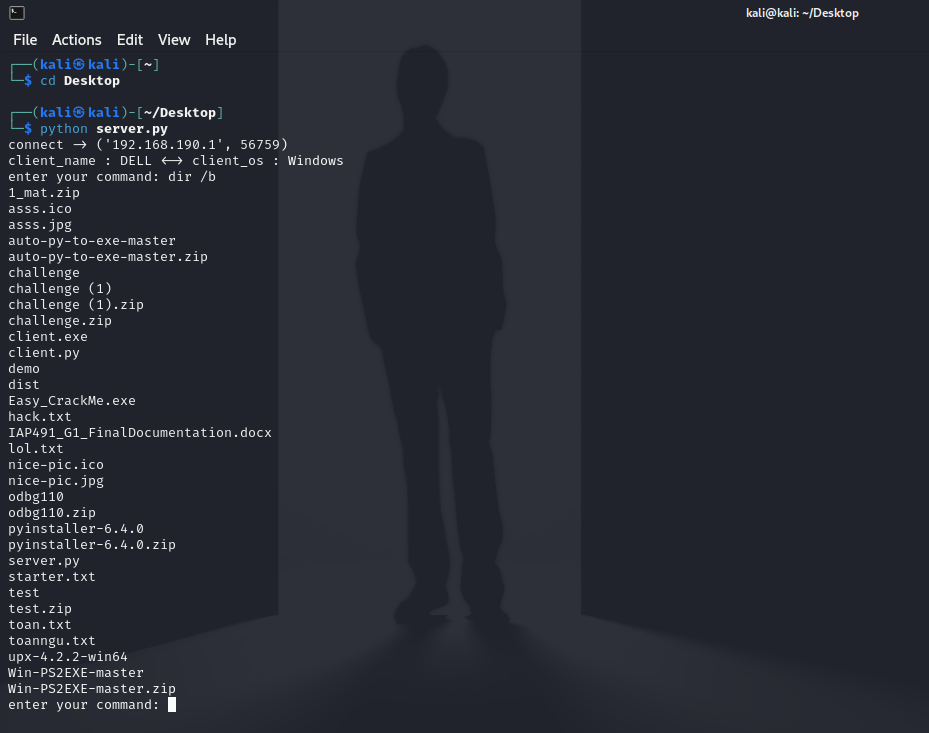
Sau khi hoàn thành gửi file image cho victim

**Về phía attacker**

Sau khi victim click vào file sẽ RCE thành công

****

Test thử 1 lệnh liệt kê file trong thư mục

****

**KẾT LUẬN**

Qua bài báo cáo này có thể thấy trên hành trình không ngừng nâng cao độ bảo mật của hệ thống máy tính và dữ liệu, việc tìm hiểu về cách thức hoạt động của Malware đã gia tăng sự hiệu quả trong việc phát hiện, thu thập thông tin và đánh giá rủi ro bảo mật hệ thống. Tìm hiểu về phương thức tấn công của tin tặc cũng là một phần quan trọng trong chiến lược an ninh mạng, cung cấp cái nhìn sâu rộng về các mẫu tấn công, kỹ thuật tấn công mới và hành vi của kẻ tấn công.

Việc triển khai Malware đòi hỏi sự tìm tòi và hiểu biết về cách thức hoạt và phát tán của loại Malware để khai thác lỗ hổng. Tuy nhiên, những thông tin thu được từ trải nghiệm này là đáng giá và đóng góp quan trọng vào việc cải thiện cả khả năng phòng ngừa lẫn phản ứng đối với các mối đe dọa mạng và lỗ hổng hệ thống.

Trong hệ thống bảo mật, lớp lá chắn bảo mật luôn phải được cập nhật và đi trước những kẻ xâm nhập. Hiện nay, các cuộc tấn công mạng đang dần trở nên tinh vi hơn, sử dụng công nghệ AI kết hợp hệ thống bảo mật đang vấn đề đáng được quan tâm. Tuy nhiên, công nghệ AI cũng tồn tại điểm yếu, các kẻ tấn công có thể lợi dụng ngược lại tìm được lỗ hổng và tấn công hệ thống. Vậy nên các nhà bảo mật luôn phải cập nhật thông tin và hiểu rõ về phương thức tấn công và cách hoạt động của các phần mềm Malware đẻ có thể đưa ra những giải pháp bảo mật tối ưu nhất.

**Tài liệu tham khảo**

[**https://vietnix.vn/malware-la-gi/**](https://vietnix.vn/malware-la-gi/)

[**https://viettelidc.com.vn/tin-tuc/malware-la-gi-nhung-thong-tin-quan-trong-ve-tan-cong-malware-3285/**](https://viettelidc.com.vn/tin-tuc/malware-la-gi-nhung-thong-tin-quan-trong-ve-tan-cong-malware-3285/)

[**https://viblo.asia/p/hieu-ro-ve-reverse-shells-LzD5ddE45jY**](https://viblo.asia/p/hieu-ro-ve-reverse-shells-LzD5ddE45jY)

[**https://whitehat.vn/threads/rce-vulnerable-va-cach-khai-thac.8255/**](https://whitehat.vn/threads/rce-vulnerable-va-cach-khai-thac.8255/)

[**https://didongviet.vn/dchannel/trojan/#ftoc-5-tong-hop-nhung-loai-trojan-pho-bien-hien-nay/**](https://didongviet.vn/dchannel/trojan/#ftoc-5-tong-hop-nhung-loai-trojan-pho-bien-hien-nay/)

[**https://fptshop.com.vn/tin-tuc/danh-gia/trojan-la-gi-cach-nhan-biet-va-phong-tranh-trojan-xam-nhap-vao-may-tinh-150686/**](https://fptshop.com.vn/tin-tuc/danh-gia/trojan-la-gi-cach-nhan-biet-va-phong-tranh-trojan-xam-nhap-vao-may-tinh-150686/)

[**https://www.aquasec.com/cloud-native-academy/cloud-attacks/reverse-shell-attack/**](https://www.aquasec.com/cloud-native-academy/cloud-attacks/reverse-shell-attack/)