**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**---🙠**🕮**🙢---**



**KHAI THÁC LỖ HỔNG PHẦN MỀM**

**NGHIÊN CỨU LỖ HỔNG CVE-2023-23397 VÀ CVE-2022-30190 TRÊN MICROSOFT**

Ngành: An toàn thông tin

*Sinh viên thực hiện***:**

**Lưu Văn Tùng – AT160456**

**Nguyễn Đức Thịnh – AT160446**

*Người hướng dẫn:*

**TS. Nguyễn Mạnh Thắng**

*Khoa An toàn thông tin – Học viện Kỹ thuật mật mã*

Hà Nội, 2023

**MỤC LỤC**

[**DANH MỤC KÝ HIỆU VIẾT TẮT III**](#_Toc134457310)

[**DANH MỤC HÌNH VẼ IV**](#_Toc134457311)

[**LỜI NÓI ĐẦU 1**](#_Toc134457312)

[**CHƯƠNG 1. Cơ sở lý thuyết liên quan đến lỗ hổng trên Microsoft 2**](#_Toc134457313)

[**1.1. Phương thức Windows NT LAN Manager 2**](#_Toc134457314)

[**1.1.1. Định nghĩa Windows NT LAN Manager 2**](#_Toc134457315)

[**1.1.2. Hoạt động của Windows NT LAN Manager 2**](#_Toc134457316)

[**1.1.3. Băm thông tin xác thực Net-NTLMv2 2**](#_Toc134457317)

[**1.2. Giới thiệu về Messaging Application Programming Interface 3**](#_Toc134457318)

[**1.2.1. Thuộc tính PidLidReminderFileParameter 3**](#_Toc134457319)

[**1.2.2. Thuộc tính PidLidReminderOverride 3**](#_Toc134457320)

[**1.3. Microsoft Support Diagnostic Tool trong microsoft 4**](#_Toc134457321)

[**1.3.1. MSDT URL 4**](#_Toc134457322)

[**1.3.2. MS-msdt MSProtocol URI 4**](#_Toc134457323)

[**1.4. Một số CVE 4**](#_Toc134457324)

[**1.5. Kết luận Chương 1 4**](#_Toc134457325)

[**CHƯƠNG 2. Tổng quan về CVE-2023-23397 và CVE-2022-30190 trên microsoft 5**](#_Toc134457326)

[**2.1. Tổng quan về lỗ hổng CVE-2023-23397 5**](#_Toc134457327)

[**2.1.1. Phát hiện lỗ hổng 5**](#_Toc134457328)

[**2.1.2. Phân tích hoạt động của lỗ hổng 5**](#_Toc134457329)

[**2.1.3. Cách thức tấn công CVE-2023-23397 với tấn công NTLM relay 8**](#_Toc134457330)

[**2.1.4. Ngăn chặn và giảm thiểu rủi ro 10**](#_Toc134457331)

[**2.2. Tổng quan về CVE-2022-30190 10**](#_Toc134457332)

[**2.2.1. Phát hiện lỗ hổng 11**](#_Toc134457333)

[**2.2.2. Phân tích Microsoft Word document bị lây nhiễm đầu tiên 11**](#_Toc134457334)

[**2.2.3. Các kịch bản khai thác lỗ hổng 11**](#_Toc134457335)

[**2.2.4. So sánh CVE-2022-30190 với CVE-2021-40444 12**](#_Toc134457336)

[**2.2.5. Ngăn chặn và giảm thiểu rủi ro 13**](#_Toc134457337)

[**CHƯƠNG 3. THỰC NGHIỆM 14**](#_Toc134457339)

[**3.1. Khai thác lỗ hổng CVE-2023-23397 14**](#_Toc134457340)

[**3.1.1. Mô hình triển khai 14**](#_Toc134457341)

[**3.1.2. Kịch bản triển khai và thực nghiệm 14**](#_Toc134457342)

[**3.1.3. Đánh giá 18**](#_Toc134457343)

[**3.2. Khai thác lỗ hổng CVE-2022-30190 18**](#_Toc134457344)

[**3.2.1. Mô hình triển khai 18**](#_Toc134457345)

[**3.2.2. Kịch bản triển khai và thực nghiệm 18**](#_Toc134457346)

[**3.2.3. Đánh giá 19**](#_Toc134457347)

[**3.3. Kết luận Chương 3 19**](#_Toc134457348)

[**KẾT LUẬN 20**](#_Toc134457349)

[**TÀI LIỆU THAM KHẢO 21**](#_Toc134457350)

# DANH MỤC HÌNH VẼ

**Hình 1.1 Trình tự tin nhắn để xác thực phiên SMB**

**Hình 2.1 Cơ chế tấn công CVE-2023-23397**

**Hình 2.2 Mô hình tấn công chuyển tiếp NTLM**

**Hình 2.3 Cách thức tấn công CVE-2023-23397 với tấn công NTLM relay**

**Hình 2.4 Ảnh minh họa PoC chứng minh thuộc tính “PidLidReminderFileParameter” đang được đặt với đường dẫn UNCHình 3.1 Mô hình triển khai CVE-2023-23397**

**Hình 3.2 Khởi chạy Responder để lắng nghe các xác thực trong giao diện mạng eth0**

**Hình 3.3 Đặt đường dẫn tệp âm thanh thành đường dẫn UNC trỏ đến máy kali**

**Hình 3.4 Outlook bỏ qua đường dẫn UNC và sử dụng file wav mặc định**

**Hình 3.5 Xem cuộc hẹn hiện tại từ outlookspy**

**Hình 3.6 Sử dụng task script**

**Hình 3.7 thông tin xác thực tại responder**

**Hình 3.8 Mô hình triển khai CVE-2022-30190**

**Hình 3.9 Kịch bản triển khai CVE-2022-30190**

# LỜI NÓI ĐẦU

Trong thời đại kỹ thuật số hiện nay, các cuộc tấn công mạng ngày càng tinh vi và phức tạp hơn bao giờ hết. Các nhà sản xuất phần mềm và nhà cung cấp dịch vụ mạng phải liên tục cập nhật sản phẩm và các giải pháp bảo mật để đối phó với các mối đe dọa mới. Việc giải quyết các lỗ hổng bảo mật trong các sản phẩm phần mềm là một việc làm rất quan trọng và cần thiết để giảm thiểu rủi ro bị tấn công mạng.

Microsoft là một công ty công nghệ lớn, công ty này đã có những đóng góp to lớn cho ngành công nghệ, đặc biệt là các sản phẩm như Windows và Office đã được sử dụng rộng rãi trên thế giới. Tuy nhiên Microsoft cũng gặp nhiều tranh cãi liên quan đến vấn đề bảo mật và quyền riêng tư. Trong đề tài này, nhóm em sẽ phân tích về hai lỗ hổng nghiêm trọng microsoft có ảnh hưởng lớn trong thời gian gần đây có mã là CVE-2023-23397 và CVE-2022-30190.

Mục tiêu của việc phân tích hai lỗ hổng CVE-2023-23397 trong Microsoft Outlook và CVE-2022-30190 trong Microsoft Office (Follina) là nhằm tìm hiểu và đánh giá mức độ nguy hiểm và tác động của các lỗ hổng này đến hệ thống và dữ liệu của người dùng. Bằng cách phân tích các lỗ hổng này, có thể hiểu rõ hơn về cách thức tấn công và điểm yếu của các sản phẩm của Microsoft, đồng thời cung cấp cho người dùng và nhà phát triển các thông tin cần thiết để tăng cường bảo mật cho hệ thống của mình.

Đề tài gồm 3 chương:

Chương 1: Cơ sở lý thuyết liên quan đến lỗ hổng trên Microsoft.

Chương 2: Tổng quan về CVE-2023-23397 và CVE-2022-30190 trên microsoft.

Chương 3: Triển khai thực nghiệm khai thác lỗ hổng.

# CƠ SỞ LÝ THUYẾT LIÊN QUAN ĐẾN LỖ HỔNG TRÊN MICROSOFT

## Giao thức xác thực NT LAN Manager

### Giới thiệu NT LAN Manager

NT LAN Manager (NTLM) là một giao thức xác thực mật khẩu được sử dụng để xác thực giữa máy khách và máy chủ. NTLM sử dụng một phương thức chứng thực thời gian thực để xác định danh tính của người dùng, yêu cầu người dùng cung cấp tên người dùng và mật khẩu. NTLM sử dụng một chuỗi băm của mật khẩu người dùng để tạo ra một mã băm và so sánh với mã băm được lưu trữ trong hệ thống để xác thực.

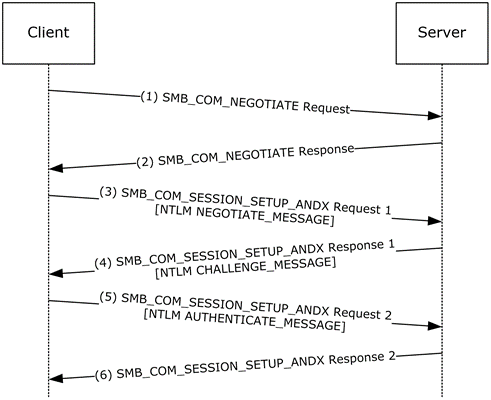
NTLM cũng hỗ trợ các tính năng như tính toàn vẹn và bảo mật thông tin trong quá trình truyền tải dữ liệu giữa máy khách và máy chủ. Tuy nhiên, NTLM đã bị thay thế bởi Kerberos vì nó không có tính năng bảo mật cao như Kerberos và không hỗ trợ tính năng đơn giản hóa đăng nhập một lần (Single Sign-On) như Kerberos. Xác thực Kerberos [MS-KILE] thay thế NTLM làm giao thức xác thực ưu tiên. Tuy nhiên, NTLM có thể được sử dụng khi Tiện ích mở rộng giao thức kerberos (KILE) không hoạt động, chẳng hạn như trong các trường hợp sau.

* Một trong các máy không hỗ trợ Kerberos.
* Máy chủ không được tham gia vào một miền.
* Cấu hình KILE không được thiết lập chính xác.
* Việc triển khai chọn sử dụng trực tiếp NLMP.

### NT LAN Manager qua Server Message Block

Server Message Block (SMB) là một giao thức chia sẻ tệp được sử dụng trong mạng Microsoft Windows. NTLM được sử dụng như một phương thức xác thực trong SMB để xác định danh tính của người dùng. Khi người dùng yêu cầu truy cập tệp trên một máy chủ, máy khách sẽ sử dụng SMB để yêu cầu máy chủ mở tệp. Khi đó, máy chủ sẽ yêu cầu xác thực người dùng bằng NTLM. Người dùng sẽ cung cấp tên người dùng và mật khẩu, sau đó NTLM sẽ được sử dụng để xác định xem người dùng có quyền truy cập vào tệp hay không.

Truyền tải NTLM qua Server Message Block (SMB) là cách sử dụng phổ biến của xác thực và mã hóa NTLM. Mặc dù KILE là phương thức xác thực ưa thích của phiên SMB, nhưng khi máy khách cố gắng xác thực với máy chủ SMB bằng giao thức KILE và không thành công, nó có thể cố gắng xác thực bằng NTLM.



Hình 1.1 Trình tự tin nhắn để xác thực phiên SMB

Bước 1 và 2: Giao thức SMB đàm phán các tùy chọn dành riêng cho giao thức bằng cách sử dụng thông báo request và response SMB\_COM\_NEGOTIATE. SMB\_COM\_NEGOTIATE được sử dụng để thiết lập phiên giao dịch đầu tiên. phiên giao dịch này bao gồm các thỏa thuận về các tham số kết nối như phiên bản giao thức, mã hóa, cấu trúc tên và định dạng thông điệp.

Bước 3: sau khi SMB\_COM\_NEGOTIATE được thiết lập phiên giao dịch đầu tiên giữa client và server, SMB\_COM\_SESSION\_SETUP\_ANDX được sử dụng để thiết lập một phiên làm việc SMB mới, trong đó client có thể thực hiện các hoạt động truy cập tài nguyên như tập tin, thư mục trên server..

Trong SMB\_COM\_SESSION\_SETUP\_ANDX, client gửi yêu cầu tới server để xác thực và thiết lập phiên làm việc. Yêu cầu này bao gồm thông tin xác thực như tên đăng nhập và mật khẩu của người dùng. Server sẽ kiểm tra thông tin xác thực và phản hồi lại với một mã thông báo xác thực. Nếu xác thực thành công, phiên làm việc sẽ được thiết lập và client sẽ có thể truy cập các tài nguyên được chia sẻ trên server.

Bước 4: Máy chủ response bằng thông báo phản hồi SMB\_COM\_SESSION\_SETUP\_ANDX trong đó NTLM CHALLENGE\_MESSAGE được nhúng. Thông báo bao gồm một số ngẫu nhiên 8 byte, được gọi là "challenge", mà máy chủ tạo và gửi trong trường ServerChallenge của thông báo.

Bước 5: Máy khách trích xuất trường ServerChallenge từ NTLM CHALLENGE\_MESSAGE và gửi NTLM AUTHENTICATE\_MESSAGE đến máy chủ. (được nhúng trong thông báo yêu cầu SMB\_COM\_SESSION\_SETUP\_ANDX).

Nếu challenge và response chứng minh rằng máy khách biết mật khẩu của người dùng, thì xác thực thành công và bối cảnh bảo mật của máy khách hiện được thiết lập trên máy chủ

Bước 6: Máy chủ gửi thông báo thành công được nhúng trong thông báo phản hồi SMB\_COM\_SESSION\_SETUP\_ANDX.

### Băm thông tin xác thực Net-NTLMv2

Băm thông tin xác thực Net-NTLMv2 là quá trình mã hóa một chuỗi thông tin xác thực sử dụng giao thức Net-NTLMv2. Giao thức này thường được sử dụng để xác thực người dùng và đăng nhập vào hệ thống mạng Windows.

Quá trình băm thông tin xác thực Net-NTLMv2 bao gồm các bước sau:

* Tạo chuỗi thử thách (challenge string): Máy chủ sẽ tạo một chuỗi thử thách ngẫu nhiên và gửi cho máy khách.
* Tạo mã hóa NTLMv2: Máy khách sẽ sử dụng thông tin đăng nhập và chuỗi thử thách để tạo ra một mã hóa NTLMv2.
* Truyền thông tin xác thực: Máy khách sẽ truyền thông tin xác thực của mình bao gồm tên đăng nhập, chuỗi thử thách và mã hóa NTLMv2 cho máy chủ.
* Băm thông tin xác thực: Máy chủ sẽ sử dụng các thông tin trên để băm (hash) thông tin xác thực bằng cách sử dụng một thuật toán mã hóa được xác định trước.

Quá trình này giúp đảm bảo tính bảo mật của thông tin xác thực khi được truyền trên mạng.

## Giới thiệu về Messaging Application Programming Interface

Messaging Application Programming Interface (MAPI) là một giao diện lập trình ứng dụng được Microsoft phát triển để hỗ trợ các ứng dụng email và messaging trên hệ thống Windows. MAPI cung cấp các API cho phép các ứng dụng gửi và nhận email, tin nhắn, lịch trình, liên lạc và các thông điệp khác giữa các ứng dụng khác nhau.

MAPI cung cấp một cơ chế để các ứng dụng có thể truy cập vào các dịch vụ email và messaging như Microsoft Exchange Server và Microsoft Outlook, cho phép chúng có thể gửi và nhận email, lập kế hoạch và quản lý liên lạc.

MAPI cũng hỗ trợ các tính năng khác nhau như mã hóa và xác thực để đảm bảo tính bảo mật của các thông tin truyền tải. Nó cũng cung cấp khả năng tương tác với các thiết bị di động và hỗ trợ đồng bộ hóa dữ liệu giữa các thiết bị khác nhau.

Các ứng dụng sử dụng MAPI bao gồm Microsoft Outlook, Microsoft Exchange Client, Windows Messaging, và nhiều ứng dụng email và messaging khác. Nó cũng được sử dụng để phát triển các ứng dụng email và messaging tùy chỉnh trên nền tảng Windows.

### Thuộc tính PidLidReminderFileParameter

Thuộc tính PidLidReminderFileParameter là một thuộc tính đối tượng trong Microsoft Outlook, được sử dụng để lưu trữ thông tin về tệp âm thanh được sử dụng để phát ra cảnh báo lịch hẹn.

Thuộc tính này là một chuỗi (string) và được sử dụng để chứa đường dẫn đầy đủ đến tệp âm thanh. Nó có mã định danh là "PidLidReminderFileParameter" và được lưu trữ trong thuộc tính mở rộng (custom property) của đối tượng lịch hẹn.

Khi một lịch hẹn có cảnh báo được thiết lập trong Microsoft Outlook, thuộc tính PidLidReminderFileParameter có thể được sử dụng để chỉ định tệp âm thanh được phát ra khi cảnh báo được kích hoạt. Ví dụ, giá trị của thuộc tính này có thể là đường dẫn đến tệp âm thanh "reminder.wav" trong thư mục mặc định của Outlook. Nếu thuộc tính này không được đặt giá trị, Outlook sẽ sử dụng âm thanh mặc định để phát ra cảnh báo.

### Thuộc tính PidLidReminderOverride

Thuộc tính PidLidReminderOverride là một thuộc tính đối tượng trong Microsoft Outlook, được sử dụng để ghi đè lặp lại các thiết lập cảnh báo mặc định của lịch hẹn.

Thuộc tính này là một giá trị Boolean và có mã định danh là "PidLidReminderOverride". Khi được đặt thành giá trị True, nó cho phép người dùng ghi đè cài đặt cảnh báo mặc định của Outlook và chọn một giá trị cảnh báo tùy chỉnh cho lịch hẹn. Nếu giá trị của thuộc tính là False, các cài đặt cảnh báo mặc định của Outlook sẽ được sử dụng.

Các giá trị khác của thuộc tính PidLidReminderOverride bao gồm:

* Giá trị Null: Cho phép Outlook tự động quyết định xem có hiển thị cảnh báo hay không dựa trên các cài đặt mặc định của ứng dụng.
* Giá trị False: Sử dụng cài đặt cảnh báo mặc định của Outlook cho lịch hẹn.
* Giá trị True: Cho phép người dùng ghi đè cài đặt cảnh báo mặc định của Outlook và chọn một giá trị cảnh báo tùy chỉnh cho lịch hẹn.

Thuộc tính PidLidReminderOverride cùng với thuộc tính PidLidReminderDelta được sử dụng để tùy chỉnh các cài đặt cảnh báo của lịch hẹn trong Outlook.

## Microsoft Support Diagnostic Tool trong microsoft

Microsoft Support Diagnostic Tool (MSDT) là một công cụ trong Microsoft Windows, được sử dụng để phát hiện và sửa chữa các vấn đề liên quan đến hệ thống hoặc ứng dụng trong Windows.

MSDT cung cấp một giao diện đồ họa dễ sử dụng để hỗ trợ người dùng phát hiện các sự cố hệ thống và xử lý các vấn đề đó. Công cụ này có thể được sử dụng để khắc phục các vấn đề liên quan đến các ứng dụng Microsoft như Microsoft Office, Microsoft Outlook, Microsoft Edge và các dịch vụ của Microsoft.

MSDT được thiết kế để giúp người dùng tự chẩn đoán và giải quyết các sự cố hệ thống cơ bản, nhưng nó không thay thế được việc sử dụng các công cụ chuyên nghiệp hơn để xử lý các sự cố phức tạp hơn.

Để sử dụng Microsoft Support Diagnostic Tool, người dùng có thể tìm kiếm "MSDT" trên máy tính của mình và chạy công cụ này. Sau đó, họ có thể chọn các phương pháp chẩn đoán khác nhau được cung cấp bởi MSDT để tìm ra nguyên nhân của sự cố hệ thống và thực hiện các bước khắc phục.

### MSDT URL

MSDT URL trong Microsoft là một đường dẫn đến công cụ Microsoft Support Diagnostic Tool (MSDT), được sử dụng để tự động phát hiện và giải quyết các vấn đề kỹ thuật trên hệ thống Windows của bạn. Để sử dụng MSDT, bạn có thể truy cập vào đường dẫn "msdt.exe" trên Windows và cung cấp các thông tin yêu cầu khi được hỏi. Tuy nhiên, không có một URL cụ thể cho MSDT, vì nó được tích hợp sẵn trong hệ thống Windows và không phải là một ứng dụng web độc lập.

### MS-msdt MSProtocol URI

MS-msdt là một URI (Uniform Resource Identifier) được sử dụng để kích hoạt Microsoft Support Diagnostic Tool (MSDT) trên máy tính chạy hệ điều hành Windows. Khi người dùng truy cập vào URI này, nó sẽ mở MSDT và cho phép người dùng chọn các tùy chọn chẩn đoán khác nhau để giải quyết sự cố hệ thống hoặc ứng dụng trên máy tính.

Tuy nhiên, điều kiện để sử dụng MS-msdt URI là MSDT phải được cài đặt trên máy tính của người dùng. Nếu MSDT chưa được cài đặt, người dùng cần truy cập trang web hỗ trợ của Microsoft để tải xuống và cài đặt công cụ trên máy tính của mình. MS-msdt cũng được sử dụng trong các liên kết hỗ trợ của Microsoft, cho phép người dùng truy cập trực tiếp vào chức năng chẩn đoán sự cố của MSDT thông qua các liên kết trên trang web hỗ trợ của Microsoft.

## Một số CVE liên quan

### CVE-2023-29324

* Nhà nghiên cứu Ben Barnea của Akamai đã tìm thấy một lỗ hổng quan trọng mới trong một thành phần của Internet Explorer, có mã CVE-2023-29324 với điểm số CVSS là 6,5.
* Lỗ hổng khiến chức năng *MapUrlToZone của* Window API nghĩ sai rằng đường dẫn từ xa là đường dẫn cục bộ.
* *MapUrlToZone* thường được sử dụng như một biện pháp bảo mật. Đặc biệt, nó được sử dụng để giảm thiểu lỗ hổng nghiêm trọng của Outlook CVE-2023-23397 được vá trong Bản vá thứ Ba của tháng Ba.
* Kẻ tấn công không được xác thực trên internet có thể sử dụng lỗ hổng bảo mật để ép buộc máy khách Outlook kết nối với máy chủ do kẻ tấn công kiểm soát. Điều này dẫn đến hành vi trộm cắp thông tin đăng nhập NTLM. Đây là một lỗ hổng zero-click, có nghĩa là nó có thể được kích hoạt mà không cần sự tương tác của người dùng.
* Tất cả các phiên bản Windows đều bị ảnh hưởng bởi lỗ hổng. Do đó, tất cả các phiên bản máy khách Outlook trên Windows đều có thể khai thác được. Tuy nhiên, theo Microsoft, các máy chủ Exchange với bản cập nhật tháng 3 đã bỏ qua tính năng dễ bị tấn công, do đó ngăn chặn các máy khách dễ bị khai thác.

Vấn đề đã được báo cáo cho Microsoft và được cập nhật vào Bản vá Thứ Ba tháng 5 năm 2023.

### CVE-2021-40444

CVE-2021-40444 là một lỗ hổng bảo mật trong phần mềm Microsoft Office. Lỗ hổng này cho phép tin tặc tấn công từ xa và thực thi mã độc trên hệ thống mà không cần sự cho phép của người dùng.

Lỗ hổng này được phát hiện trong một tệp PowerPoint bị lỗi được gửi qua email hoặc truyền qua mạng, và có thể được kích hoạt khi người dùng mở tệp tin đó bằng Microsoft Office trên máy tính của mình. Khi lỗ hổng này được khai thác, tin tặc có thể thực thi mã độc trên hệ thống bị nhiễm và chiếm quyền kiểm soát hoàn toàn hệ thống đó.

Microsoft đã phát hành một bản vá khẩn cấp để khắc phục lỗ hổng này. Người dùng nên cập nhật các bản vá và phần mềm của mình để đảm bảo an toàn cho hệ thống của mình. Ngoài ra, người dùng cũng nên hạn chế mở tệp tin không rõ nguồn gốc hoặc từ các nguồn không tin cậy để đảm bảo an toàn hơn cho hệ thống của mình.

# Tổng quan về CVE-2023-23397 và CVE-2022-30190 trên microsoft

## Tổng quan về lỗ hổng CVE-2023-23397

**CVE-2023-23397** là một lỗ hổng nâng cao đặc quyền/bỏ qua xác thực quan trọng trong Outlook, được phát hành trong March Patch Tuesday của Microsoft. Lỗ hổng ảnh hưởng đến tất cả các phiên bản của Windows Outlook, được xếp hạng 9,8 CVSS và là một trong hai zero-day được tiết lộ vào ngày 14 tháng 3.

### Phát hiện lỗ hổng

CVE-2023-23397 đã được khai thác tích cực ít nhất từ tháng 4 năm 2022 và được sử dụng để xâm phạm mạng của ít nhất 15 tổ chức chính phủ, quân đội, năng lượng và vận tải ở châu Âu.

Mặc dù Microsoft công khai liên kết các cuộc tấn công này với "một tác nhân đe dọa có trụ sở tại Nga", Redmond cũng cho biết trong một báo cáo phân tích mối đe dọa riêng tư mà BleepingComputer đã xem rằng họ tin rằng nhóm tấn công là APT28 (còn được theo dõi là STRONTIUM, Sednit, Sofacy và Fancy Bear) .

Tác nhân đe dọa này trước đây đã được liên kết với Tổng cục Chính của Bộ Tổng tham mưu Lực lượng Vũ trang Liên bang Nga (GRU), cơ quan tình báo quân sự của Nga.

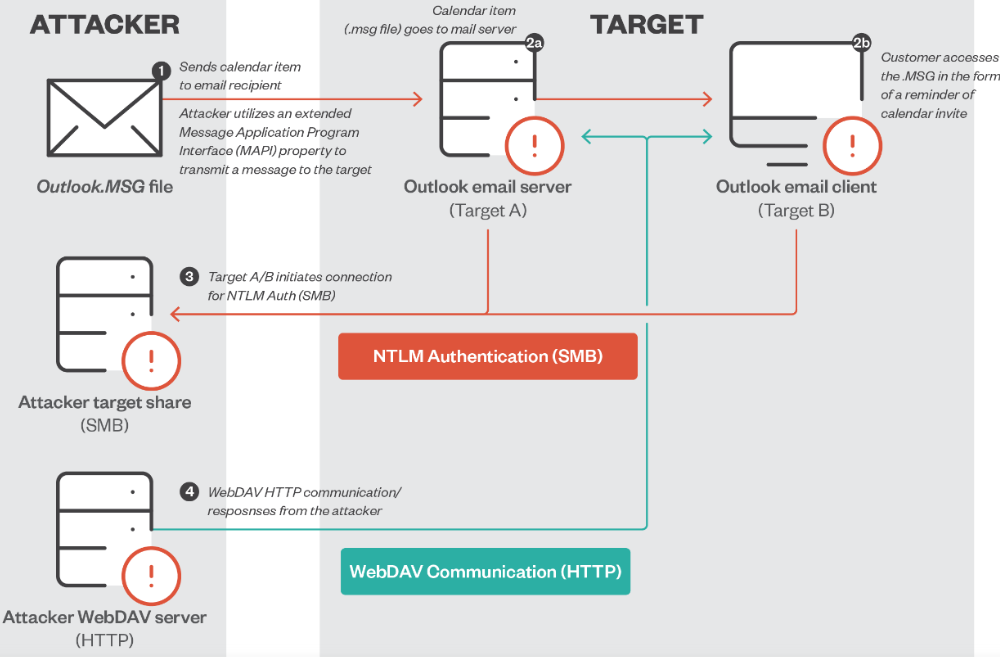
Thông tin đăng nhập mà chúng đánh cắp trong các cuộc tấn công này đã được sử dụng để di chuyển ngang và thay đổi quyền đối với thư mục hộp thư Outlook, một chiến thuật cho phép chúng lọc email từ các tài khoản cụ thể.

Nhóm Ứng phó Sự cố của Microsoft cho biết thêm: "Mặc dù tận dụng các hàm băm NTLMv2 để giành quyền truy cập trái phép vào tài nguyên không phải là một kỹ thuật mới, nhưng việc khai thác CVE-2023-23397 là mới lạ và lén lút".

"Ngay cả khi người dùng báo cáo lời nhắc đáng ngờ về các tác vụ, việc xem xét bảo mật ban đầu đối với các tin nhắn, tác vụ hoặc mục lịch có liên quan cũng không dẫn đến việc phát hiện ra hoạt động độc hại. Hơn nữa, việc thiếu bất kỳ tương tác bắt buộc nào của người dùng góp phần tạo nên tính chất độc nhất của lỗ hổng này ."

### Phân tích hoạt động của lỗ hổng

**CVE-2023-23397** là lỗ hổng nâng cao đặc quyền (EoP) trong Microsoft Outlook. Đây là một zero-touch exploit, có nghĩa là lỗ hổng bảo mật yêu cầu mức độ phức tạp thấp để khai thác và không yêu cầu tương tác của người dùng.



**Hình 2.1 Cơ chế tấn công CVE-2023-23397**

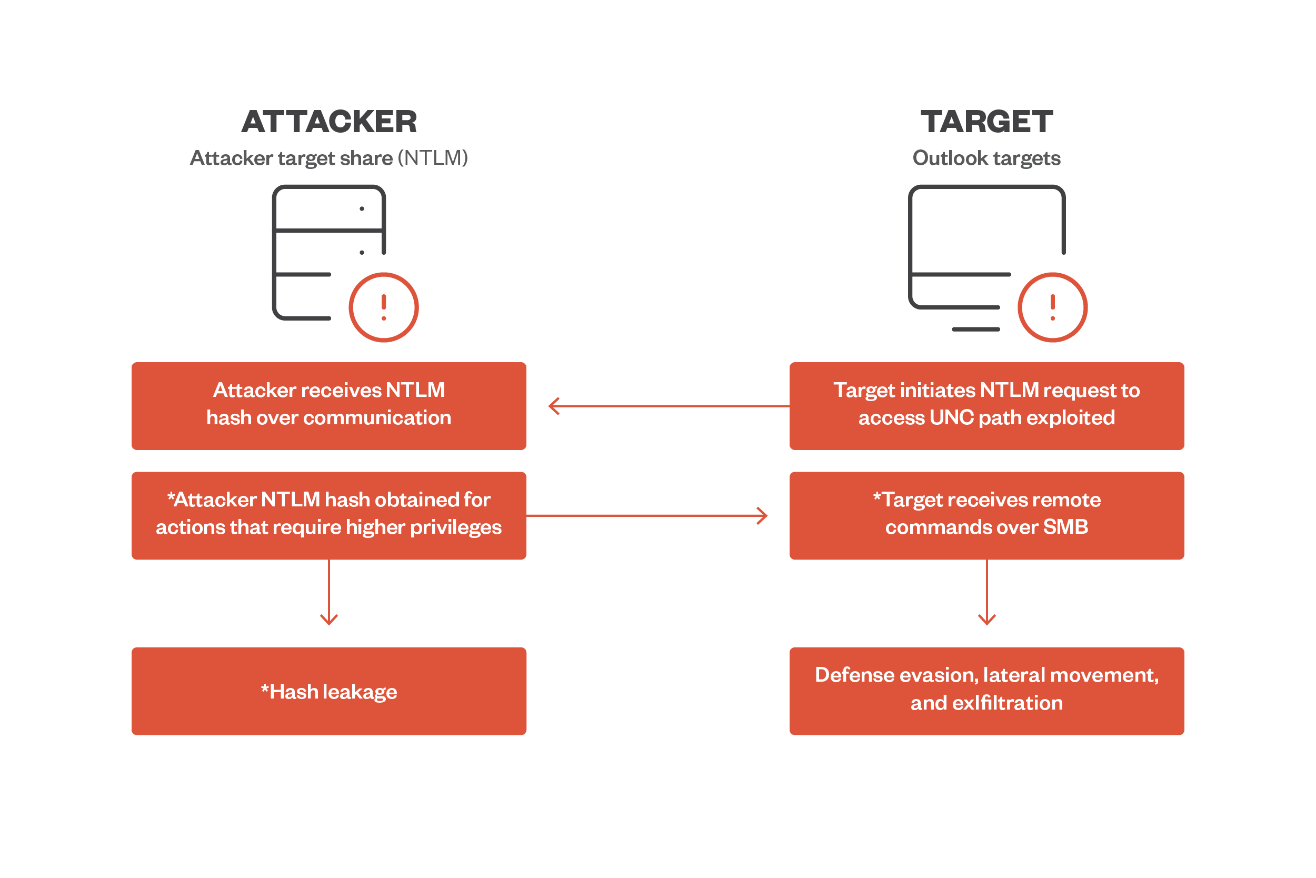
Tin tặc đã khai thác lỗ hổng **CVE-2023-23397** bằng cách lợi dụng tính năng tạo lịch hẹn phổ biến trên Outlook – cho phép gửi email thông báo đến người dùng, từ đó đánh cắp mã băm NTLM của người dùng từ xa.

Kẻ tấn công gửi một tin nhắn cho nạn nhân với thuộc tính Message Application Program Interface (MAPI) mở rộng với đường dẫn Universal Naming Convention (UNC) tới  Server Message Block (SMB, via TCP 445) do kẻ tấn công kiểm soát. Kẻ tấn công gửi lời mời lịch độc hại.msg — định dạng thông báo hỗ trợ lời nhắc trong Outlook — để kích hoạt điểm API dễ bị tấn công PlayReminderSound bằng cách sử dụng “PidLidReminderFileParameter” (tùy chọn âm thanh cảnh báo tùy chỉnh cho lời nhắc).

Khi nạn nhân kết nối với máy chủ SMB của kẻ tấn công, máy chủ này sẽ tự động gửi thông báo New Technology LAN Manager (NTLM) tới người dùng, tin nhắn này có thể được sử dụng để xác thực đối với các hệ thống khác hỗ trợ xác thực NTLM.

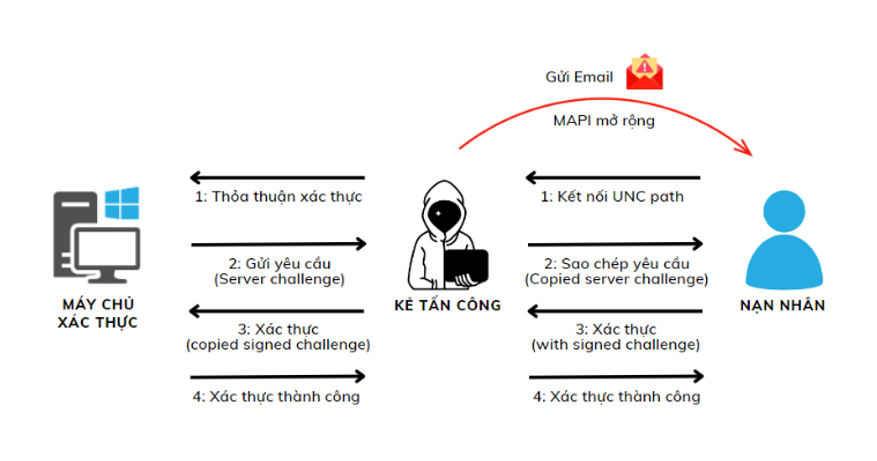
Băm NTLMv2 là giao thức mới nhất mà Windows sử dụng để xác thực và giao thức này được dùng cho một số dịch vụ với mỗi phản hồi chứa biểu diễn băm của thông tin người dùng, chẳng hạn như tên người dùng và mật khẩu. Do đó, kẻ tấn công có thể thực hiện một cuộc tấn công chuyển tiếp NTLM để giành quyền truy cập vào các dịch vụ khác hoặc xâm phạm toàn bộ miền nếu người dùng bị xâm phạm là quản trị viên. Mặc dù các dịch vụ trực tuyến như Microsoft 365 không dễ bị tấn công bởi vì chúng không hỗ trợ xác thực NTLM, ứng dụng Microsoft 365 Windows Outlook vẫn dễ bị tấn công.

Tương tác của người dùng là không cần thiết để kích hoạt (ngay cả trước khi xem trước tin nhắn), cũng như không yêu cầu đặc quyền cao. CVE-2023-23397 là một lỗ hổng zero-touch được kích hoạt khi nạn nhân nhận được lời nhắc và thông báo (ví dụ: khi một cuộc hẹn hoặc nhiệm vụ nhắc năm phút trước thời gian được chỉ định). Rất khó để chặn lưu lượng SMB gửi đi cho người dùng từ xa. Kẻ tấn công có thể sử dụng cùng thông tin đăng nhập để có quyền truy cập vào các tài nguyên khác.



**Hình 2.2 Mô hình tấn công chuyển tiếp NTLM**

### Cách thức tấn công CVE-2023-23397 với tấn công NTLM relay



**Hình 2.3 Cách thức tấn công CVE-2023-23397 với tấn công NTLM relay**

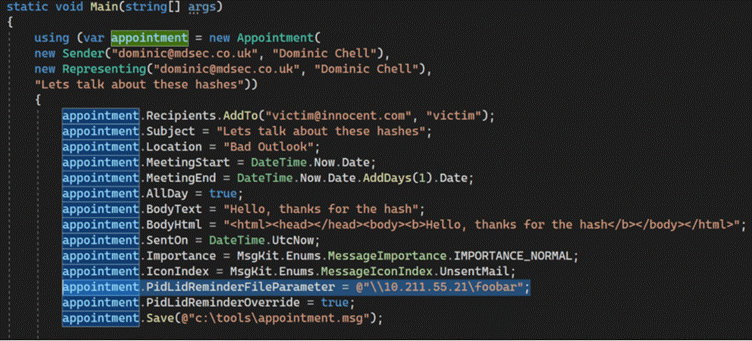
Kẻ tấn công tạo cuộc hẹn bằng cách tùy chỉnh thuộc tính trong MAPI (Message Application Program Interface - một API dành cho Microsoft Windows cho phép các chương trình nhận biết và quản lý email) đáng lẽ phải bao gồm thông tin về cuộc hẹn như chủ đề, thời gian, thành phần tham gia… được lưu vào file có định dạng .msg. Tuy nhiên kẻ tấn công lại đưa vào một đường dẫn UNC độc hại thay vì tên của một file .wav hoặc file âm thanh để có thể kết nối đến máy chủ chia sẻ tài nguyên SMB (TCP 445) do chúng kiểm soát. Khi nhận được email này, máy tính client thực hiện gửi yêu cầu xác thực NTLM đến máy chủ của kẻ tấn công.

Theo Microsoft, lỗ hổng lợi dụng 2 thuộc tính trong MAPI gồm: “PidLidReminderFileParamete”, “PidLidReminderOverride” để có thể thực thi theo sự tính toán của kẻ tấn công.

Trước tiên, thuộc tính “PidLidReminderFileParameter” là một giá trị chỉ định tên tệp cho file .wav hoặc file audio, được phát dưới dạng âm báo và âm thanh thông báo lời nhắc khi cuộc họp đã trôi qua hoặc một sự kiện đã quá hạn. Và kẻ tấn công đã lợi dụng thuộc tính này để chèn đường dẫn UNC vào.

Tiếp theo, thuộc tính “PidLidReminderOverride” sẽ đảm bảo file .msg được sử dụng khi đặt giá trị thành “True”.

Dưới đây là hình minh họa PoC chứng minh thuộc tính “PidLidReminderFileParameter” đang được đặt với đường dẫn UNC.

  
**Hình 2.4 Ảnh minh họa PoC chứng minh thuộc tính “PidLidReminderFileParameter” đang được đặt với đường dẫn UNC**

Khi hai thuộc tính này được kích hoạt (gửi email) sử dụng đường dẫn UNC sẽ tạo các yêu cầu truy cập tài nguyên bất kỳ do kẻ tấn công chỉ định và tham gia vào quá trình xác thực NTLM dẫn đến rò rỉ các giá trị băm nhạy cảm có chứa thông tin xác thực người dùng.

Với thông tin này, kẻ tấn công sẽ có thể lấy được các thông tin đăng nhập ở dạng văn bản rõ hoặc thực hiện tấn công NTLM relay.

### Ngăn chặn và giảm thiểu rủi ro

Lỗ hổng này đang được khai thác rộng rãi hiện nay. Một số bước được đề xuất theo khuyến nghị của Microsoft để giảm thiểu và tránh cuộc tấn công này là

* Thêm người dùng vào Nhóm bảo mật người dùng được bảo vệ, điều này ngăn việc sử dụng NTLM làm cơ chế xác thực.
* Chặn TCP 445/SMB gửi đi từ mạng của bạn để tránh mọi kết nối sau khai thác.
* Sử dụng tập lệnh PowerShell do Microsoft phát hành để quét máy chủ Exchange nhằm phát hiện bất kỳ nỗ lực tấn công nào.
* Tắt dịch vụ WebClient để tránh kết nối webdav.

Trước tình hình ngày càng gia tăng của các cuộc tấn công mạng và những lỗ hổng mới được phát hiện mỗi ngày, CVE-2023-23397 trên Microsoft Outlook là một minh chứng rõ ràng cho sự cần thiết của việc bảo vệ hệ thống và dữ liệu cá nhân nhằm tránh bị kẻ xấu thu thập thông tin như tài khoản, địa chỉ email làm mục tiêu để tấn công. Việc nhanh chóng cập nhật bản vá và áp dụng các giải pháp an ninh khác trong doanh nghiệp hoặc tổ chức cần được thực hiện luôn và ngay.

## Tổng quan về CVE-2022-30190

CVE-2022-30190 có tên là follina trong microsoft office. Lỗ hổng được các chuyên gia phát hiện một cách tình cờ khi phân tích mẫu mã độc được tải lên Virus Total, từ đó mới nhận thấy nó đang bị khai thác trên thực tế.

Tuy điểm CVSS không quá cao nhưng chỉ bằng cách lừa người dùng mở hoặc xem một tài liệu Word có đính kèm link HTML độc hại thì mã độc đã được triển khai trên máy của nạn nhân. Nó sẽ tận dụng công cụ chẩn đoán (MS-MSDT) và trình dòng lệnh (PowerShell) có sẵn trên Windows để thực thi mã từ xa trên thiết bị của nạn nhân từ đó cài đặt chương trình, xem, thay đổi hoặc xóa dữ liệu, tạo tài khoản mới.

### Phát hiện lỗ hổng

Để phát hiện lỗ hổng bảo mật CVE-2022-30190, thực hiện các bước sau:

1. Cập nhật và vá lỗ hổng: Việc cập nhật và vá các lỗ hổng bảo mật là điều quan trọng nhất để đảm bảo an toàn cho hệ thống của bạn. Microsoft đã phát hành một bản vá để khắc phục lỗ hổng CVE-2022-30190. Vì vậy, hãy đảm bảo rằng bạn đã cập nhật hệ thống của mình đầy đủ và thực hiện các bản vá lỗi bảo mật.
2. Sử dụng phần mềm antivirus: Sử dụng phần mềm antivirus có thể giúp phát hiện các tệp độc hại được liên kết với lỗ hổng CVE-2022-30190. Hãy đảm bảo rằng các phần mềm antivirus của bạn đã được cập nhật và đang chạy đầy đủ.
3. Kiểm tra các nội dung của tài liệu: Trong trường hợp lỗ hổng này được khai thác thông qua các tài liệu Excel được tạo ra để khai thác lỗ hổng, kiểm tra nội dung của các tài liệu được mở để đảm bảo tính hợp pháp và đáng tin cậy của tài liệu.
4. Theo dõi các lưu lượng mạng: Hãy theo dõi các lưu lượng mạng đến và đi từ hệ thống của bạn, đặc biệt là các kết nối đến các địa chỉ IP đáng ngờ hoặc các lưu lượng được mã hóa với cổng bất thường.
5. Sử dụng các công cụ phát hiện xâm nhập: Các công cụ phát hiện xâm nhập như snort, Suricata... có thể giúp phát hiện các tệp độc hại được liên kết với lỗ hổng CVE-2022-30190 bằng cách theo dõi các lưu lượng mạng.
6. Học hỏi từ các báo cáo về các cuộc tấn công khác: Việc theo dõi các cuộc tấn công tương tự hoặc các báo cáo về các cuộc tấn công từ các trang tin tức, các nhà nghiên cứu bảo mật, các hãng an ninh mạng sẽ giúp bạn hiểu được cách thức cuộc tấn công được thực hiện và biết thêm về các kỹ thuật và công cụ được sử dụng để khai thác lỗ hổng.

### Phân tích Microsoft Word document bị lây nhiễm đầu tiên

Lỗ hổng bảo mật CVE-2022-30190 có liên quan đến việc giải mã các tài liệu Excel được khai thác. Vì vậy, để phân tích một tài liệu Microsoft Word bị lây nhiễm đầu tiên của CVE-2022-30190, bạn có thể thực hiện các bước sau:

a. Chuyển đổi tài liệu Word sang định dạng văn bản đơn giản như .txt, .rtf hoặc .html để xem mã nguồn của tài liệu.

b. Xem mã nguồn của tài liệu để tìm kiếm các chuỗi ký tự đáng ngờ hoặc các đoạn mã lạ.

c. Kiểm tra xem tài liệu có chứa liên kết đến các tài liệu Excel hay không. Nếu có, kiểm tra các tệp Excel liên quan để xác định xem chúng có được mã hóa hay không.

d. Sử dụng các công cụ phân tích mã độc như IDA Pro, OllyDbg, hoặc Immunity Debugger để phân tích các mã độc bên trong tài liệu.

e. Sử dụng một công cụ phân tích mã độc chuyên dụng để phát hiện các mã độc bên trong tài liệu. Các công cụ phân tích mã độc nổi tiếng bao gồm VirusTotal, Hybrid Analysis hoặc Cuckoo Sandbox.

f. Đối với các mã độc có chứa Macro, có thể sử dụng một công cụ như oledump để phân tích và tìm thấy các Macro trong tài liệu.

g. Kiểm tra các thành phần của tài liệu, như các hình ảnh hoặc bảng, để đảm bảo chúng không bị lây nhiễm bởi phần mềm độc hại.

h. Tìm kiếm bất kỳ thông tin nào về người gửi hoặc thông tin liên quan đến tài liệu để đảm bảo tính xác thực của nó.

i. Đối với các tài liệu quan trọng hơn, nên sử dụng các công cụ phân tích thủ công hơn để phân tích mã độc chi tiết hơn.

### Các kịch bản khai thác lỗ hổng

Lỗ hổng **CVE-2022-30190** có thể bị khai thác bằng nhiều cách khác nhau để tấn công người dùng. Dưới đây là một số kịch bản khai thác lỗ hổng này:

1. Tấn công phần mềm độc hại từ xa: Tin tặc có thể khai thác lỗ hổng này để thực thi mã độc từ xa trên máy tính của người dùng. Khi thành công, phần mềm độc hại có thể làm cho máy tính hoạt động chậm hơn, thu thập thông tin cá nhân của người dùng hoặc thậm chí điều khiển từ xa máy tính của người dùng.
2. Đánh cắp thông tin cá nhân: Nếu tin tặc khai thác thành công lỗ hổng này, họ có thể tiếp cận các thông tin cá nhân của người dùng, chẳng hạn như tài khoản đăng nhập và mật khẩu, thông tin thẻ tín dụng, thông tin cá nhân và lịch sử duyệt web của người dùng.
3. Tấn công tiêm cái Rootkit: Nếu tin tặc khai thác lỗ hổng này, họ có thể cài đặt tiêm cái rootkit để kiểm soát máy tính của người dùng. Điều này cho phép tin tặc có quyền truy cập và kiểm soát hoàn toàn máy tính của người dùng mà không được phép.

Vì vậy, người dùng nên cập nhật trình duyệt Chromium của mình lên phiên bản mới nhất để tránh bị khai thác lỗ hổng này và giữ an toàn cho thông tin cá nhân của mình.

### So sánh CVE-2022-30190 với CVE-2021-40444

CVE-2021-40444 là một lỗ hổng bảo mật trong phần mềm Microsoft Office được phát hiện vào năm 2021. Lỗ hổng này cho phép kẻ tấn công tạo ra tài liệu độc hại được thiết kế để khai thác lỗ hổng thông qua một công cụ phân tích tài liệu của Office. Nếu người dùng mở tài liệu này, kẻ tấn công có thể thực hiện mã độc trên hệ thống của nạn nhân.

CVE-2022-30190 cũng là một lỗ hổng bảo mật trong phần mềm Microsoft Office. Lỗ hổng này được phát hiện vào năm 2022 và dự báo sẽ được khai thác để tiến hành các cuộc tấn công nhắm vào các doanh nghiệp. Lỗ hổng này cho phép kẻ tấn công thực thi mã từ xa thông qua một tài liệu Excel được tạo ra để khai thác lỗ hổng.

Tổng quan về hai lỗ hổng này cho thấy cả hai đều rất nguy hiểm và có thể cho phép kẻ tấn công thực hiện các cuộc tấn công từ xa. Tuy nhiên, CVE-2022-30190 được cho là khó khăn hơn khi tạo ra tài liệu tấn công hơn so với CVE-2021-40444 . Do đó, nó có thể đòi hỏi kinh nghiệm kỹ thuật cao hơn để khai thác lỗ hổng này.

### Ngăn chặn và giảm thiểu rủi ro

Để ngăn chặn và giảm thiểu rủi ro của lỗ hổng **CVE-2022-30190**, người dùng nên thực hiện các hành động sau đây:

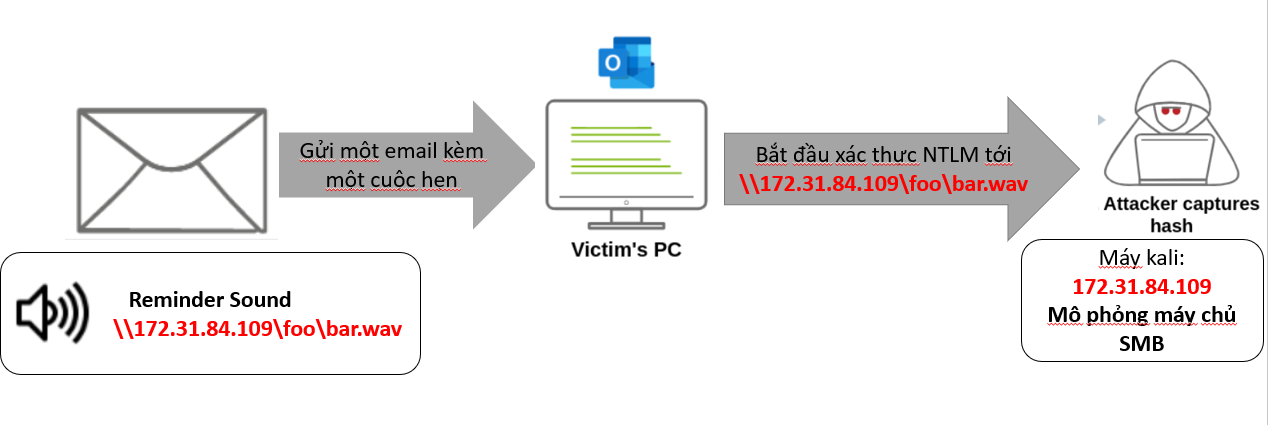
1. Cập nhật trình duyệt: Người dùng nên cập nhật trình duyệt Chromium của mình lên phiên bản mới nhất để đảm bảo được sửa chữa cho lỗ hổng này.
2. Sử dụng Antivirus: Người dùng nên sử dụng phần mềm diệt virus/antivirus để ngăn chặn lọt vào máy tính của mình các phần mềm độc hại tràn vào máy tính qua các kênh tấn công khác.
3. Cẩn trọng khi truy cập website: Người dùng nên cẩn trọng khi truy cập và download các tệp tin từ các website lạ hoặc đích danh và không tin tưởng.
4. Sử dụng Firewall: Người dùng có thể sử dụng tường lửa để ngăn chặn các kết nối không được ủy quyền đến các máy tính bên ngoài.
5. Không mở các tệp tin kỳ lạ: Người dùng không nên mở các tệp tin gửi đến từ nguồn không rõ ràng hoặc không đáng tin cậy.

Vì vậy , để giảm thiểu rủi ro của lỗ hổng này, người dùng nên cập nhật trình duyệt Chromium và bảo vệ máy tính của mình bằng các phần mềm diệt virus, tường lửa và tránh truy cập các website đích danh hoặc không đáng tin.

# THỰC NGHIỆM

## Khai thác lỗ hổng CVE-2023-23397

### Mô hình triển khai

Chuẩn bị: máy kali IP:172.31.84.109, windows 10 cài đặt office Version 2208 Build 16.0.15601.20142 

**Hình 3.1 Mô hình triển khai CVE-2023-23397**

### Kịch bản triển khai và thực nghiệm

#### Kịch bản

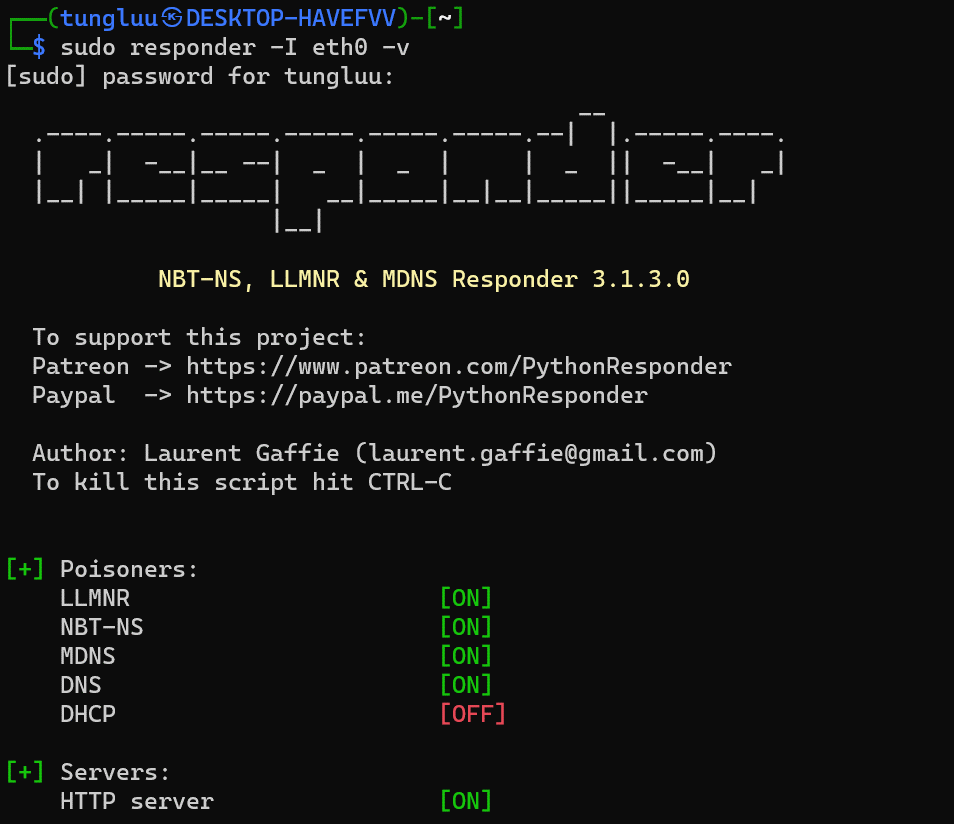
Trên máy ảo win10 cài đặt outlook Version 2208 Build 16.0.15601.20142 tạo lời mời lịch độc hại bao gồm tham chiếu đến tệp sound trỏ đến tệp chia sẻ mạng trong máy của máy tấn công (kali). Email Outlook lưu trữ tham chiếu đến tệp sound trong tham số nội bộ có tên là PidLidReminderFileParameter. Để đảm bảo rằng lời nhắc nhúng trong email độc hại sẽ được ưu tiên hơn cấu hình lời nhắc mặc định của máy win, nhóm em đặt tham số PidLidReminderOverride thành true. Thiết lập thuộc tính PidLidReminderFileParameter trỏ đến mạng chia sẻ, attacker có thể thực thi một đường dẫn Universal Naming Convention(UNC) thay vì tệp cục bộ. UNC được sử dụng trong hệ điều hành Windows để tìm tài nguyên mạng (files, printers, shared documents). Các đường dẫn này bao gồm dấu gạch chéo ngoặc kép, địa chỉ IP hoặc tên của máy tính lưu trữ resource, share name và file name. Khi nhận được email độc hại, đường dẫn UNC sẽ hướng đến chia sẻ SMB, kích hoạt lỗ hổng. Điều này khiến hệ thống bắt đầu quá trình xác thực NTLM đối với máy của kẻ tấn công, mô phỏng máy chủ SMB tại máy kali bắt hàm băm Net-NTLMv2

#### Triển khai

Cài đặt responder:

Victim sẽ chống lại quá trình xác thực của attacker trên port 445 nên nhóm em sẽ thiết lập responder để xử lý tiến trình xác thực và chiếm lấy NTLMv2-SSP Hash. Responder sẽ mô phỏng SMB server và nắm bắt bất kỳ xác thực nào.

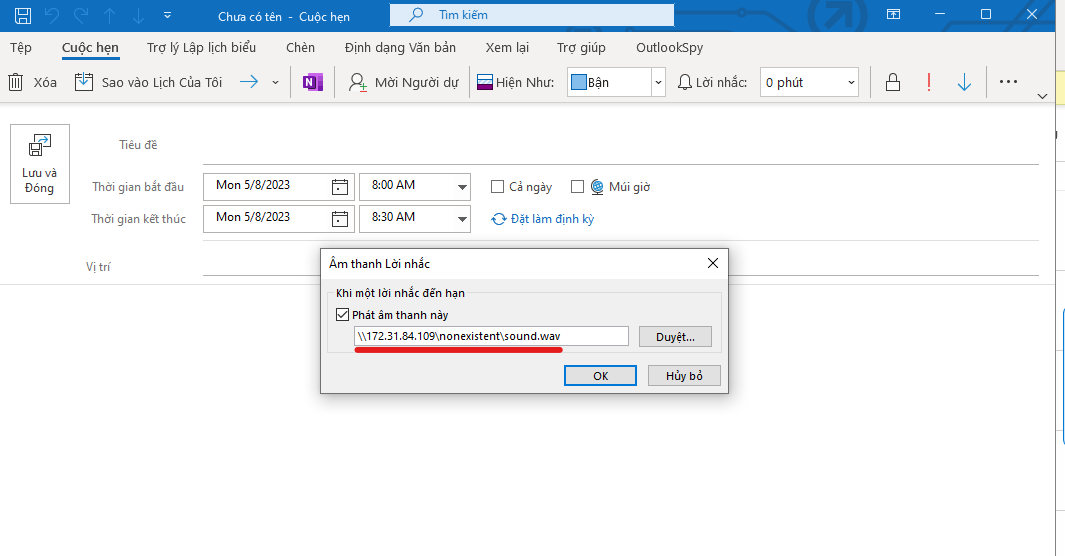
Khởi chạy Responder để lắng nghe các xác thực trong giao diện mạng eth0



**Hình 3.2 Khởi chạy Responder để lắng nghe các xác thực trong giao diện mạng eth0**

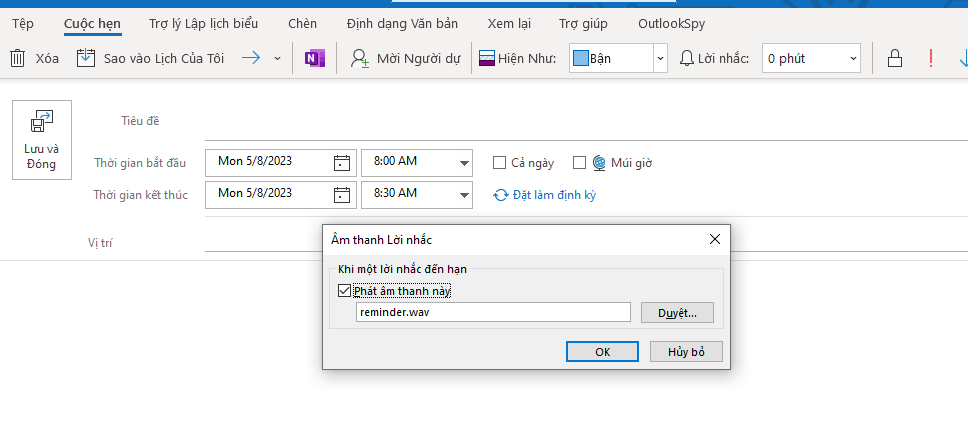
Trong lần thử đầu tiên, nhóm em tạo cuộc hẹn theo cách thủ công và chỉnh sửa đường dẫn đến file sound của lời nhắc để trỏ đến một shared folder.

Đặt đường dẫn tệp âm thanh thành đường dẫn UNC trỏ đến máy kali:



**Hình 3.3 Đặt đường dẫn tệp âm thanh thành đường dẫn UNC trỏ đến máy kali**

Tuy nhiên trên outlook sẽ bỏ qua đường dẫn UNC và trở lại sử dụng file wav mặc định.

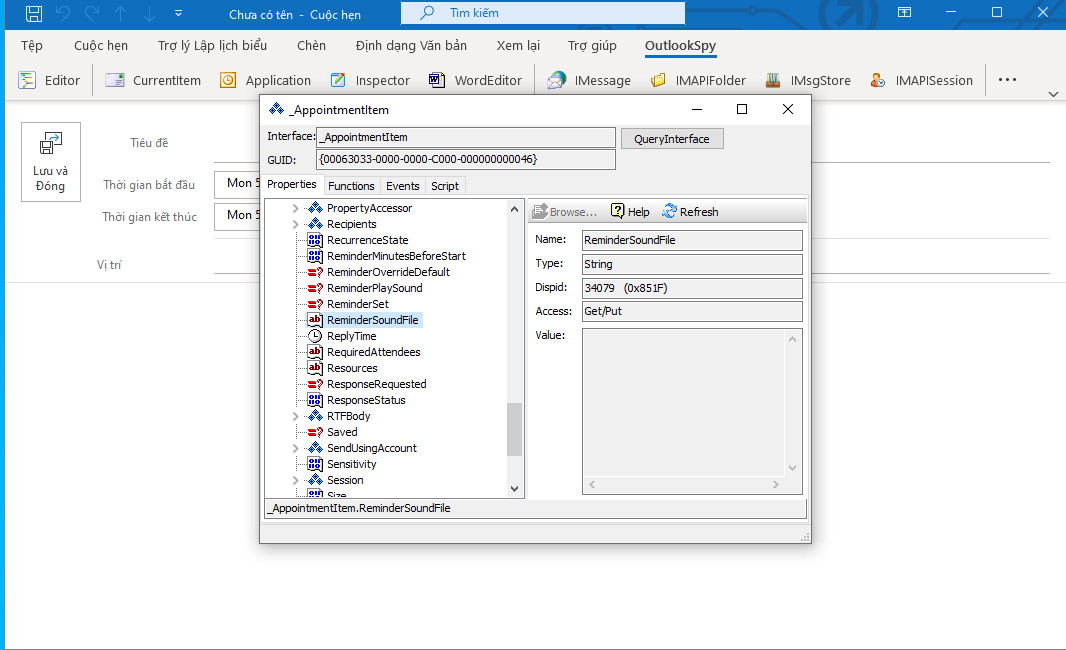


**Hình 3.4 Outlook bỏ qua đường dẫn UNC và sử dụng file wav mặc định**

Sử dụng plugin outlookspy:

Outlook không thể đặt file sound của thông báo thành đường dẫn UNC, có thể sử dụng plugin OutlookSpy để chỉnh sửa các thuộc tính trong outlook. Plugin này sẽ cho phép truy cập trực tiếp vào tất cả các tham số nội bộ của Outlook, bao gồm cả file sound của thông báo.

Để xem cuộc hẹn hiện tại từ outlookspy, click outlookspy sau đó click *currentItem* trên *taskbar*



**Hình 3.5 Xem cuộc hẹn hiện tại từ outlookspy**

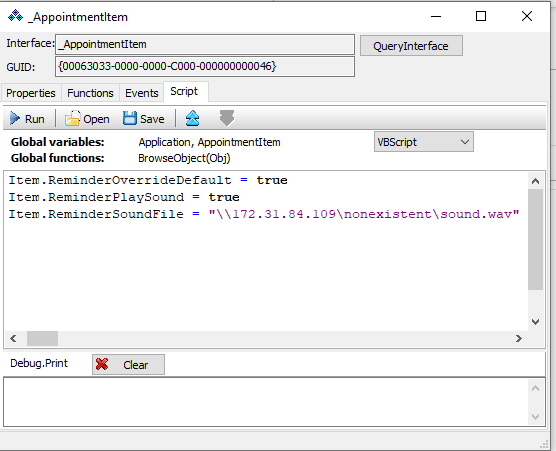
Có thể xem được các thông số liên quan đến lời nhắc của cuộc hẹn. Nhóm em muốn thiết lập tham số reminderSoundFile vào đường dẫn UNC trở tới máy kali và đặt hai tham số ReminderOverrideDefault và ReminderPlaySound thành true.

**ReminderPlaySound**: giá trị boolean cho biết liệu âm thanh có được phát cùng với lời nhắc hay không.

**ReminderOverrideDefault**: giá trị boolean cho biết ứng dụng khách Outlook đang nhận sẽ phát âm thanh được chỉ định bởi ReminderSoundFile, thay vì âm thanh mặc định.

**ReminderSoundFile**: chuỗi có đường dẫn đến tệp âm thanh sẽ được sử dụng.

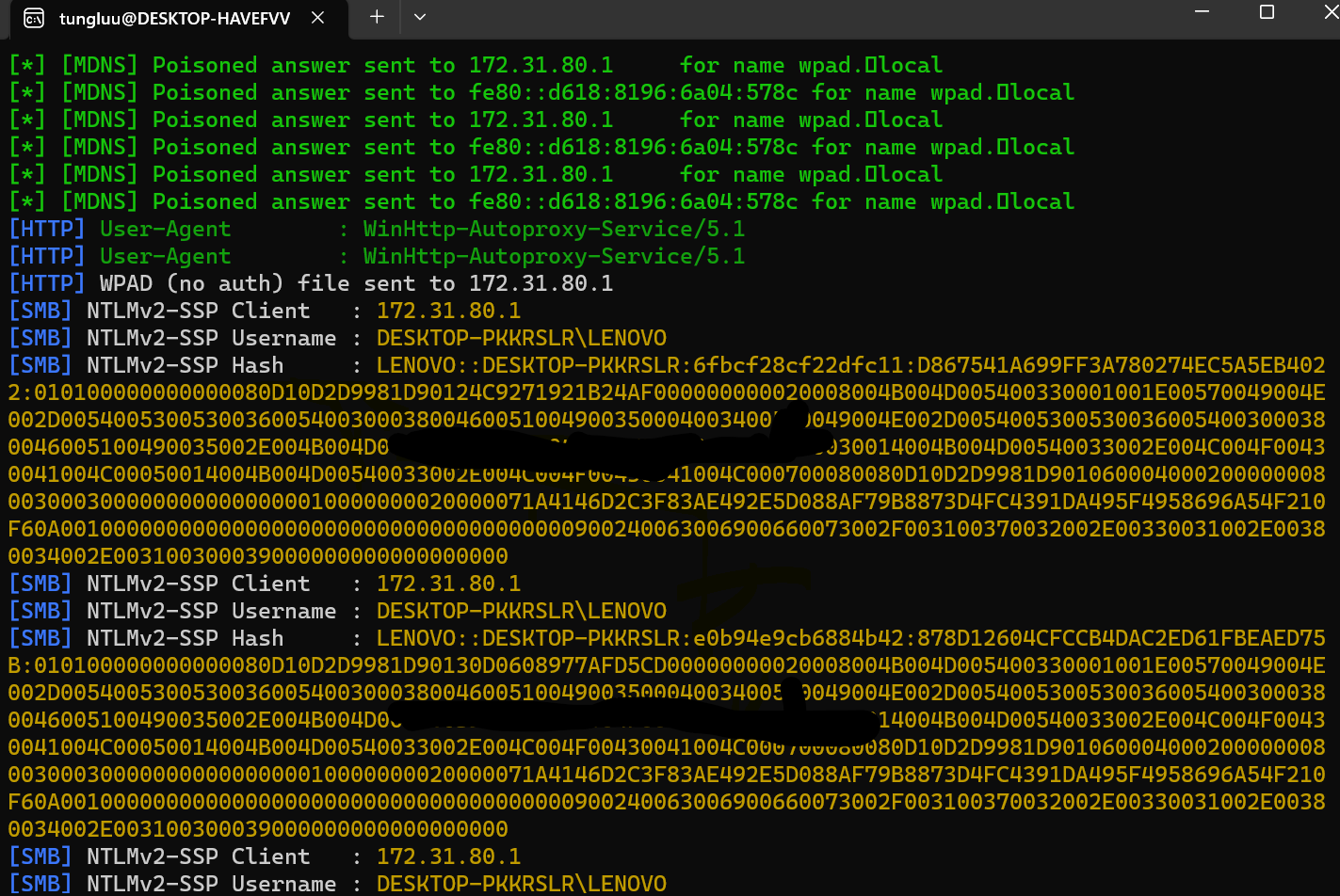
Sử dụng task script đoạn script dưới sẽ thay đổi các tham số thành các giá trị cần thiết



**Hình 3.6 Sử dụng task script**

Bấm run để các thay đổi được áp dụng, chuyển sang tab properties kiểm tra các tham số thanh đổi thành công hay chưa. Chỉnh lời nhắc thành 0 phút rồi save. Đến giờ lời nhắc một hộp thoại sẽ hiển thị lời nhắc.

Tại máy kali nhận được thông tin xác thực tại responder



**Hình 3.7 thông tin xác thực tại responder**

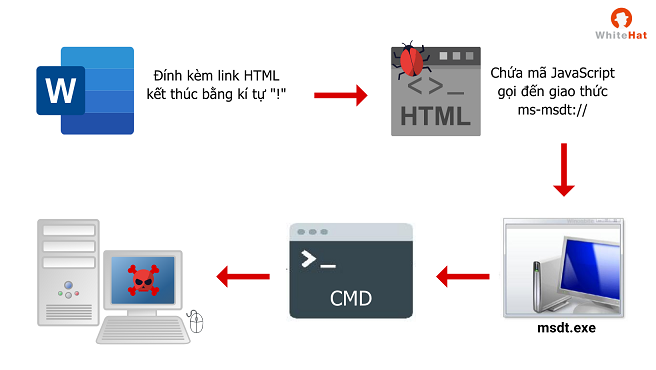
### Đánh giá

Trước tình hình ngày càng gia tăng của các cuộc tấn công mạng và những lỗ hổng mới được phát hiện mỗi ngày, **CVE-2023-23397** trên Microsoft Outlook là một minh chứng rõ ràng cho sự cần thiết của việc bảo vệ hệ thống và dữ liệu cá nhân nhằm tránh bị kẻ xấu thu thập thông tin như tài khoản, địa chỉ email làm mục tiêu để tấn công. Việc nhanh chóng cập nhật bản vá và áp dụng các giải pháp an ninh khác trong doanh nghiệp hoặc tổ chức cần được thực hiện sớm.

## Khai thác lỗ hổng CVE-2022-30190

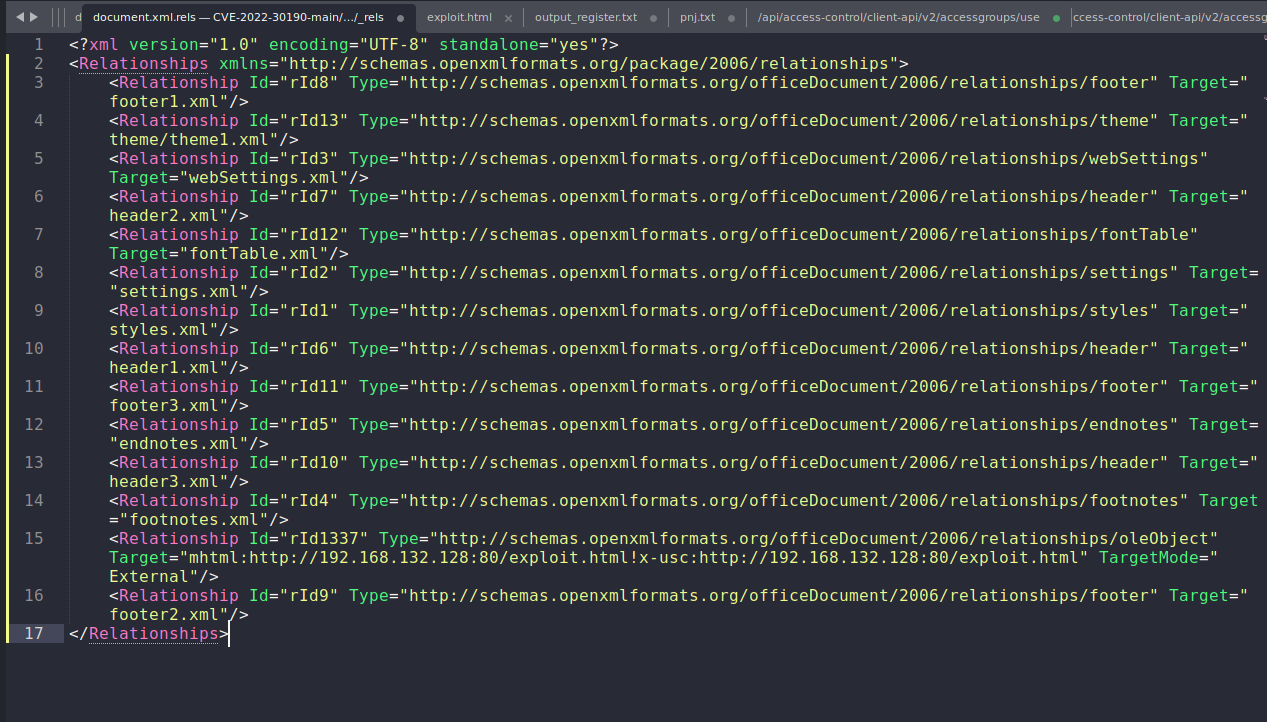
### Mô hình triển khai

Tài liệu Word chứa phần tham chiếu đến mã khai thác (link file HTML có chứa mẫu mã độc). Bằng cách này, mẫu mã độc sẽ “làm khó” các phần mềm diệt virus (AV) sử dụng phương pháp phân tích file tĩnh (static analysis - phân tích, kiểm tra các mã độc hại mà không cần chạy chúng). Trong trường hợp này, các AV chỉ có thể phát hiện khi mẫu mã độc đã được thực thi trên máy nạn nhân.



**Hình 3.8 Mô hình triển khai CVE-2022-30190**

Triển khai:



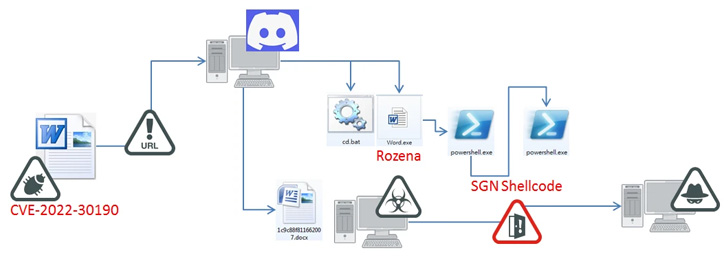
### Kịch bản triển khai và thực nghiệm

3.2.2.1 Kịch bản triển khai

Trên máy chủ kali tạo ra một file word khi mở ra, sẽ kết nối với URL CDN của Discord để truy xuất tệp HTML (“index.htm”) để lần lượt gọi tiện ích chẩn đoán bằng cách sử dụng một Lệnh PowerShell để tải xuống tải trọng giai đoạn tiếp theo từ cùng một không gian đính kèm CDN.

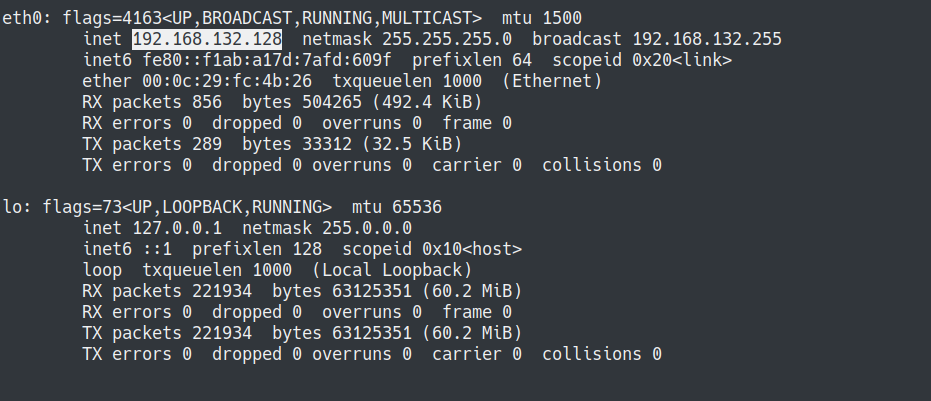
Điều này bao gồm bộ cấy Rozena (“Word.exe”) và một tệp bó (“cd.bat”) được thiết kế để chấm dứt các quy trình MSDT, thiết lập sự tồn tại của cửa hậu bằng cách sửa đổi Windows Registry và tải xuống một tài liệu Word vô hại làm mồi nhử.

Chức năng cốt lõi của phần mềm độc hại là tiêm shellcode khởi chạy shell ngược tới máy chủ của kẻ tấn công (“microsofto.duckdns[.]org”), cuối cùng cho phép kẻ tấn công kiểm soát hệ thống cần thiết để giám sát và nắm bắt thông tin, đồng thời duy trì một cửa hậu cho hệ thống bị xâm nhập.

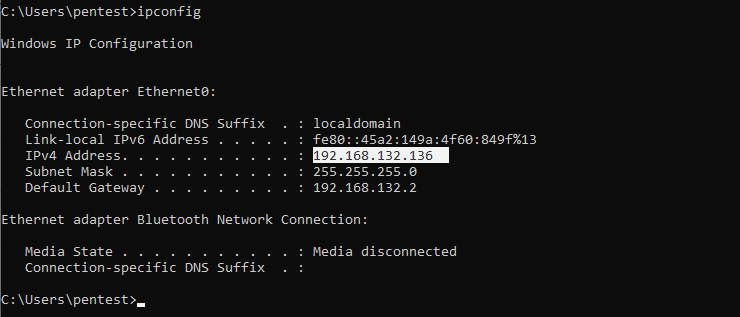


**Hình 3.9 Kịch bản triển khai CVE-2022-30190**

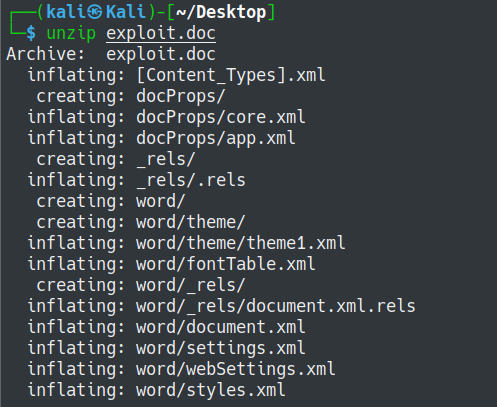
IP máy kẻ tấn công:



IP máy nạn nhân:



Tất cả bắt đầu với tài liệu từ độc hại. Tất cả các tài liệu word về cơ bản là các tập tin được đóng gói. Bất kỳ ai cũng có thể giải nén sau đó bằng lệnh unzip.

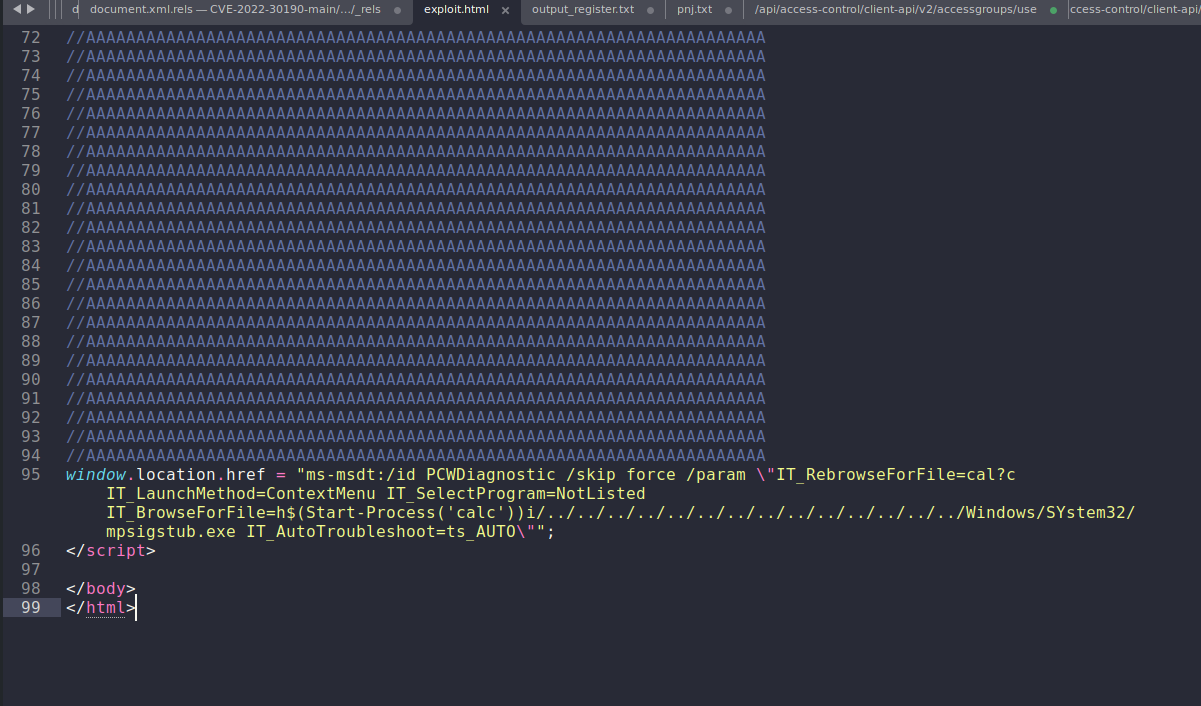


Sau khi unzip, sẽ hiển thị các tệp được chứa trong file word. Tệp cụ thể được đề cập ở đây là word/\_rels/document.xml.rels.

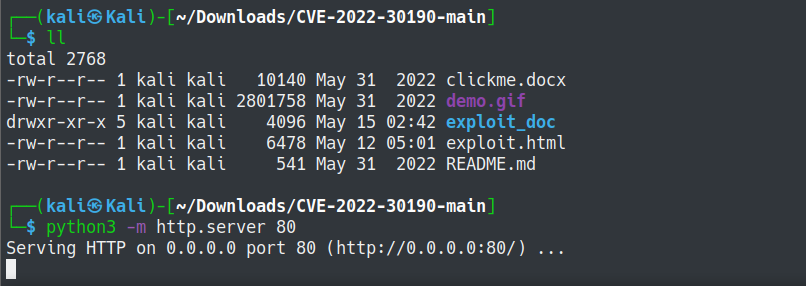
File document.xml.rels là một file XML ánh xạ các mối quan hệ trong tài liệu (chủ sở hữu hình ảnh/bảng/phông chữ) với các tài nguyên bên ngoài (hình ảnh được lưu trữ trực tuyến/video). Việc khai thác sẽ sử dụng chức năng này. Thay đổi giá trị Type thuộc ID=”rId1337” thành IP của kẻ tấn công.



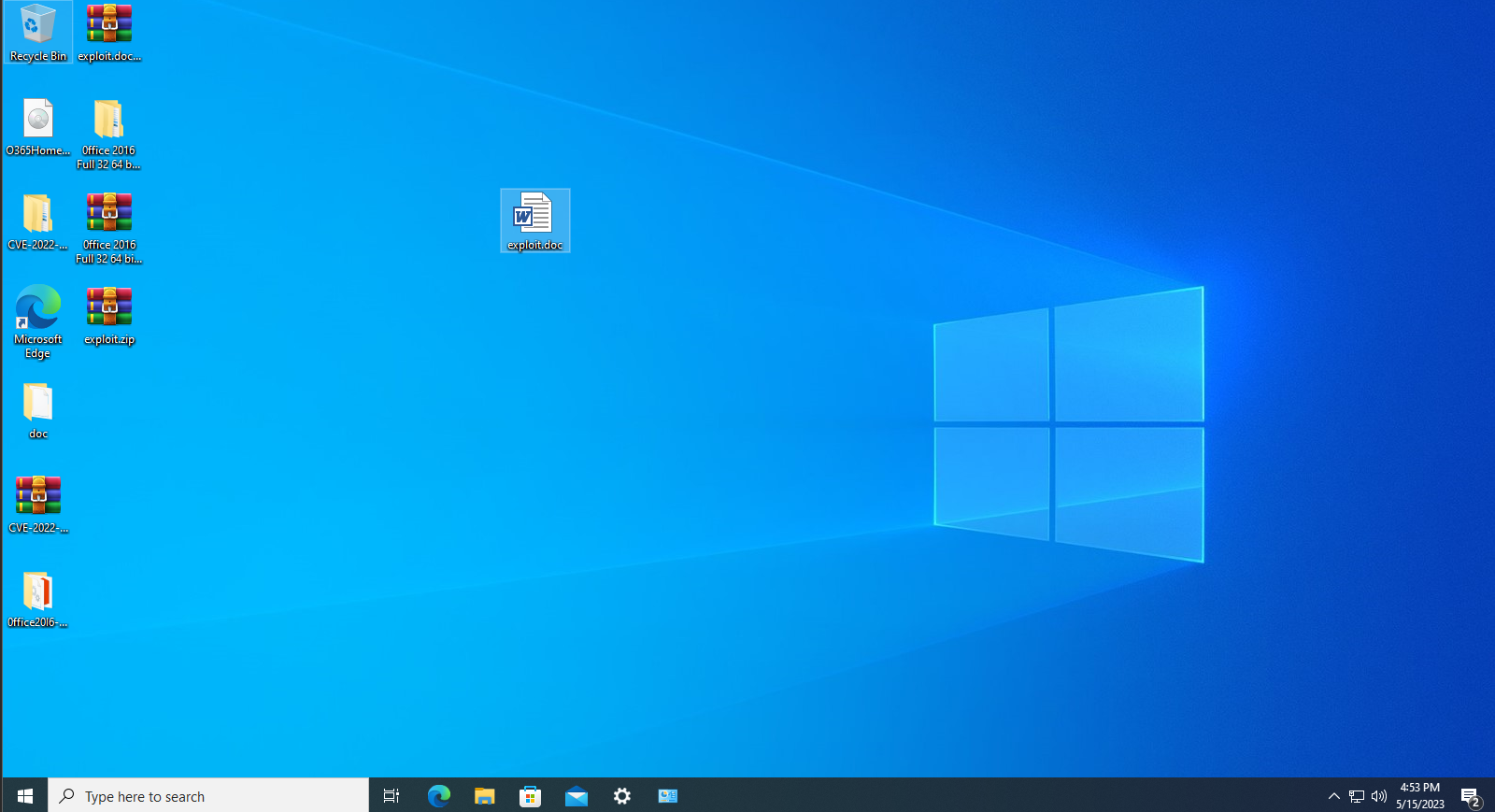
Payload dưới đây được lưu trữ trên một máy chủ từ xa. Ban đầu, các nhà nghiên cứu phát hiện ra rằng công cụ MSTD yêu cầu mã pin để chạy bất kỳ mã nào và do đó mọi người nghĩ rằng việc khai thác này sẽ không thể thực hiện được. Tuy nhiên, một nhà nghiên cứu đã phát hiện ra rằng do tải trọng được lưu trữ trên máy chủ từ xa lớn hơn 4096 byte, MSTD sẽ tiếp tục chạy mã tùy ý để thực thi mã từ xa cho bất kỳ kẻ tấn công nào.



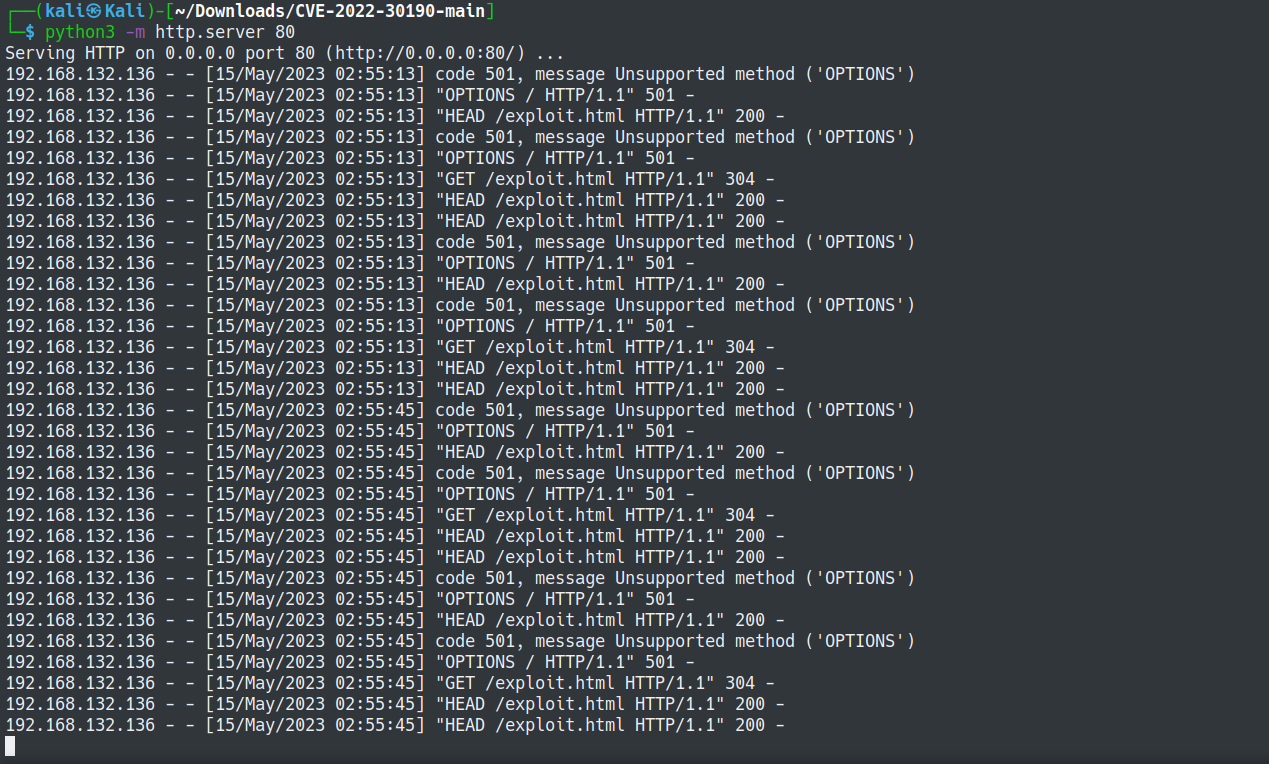
Khởi chạy máy chủ chứa payload này:



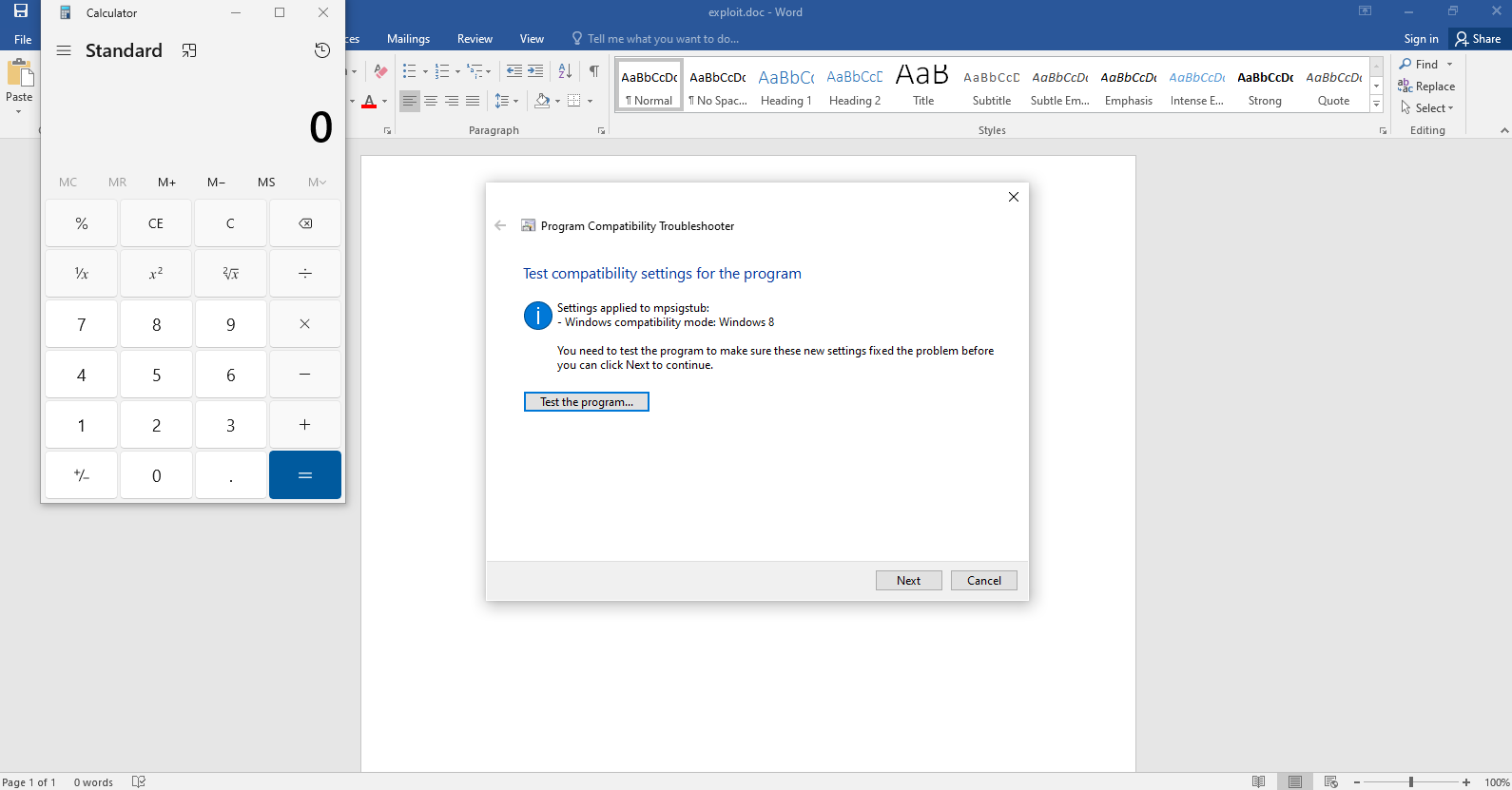
Tiếp theo, cần gửi file word đã đóng gói chứa mã khai thác đến nạn nhân, có thể thông qua hình thức gửi email lừa đảo.



Sau khi người dùng mở file này, máy chủ web lưu trữ payload sẽ nhận được tất cả request gọi đến:



Ứng dụng máy tính sẽ được mở trên máy nạn nhân mà không cần bất kỳ hành động nào khác.



Điều này chứng tỏ, cuộc tấn công đã thành công.

### Đánh giá

Hiện nay, CVE-2022-30190 là một lỗ hổng bảo mật nghiêm trọng trong Microsoft Support Diagnostic Tool (MSDT), ảnh hưởng đến Microsoft Office phiên bản Office 2013/2016/2019/2021 và các phiên bản Professional Plus. Lỗ hổng này cho phép đối tượng tấn công thực thi mã tùy ý; từ đó có quyền xem, thay đổi hoặc xóa dữ liệu,...., lỗ hổng này có thể nằm trong cuộc tấn công có chủ đích (APT)

# KẾT LUẬN

Ba chương của đề tài này đã thể hiện được rằng những mục tiêu đặt ra khi thực hiện đề tài đều đã đạt được. Cụ thể: đã tìm hiểu và xây dựng mô phỏng lại các lỗ hổng CVE-2023-23397 và CVE-2022-30190

Ngoài ra, qua quá trình nghiên cứu và thực hiện đề tài cũng đã mang lại rất nhiều kiến thức và kỹ năng làm việc nhóm cho chúng em. Đây là một trong những cơ hội quý giá giúp sinh viên phát triển và hoàn thiện bản thân. Dù vậy, để nói về các lỗ hổng 0-day mới trong microft vẫn còn nhiều vấn đề liên quan mà nghiên cứu này chưa thực hiện được. Việc tiếp tục phát triển và hoàn thiện hơn những vấn đề còn tồn tại cũng chính là hướng phát triển tương lai của đề tài.

# TÀI LIỆU THAM KHẢO

[1] https://bhavsec.com/posts/outlook-zeroday-cve-2023-23397/

[2] https://www.ired.team/offensive-security/initial-access/netntlmv2-hash-stealing-using-outlook

[3] https://whitehat.vn/threads/phan-tich-ve-lo-hong-cve-2023-23397-trong-microsoft-outlook.17176/

[4] <https://www.bleepingcomputer.com/news/security/microsoft-shares-tips-on-detecting-outlook-zero-day-exploitation/>

[5] https://gauthamprasath.medium.com/follina-msdt-vulnerability-cve-2022-30190-analysis-and-poc-29f61cd2c07f

[6] https://ethical.blue/textz/n/32

[7] https://github.com/winstxnhdw/CVE-2022-30190

[8] https://github.com/Malwareman007/Deathnote

[9] https://whitehat.vn/threads/goc-nhin-chuyen-gia-ve-cve-2022-30190-trong-microsoft-office.16612/