REPORT S11/L5

Progetto 1

Traccia

Utilizzo di Windows PowerShell

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell.

Svolgimento

PowerShell è un linguaggio di scripting e una shell a riga di comando sviluppato da Microsoft per gestire e automatizzare i sistemi operativi Windows e altri prodotti Microsoft.

È costruito sul .NET Framework e fornisce funzionalità attraverso i suoi comandi integrati, chiamati cmdlet.

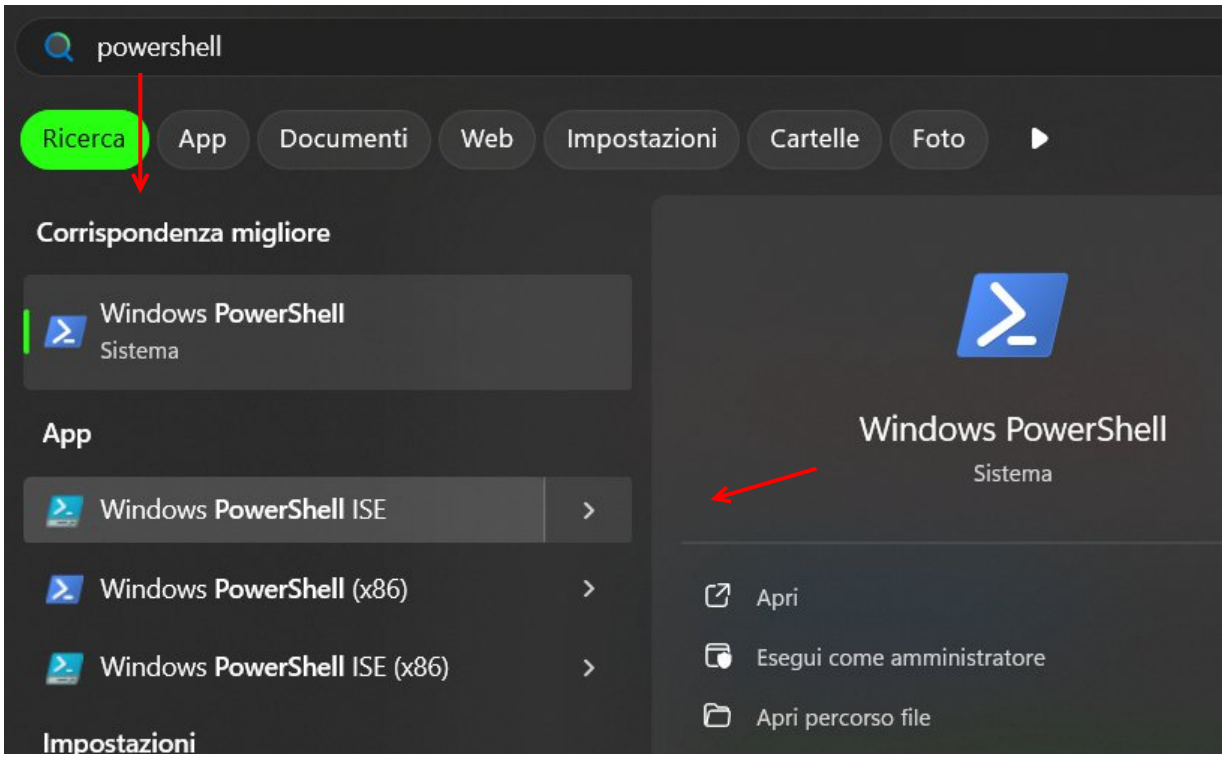
PowerShell è utilizzato per automatizzare e gestire le attività dei sistemi Windows, essendo particolarmente utile per gli amministratori di sistema e professionisti IT.

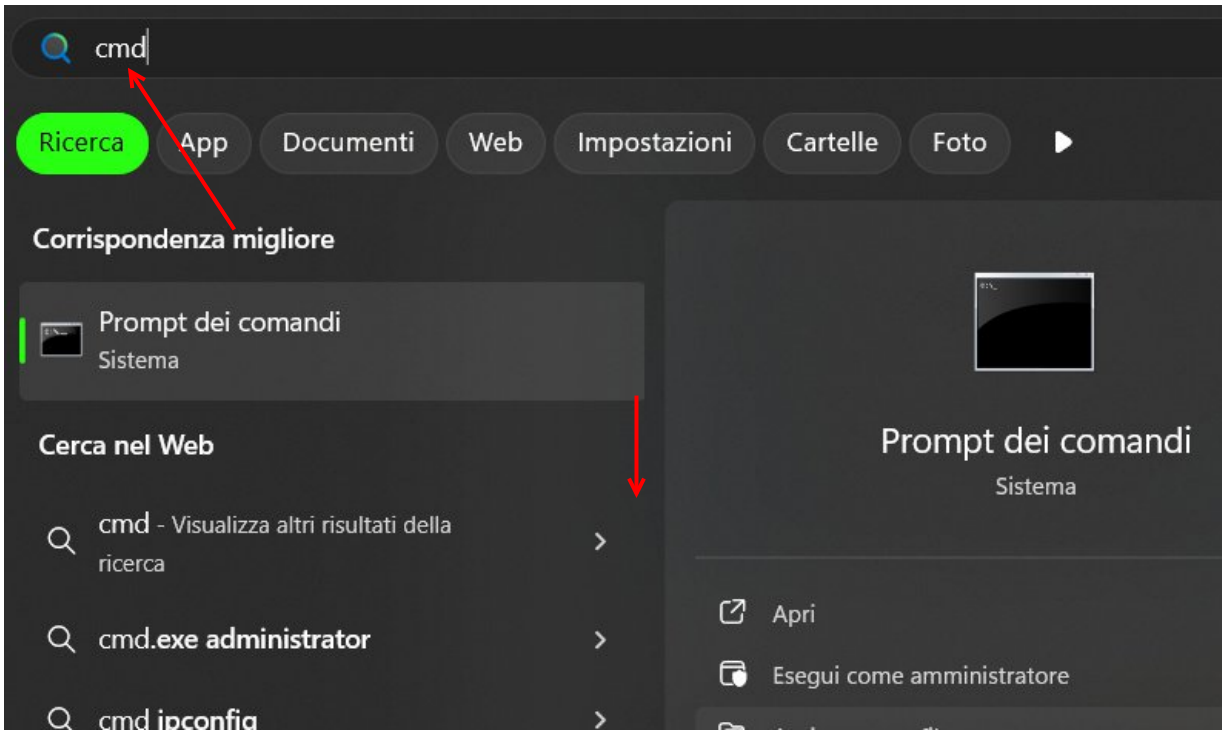
L'obiettivo del laboratorio è quello di esplorare alcune funzionalità della PowerShell.

- Parte 1: Accesso alla console PowerShell.
- Parte 2: Esplorare i comandi di Command Prompt e PowerShell.
- Parte 3: Esplorare i cmdlets.
- Parte 4: Esplorare i comandi netstat usando PowerShell.
- Parte 5: Svuotare il cestino usando PowerShell.

Parte 1: Accesso alla console PowerShell

Per avviare la PowerShell premi il punsante Win, poi digitiamo powershell, poi clicchiamo su Apri. Per avviare il command prompt seguiamo gli stessi passaggi.





Parte 2: Esplorare i comandi di Command Prompt e PowerShell

Come primo comando inseriamo **dir in entrambe le finestre e vediamo il risultato**

```
PS C:\Users\Alberto> dir


    Directory: C:\Users\Alberto


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        26/10/2024     17:23                .ms-ad
d-----        19/02/2025     14:44                .VirtualBox
d-----        24/12/2024     10:42                Apple
d-----        19/12/2024     18:22                Cisco Packet Tracer 8.2.2
d-r---        20/02/2025     09:02                Contacts
d-r---        20/02/2025     09:02                Desktop
d-r---        20/02/2025     09:02                Documents
d-r---        20/02/2025     09:02                Downloads
d-----        28/11/2024     07:36                dwhelper
d-r---        20/02/2025     09:02                Favorites
d-r---        20/02/2025     09:02                Links
d-r---        20/02/2025     09:02                Music
d-r---        26/10/2024     16:29                OneDrive
d-r---        20/02/2025     09:02                Pictures
d-r---        20/02/2025     09:02                Saved Games
d-r---        20/02/2025     09:02                Searches
d-r---        20/02/2025     09:02                Videos
d-----        18/02/2025     14:56                VirtualBox VMs
-a----        19/12/2024     10:28            180 .packettracer
```

```
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 3007-A73F

 Directory di C:\Users\Alberto

20/02/2025  09:02    <DIR>          .
20/02/2025  08:57    <DIR>          ..
26/10/2024  16:23    <DIR>          .ms-ad
19/12/2024  10:28               180 .packettracer
19/02/2025  14:44    <DIR>          .VirtualBox
24/12/2024  10:42    <DIR>          Apple
19/12/2024  18:22    <DIR>          Cisco Packet Tracer 8.2.2
20/02/2025  09:02    <DIR>          Contacts
20/02/2025  09:02    <DIR>          Desktop
20/02/2025  09:02    <DIR>          Documents
20/02/2025  09:02    <DIR>          Downloads
28/11/2024  07:36    <DIR>          dwhelper
20/02/2025  09:02    <DIR>          Favorites
20/02/2025  09:02    <DIR>          Links
20/02/2025  09:02    <DIR>          Music
26/10/2024  15:29    <DIR>          OneDrive
20/02/2025  09:02    <DIR>          Pictures
20/02/2025  09:02    <DIR>          Saved Games
20/02/2025  09:02    <DIR>          Searches
20/02/2025  09:02    <DIR>          Videos
18/02/2025  14:56    <DIR>          VirtualBox VMs
               1 File            180 byte
              20 Directory  136.947.908.608 byte disponibili
```

Entrambe le finestre forniscono un elenco di sottodirectory e file e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell vengono anche mostrati gli attributi / le modalità.

Anche provando altri comandi base il risultato sarà simile in entrambe le finestre.

Parte 3: Esplorare i cmdlets

I comandi PowerShell, cmdlet, sono costruiti sotto forma di ***verbo-sostantivo stringa***. Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, usiamo Get-Alias dir nel prompt di PowerShell, ottenendo:

```
PS C:\Users\Alberto> Get-Alias dir

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           dir -> Get-ChildItem
```

Questo singnifica che nella powerShell possiamo usare indistintamente i comandi *dir* e *Get-ChildItem*, ottenendo lo stesso risultato.

```
PS C:\Users\Alberto> Get-ChildItem


    Directory: C:\Users\Alberto


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        26/10/2024     17:23                .ms-ad
d-----        19/02/2025     14:44                .VirtualBox
d-----        24/12/2024     10:42                Apple
d-----        19/12/2024     18:22                Cisco Packet Tracer 8.2.2
d-r---        20/02/2025     09:02                Contacts
d-r---        20/02/2025     09:02                Desktop
d-r---        20/02/2025     09:02                Documents
d-r---        20/02/2025     09:02                Downloads
d-----        28/11/2024     07:36                dwhelper
d-r---        20/02/2025     09:02                Favorites
d-r---        20/02/2025     09:02                Links
d-r---        20/02/2025     09:02                Music
d-r---        26/10/2024     16:29                OneDrive
d-r---        20/02/2025     09:02                Pictures
d-r---        20/02/2025     09:02                Saved Games
d-r---        20/02/2025     09:02                Searches
d-r---        20/02/2025     09:02                Videos
d-----        18/02/2025     14:56                VirtualBox VMs
-a----        19/12/2024     10:28            180 .packettracer
```

Parte 4: Esplorare i comandi netstat usando PowerShell

Inseriamo il comando *netstat --h* per vedere le opzioni disponibili per netstat.

```
PS C:\Users\Alberto> netstat --h

Mostra le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]
```

Per visualizzare la tabella di routing con i percorsi attivi, usiamo il comando *netstat -r*

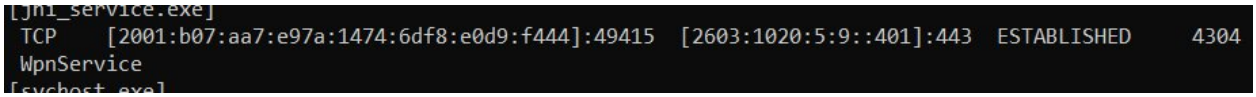
```
PS C:\Users\Alberto> netstat -r
===========================================================================
Elenco interfacce
  7...d4 f3 2d 5b c6 f7 ......Microsoft Wi-Fi Direct Virtual Adapter
  4...d6 f3 2d 5b c6 f6 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 11...d4 f3 2d 5b c6 f6 ......Intel(R) Wi-Fi 6E AX211 160MHz
  6...10 98 19 03 63 6c ......Realtek PCIe GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0    192.168.1.254     192.168.1.54     30
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0      255.255.0.0     192.168.1.59     192.168.1.54     31
      192.168.1.0    255.255.255.0         On-link      192.168.1.54    286
     192.168.1.54  255.255.255.255         On-link      192.168.1.54    286
    192.168.1.255  255.255.255.255         On-link      192.168.1.54    286
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.1.54    286
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.1.54    286
===========================================================================
```

Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Inseriamo il comando *netstat -abno*, dopo aver avviato la PowerShell come amministratore.

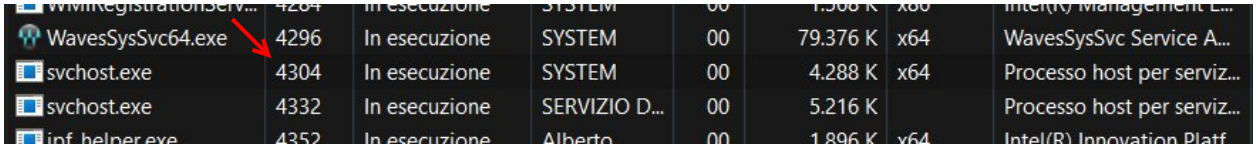
```
PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:135              0.0.0.0:0              LISTENING       1520
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445              0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:5040             0.0.0.0:0              LISTENING       7116
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:7680             0.0.0.0:0              LISTENING       4332
```

Possiamo anche rintracciare il processo che ha stabilito la connessione attiva, mostrata in PowerShell. Apriamo il Task Manager, andiamo nella sezione Dettagli e mettiamo in ordine i processi in base al PID. Cerchiamo all'interno della finestra il processo con PID 4304, che compare in entrambe le finestre.

Lato powerShell vediamo:



Mentre nel Task Manager riconduciamo questo processo a *svchost.exe*, sappiamo che è un processo dell'utente *SYSTEM* e che usa 4288Kb di memoria:

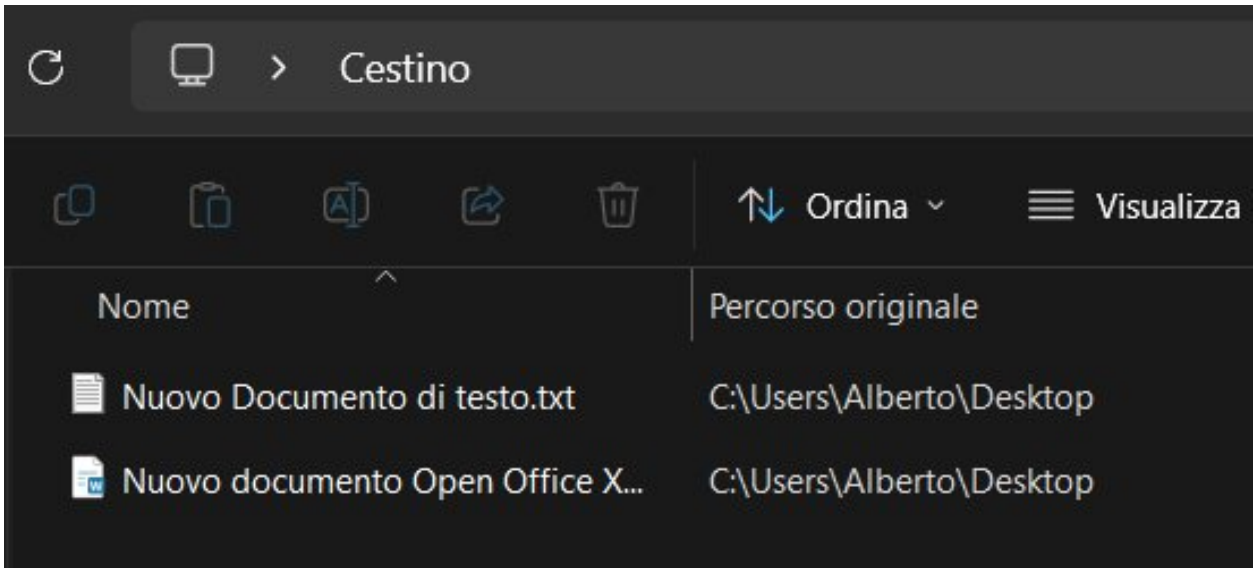


Parte 5: Svuotare il cestino usando PowerShell

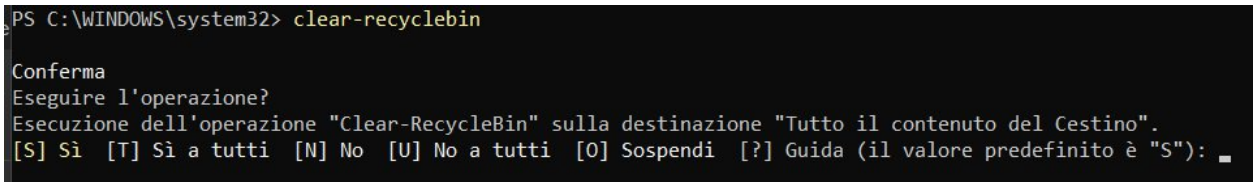
I comandi PowerShell possono semplificare la gestione di una grande rete di computer. Ad esempio, se si desidera implementare una nuova soluzione di sicurezza su tutti i server della rete, è possibile utilizzare un comando o uno script PowerShell per implementare e verificare che i servizi siano in esecuzione. È inoltre possibile eseguire i comandi PowerShell per semplificare le azioni che richiederebbero più passaggi per l'esecuzione utilizzando gli strumenti desktop grafici di Windows.

Per questo esmepio inseriamo alcuni files vuoti nel cestino e proveremo ad eliminarli definitivamente con un comando PowerShell.

Vediamo infatti che adesso nel cestino sono presenti due file di testo

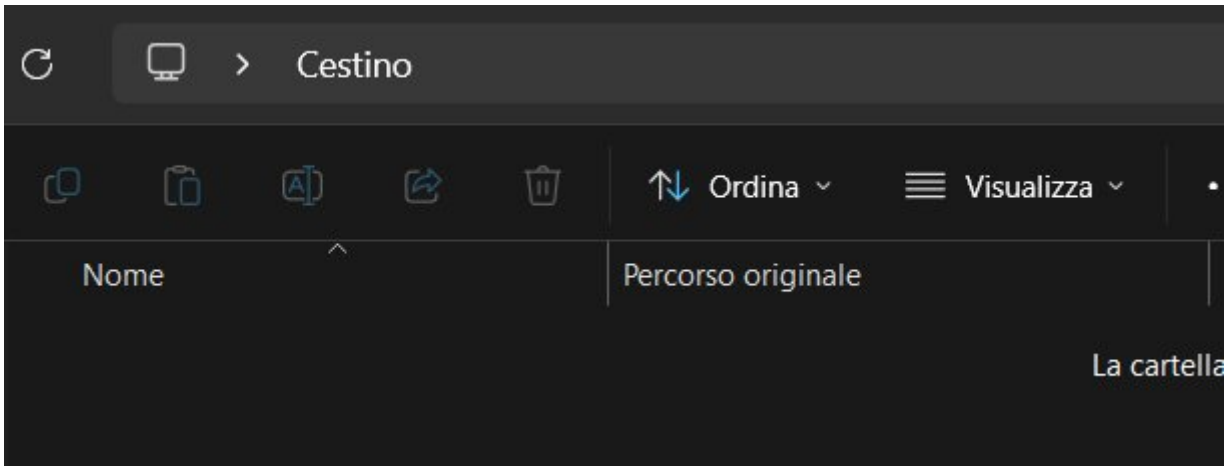


Nella console PowerShell inseriamo il comando *clear-recyclebin*



Inseriamo T per dare la conferma dell'eliminazione di tutti i files e diamo Invio.

Dopo ciò la finestra del cestino risulterà vuota:



Progetto 2

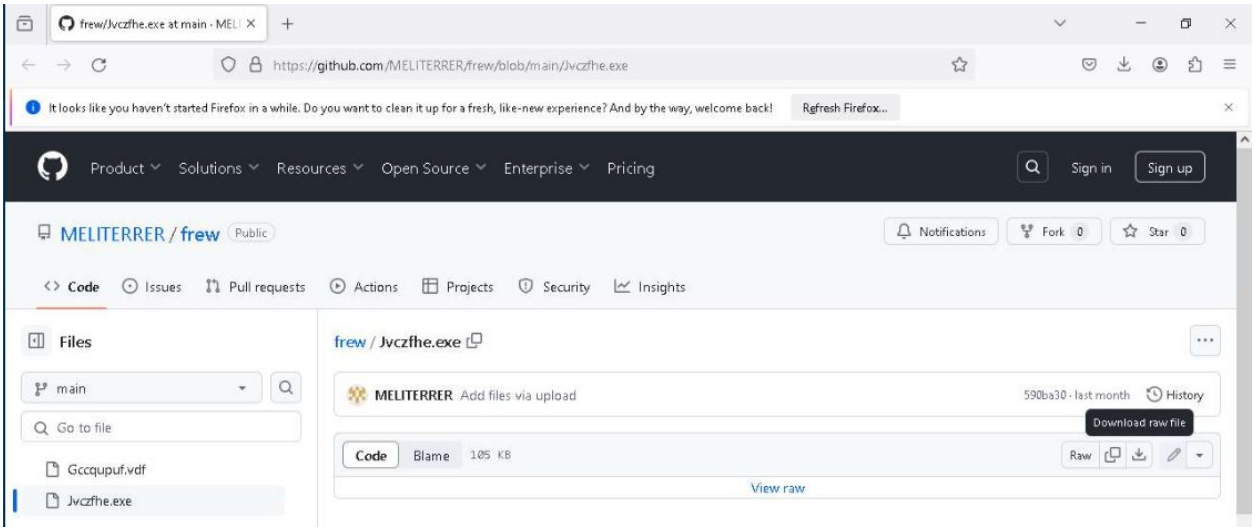
Traccia

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.

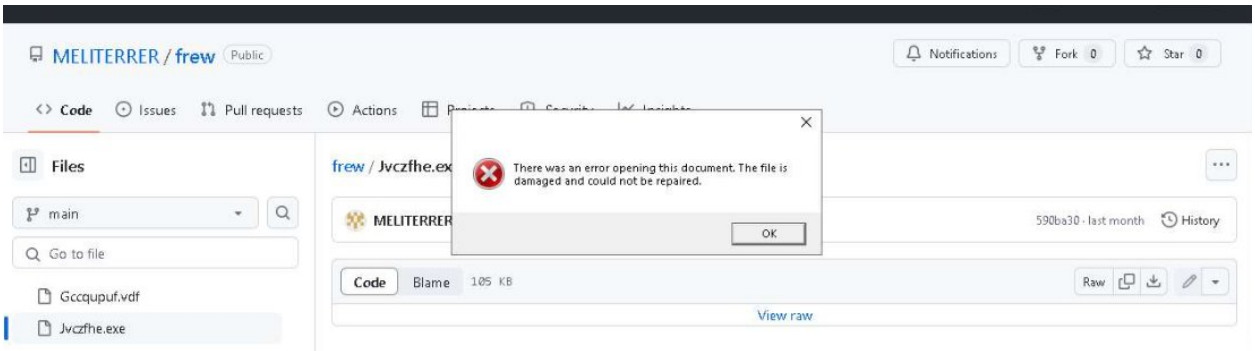
https ://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

Svolgimento

Il link fornito rimanda al sito ANY.RUN dove è stata effettuata un'analisi dinamica riguardante un file eseguibile denominato *Jvczfhe.exe* caricato nella repository su GitHub gestita dall'utente "MELITERRER".



Jvczfhe.exe è un file eseguibile sospetto che potrebbe contenere codice malevolo. Dagli screen infatti vediamo che quando l'utente prova ad eseguirlo si apre una finestra di errore. Questo comportamento potrebbe essere associato ad attività dannose, come il download di ulteriori malware, il furto di informazioni sensibili o l'apertura di backdoor nel sistema infetto.



Durante l'analisi del file si notano i seguenti comportamenti sospetti:

- Alterazione di chiavi di registro o file di sistema per garantire la persistenza.
- Tentativi di connettersi a server remoti.
- Avvio di processi non autorizzati o inaspettati.

Questi comportamenti indicano che *Jvczfhe.exe* potrebbe essere progettato per compromettere la sicurezza del sistema, rubare informazioni sensibili o fornire accesso remoto non autorizzato agli aggressori.

L'analisi comportamentale del file non evidenzia indicatori esplicitamente malevoli, ma mostra diverse attività sospette che potrebbero indicare la presenza di un malware. Durante l'esecuzione, è stato osservato che un processo ha rilasciato un eseguibile di Windows, come *firefox.exe*, una tecnica spesso utilizzata per mascherare attività dannose sfruttando file affidabili. In sintesi si evidenzia che:

- Il malware lancia eseguibili legittimi, come "firefox.exe", probabilmente per mascherare le sue attività malevole e confondere gli strumenti di sicurezza;
- Avvia un prompt dei comandi;
- Utilizza TIMEOUT.EXE per ritardare l'esecuzione: questo ritardo nell'esecuzione è una tecnica spesso utilizzata per eludere l'analisi automatizzata.
- Legge le impostazioni di sicurezza di Internet Explorer, il che potrebbe indicare un tentativo di abbassare le difese del browser o sfruttare vulnerabilità specifiche.
- Controlla le impostazioni di trust di Windows, possibilmente per identificare l'ambiente in cui è in esecuzione e adattare il suo comportamento di conseguenza.
- Stabilisce connessioni su porte inusuali tramite processi come *InstallUtil.exe*.
- Alcune applicazioni avviate dal malware terminano in modo anomalo, il che potrebbe essere un metodo per distrarre l'utente o i sistemi di sicurezza.
- Il malware è in grado di lanciare se stesso, garantendo la sua esecuzione anche dopo un riavvio del sistema.

Il grafico mostra infatti che durante l'esecuzione del file, viene usato firefox per mascherare l'esecuzione del codice malevole tramite *installutil.exe* e *muadnrd.exe*

Dalla scheda *Task* possiamo estrarre altre informazioni utili come il verdetto dell'analisi, il giorno che è stata fatta, il sistema operativo, le firme digitali e cosa importante, gli indicatori:

- L'attività ha app terminate con un errore
- Il file eseguibile è stato rimosso
- L'attività contiene diverse app in esecuzione
- Minacce conosciute

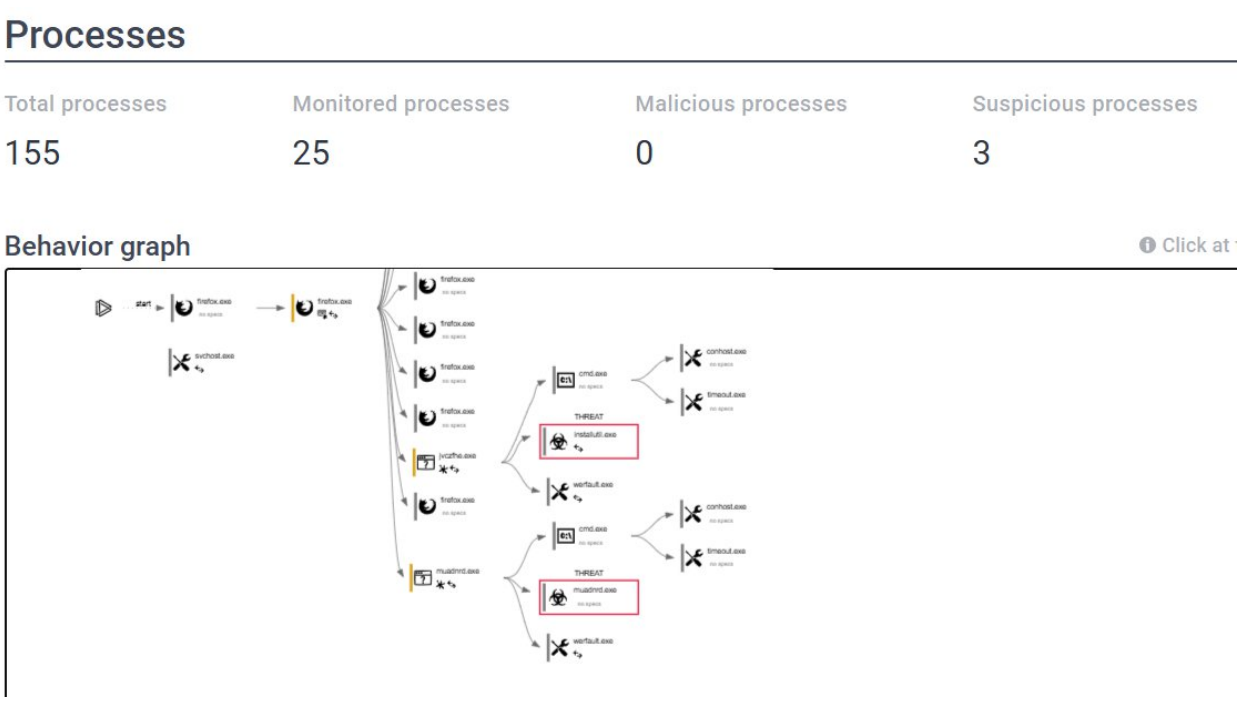
Un altro aspetto preoccupante è stato l'avvio di un'applicazione che, successivamente, ha subito un arresto anomalo. Questo comportamento potrebbe indicare tentativi di sfruttamento di vulnerabilità o di test sulla stabilità del sistema, come se l'attaccante stia cercando di verificare la robustezza del sistema o di eludere i meccanismi di sicurezza.

Inoltre, è stata rilevata una connessione a una porta insolita da parte del processo *InstallUtil.exe*, un comportamento che spesso è associato a comunicazioni con server di comando e controllo (C&C). Questo può implicare che il programma di attacco stia cercando di inviare o ricevere dati sensibili, come informazioni rubate, o di ricevere ulteriori istruzioni per attività dannose.

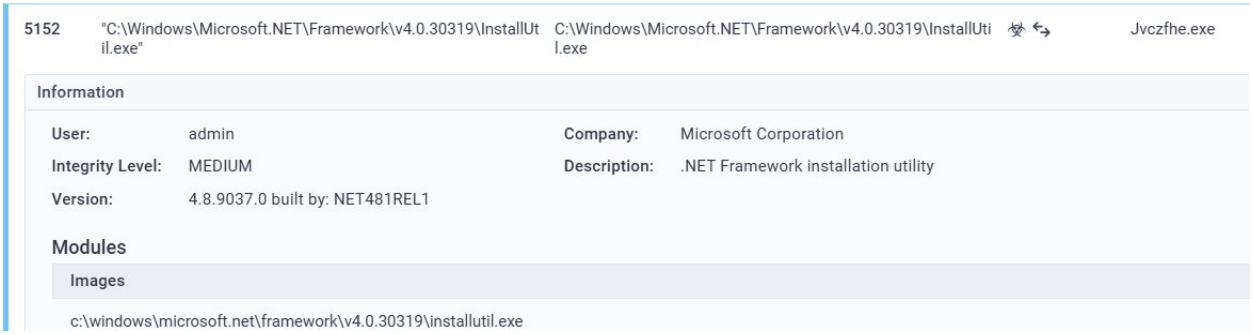
Infine *Muadrnd.exe* si è riavviato autonomamente, il che suggerisce la presenza di un meccanismo di persistenza. Questo indica che l'attaccante ha implementato una tecnica per garantire che il malware rimanga in esecuzione anche dopo una chiusura forzata, rendendo più difficile rimuovere l'infezione e mantenendo il controllo del sistema compromesso.

Nonostante non ci siano indicatori chiaramente malevoli, il comportamento complessivo del file fa pensare che potrebbe essere una minaccia, come un trojan, spyware o un downloader di altri tipi di malware. Questo tipo di file potrebbe agire in modo furtivo, senza manifestarsi immediatamente come una minaccia evidente, ma comunque essere in grado di compromettere il sistema o consentire l'infezione con ulteriori malware.

In questi casi, è fondamentale monitorare il comportamento sospetto e analizzare ulteriormente i file coinvolti per determinare la reale natura del rischio. Dalla sezione riguardante i processi, possiamo vedere e analizzare nello specifico i processi sospetti.



Cliccando sui processi sospetti veniamo indirizzati nella sezione specifica.



Da questa capiamo che il processo *InstallUtil.exe* (strumento legittimo di Microsoft .NET Framework, usato per installare/disinstallare componenti .NET, potrebbe essere stato sfruttato per scopi malevoli.Il processo è stato avviato dall'utente admin con un livello di integrità MEDIUM, quindi senza privilegi elevati.

Analizzando i moduli caricati, si notano librerie di sistema comuni (*ntdll.dll, kernel32.dll, mscoree.dll*), usate sia dai normali processi Windows che dai malware. Tuttavia, l'aspetto sospetto è la correlazione tra InstallUtil.exe e il file chiamato Jvczfhe.exe, che potrebbe essere un payload malevolo. Questo potrebbe indicare l'esecuzione di uno script malevolo o di un payload .NET che tenta di evitare il rilevamento.

Per concludere facciamo attenzione anche al fatto che il programma *Jvczfhe.exe* è associato ad un repository GitHub dell'utente "MELITERRER". L'uso di piattaforme legittime come GitHub per la distribuzione di malware rappresenta una tendenza crescente tra i cybercriminali. Gli attaccanti infatti sfruttano la fiducia riposta dagli utenti in queste piattaforme per ingannarli e indurli a scaricare ed eseguire file dannosi.

In particolare, si possono caricare file malevoli anche nei commenti di repository popolari, generando link di download che sembrano legittimi. Questo metodo sfrutta la fiducia degli utenti nei confronti del repository originale, aumentando la probabilità che scarichino ed eseguano il malware. È fondamentale pertanto verificare sempre l'autenticità e l'integrità dei file scaricati, anche quando provengono da fonti apparentemente affidabili.

Per nascondere la sua presenza e garantire la presenza sul sistema, *Jvczfhe.exe* utilizza diverse tecniche:

- Apporta cambiamenti alle chiavi di registro per assicurarsi l'esecuzione automatica all'avvio del sistema, rendendo più difficile la sua rimozione.
- Esegue o inietta codice in processi legittimi di Windows, come "firefox.exe" o "InstallUtil.exe", per mascherare le sue attività e sfuggire alla rilevazione da parte dei software di sicurezza.