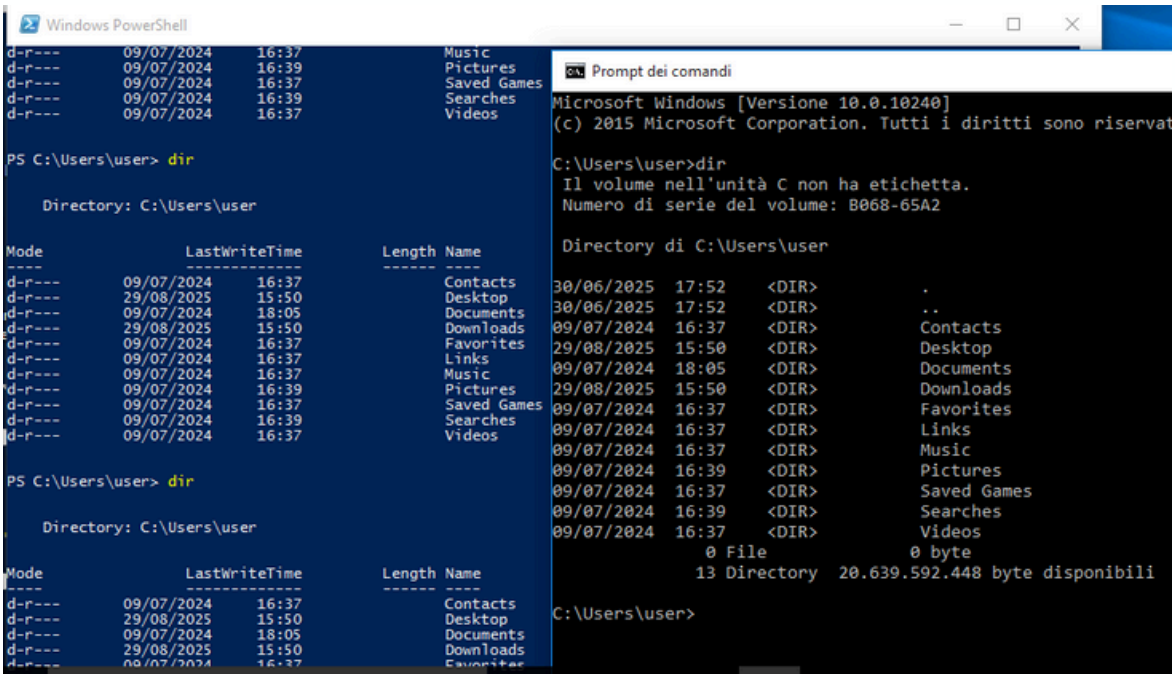
Esercizio per il progetto settimanale Unit 3 - S11 - L5

- Esplorare alcune funzionalità di Windows **PowerShell**
- Studio **IoC** - tramite link di anyrun spiegare le minacce presenti

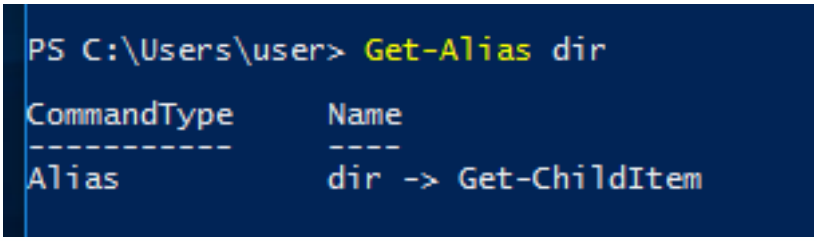
Parte 1 - Accedere alla console PowerShell.
a. Fai clic su Start. Cerca e seleziona powershell.
b. Fai clic su Start. Cerca e seleziona prompt dei comandi (command prompt).

Parte 2 - Esplorare i comandi del Prompt dei Comandi e di PowerShell.
a. Inserisci dir al prompt in entrambe le finestre.
ipconfig e ping sono i medesimi.



Parte 3

Parte 3 - Esplorare i cmdlet. a. I comandi PowerShell, chiamati cmdlet, sono costruiti nella forma di una stringa verbo-nome. Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, inserisci Get-Alias dir al prompt di PowerShell.



Qual è il comando PowerShell per dir?

Get-ChildItem è il nome ufficiale del cmdlet che svolge la funzione di listare elementi (file, directory, chiavi di registro, ecc.) in PowerShell.
Quando scriviamo dir in PowerShell, in realtà stai eseguendo il cmdlet Get-ChildItem

I **cmdlet** (pronunciati "command-let") sono i comandi nativi e specializzati di Microsoft PowerShell.

- Funzione: Eseguono operazioni amministrative singole e specifiche (es. Get-Service, Stop-Process).
- Output: Restituiscono oggetti .NET (dati strutturati) anziché testo, rendendoli ideali per l'automazione e per l'uso nella pipeline (|).
- Struttura Verbo-Nome: Tutti i cmdlet seguono la convenzione fissa Azione-Risorsa (es. Get-Service, Set-Item), rendendoli estremamente intuitivi.
- Orientamento agli Oggetti: A differenza dei comandi tradizionali che usano solo testo, i cmdlet producono e consumano oggetti .NET (dati strutturati). Questo permette una manipolazione e un'analisi dei dati molto più potenti e precise.
- Pipeline: L'output basato su oggetti consente un uso efficace della pipeline (|), che connette più cmdlet in sequenza per automatizzare attività complesse (es. filtrare, ordinare o modificare i dati).
- Scopo: Sono progettati per eseguire operazioni monofunzione per l'amministrazione, la configurazione e l'automazione di sistemi, sia Windows che multipiattaforma.

Parte 4

a. Al prompt di PowerShell, inserisci netstat -h per vedere le opzioni disponibili per il comando netstat.

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

Visualizza statistiche relative ai protocolli e alle
connessioni di rete TCP/IP correnti.

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

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -b            Visualizza il file eseguibile utilizzato per la creazione
                di ogni connessione o porta di ascolto. Alcuni file
                eseguibili conosciuti includono più componenti indipendenti.
```

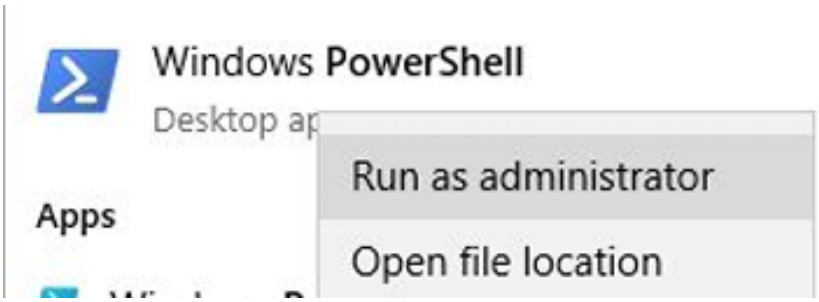
b. Per visualizzare la tabella di routing con le rotte attive, inserisci netstat -r al prompt.

```
PS C:\Users\user> netstat -r
===========================================================================
Elenco interfacce
  4...08 00 27 af 44 7c ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0     192.168.50.1   192.168.50.107    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
    192.168.50.0    255.255.255.0         On-link    192.168.50.107    266
   192.168.50.107  255.255.255.255         On-link    192.168.50.107    266
   192.168.50.255  255.255.255.255         On-link    192.168.50.107    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.50.107    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.50.107    266
===========================================================================
Route permanenti:
   Indirizzo rete            Mask   Indir. gateway Metrica
          0.0.0.0          0.0.0.0     192.168.50.1  Predefinito
===========================================================================

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  1    306 ::1/128                  On-link
  1    306 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
```

Qual è il gateway IPv4?

192.168.50.1

c. Apri ed esegui una seconda PowerShell con privilegi elevati. Fai clic su Start. Cerca PowerShell e fai clic con il pulsante destro su Windows PowerShell e seleziona Esegui come amministratore. Fai clic su Sì per consentire a questa app di apportare modifiche al tuo dispositivo



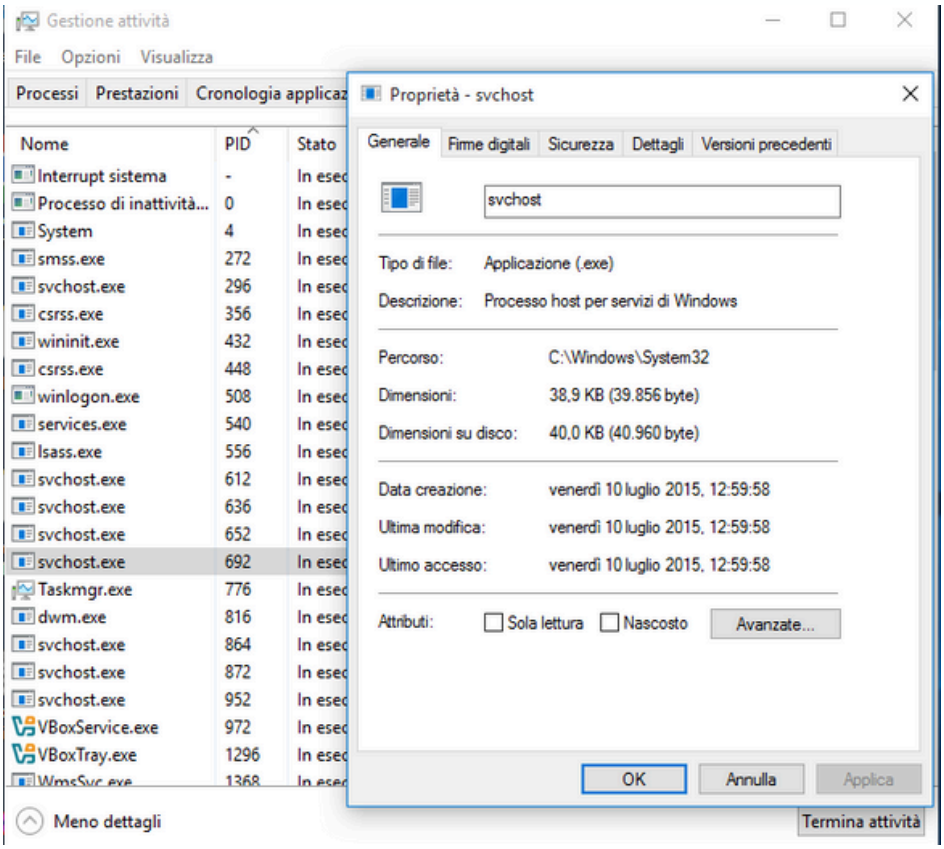
d. Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Inserisci **netstat -abno** al prompt.

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Windows\system32> netstat -abno

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:7              0.0.0.0:0              LISTENING       2196
 [tcpsvcs.exe]
  TCP    0.0.0.0:9              0.0.0.0:0              LISTENING       2196
 [tcpsvcs.exe]
  TCP    0.0.0.0:13             0.0.0.0:0              LISTENING       2196
 [tcpsvcs.exe]
  TCP    0.0.0.0:17             0.0.0.0:0              LISTENING       2196
 [tcpsvcs.exe]
  TCP    0.0.0.0:19             0.0.0.0:0              LISTENING       2196
 [tcpsvcs.exe]
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       692
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       2064
 [mqsvc.exe]
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       2064
 [mqsvc.exe]
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       2064
 [mqsvc.exe]
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       2064
 [mqsvc.exe]
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       872
  TermService
 [svchost.exe]
  TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING       2800
 [postgres.exe]
  TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING       2452
 [tomcat7.exe]
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       2452
 [tomcat7.exe]
  TCP    0.0.0.0:8443           0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49408          0.0.0.0:0              LISTENING       432
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49409          0.0.0.0:0              LISTENING       296
  EventLog
```

e. Apri Gestione Attività (Task Manager). Naviga alla scheda Dettagli Details). Fai clic sull'intestazione PID in modo che i PID siano in ordine

f. Seleziona uno dei PID dai risultati di `netstat -abno`. PID 756 è usato in questo esempio.

g. Individua il PID selezionato in Gestione Attività. Fai clic con il pulsante destro sul PID selezionato in Gestione Attività per aprire la finestra di dialogo Proprietà Properties) per maggiori informazioni.



Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Ho deciso di attenzionare il PID 692, le informazioni sul processo svchost.exe (PID 692) si dividono tra i dati in tempo reale forniti da Gestione attività e i metadati statici del file.

Dati dal Processo (Stato Reale)

Il processo è in stato In esecuzione sotto un utente di sistema (SERVIZIO LOCALE) e la sua funzione è quella di essere il Processo host per servizi di Windows. L'utilizzo delle risorse è molto basso, con CPU a 00 e Memoria a 2.748 K.

Dati del File (Dettagli)

Nella scheda Dettagli di un file di sistema come svchost.exe si trovano le informazioni che ne attestano l'identità e l'origine:

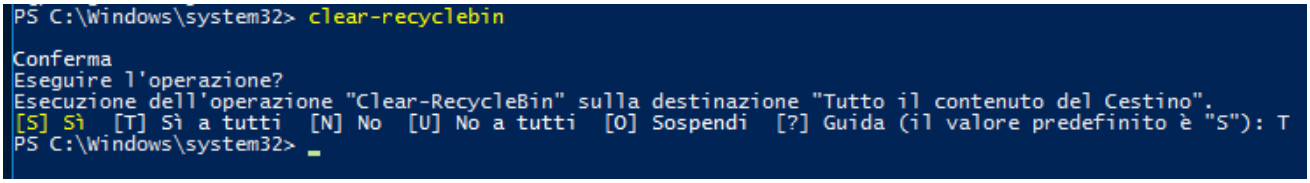
- Versione del File e del Prodotto (i numeri di versione specifici del file e del sistema operativo).
- Nome del Prodotto (es. "Microsoft Windows Operating System").
- Copyright (es. "Microsoft Corporation").

Queste informazioni servono principalmente per confermare l'autenticità e l'integrità del file, garantendo che non si tratti di un malware mascherato. Possiamo verificare anche il nome originale del file cosi da evitare file mascherati

Svuotare il cestino usando PowerShell.

I comandi PowerShell possono semplificare la gestione di una grande rete di computer. Ad esempio, se volessi implementare una nuova soluzione di sicurezza su tutti i server della rete, potresti usare un comando o uno script PowerShell per implementare e verificare che i servizi siano in esecuzione. Puoi anche eseguire comandi PowerShell per semplificare azioni che richiederebbero più passaggi per essere eseguite usando gli strumenti grafici del desktop di Windows.

a. Apri il Cestino. Verifica che ci siano elementi che possono essere eliminati
b. Se non ci sono file nel Cestino, crea alcuni file, come un file e mettili nel Cestino.
c. In una console PowerShell, inserisci clear-recyclebin al prompt.



Cosa è successo ai file nel Cestino?

I File presenti nel Cestino sono stati eliminati.

Esercizio 2: Studio Ioc

- Studio **IoC** - tramite link di anyrun spiegare le minacce presenti

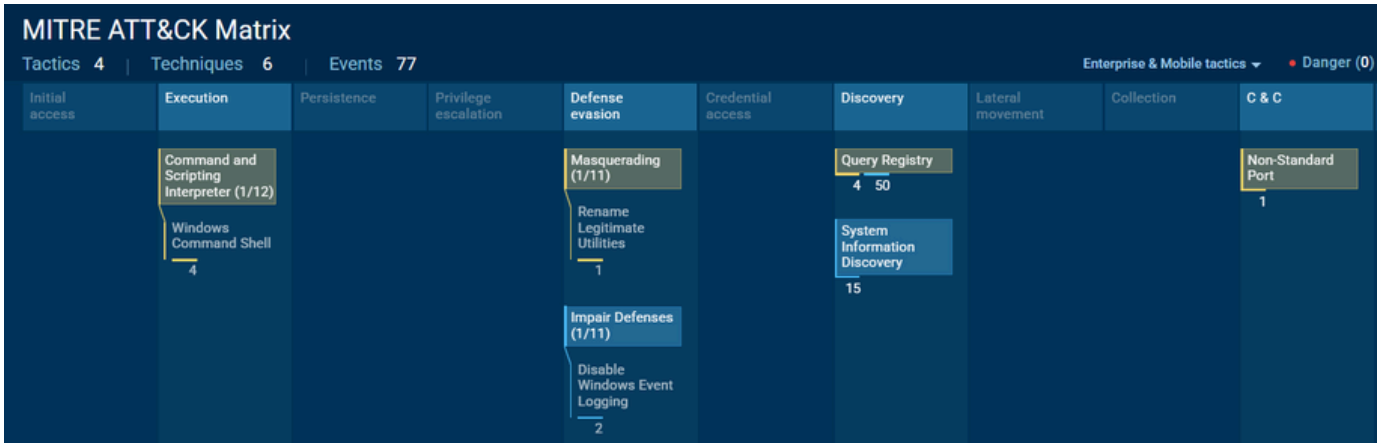
https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

Tramite text report possiamo notare subito il verdetto (attività malevola), ci fornisce l'URL di origine (GitHub) e gli hash dei file che ci indicano le compromissioni.

General Info

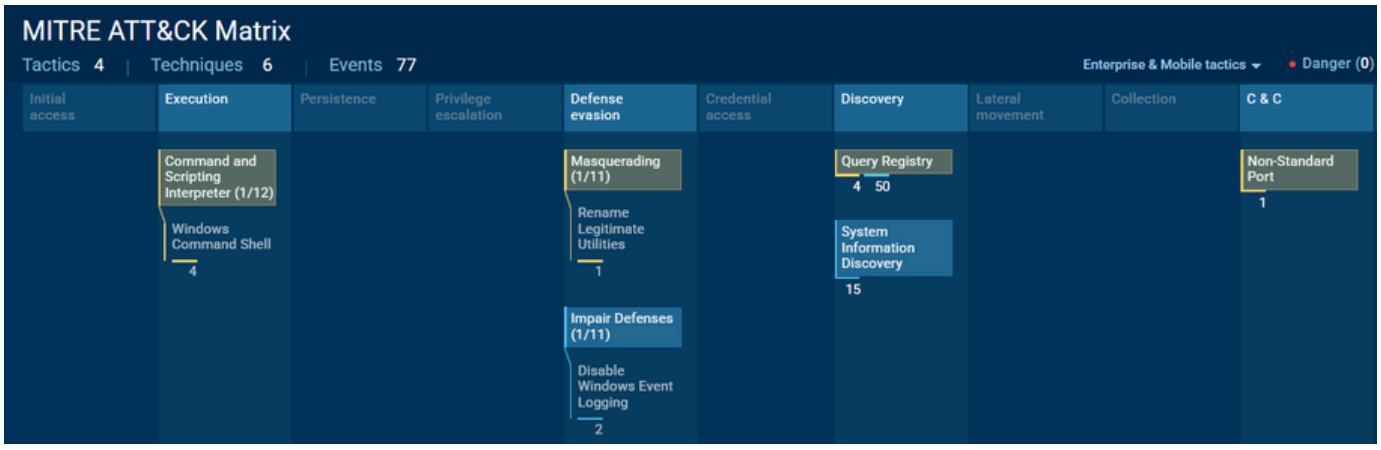
URL:	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
Full analysis:	https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Il malware come possiamo vedere nel grafico ha usato diverse tecniche tra cui quelle di **aggiramento** e di **esecuzione**, ha tentato di disattivare il windows event logger per cancellare le prove e ha usato **cmd.exe** e **timeout.exe** per evitare che venisse scoperto durante un analisi

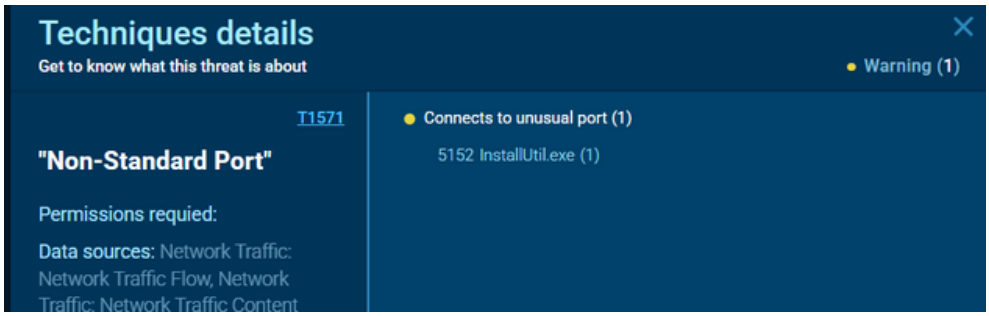


Il Malware ha cercato di raccogliere informazioni tramite l'azione discovery leggendo chiavi di registro ha poi modificato le chiavi di registro di Firefox per mascherarsi nel browser e stabilire una persistenza

Il processo identificato con PID 6596 (associato a firefox.exe) ha eseguito numerose operazioni di scrittura e cancellazione sulle chiavi di registro di firefox



Come passaggio finale il malware ,per abilitare lo scambio di dati, ha stabilito connessioni di rete esterne su porte non standard per comunicare con il suo server, il malware è pericoloso perchè cerca di nascondere le sue traccie e mascherarsi, caratteristiche comuni di un trojan.



1 - Stabilire la Persistenza Tramite l'Avvio di Firefox

L'obiettivo primario è garantire che il componente malevolo venga eseguito ogni volta che l'utente lancia il browser.

- Azione: Scrittura (write) sulla Chiave di Avvio
- Chiave: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\exeLauncher
- Significato: Il malware modifica la chiave di registro che definisce il meccanismo di lancio di Firefox. Questo gli permette di iniettarsi nel processo legittimo o di far eseguire il proprio codice in un passaggio intermedio, assicurandosi così la persistenza sul sistema.

2 - Manipolazione delle Impostazioni Interne del Browser

Dopo aver stabilito la persistenza, il malware procede ad alterare il comportamento e l'aspetto interno di Firefox.

- Azione: Scrittura Ripetuta su varie impostazioni interne.
- Chiavi:HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings e altre chiavi relative al percorso e al tema.
- Significato: Alterando le impostazioni dell'interfaccia utente (UISettings), il malware si prepara a modificare la visualizzazione dei contenuti all'interno del browser. Questo è un passo critico che può portare al dirottamento del traffico, all'iniezione di annunci malevoli o alla modifica delle pagine web visualizzate dall'utente per scopi fraudolenti.

In sintesi, l'attacco dimostra che il malware ha preso di mira specificamente il profilo e le configurazioni di Firefox, cercando di stabilire un punto d'appoggio per nascondere la sua presenza e alterare il normale funzionamento del browser a danno dell'utente.