

Analisi statica basica

Sommario

Traccia esercizio principale	2
Traccia esercizio facoltativo	2
Requisiti.....	2
Svolgimento esercizio principale	4
Cosa sono le librerie e perché sono importanti?	4
Librerie del malware	4
Colonne della tabella	5
Analisi delle librerie	5
Analisi delle sezioni	6

Traccia esercizio principale

Rispondere ai seguenti quesiti, con riferimento al file eseguibile:

C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe

- Indicare le **librerie importate** dal malware, fornendo una **descrizione** per ognuna di esse tramite AI;
- Indicare le **sezioni** di cui si compone il malware, fornendo una **descrizione** per ognuna di essa tramite AI.

Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare.

Traccia esercizio facoltativo

- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

Requisiti

Scaricare il Flare VM

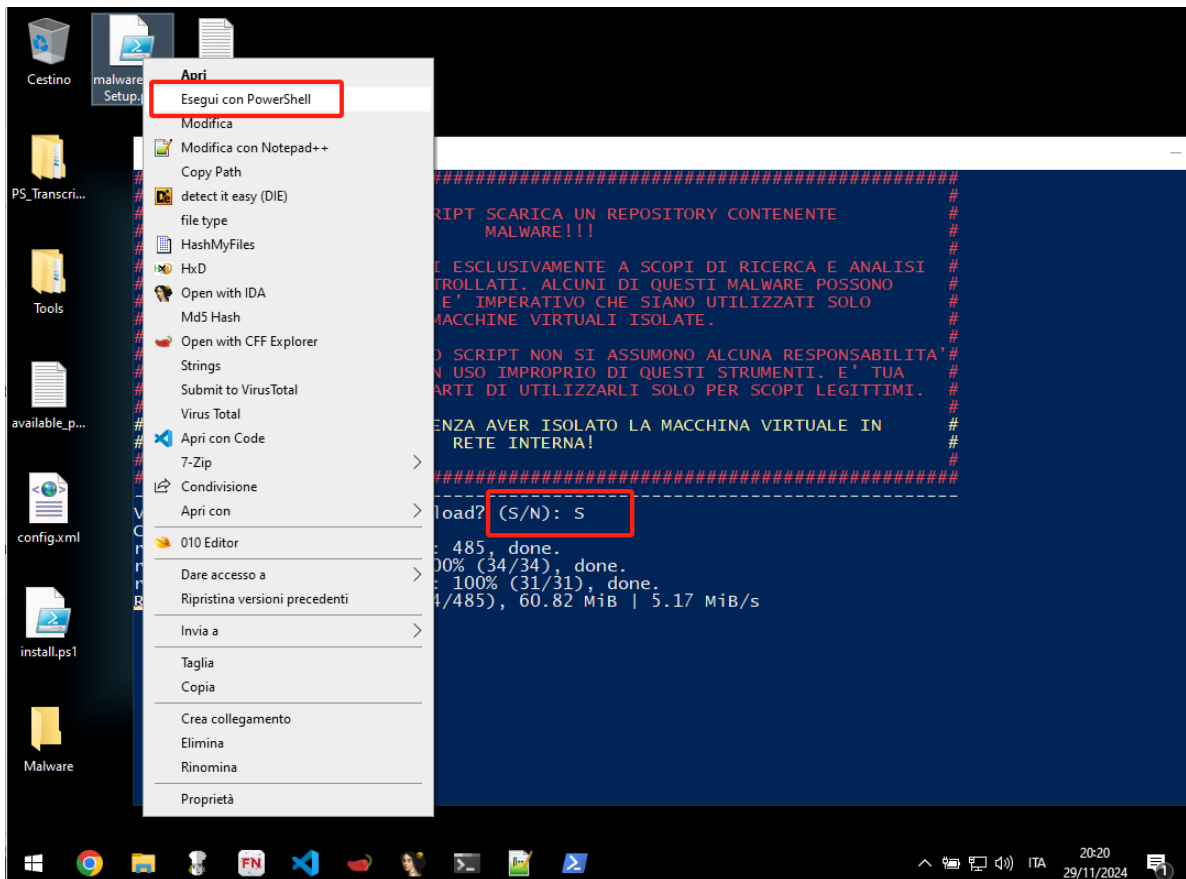
<https://drive.google.com/file/d/1q12YsFS7Gildlp-U8bakTmuxVoyZk9IU/view?usp=sharing>

Nella VM mettere in bridge e scaricare la repository

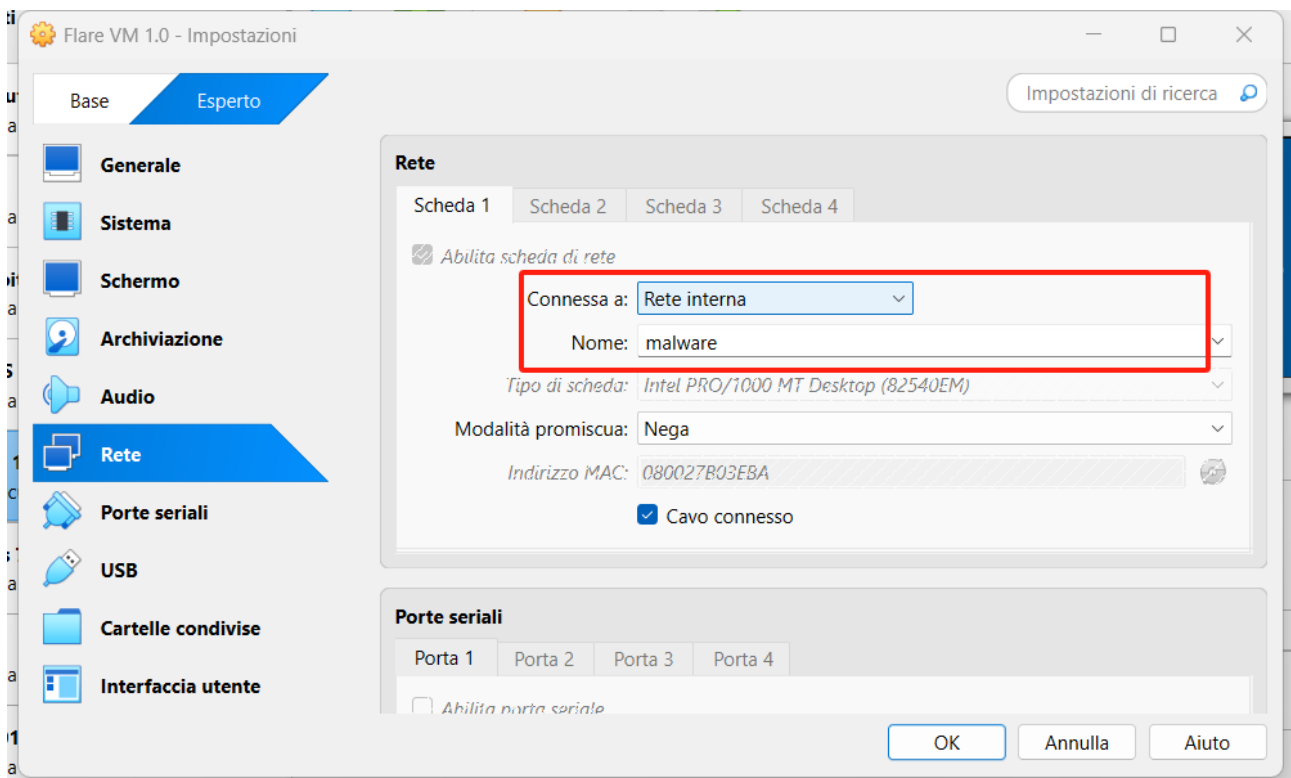
```
○○○

# Autore: Paolo Rampino <liadserv@gmail.com>-
# Avviso legale-
Write-Host "#####" -ForegroundColor Red
Write-Host "# " -ForegroundColor Red
Write-Host "# .... ATTENZIONE: QUESTO SCRIPT SCARICA UN REPOSITORY CONTENENTE....." -ForegroundColor Red
Write-Host "# ..... MALWARE!!!" -ForegroundColor Red
Write-Host "# " -ForegroundColor Red
Write-Host "# QUESTI FILE SONO DESTINATI ESCLUSIVAMENTE A SCOPI DI RICERCA E ANALISI" -ForegroundColor Red
Write-Host "# .. MALWARE IN AMBIENTI CONTROLLATI. ALCUNI DI QUESTI MALWARE POSSONO .." -ForegroundColor Red
Write-Host "# ..... INFETTARE LA RETE. E' IMPERATIVO CHE SIANO UTILIZZATI SOLO .." -ForegroundColor Red
Write-Host "# ..... IN MACCHINE VIRTUALI ISOLATE....." -ForegroundColor Red
Write-Host "# " -ForegroundColor Red
Write-Host "# LA SCUOLA E L'AUTORE DELLO SCRIPT NON SI ASSUMONO ALCUNA RESPONSABILITA'" -ForegroundColor Red
Write-Host "# .. PER DANNI DERIVANTI DA UN USO IMPROPRIO DI QUESTI STRUMENTI. E' TUA .." -ForegroundColor Red
Write-Host "# .. RESPONSABILITA' ASSICURARTI DI UTILIZZARLI SOLO PER SCOPI LEGITTIMI.." -ForegroundColor Red
Write-Host "# " -ForegroundColor Red
Write-Host "# .. NON AVVIARE NESSUN FILE SENZA AVER ISOLATO LA MACCHINA VIRTUALE IN .." -ForegroundColor Red
Write-Host "# ..... RETE INTERNA!" -ForegroundColor Red
Write-Host "# " -ForegroundColor Red
Write-Host "#####" -ForegroundColor White

# Richiede conferma dall'utente prima di procedere-
$confirm = Read-Host "Vuoi continuare con il download? (S/N)"-
if ($confirm -eq "S" -or $confirm -eq "s") {-
    ..cd $([Environment]::GetFolderPath("Desktop"))-
    ..if (Test-Path -Path ".\Malware") {-
        ..Remove-Item .\Malware -Recurse -Force-
    }-
    ..git clone https://github.com/Akir4d/The-MALWARE-Repo.git Malware-
    ..cd .\Malware-
    ..git restore --source=HEAD :/-
} else {-
    ..Write-Host "Operazione annullata dall'utente." -ForegroundColor Green-
}
```



Riavviare in rete interna isolate



Svolgimento esercizio principale

Cosa sono le librerie e perché sono importanti?

Le librerie dinamiche (*Dynamic Link Libraries*, DLL) contengono funzioni che un programma può richiamare per eseguire operazioni specifiche. Ad esempio, una funzione in una DLL può servire per leggere un file, creare un processo, o effettuare una connessione di rete.

Quando un programma eseguibile (come *calcolatriceinnovativa.exe*) vuole utilizzare una funzione, importa la DLL che la contiene. Il fatto che un file importi determinate librerie e funzioni aiuta a capire cosa fa il programma e, nel caso di un malware, quali operazioni malevole potrebbe compiere.

Librerie del malware

Si è aperto il file incriminato con CFF explorer, sezione "Import Directory"

Property	Value
File Name	C:\Users\flare\Desktop\Malware\calcolatriceinnovativa.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	112.50 KB (115200 bytes)
PE Size	112.50 KB (115200 bytes)
Created	Friday 29 November 2024, 20.21.04
Modified	Friday 29 November 2024, 20.21.04
Accessed	Friday 29 November 2024, 20.35.01
MD5	D2F8843D1128B0421BA7A25999A59F32
SHA-1	C50F22713B54E2FB476BFF5DDA83B76B493212C

Property	Value
CompanyName	Корпорация Майкрософт
FileDescription	Калькулятор для Windows
FileVersion	5.1.2600.0 (xpclient.010817-1148)
InternalName	CALC
LegalCopyright	© Корпорация Майкрософт. Все права защищены.
OriginalFilename	CALC.EXE
ProductName	Операционная система Microsoft® Windows®

Module Name	Imports	OFs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFFF	FFFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000
KERNEL32.dll	30	00012C2C	FFFFFFFF	FFFFFFFF	000131D4	00001020
GDI32.dll	3	00012C1C	FFFFFFFF	FFFFFFFF	0001320C	00001010
USER32.dll	69	00012CB0	FFFFFFFF	FFFFFFFF	000136A4	000010A4

Colonne della tabella

1. **Module Name:**
 - Nome della libreria (*module*) importata dal programma. Ogni riga rappresenta una libreria diversa.
2. **Imports:**
 - Numero di funzioni richiamate (*importate*) dalla libreria. Ad esempio:
 - SHELL32.dll ha **1 funzione importata**.
 - USER32.dll ha **69 funzioni importate**.
3. **OFTs (Original First Thunks):**
 - Indirizzo di memoria che punta al nome della funzione importata. Questo valore è utile per il caricamento del file PE in memoria.
4. **TimeStamp:**
 - Questo campo normalmente indica il timestamp della libreria. In molti malware, questo campo viene impostato a **FFFFFFF** per confondere o evadere i sistemi di analisi.
5. **ForwarderChain:**
 - Può contenere il riferimento a un'altra libreria che offre la stessa funzione (forwarding). Anche qui, il valore **FFFFFFF** è un comportamento comune nei malware.
6. **Name RVA:**
 - L'indirizzo relativo virtuale (RVA) in cui si trova il nome della libreria nel file.
7. **FTs (IAT):**
 - Entry nella tabella di importazione (*Import Address Table*), che viene utilizzata dal programma per richiamare effettivamente le funzioni.

Analisi delle librerie

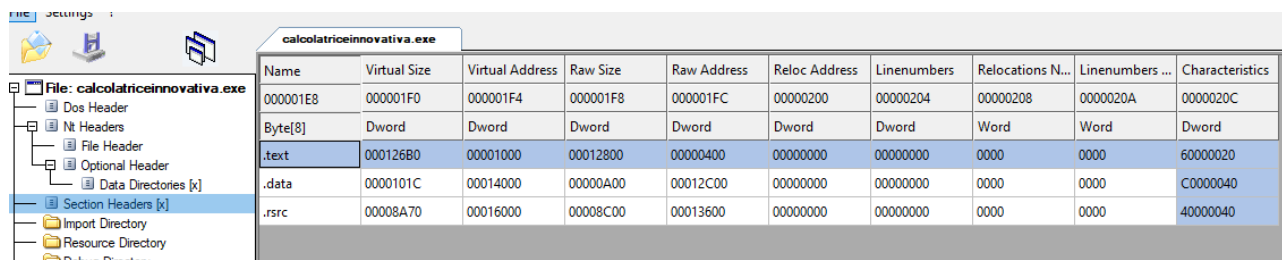
Vediamo cosa significano le librerie mostrate:

1. **SHELL32.dll:**
 - Questa libreria contiene funzioni per operazioni legate al sistema, come l'interazione con il file system (es. aprire file, copiare, eliminare).
 - Uso potenziale da parte di malware: manipolare file, eseguire comandi di sistema.
2. **msvcrt.dll:**
 - È la libreria runtime di Microsoft C, che fornisce funzioni comuni come gestione di stringhe, operazioni matematiche e gestione della memoria.
 - Uso potenziale da parte di malware: attività generiche di supporto al codice malevolo.
3. **ADVAPI32.dll:**
 - Contiene funzioni per l'accesso al registro di sistema e per la gestione della sicurezza (es. permessi, token di accesso).
 - Uso potenziale da parte di malware: modificare chiavi di registro, cambiare permessi o creare utenti malevoli.
4. **KERNEL32.dll:**
 - Una delle librerie fondamentali di Windows, contiene funzioni per la gestione di memoria, processi, file e sincronizzazione.
 - Uso potenziale da parte di malware: creare nuovi processi/thread, leggere/scrivere file, allocare memoria per payload malevoli.
5. **GDI32.dll:**
 - Fornisce funzioni per la grafica, come il rendering di immagini e disegni.
 - Uso potenziale da parte di malware: creare finestre false o modificare elementi visivi per ingannare l'utente.

6. USER32.dll:

- Contiene funzioni relative all'interfaccia utente, come la gestione di finestre, input da tastiera e mouse.
- Uso potenziale da parte di malware: spiare l'input dell'utente (keylogging), creare finestre per phishing.

Analisi Section Headers



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001E8	000001F0	000001F4	000001F8	000001FC	00000200	00000204	00000208	0000020A	0000020C
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000126B0	00001000	00012800	00000400	00000000	00000000	0000	0000	60000020
.data	0000101C	00014000	00000A00	00012C00	00000000	00000000	0000	0000	C0000040
.rsrc	00008A70	00016000	00008C00	00013600	00000000	00000000	0000	0000	40000040

L'analisi della sezione **Section Headers** di un file eseguibile fornisce informazioni sulle diverse parti del file e sul loro scopo. Ogni sezione ha caratteristiche specifiche che possono indicare come il file si comporta o cosa contiene.

Descrizione delle sezioni principali

Il file in analisi contiene tre sezioni principali:

1. .text:

- **Contenuto:** Questa sezione è dedicata al codice eseguibile del programma. È la parte che viene eseguita dalla CPU.
- **Dimensioni:**
 - **Virtual Size:** 0x1F4 (500 byte in memoria).
 - **Raw Size:** 0x200 (512 byte nel file).
 - La differenza indica un allineamento dei dati.
- **Caratteristiche:** Il valore 60000020 indica che questa sezione è **eseguibile** e **leggibile**, ma non **scrivibile**.

2. .data:

- **Contenuto:** Contiene dati modificabili usati dal programma, come variabili globali o configurazioni necessarie durante l'esecuzione.
- **Dimensioni:**
 - **Virtual Size:** 0x400 (1024 byte in memoria).
 - **Raw Size:** 0x200 (512 byte nel file).
 - La differenza indica che questa sezione utilizzerà più memoria rispetto allo spazio occupato nel file.
- **Caratteristiche:** Il valore C0000040 indica che questa sezione è **leggibile** e **scrivibile**, ma non **eseguibile**.

3. .rsrc:

- **Contenuto:** Contiene risorse del programma, come icone, stringhe di testo o dati aggiuntivi.
- **Dimensioni:**
 - **Virtual Size:** 0x1360 (4960 byte in memoria).
 - **Raw Size:** 0x1360 (4960 byte nel file).
 - Le dimensioni coincidono, indicando che questa sezione non ha dati aggiunti in memoria.
- **Caratteristiche:** Il valore 40000040 indica che questa sezione è **leggibile**, ma non **eseguibile** né **scrivibile**.

Valori chiave nella parte inferiore

1. Code Entry Point:

- **Valore:** 0x11FB2
- Si tratta dell'indirizzo in memoria dove inizia l'esecuzione del codice. È il punto da cui il sistema operativo avvia il programma.

2. Import Address Table (IAT):

- **Posizione:** 0x1000
- Questa tabella elenca le funzioni utilizzate dal file eseguibile, importate da librerie esterne (DLL). Esaminare questa tabella è essenziale per comprendere il comportamento del programma.

3. Debug Directory:

- **Posizione:** 0x14200
- Questa directory contiene informazioni di supporto per il debugging. Se presente, può fornire dettagli utili per l'analisi.

Hex Dump

L'Hex Dump in basso mostra il contenuto binario della sezione selezionata (probabilmente .rsrc). A sinistra si trovano i byte in formato esadecimale, mentre a destra i dati leggibili in formato ASCII.

- **Elementi da cercare:**

- **Stringhe leggibili** (colonna ASCII): Potrebbero includere URL, indirizzi IP, nomi di file o altri dati utili.
- **Dati offuscati o crittografati:** Se i byte non formano stringhe comprensibili, potrebbe trattarsi di dati codificati.

Svolgimento esercizio facoltativo

Mascheramento

- **Descrizione:** Il malware si presenta come un programma legittimo, in questo caso una "calcolatrice innovativa". Questa tecnica è comune nei malware per ingannare gli utenti e spingerli a eseguire il file senza sospetti.
- **Scopo:**
 - Aumentare la probabilità che l'utente esegua il file.
 - Ridurre il rischio di essere identificato come malware da utenti meno esperti.

Tecniche di evasione

1. Codice compresso o crittografato

- **Indicazioni:**
 - La presenza di codice compresso o crittografato è spesso un segno di offuscamento, una tecnica utilizzata per nascondere il reale comportamento del malware.
 - Il rapporto di compressione $\text{zlib} < 0.3$ suggerisce che il codice sia stato compresso per ridurre la leggibilità durante l'analisi.
- **Effetto:**
 - Rende più difficile per gli analisti comprendere il comportamento del malware senza decomprimere o deoffuscare il codice.

2. Sezione .text eseguibile

- **Indicazioni:**
 - Contiene codice che viene effettivamente eseguito.
 - Il possibile uso di compressione nella sezione .text può indicare ulteriori livelli di offuscamento del codice dannoso.
- **Effetto:**
 - Nasconde il funzionamento del malware e aumenta la difficoltà dell'analisi statica.

3. Scarsa attività quando eseguito

- **Indicazioni:**
 - Il malware potrebbe essere progettato per rimanere dormiente o inattivo se rileva un ambiente di analisi (es. sandbox o macchine virtuali).
- **Effetto:**
 - Riduce la possibilità di essere rilevato durante l'analisi dinamica.

4. Rilevamento di macchine virtuali

- **Indicazioni:**
 - I malware includono spesso tecniche per rilevare se vengono eseguiti in ambienti virtuali utilizzati per l'analisi (es. VirtualBox, VMware).
- **Effetto:**
 - Evitano di attivarsi in questi ambienti, ostacolando l'analisi da parte dei ricercatori.

Funzionalità di accesso remoto

- **Descrizione:**
 - La presenza di funzionalità di accesso remoto suggerisce che il malware potrebbe essere utilizzato come un **RAT (Remote Access Trojan)**.
 - Questo tipo di malware consente a un attaccante di:
 - Controllare il computer della vittima.
 - Accedere a file, webcam, microfono o altre risorse.
- **Indicazioni:**

- Il malware potrebbe utilizzare funzioni di rete per comunicare con un server di comando e controllo (C2).
- Potrebbe essere in grado di eseguire comandi arbitrari sul sistema della vittima.

Cattura di input

- **Descrizione:**
 - L'uso di un oggetto **DirectInput** è tipico per catturare l'input da tastiera. Questa funzionalità è comunemente associata a **keylogger**.
- **Scopo:**
 - Registrare tutto ciò che viene digitato sulla tastiera, inclusi:
 - Password.
 - Informazioni sensibili.
 - Credenziali di accesso.
- **Effetto:**
 - Questo comportamento rappresenta una grave minaccia alla privacy e alla sicurezza degli utenti colpiti.

Conclusioni

Il malware analizzato presenta le seguenti caratteristiche principali:

1. **Mascheramento:**
 - Si presenta come un'applicazione legittima per ingannare gli utenti.
2. **Tecniche di evasione:**
 - Usa compressione o crittografia per nascondere il codice.
 - Adotta comportamenti dormienti per evitare il rilevamento in ambienti virtuali.
3. **Funzionalità dannose:**
 - Include funzionalità di accesso remoto che consentono il controllo del sistema della vittima.
 - Implementa tecniche di cattura dell'input, suggerendo uno scopo di keylogging.