Zurich 26.11.2024

Attività di Analisi del Malware

Oggetto: Sarà condiviso un malware relativamente innocuo.

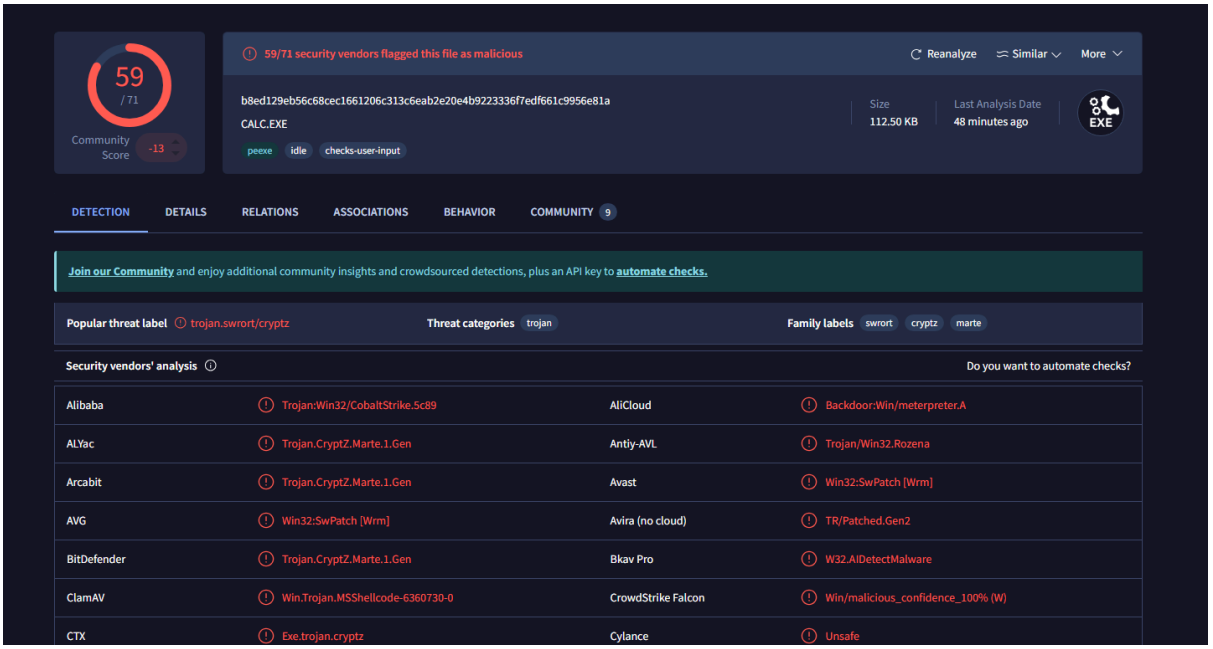
Compiti:

1. **Analisi Statica**: Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.

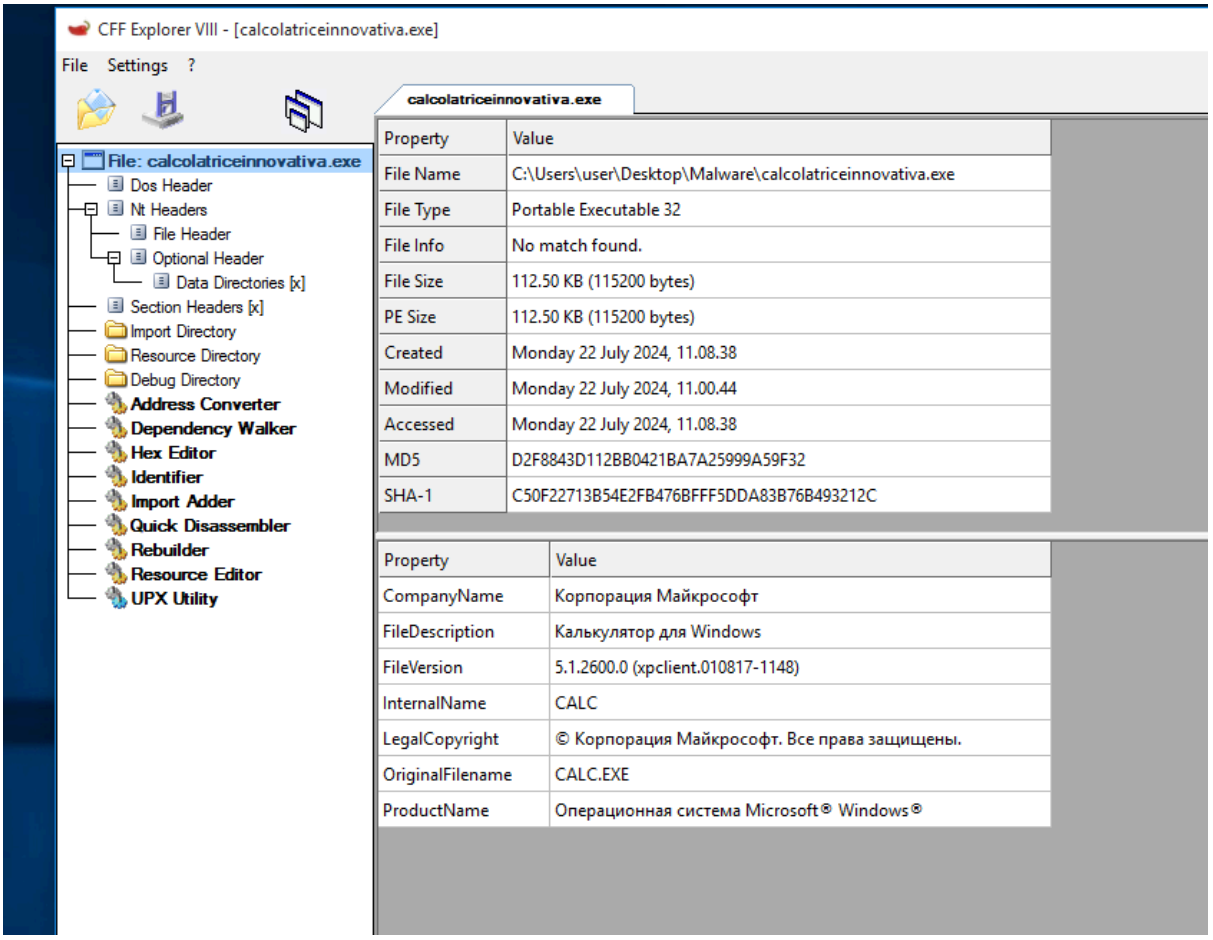
2. **Analisi Dinamica**: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

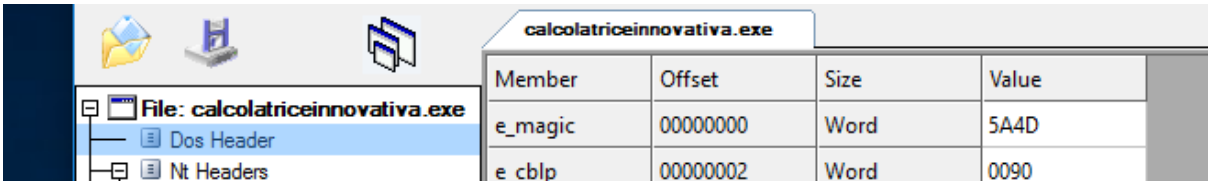
Svolgimento

Dopo aver scaricato il file “calcolatriceinnovativa.exe” siamo andati ad analizzarlo.
Andiamo a fare l’analisi statica innanzitutto.

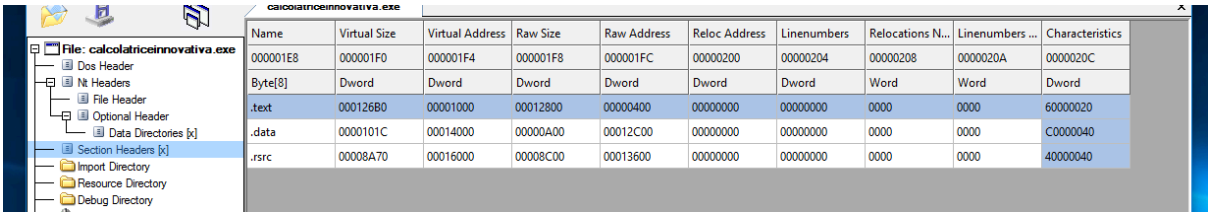


Questa una prima analisi data da virustotal.
Proseguiamo alla scansione del file con CFF explorer.

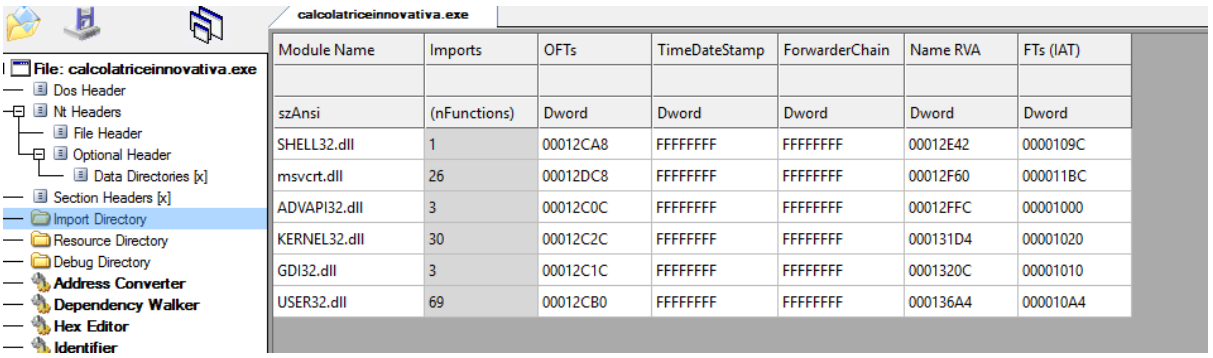




Capiamo che è un eseguibile dal valore 5A4D nella sezione e_magic

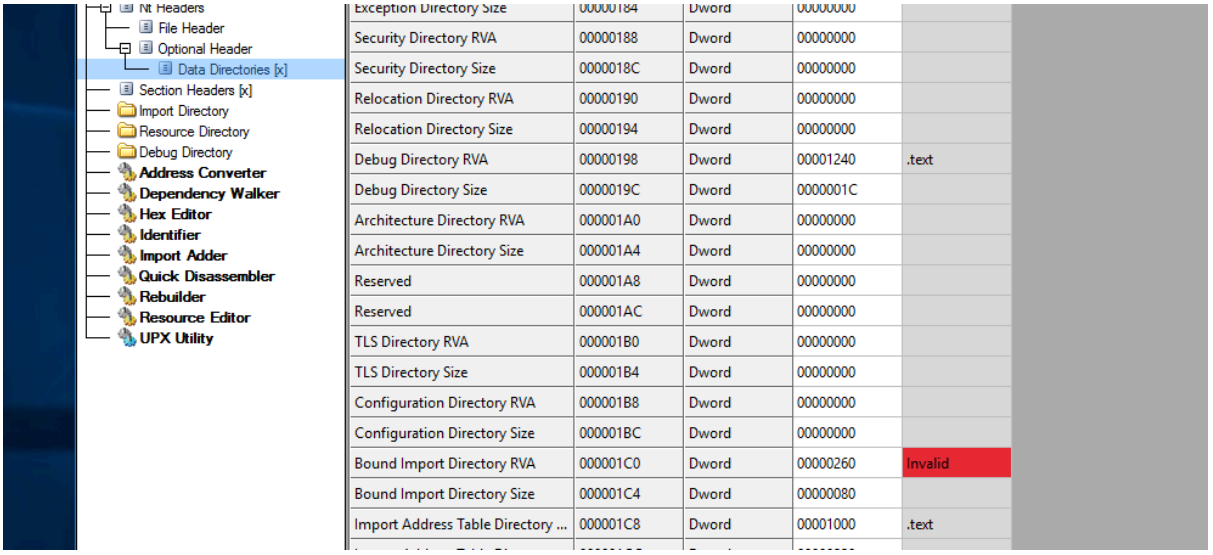


Non contiene la sezione .rdata, quindi forse non è molto complesso come malware, oppure è possibile che chi l'ha progettato voleva appositamente che non fosse troppo "pesante".



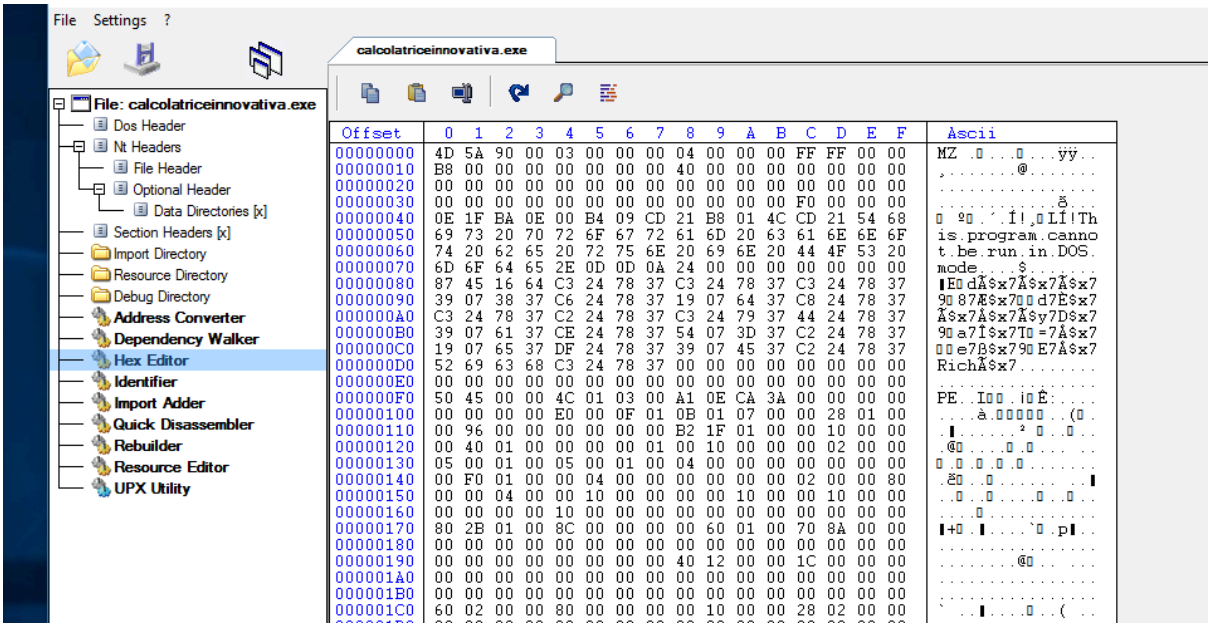
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFFF	FFFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000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

Va a caricare alcune delle librerie più importanti in ambiente Windows per avere accesso come root/amministratore al sistema e poter leggere/creare/modificare/cancellare le librerie.

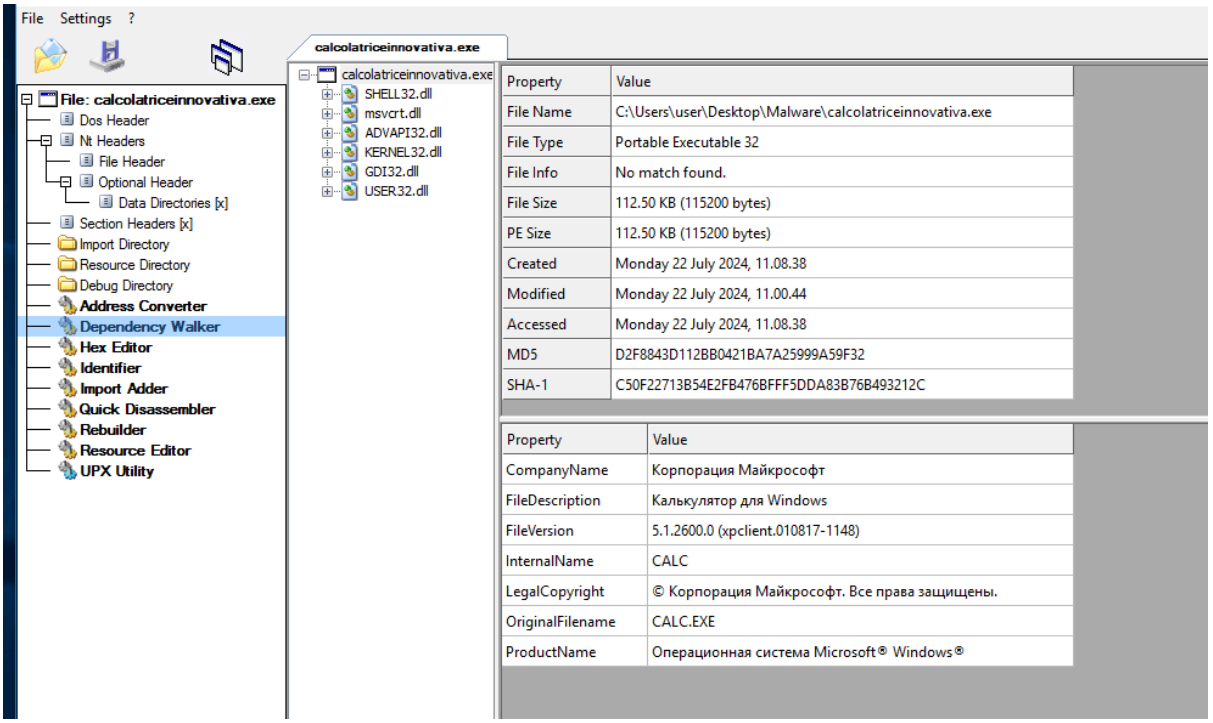


Exception Directory Size	00000184	Dword	00000000	
Security Directory RVA	00000188	Dword	00000000	
Security Directory Size	0000018C	Dword	00000000	
Relocation Directory RVA	00000190	Dword	00000000	
Relocation Directory Size	00000194	Dword	00000000	
Debug Directory RVA	00000198	Dword	00001240	.text
Debug Directory Size	0000019C	Dword	0000001C	
Architecture Directory RVA	000001A0	Dword	00000000	
Architecture Directory Size	000001A4	Dword	00000000	
Reserved	000001A8	Dword	00000000	
Reserved	000001AC	Dword	00000000	
TLS Directory RVA	000001B0	Dword	00000000	
TLS Directory Size	000001B4	Dword	00000000	
Configuration Directory RVA	000001B8	Dword	00000000	
Configuration Directory Size	000001BC	Dword	00000000	
Bound Import Directory RVA	000001C0	Dword	00000260	Invalid
Bound Import Directory Size	000001C4	Dword	00000080	
Import Address Table Directory ...	000001C8	Dword	00001000	.text

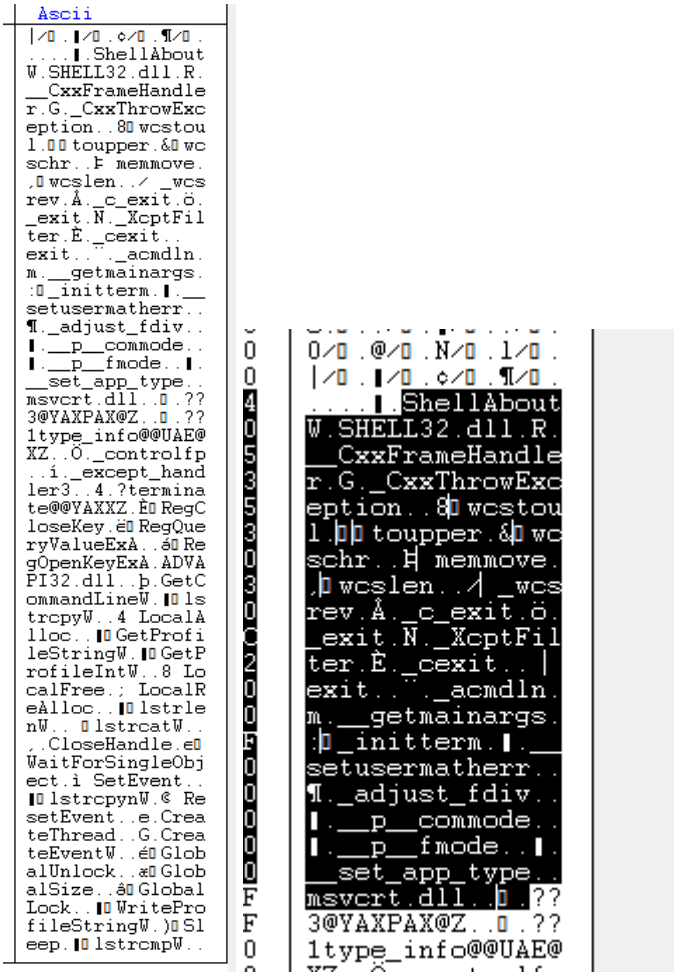
In Optional Header/Data Directories troviamo un valore “Invalid”, ciò vuol dire che il file potrebbe essere “corrotto”



Nell’Hex Editor notiamo “this program cannot be run in DOS” e questo ci insospettisce.



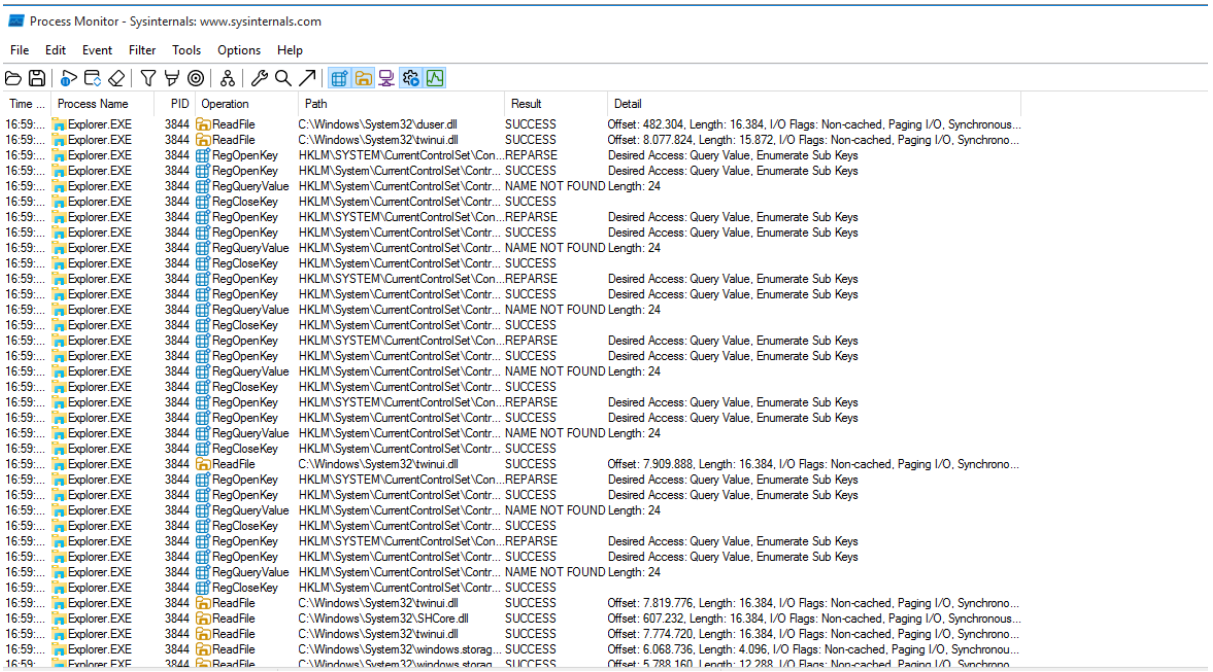
Molto strano che un programma su Windows in lingua inglese o italiana abbia come proprietà Microsoft Corporation, ma scritto in russo



In questi codici Ascii capiamo che:

- `CxxThrowException`. Questo indica che il programma è stato scritto in C++
- Vengono utilizzate funzioni per manipolare stringhe, come `wcslen` (lunghezza di una stringa Unicode) e `memcpy` (copia di un blocco di memoria).
- Il codice sembra contenere operazioni di inizializzazione, come `_initterm` e `setusermatherr`, che preparano l'ambiente di esecuzione del programma.
- Il codice sembra contenere numerose chiamate a funzioni di librerie di sistema, come `SHELL32.dll`, che suggerisce che il programma interagisce con il sistema operativo a basso livello.
- Ci sono riferimenti a funzioni per la gestione degli eventi, come `WaitForSingleObject` e `SetEvent`, suggerendo che il programma potrebbe essere un'applicazione con interfaccia grafica o un servizio in background.
- Sono presenti chiamate a funzioni per allocare e deallocare memoria, come `LocalAlloc` e `LocalFree`, suggerendo che il programma gestisce dinamicamente la memoria durante l'esecuzione.

Passiamo alla fase dinamica utilizzando il tool Procmon.



```
Time ...  Process Name   PID  Operation       Path                                     Result           Detail
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\duser.dll            SUCCESS          Offset: 482.304, Length: 16.384, I/O Flags: Non-cached, Paging I/O, Synchronous...
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\twinui.dll           SUCCESS          Offset: 8.077.824, Length: 15.872, I/O Flags: Non-cached, Paging I/O, Synchrono...
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\twinui.dll           SUCCESS          Offset: 7.909.888, Length: 16.384, I/O Flags: Non-cached, Paging I/O, Synchrono...
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\SYSTEM\CurrentControlSet\Con...REPARSE               Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegOpenKey      HKLM\System\CurrentControlSet\Contr...   SUCCESS          Desired Access: Query Value, Enumerate Sub Keys
16:59:... Explorer.EXE   3844 RegQueryValue   HKLM\System\CurrentControlSet\Contr...   NAME NOT FOUND Length: 24
16:59:... Explorer.EXE   3844 RegCloseKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\twinui.dll           SUCCESS          Offset: 7.819.776, Length: 16.384, I/O Flags: Non-cached, Paging I/O, Synchrono...
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\SHCore.dll           SUCCESS          Offset: 607.232, Length: 16.384, I/O Flags: Non-cached, Paging I/O, Synchronous...
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\twinui.dll           SUCCESS          Offset: 7.774.720, Length: 16.384, I/O Flags: Non-cached, Paging I/O, Synchrono...
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\windows.storag...    SUCCESS          Offset: 6.068.736, Length: 4.096, I/O Flags: Non-cached, Paging I/O, Synchronou...
16:59:... Explorer.EXE   3844 ReadFile        C:\Windows\System32\windows.storag...    SUCCESS          Offset: 5.788.160, Length: 12.288, I/O Flags: Non-cached, Paging I/O, Synchrono...
```

L'output di Process Monitor indica che il processo "Explorer.exe" (il processo principale di Windows Explorer) sta effettuando numerose operazioni di lettura e scrittura sul registro di sistema. In particolare, sembra concentrarsi sulle chiavi all'interno di `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`.

Comportamenti sospetti:

- **Numero elevato di accessi al registro:** Un numero così elevato di operazioni di lettura e scrittura sul registro, soprattutto concentrate su una singola chiave, può

essere un segnale di un'attività sospetta. I malware spesso modificano il registro per persistere nel sistema, autoavviarsi o disabilitare le funzionalità di sicurezza.
- **Chiavi di registro bersagliate:** Le chiavi del registro di sistema che vengono accesse sono comunemente utilizzate dai malware per modificare le impostazioni di sistema, caricare driver o eseguire codice arbitrario.

Possibili interpretazioni:

Sulla base di queste osservazioni, è possibile ipotizzare che il malware stia:

- **Cercando di persistere nel sistema:** Modificando le chiavi di avvio automatico o installando driver nascosti.
- **Raccolgendo informazioni:** Leggendo le impostazioni di sistema per acquisire dati sensibili o identificare altre vulnerabilità.
- **Interferendo con le funzionalità di sicurezza:** Disabilitando il firewall, l'antivirus o altre protezioni.
- **Preparando l'ambiente per un'infezione più complessa:** Modificando le impostazioni del sistema per facilitare l'esecuzione di altri moduli dannosi.

Cosa fare:

1. **Non spegnere il computer:** Potrebbe interrompere l'attività del malware e rendere più difficile l'analisi.
2. **Disconnettersi da internet:** Per evitare che il malware comunichi con i suoi server di comando e controllo.
3. **Avviare la modalità provvisoria:** In modalità provvisoria vengono caricati solo i servizi e i driver essenziali, limitando così le attività del malware.
4. **Eseguire una scansione completa con un antivirus aggiornato:** Utilizzare un antivirus affidabile per rilevare e rimuovere il malware.
5. **Utilizzare strumenti di rimozione malware:** Se l'antivirus non riesce a rimuovere il malware, provare a utilizzare strumenti specializzati come Malwarebytes o HitmanPro.
6. **Creare un backup dei dati importanti:** Prima di eseguire qualsiasi azione, è consigliabile creare un backup dei dati importanti per evitare perdite in caso di problemi.