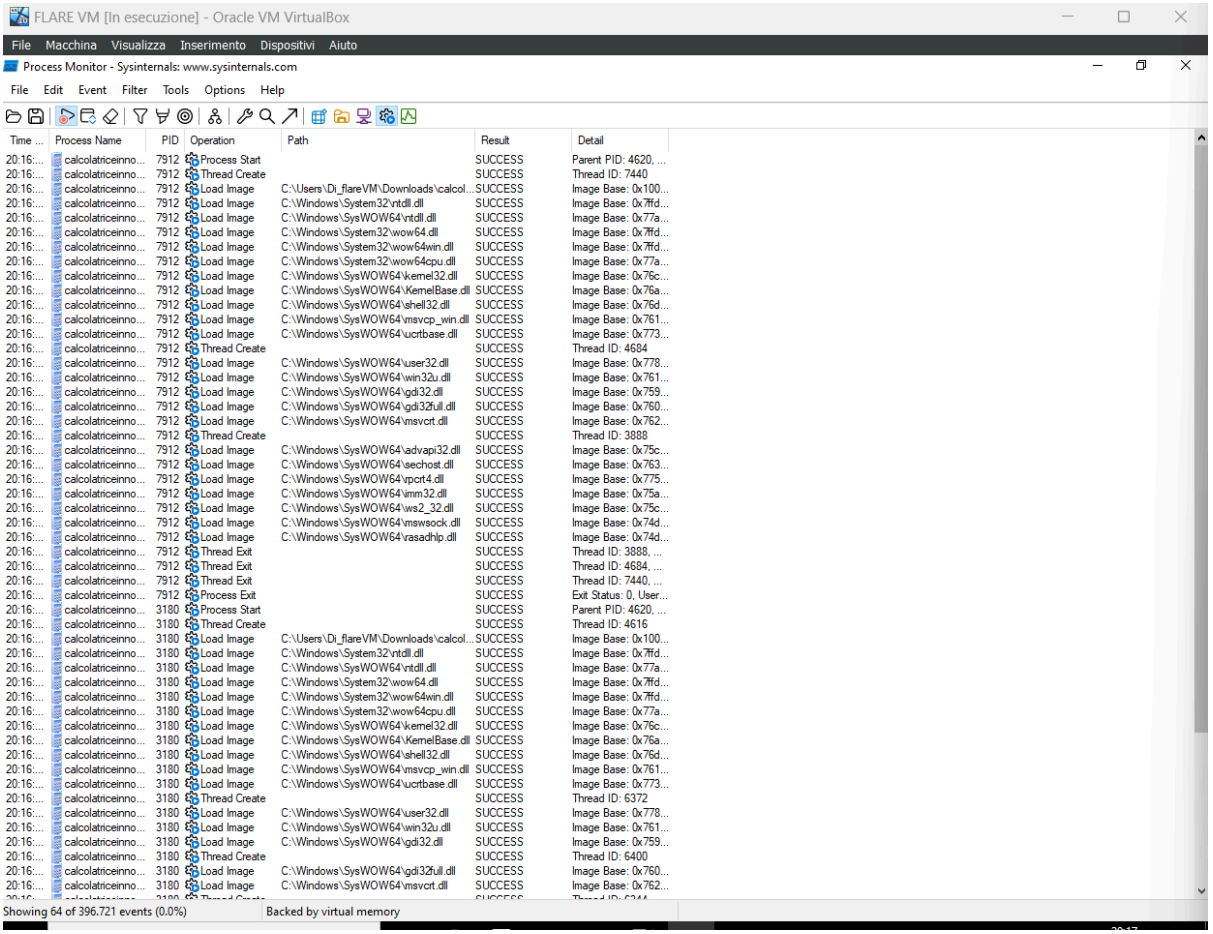
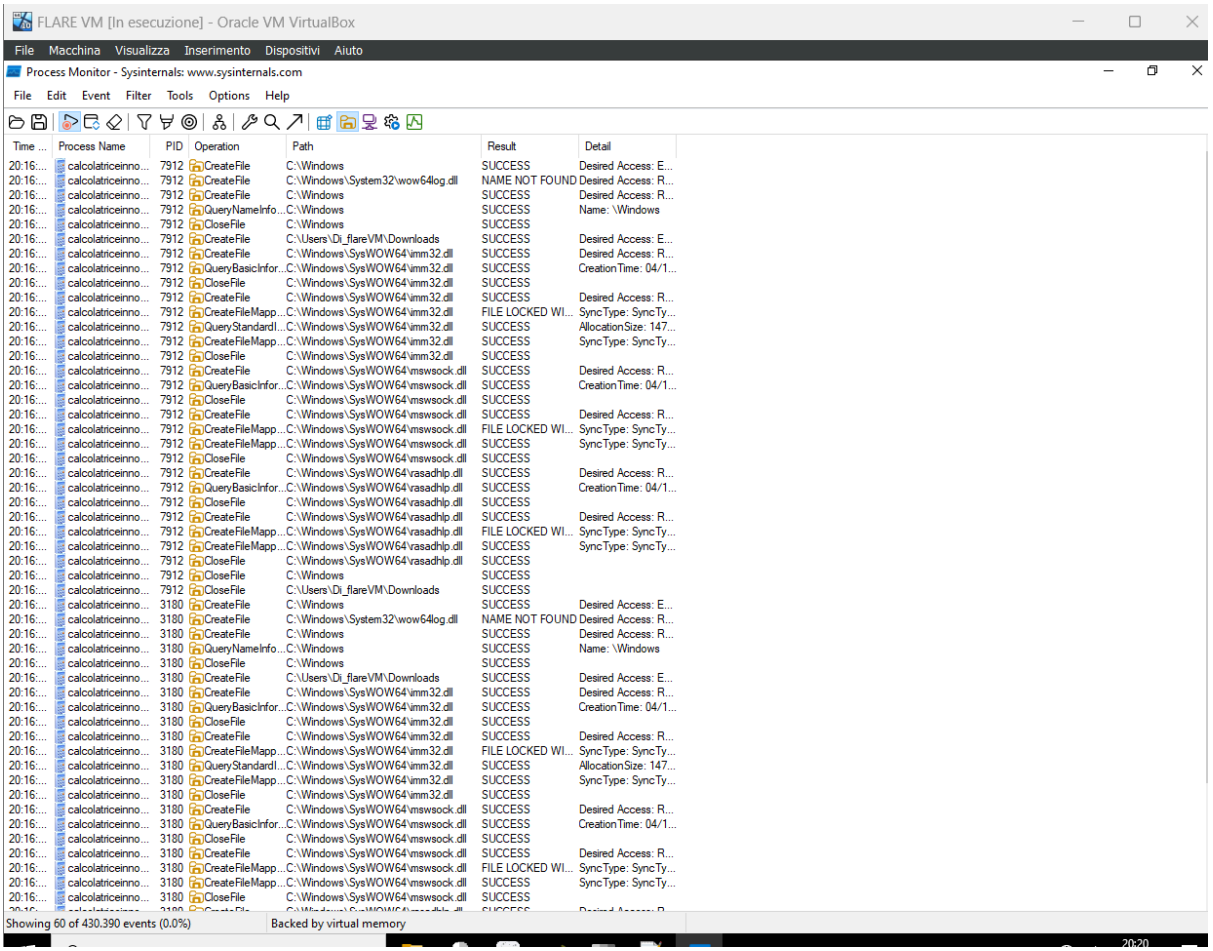

FLARE VM [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
20:16:... calcolatriceinno... 7912 Process Start SUCCESS Parent PID: 4620, ...
20:16:... calcolatriceinno... 7912 Thread Create SUCCESS Thread ID: 7440
20:16:... calcolatriceinno... 7912 Load Image C:\Users\Di_flareVM\Downloads\calcol... SUCCESS Image Base: 0x100...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\System32\ntdll.dll SUCCESS Image Base: 0x7ffd...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\ntdll.dll SUCCESS Image Base: 0x77a...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\System32\wow64.dll SUCCESS Image Base: 0x7ffd...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\System32\wow64win.dll SUCCESS Image Base: 0x7ffd...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\System32\wow64cpu.dll SUCCESS Image Base: 0x77a...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\kernel32.dll SUCCESS Image Base: 0x76c...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\KernelBase.dll SUCCESS Image Base: 0x76a...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\shell32.dll SUCCESS Image Base: 0x76d...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\msvcp_win.dll SUCCESS Image Base: 0x761...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\ucrtbase.dll SUCCESS Image Base: 0x773...
20:16:... calcolatriceinno... 7912 Thread Create SUCCESS Thread ID: 4684
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\user32.dll SUCCESS Image Base: 0x778...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\win32u.dll SUCCESS Image Base: 0x761...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\gdi32.dll SUCCESS Image Base: 0x759...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\gdi32full.dll SUCCESS Image Base: 0x760...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\msvcrt.dll SUCCESS Image Base: 0x762...
20:16:... calcolatriceinno... 7912 Thread Create SUCCESS Thread ID: 3888
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\advapi32.dll SUCCESS Image Base: 0x75c...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\sechost.dll SUCCESS Image Base: 0x763...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\vpcrt4.dll SUCCESS Image Base: 0x775...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\rpcrt4.dll SUCCESS Image Base: 0x75a...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\ws2_32.dll SUCCESS Image Base: 0x75c...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\mswsock.dll SUCCESS Image Base: 0x74d...
20:16:... calcolatriceinno... 7912 Load Image C:\Windows\SysWOW64\wasadhlp.dll SUCCESS Image Base: 0x74d...
20:16:... calcolatriceinno... 7912 Thread Exit SUCCESS Thread ID: 3888, ...
20:16:... calcolatriceinno... 7912 Thread Exit SUCCESS Thread ID: 4684, ...
20:16:... calcolatriceinno... 7912 Thread Exit SUCCESS Thread ID: 7440, ...
20:16:... calcolatriceinno... 7912 Process Exit SUCCESS Exit Status: 0, User...
20:16:... calcolatriceinno... 3180 Process Start SUCCESS Parent PID: 4620, ...
20:16:... calcolatriceinno... 3180 Thread Create SUCCESS Thread ID: 4616
20:16:... calcolatriceinno... 3180 Load Image C:\Users\Di_flareVM\Downloads\calcol... SUCCESS Image Base: 0x100...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\System32\ntdll.dll SUCCESS Image Base: 0x7ffd...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\ntdll.dll SUCCESS Image Base: 0x77a...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\System32\wow64.dll SUCCESS Image Base: 0x7ffd...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\System32\wow64win.dll SUCCESS Image Base: 0x7ffd...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\System32\wow64cpu.dll SUCCESS Image Base: 0x77a...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\kernel32.dll SUCCESS Image Base: 0x76c...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\KernelBase.dll SUCCESS Image Base: 0x76a...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\shell32.dll SUCCESS Image Base: 0x76d...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\msvcp_win.dll SUCCESS Image Base: 0x761...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\ucrtbase.dll SUCCESS Image Base: 0x773...
20:16:... calcolatriceinno... 3180 Thread Create SUCCESS Thread ID: 6372
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\user32.dll SUCCESS Image Base: 0x778...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\win32u.dll SUCCESS Image Base: 0x761...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\gdi32.dll SUCCESS Image Base: 0x759...
20:16:... calcolatriceinno... 3180 Thread Create SUCCESS Thread ID: 6400
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\gdi32full.dll SUCCESS Image Base: 0x760...
20:16:... calcolatriceinno... 3180 Load Image C:\Windows\SysWOW64\msvcrt.dll SUCCESS Image Base: 0x762...
Showing 64 of 396.721 events (0.0%)
Backed by virtual memory



Azioni del malware sul file system

Dalle attività sul file system si può osservare:

1. **Esecuzione e caricamento**:
    - Il malware viene eseguito dalla cartella `"C:\Users\user\Desktop\Malware"`.
    - Tenta di accedere a vari file di sistema e DLL, probabilmente per caricarli in memoria.
2. **Accesso a file di sistema**:
    - Accede a numerose DLL di sistema in `C:\Windows\SysWOW64`, incluse `apphelp.dll`, `kernel32.dll`, `user32.dll`, e `ws2_32.dll` (per funzionalità di rete).
    - Questo potrebbe essere per nascondere la sua attività o per utilizzare funzioni di sistema legittime.

3. **Operazioni di lettura e mapping**:
    - Esegue operazioni di lettura su alcune DLL, come `apphelp.dll` e `ws2_32.dll`.
    - Crea file mapping per diverse DLL, il che potrebbe indicare tentativi di iniezione di codice o manipolazione della memoria.
4. **Interrogazioni di sicurezza**:
    - Esegue molte query di sicurezza sui file, che potrebbero essere dei tentativi di identificare le impostazioni di sicurezza del sistema o di cercare vulnerabilità.
5. **Attività di rete**:
    - Il caricamento di `ws2_32.dll` e `mswsock.dll` suggerisce che il malware potrebbe tentare di stabilire connessioni di rete.
6. **Persistenza e nascondimento**:
    - Non ci sono chiari segni di tentativi di persistenza nel sistema dai log forniti, ma potrebbe essere una fase successiva non catturata in questo log.
7. **Potenziale keylogging o cattura di input**:
    - Il caricamento di `imm32.dll` e `user32.dll` potrebbe indicare tentativi di intercettare l'input dell'utente.
8. **Esplorazione del sistema**:
    - Le numerose query sui file di sistema potrebbero indicare che il malware sta raccogliendo informazioni sul sistema host.
9. **Possibile offuscamento**:
    - L'accesso a molte DLL di sistema potrebbe essere un tentativo di mascherare la sua vera natura mescolando la sua attività con operazioni di sistema normali.

Azioni del malware su processi e thread

Dalle attività sui processi e thread si può osservare:

1. **Caricamento delle librerie**:
    - Il processo inizia caricando numerose librerie di sistema Windows (DLL),
    - principalmente da `C:\Windows\System32` e `C:\Windows\SysWOW64`.
2. **Creazione di thread**:
    - Durante l'esecuzione, il malware crea diversi thread per eseguire le sue operazioni in parallelo.
3. **Operazioni riuscite**:
    - Tutte le operazioni mostrate risultano in "SUCCESS", il che indica che il malware è riuscito a eseguire le sue azioni senza errori.
4. **Terminazione del processo**:
    - Il processo termina dopo aver completato numerose operazioni di caricamento e creazione di thread.

FACOLTATIVO

Azioni del malware sul file system

Dalle attività sul file system si può osservare:

1. **Esecuzione e caricamento**:
    - Il malware viene eseguito dalla cartella `"C:\Users\user\Desktop\Malware"`, come confermato dal log.
    - Tenta di accedere a vari file di sistema e DLL, come `ntdll.dll`, `kernel32.dll`, `user32.dll`, `gdi32.dll`, probabilmente per caricarli in memoria e utilizzarli per le sue operazioni.
2. **Accesso a file di sistema**:
    - Accede a numerose DLL di sistema in `C:\Windows\SysWOW64`, incluse `apphelp.dll`,

`kernel32.dll`, `user32.dll`, `ws2_32.dll`, e altre librerie associate a funzionalità di rete.
    - Questo comportamento è comune sia per eseguibili legittimi sia per malware, che può sfruttare funzioni di sistema legittime per eseguire le sue azioni malevole.
3. **Operazioni di lettura e mapping**:
    - Esegue operazioni di lettura su diverse DLL, come `apphelp.dll` e `ws2_32.dll`, suggerendo che il malware sta accedendo a risorse di sistema importanti.
    - Crea file mapping per alcune DLL, il che potrebbe indicare tentativi di iniezione di codice o manipolazione della memoria.
4. **Interrogazioni di sicurezza e registro di sistema**:
    - Il malware esegue numerose query sul registro di sistema di Windows, in particolare su chiavi relative a **WinSock** e configurazioni di rete, suggerendo che sta raccogliendo informazioni di rete o tentando di modificare le impostazioni di rete.
5. **Attività di rete**:
    - Il caricamento di `ws2_32.dll` e `mswsock.dll` suggerisce che il malware potrebbe avere funzionalità di rete, anche se non sono state osservate connessioni di rete effettive nei log.
6. **Persistenza e nascondimento**:
    - Non ci sono chiari segni di tentativi di persistenza nel sistema nei log esaminati, ma potrebbe essere una fase successiva non catturata.
7. **Potenziale keylogging o cattura di input**:
    - Il caricamento di `imm32.dll` e `user32.dll` potrebbe indicare che il malware tenta di intercettare l'input dell'utente, potenzialmente per il keylogging.
8. **Esplorazione del sistema**:
    - Le numerose query su file di sistema e registro suggeriscono che il malware sta raccogliendo informazioni critiche sul sistema host.

9. **Possibile offuscamento**:
    - L'accesso a molte DLL di sistema potrebbe essere un tentativo di mascherare la sua vera natura mescolando le sue attività con operazioni di sistema legittime.

Azioni del malware su processi e thread

Dalle attività sui processi e thread si può osservare:

1. **Caricamento delle librerie**:
    - Il malware carica numerose librerie di sistema Windows (DLL), come `ntdll.dll`, `kernel32.dll`, `user32.dll`, `gdi32.dll`, e altre associate a funzionalità di sistema e di rete.
2. **Creazione di thread**:
    - Durante l'esecuzione, il malware crea alcuni thread aggiuntivi, potenzialmente per eseguire operazioni parallele, sfruttando più risorse del sistema.
3. **Operazioni riuscite**:
    - Le operazioni monitorate risultano in "SUCCESS", indicando che il malware è riuscito a eseguire le sue azioni senza errori.
4. **Breve durata di esecuzione**:
    - Il processo termina rapidamente con un codice di uscita 0, il che indica una terminazione senza errori. Tuttavia, ciò non esclude che altre azioni dannose siano state eseguite non visibili nei log esaminati.

Considerazioni finali

Il malware **calcolatriceinnovativa.exe** si comporta come un possibile malware di ricognizione, progettato per raccogliere informazioni sul sistema infetto senza compiere azioni distruttive immediate. Il caricamento di numerose librerie di sistema e le operazioni sul file system e sul registro indicano che il malware potrebbe essere nella fase

di preparazione per azioni più complesse, come l'intercettazione di input (keylogging), la modifica delle impostazioni di rete o il controllo del sistema tramite funzionalità di rete non ancora visibili.

Il malware potrebbe tentare di nascondersi attraverso l'uso di componenti di sistema legittimi, rendendo difficile l'individuazione e l'analisi. Sebbene non siano state osservate azioni manifestamente malevole nei log esaminati, il comportamento suggerisce che il malware potrebbe evolversi per scaricare ulteriori payload malevoli o stabilire una connessione con un server di comando e controllo per eseguire altre operazioni.