Analisi dinamica basica

Sommario

Traccia esercizio principale

Rispondere ai seguenti quesiti, con riferimento al file eseguibile:

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

- Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor, fornendo una **descrizione** tramite AI;
- Identificare eventuali azioni del malware su **processi e thread** utilizzando Process Monitor, fornendo una **descrizione** tramite AI.

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

Traccia esercizio facoltativo

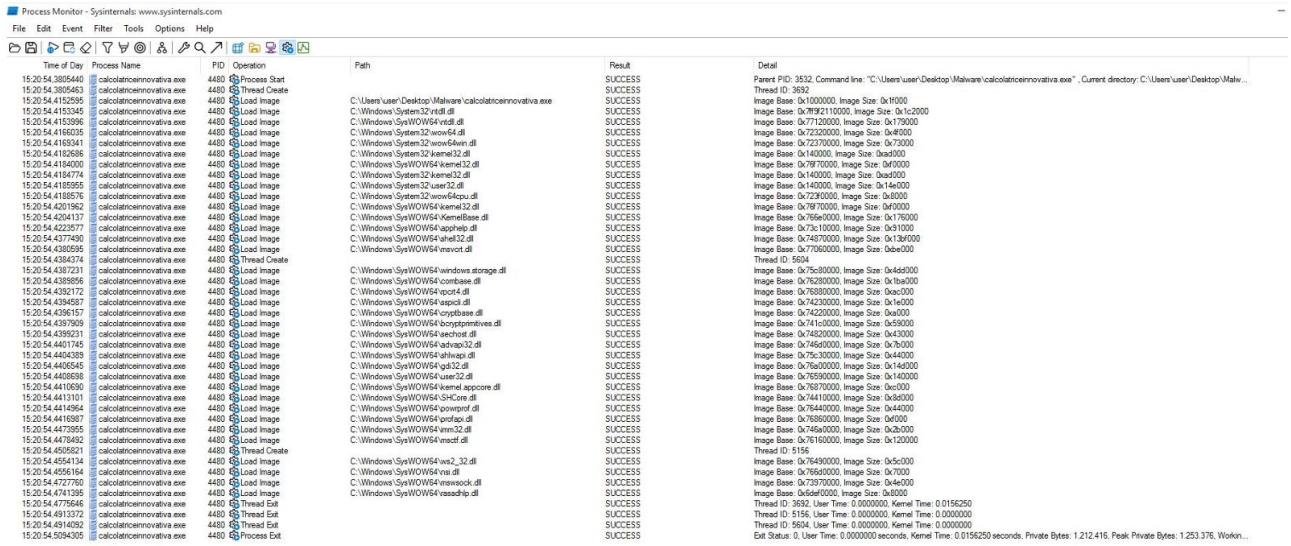
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

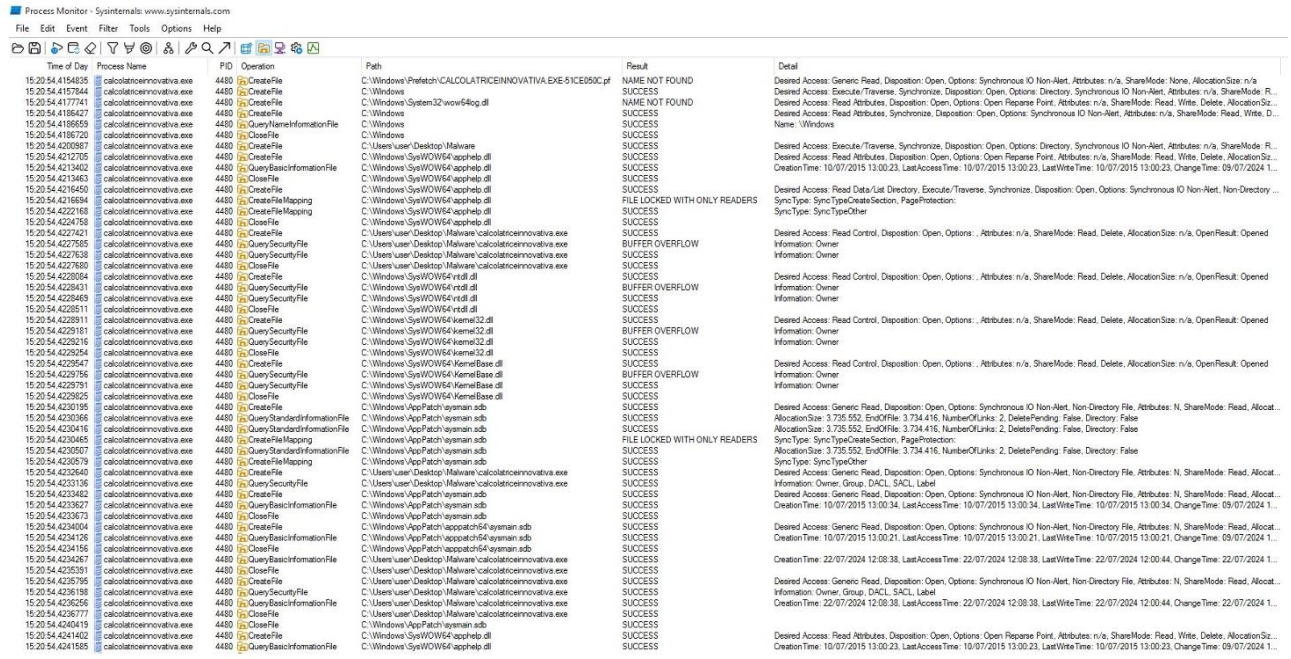
Requisiti

Vedi report M6\W21\D5

Svolgimento esercizio principale

Avviare “calcolatriceinnovativa.exe” e avviare procmon (Process Monitor)





1. Esecuzione e caricamento:

- Il file è stato eseguito dalla directory **C:\Users\user\Desktop\Malware**.
- Durante l'esecuzione, ha tentato di accedere a numerosi file di sistema e librerie **DLL** per caricarli in memoria.
- Il comportamento osservato include il caricamento di DLL standard di Windows da directory come:
  - C:\Windows\System32
  - C:\Windows\SysWOW64
- Tra le DLL caricate si trovano:
  - **apphelp.dll**, **kernel32.dll**, **user32.dll**, **ws2_32.dll**, **mswsock.dll**, **imm32.dll**.

2. Accesso a file di sistema e librerie:

- L'accesso a queste DLL potrebbe essere riconducibile a:
    - Mascheramento di attività malevole utilizzando funzioni di sistema legittime.
    - Utilizzo di funzionalità di rete avanzate o vulnerabilità di sistema.
- Sono state eseguite operazioni di lettura e mapping di memoria sulle DLL, come su ws2_32.dll e apphelp.dll, indicando possibili tentativi di:
    - Iniezione di codice.
    - Manipolazione della memoria.

---

3. Operazioni su thread e processi:

- Il processo ha creato diversi thread durante l'esecuzione, probabilmente per eseguire operazioni parallele.
- Non ci sono segni di persistenza, ma è possibile che il malware stia preparando fasi successive non catturate nei log.

---

4. Attività di rete:

- Il caricamento di librerie di rete, come **ws2_32.dll** e **mswsock.dll**, indica che il file potrebbe tentare di stabilire connessioni di rete.
- Questo potrebbe essere preparatorio per attività di comunicazione remota o per contattare server di comando e controllo (C2).

---

5. Interrogazioni di sicurezza:

- Numerose query di sicurezza sui file di sistema sono state osservate. Queste potrebbero essere tentativi di:
    - Identificare le impostazioni di sicurezza.
    - Cercare file o configurazioni vulnerabili per sfruttarle.

---

6. Possibili funzionalità malevole:

- **Persistenza e nascondimento:**
    - Non ci sono chiari segni di tentativi di persistenza nei log analizzati, ma il malware potrebbe mirare a stabilire una presenza nel sistema in fasi successive.
- **Keylogging o intercettazione di input:**
    - Il caricamento di **imm32.dll** e **user32.dll** potrebbe indicare tentativi di intercettare l'input dell'utente.

- **Esplorazione del sistema:**
    - Le numerose interrogazioni e accessi ai file di sistema suggeriscono che il malware stia raccogliendo informazioni sull'ambiente host.
- **Offuscamento:**
    - L'accesso a molte DLL di sistema può essere un tentativo di confondere un'analisi manuale, mescolando attività malevole con operazioni legittime.

Conclusione combinata:

Le attività osservate indicano che calcolatriceinnovativa.exe è potenzialmente un **malware in fase iniziale di esecuzione**, con l'obiettivo di:

1. Caricare librerie di sistema e manipolare la memoria.
2. Prepararsi per attività malevole, come:
    - Connessioni di rete.
    - Raccolta di input o dati sensibili (potenziale keylogging).
    - Esplorazione del sistema per trovare vulnerabilità o configurazioni sfruttabili.
3. Mascherare la sua vera natura utilizzando funzioni di sistema legittime.

Azioni consigliate:

1. **Eseguire un'analisi statica:**
    - Utilizzare strumenti come **PEStudio** o **IDA Pro** per analizzare eventuali funzioni sospette o codice incorporato.
2. **Monitorare l'attività di rete:**
    - Utilizzare **Wireshark** per rilevare connessioni sospette e analizzare il traffico.
3. **Eseguire il file in un ambiente sandbox:**
    - Testare il comportamento del file in una sandbox come **Cuckoo Sandbox** per osservare eventuali azioni non visibili nei log.
4. **Isolamento preventivo:**
    - Isolare l'host compromesso per evitare ulteriori danni o propagazioni.
5. **Analizzare le connessioni dei server:**
    - Se rilevati contatti con server esterni, verificare gli indirizzi IP e i domini per identificare eventuali server di comando e controllo.
6. **Rimuovere il file:**
    - Se confermata la natura malevola, eliminare il file e ripristinare il sistema a uno stato precedente sicuro.

Questo comportamento, associato alle informazioni osservate nei log, indica che il malware è progettato per stabilire una presenza iniziale e successivamente attivare payload più dannosi.

Svolgimento esercizio facoltativo

Considerazione finale sul malware in analisi

Sulla base delle informazioni raccolte ed elaborate, il malware analizzato sembra essere progettato per raccogliere informazioni preliminari sul sistema senza compiere azioni distruttive immediate. Il comportamento osservato, come il caricamento di librerie di rete (**ws2_32.dll**, **mswsock.dll**) e numerose query al registro di sistema, suggerisce un possibile **malware di ricognizione**. Questo tipo di malware è comunemente utilizzato per identificare vulnerabilità o configurazioni utili a fasi successive di un attacco, come il download di payload aggiuntivi o l'ottenimento di accesso remoto.

La breve durata di esecuzione e l'assenza di attività manifestamente malevole nei log potrebbero indicare che il file è stato progettato per operare in modo furtivo, evitando di generare anomalie evidenti. Tuttavia, non si può escludere che il malware abbia eseguito azioni dannose non catturate nei log forniti.

In conclusione, l'analisi suggerisce che il malware rappresenti una **minaccia potenziale**, con un comportamento iniziale focalizzato sulla raccolta di informazioni e sul mascheramento della propria attività. Si consiglia un'ulteriore analisi in un ambiente controllato per verificare eventuali comportamenti non rilevati in questa fase.