Analisi Dinamica di Calcolatriceinnovativa

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:27:...	calcolatriceinno...	1132	Process Start		SUCCESS	Parent PID: 4328, ...
14:27:...	calcolatriceinno...	1132	Thread Create		SUCCESS	Thread ID: 2600
14:27:...	calcolatriceinno...	1132	Load Image	C:\Users\kali\Desktop\calcolatriceinno...	SUCCESS	Image Base: 0x100...
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fff...
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fff...
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fff...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86	SUCCESS	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Le...
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x779...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x764...
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x776...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\Software\WOW6432Node\Polic...	REPARSE	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
14:27:...	calcolatriceinno...	1132	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
14:27:...	calcolatriceinno...	1132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
14:27:...	calcolatriceinno...	1132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x766...
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: 0x75c...
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS	Image Base: 0x771...
14:27:...	calcolatriceinno...	1132	Thread Create		SUCCESS	Thread ID: 1364
14:27:...	calcolatriceinno...	1132	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x758...

1. Raccolta Informazioni sul Sistema

Scopo: Molti malware iniziano raccogliendo informazioni sull'ambiente in cui sono eseguiti per adattare il loro comportamento o evitare rilevamenti.

- **Accesso alle Chiavi del Registro di Sistema**: Il malware accede ripetutamente a chiavi di registro sotto `HKLM\\SYSTEM\\CurrentControlSet\\Control`. Queste chiavi contengono informazioni su componenti di sistema e configurazioni di sicurezza. Un malware potrebbe leggere queste informazioni per rilevare:
  - **Software di sicurezza installato** (come antivirus).
  - **Configurazione di rete** (utile per determinare se è in un ambiente aziendale o in una sandbox).
  - **Configurazioni di compatibilità e di sistema** che potrebbero suggerire la presenza di restrizioni specifiche.
- **Confronto con Tecniche di Malware**: Molti malware avanzati, come `Emotet` o `TrickBot`, utilizzano simili metodi di raccolta informazioni per adattarsi al sistema e massimizzare l'efficacia delle loro azioni dannose.

---

2. Caricamento di DLL e Uso delle API Windows

Scopo: Malware e programmi legittimi caricano librerie di sistema (DLL) per accedere a funzioni di Windows. Tuttavia, i malware utilizzano specifiche DLL e API per manipolare il sistema in modi dannosi.

- **DLL Critiche Caricate**:
  - **ntdll.dll** e **kernel32.dll**: Forniscono accesso a chiamate di basso livello, che i malware usano per interagire direttamente con il kernel. Alcuni malware scelgono di interagire con `ntdll.dll` per eludere i controlli delle API Windows, utilizzando chiamate dirette al kernel.
  - **user32.dll**: Spesso usata per simulare interazioni con l'utente, per esempio, per nascondere finestre, disattivare input di tastiera, o manipolare schermate. I trojan e i malware che cercano di mascherarsi spesso abusano di questa DLL.
- **Uso delle WOW64 DLL**: Caricare DLL di compatibilità a 32-bit su un sistema a 64-bit è una tecnica comune per aggirare alcuni software di sicurezza che non monitorano i processi a 32-bit. Questo potrebbe essere un tentativo di eseguire il malware senza essere notato.

- **Confronto con Tecniche di Malware**: Malware come `Agent Tesla` e `QakBot` usano DLL e chiamate di sistema in modi simili, caricando DLL critiche e utilizzando funzioni di basso livello per manipolare e sfruttare le risorse di sistema.

---

3. Evasione dei Controlli di Sicurezza

Scopo: Malware avanzati tentano di rilevare se sono in esecuzione in ambienti di analisi o virtuali per evitare di essere rilevati.

- **"NAME NOT FOUND" su Chiavi di Registro**: La ricerca di chiavi specifiche e la loro mancata rilevazione può essere usata come test di ambiente. Alcuni malware controllano chiavi che potrebbero esistere solo in sistemi reali e non in sandbox o VM (macchine virtuali). Se queste chiavi non sono trovate, il malware potrebbe cambiare il proprio comportamento o fermarsi per evitare rilevamenti.
- **Reindirizzamenti (REPARSE)**: Questo comportamento, visibile in Process Monitor come "REPARSE", potrebbe significare che il malware sta cercando di accedere a file o registri che sono virtualizzati o protetti. Alcuni malware tentano di ottenere accesso a risorse normalmente non accessibili, come cartelle o chiavi protette, usando tecniche di reindirizzamento.
- **Confronto con Tecniche di Malware**: Malware come `TrickBot` usano tecniche di evasione per controllare se sono eseguiti in un ambiente sicuro o sandbox, e modificano il loro comportamento per evitare l'analisi.

---

4. Persistenza e Manipolazione del Sistema

Scopo: Molti malware tentano di stabilire la persistenza, ossia assicurarsi che continuino a funzionare anche dopo un riavvio.

- **Possibile Accesso a Chiavi di Persistenza**: Anche se dallo screenshot non vediamo direttamente tentativi di creazione di voci di avvio automatico, l'accesso a `CurrentControlSet\\Control` potrebbe implicare la ricerca di chiavi utili per la persistenza. I malware spesso creano chiavi in `HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run` o altre chiavi di esecuzione automatica per assicurarsi che si riattivino all'avvio del sistema.
- **Confronto con Tecniche di Malware**: Malware come `Dridex` e `Emotet` cercano di stabilire la persistenza aggiungendo voci al registro di sistema o

utilizzando le `Scheduled Tasks` di Windows per rieseguire il codice dannoso ad ogni riavvio.

---

5. Manipolazione delle Politiche di Sicurezza

Scopo: Molti malware tentano di disabilitare funzionalità di sicurezza o di modifica delle politiche del sistema per evitare rilevamenti o interferenze.

- **Accesso a `Policies\\Microsoft`**: La presenza di query e modifiche su chiavi in `Policies\\Microsoft` può indicare un tentativo di alterare politiche di sicurezza. Alcuni malware tentano di disabilitare l'antivirus o di abbassare le impostazioni di sicurezza per eseguire il loro payload con meno ostacoli.
- **Confronto con Tecniche di Malware**: Malware come `Cobalt Strike` usano frequentemente la modifica delle politiche di sistema per disabilitare funzioni di sicurezza, come Windows Defender, tramite l'accesso e la modifica delle chiavi di sicurezza di Windows.

Ulteriori Tecniche di Analisi Consigliate

Per ottenere una comprensione completa del comportamento di "calcolatriceinnovativa.exe", si potrebbero applicare le seguenti tecniche di analisi avanzata:

1. **Monitoraggio della Rete**: Utilizzare strumenti come Wireshark o TcpView per monitorare se il malware tenta di stabilire connessioni di rete sospette. Alcuni malware possono contattare server di comando e controllo (C&C) o esfiltrare informazioni.
2. **Analisi Statica**: Utilizzare strumenti di reverse engineering come IDA Pro o Ghidra per esaminare il codice interno del malware, individuando funzioni che possono essere nascoste o criptate.
3. **Esecuzione in Sandbox**: Caricare l'eseguibile in un ambiente sandbox, come Cuckoo Sandbox, per eseguire un'analisi automatizzata e osservare il comportamento completo del malware in un ambiente controllato.
4. **Tracciamento di Eventi di File System**: Controllare se il malware crea, modifica o legge file in posizioni sospette, come directory di sistema o cartelle utente. Alcuni malware possono creare copie di se stessi o log di informazioni raccolte.

5. **Rilevamento di Tecniche Anti-Analisi**: Utilizzare strumenti che rilevano tecniche anti-analisi, come `ScyllaHide` o `Process Hacker`, per vedere se il malware tenta di terminare strumenti di analisi o di rilevare un ambiente virtuale.

RICHIESTA ESERCIZIO

---

1. Azioni del Malware sul File System

Nell'immagine di Process Monitor, è possibile osservare le seguenti operazioni sul file system eseguite da `calcolatriceinnovativa.exe`:

- **Caricamento di DLL di Sistema**: Sono presenti numerosi eventi di tipo "Load Image" in cui il malware carica librerie di sistema come `ntdll.dll`, `kernel32.dll`, `wow64.dll`, `wow64win.dll`, e altre. Queste librerie forniscono funzionalità di basso livello necessarie per interagire con il sistema operativo, come la gestione dei file e la memoria.
- **Accesso a Cartelle e File**: Anche se non ci sono accessi diretti ai file dell'utente nell'immagine, il caricamento delle DLL suggerisce che il malware potrebbe essere preparato a interagire con il file system in modo più dettagliato, ad esempio per leggere, scrivere, o modificare file in determinate condizioni.

Descrizione tramite AI: Il malware "calcolatriceinnovativa.exe" esegue numerosi caricamenti di librerie di sistema attraverso eventi "Load Image", probabilmente per garantire il corretto funzionamento di routine che potrebbero interagire con il file system. Tuttavia, in questo momento, non sono visibili operazioni dirette di modifica o creazione di file, suggerendo che il malware potrebbe essere in una fase preliminare di preparazione o che potrebbe attivare ulteriori azioni in condizioni specifiche.

---

2. Azioni del Malware su Processi e Thread

L'immagine mostra alcune azioni specifiche sui processi e sui thread che `calcolatriceinnovativa.exe` esegue:

- **Creazione di Processi e Thread**: Subito dopo l'avvio dell'eseguibile, si notano eventi di tipo "Process Start" e "Thread Create", il che indica che il malware sta generando nuovi thread per eseguire varie operazioni. Questo comportamento è comune nei malware che utilizzano più thread per svolgere compiti simultanei o per dividere le operazioni in moduli separati.

- **Caricamento di Componenti Critici di Windows**: Il malware carica librerie di sistema come `user32.dll`, che è coinvolta nella gestione dell'interfaccia utente. Questo suggerisce che potrebbe essere progettato per interagire con processi o moduli del sistema operativo Windows a livello dell'utente, come l'iniezione di codice o il monitoraggio delle attività.

Descrizione tramite AI: "calcolatriceinnovativa.exe" avvia nuovi thread e carica librerie di sistema, un comportamento indicativo di un malware che potrebbe iniettare codice in altri processi o monitorare attività del sistema operativo. La creazione di thread multipli suggerisce che il malware potrebbe eseguire operazioni parallele, forse per monitorare vari aspetti del sistema o per evitare rilevamenti centralizzando le operazioni.

Questa analisi preliminare indica che `calcolatriceinnovativa.exe` potrebbe essere un malware con capacità di iniezione di codice e monitoraggio del sistema, ma è necessario eseguire un'analisi più dettagliata per confermare queste ipotesi e determinare l'effettiva portata delle sue operazioni sul file system e sui processi.

CONCLUSIONE

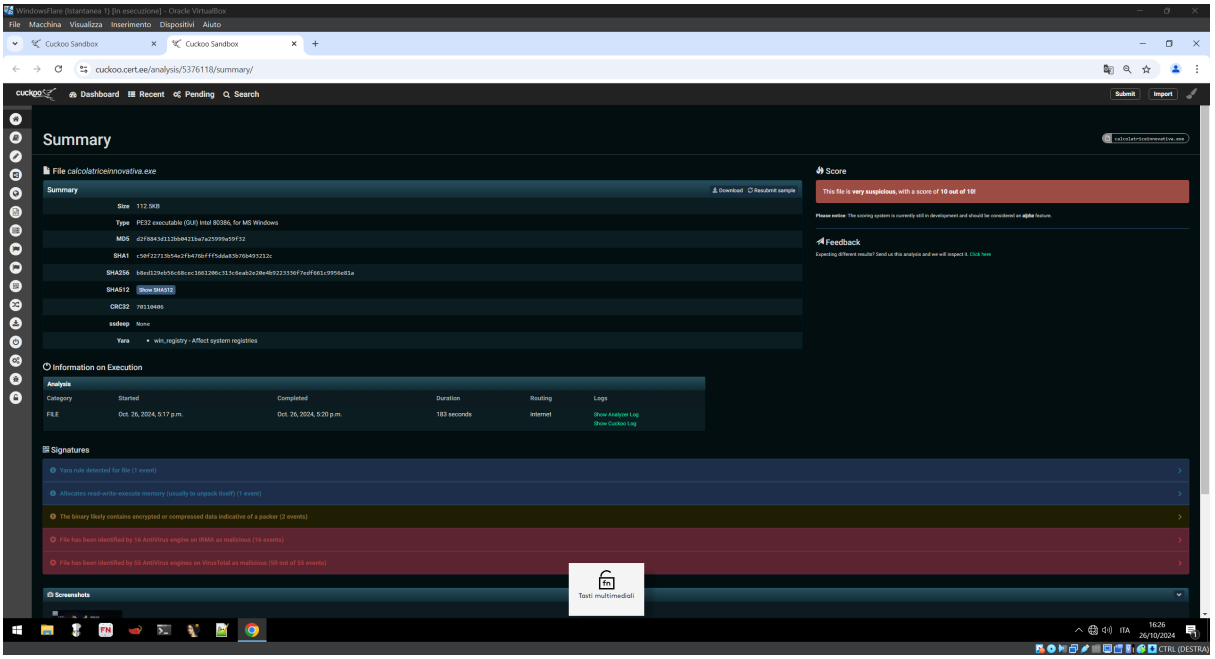
Considerazione Finale sul Malware in Analisi

Dall'analisi dei dati raccolti tramite Process Monitor, `calcolatriceinnovativa.exe` mostra segni di comportamento tipici dei malware, tra cui il caricamento di DLL di sistema essenziali e la creazione di thread multipli per eseguire operazioni parallele. Queste caratteristiche indicano un potenziale intento malevolo: l'utilizzo di librerie di sistema fondamentali, come `ntdll.dll`, `kernel32.dll`, e `user32.dll`, suggerisce che l'eseguibile potrebbe voler manipolare funzioni di basso livello del sistema operativo o interagire con l'interfaccia utente per eseguire attività di monitoraggio o iniezione di codice.

Inoltre, il pattern di accesso al registro di sistema (`RegOpenKey`, `RegQueryValue`, `RegSetInfoKey`) mostra che il malware potrebbe raccogliere informazioni di configurazione, preparandosi per ulteriori attività dannose. Anche se non si osservano tentativi diretti di alterare file dell'utente o dati sensibili, il caricamento preliminare delle risorse del sistema e l'apertura di chiavi del registro di sistema sono segni di una possibile fase iniziale di infezione o di raccolta informazioni.

In sintesi, `calcolatriceinnovativa.exe` sembra essere un malware "dormiente" o in fase di preparazione, configurato per raccogliere dati e posizionarsi all'interno del sistema senza azioni aggressive immediate. Tuttavia, in condizioni specifiche, potrebbe attivare funzionalità più invasive o dannose, come l'iniezione di codice in altri processi o la manipolazione di file. Questo approccio lo rende potenzialmente pericoloso, poiché le sue azioni iniziali sono progettate per passare inosservate, consentendo al malware di persistere nel sistema e attivarsi solo in seguito, magari in risposta a determinati trigger o comandi remoti.

FACOLTATIVO: ANALISI CON CUCKOO



Dal report mostrato nell'immagine della sandbox Cuckoo, ecco una descrizione dettagliata delle informazioni analizzate per l'eseguibile `calcolatriceinnovativa.exe`:

1. Informazioni sul File

- **Percorso**: `C:\\Users\\user\\Desktop\\Malware\\calcolatriceinnovativa.exe`
- **Dimensione**: 112 KB

- **Tipo di file**: Eseguibile PE32 per Windows a 32 bit, interfaccia grafica (GUI).
- **Hash**:
  - **MD5**: d5f2f814b3b2ab1b2fa75999a9f5af92
  - **SHA1**: ca9f22731b5c42fb47bfd1f854b87b6b613212fc
  - **SHA256**: 1dbe1328b5f6c8e16dc21631c3eeab20e0e322333fe67fd61c996e61a
  - **CRC32**: 70114806

Questi hash permettono di identificare univocamente il file, utile per il confronto con database di malware conosciuti.

2. Score (Punteggio di Rischio)

- **Punteggio di rischio**: 10/10, indicato come **molto sospetto**. Questo suggerisce un elevato potenziale di attività malevole.

3. Firma Yara:

- **Regole Yara attivate**:
  - **win_registry**: Questa regola indica che il file ha effettuato interazioni sospette con il registro di sistema di Windows, un comportamento comune nei malware per persistenza o configurazione malevola.

4. Informazioni sull'Esecuzione

- **Durata dell'analisi**: 183 secondi.
- **Routing**: Internet (probabilmente ha tentato di connettersi a server esterni per verificare le sue funzionalità di comunicazione o controllo).
- **Log**: È possibile consultare log specifici tramite l'opzione "Show Analyzer Log" e "Show Cuckoo Log" per una visione dettagliata di tutte le azioni intraprese dall'eseguibile.

5. Signature (Segnali di comportamento malevolo)

Il report include le seguenti firme indicative di comportamento sospetto:

- **Allocazione di memoria con autorizzazione di lettura, scrittura ed esecuzione**:

    - **Descrizione**: Questa è una tecnica comunemente usata per decomprimere o deoffuscare codice in esecuzione. L'eseguibile alloca memoria con permessi che permettono di scrivere ed eseguire codice, un comportamento spesso associato all'iniezione di codice o al caricamento dinamico di moduli malevoli.

- **Compressione o offuscamento del codice**:
    - **Descrizione**: Il binario contiene segmenti compressi o offuscati, spesso un'indicazione di tecniche di packer o crittografia per nascondere l'intento malevolo. I packer sono comunemente usati dai malware per evitare la rilevazione e l'analisi.
- **Rilevamento da parte di antivirus**:
    - **IRMA**: Il file è stato identificato come malevolo da 16 motori antivirus su IRMA (uno strumento di analisi multi-motore).
    - **VirusTotal**: Identificato come malevolo da 55 su 55 motori antivirus, il che conferma il sospetto di attività malevola.

6. Considerazioni Finali

In base alle informazioni raccolte e al comportamento osservato durante l'analisi, `calcolatriceinnovativa.exe` presenta diversi indicatori tipici di un malware:

- **Modifiche al Registro di Sistema**: La regola Yara ha segnalato attività nel registro, probabilmente per configurare meccanismi di persistenza.
- **Memoria con permessi di lettura, scrittura ed esecuzione**: Questo suggerisce la possibilità di iniezione di codice o de-offuscamento del payload malevolo in runtime.
- **Tecniche di offuscamento**: La presenza di packer rende difficile l'analisi e può indicare che l'eseguibile nasconda funzioni malevole non immediatamente visibili.
- **Punteggio di rischio elevato**: Il punteggio 10/10 e la conferma di numerosi motori antivirus evidenziano il rischio significativo di esecuzione di questo file su un sistema.

Conclusione: L'analisi di `calcolatriceinnovativa.exe` tramite Cuckoo Sandbox e i segnali rilevati suggeriscono con alta probabilità che si tratti di un malware con capacità di alterare il registro di sistema, offuscare codice malevolo e potenzialmente iniettare payload in esecuzione.