**AMATO SARA**

**S9 L2**

**Analisi del Malware**

L'obiettivo dell'attività è stato analizzare un campione di malware, attraverso due metodologie principali:

Analisi Statica:

Studio del codice e delle sue proprietà senza eseguire il malware.

Analisi Dinamica:

Esecuzione controllata del malware in un ambiente isolato per osservare il comportamento.

Gli strumenti utilizzati per questa analisi sono:

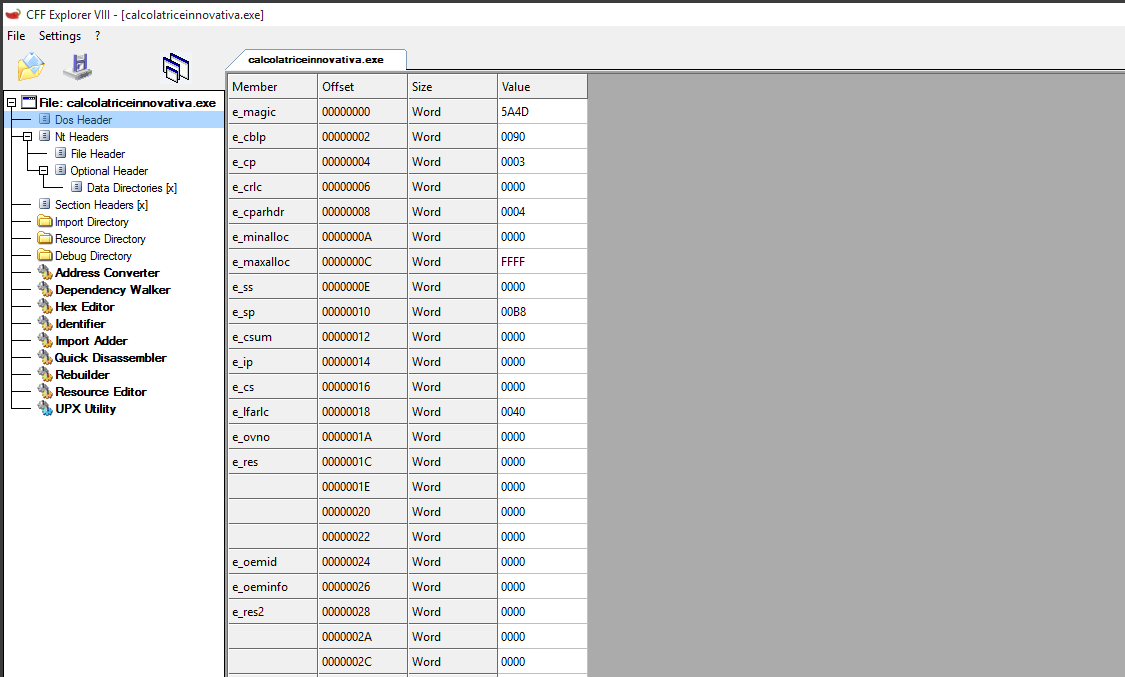
CFF Explorer VIII: Per l'analisi statica delle proprietà del file.

Cuckoo Sandbox: Per l'analisi dinamica in un ambiente virtualizzato.

L'analisi condotta su "calcolatriceinnovativa.exe" attraverso gli strumenti CFF Explorer e Cuckoo Sandbox ha rivelato un malware altamente sofisticato e pericoloso. L'obiettivo di questa relazione è fornire una panoramica completa dei risultati ottenuti, evidenziando le principali caratteristiche del malware e le sue potenziali minacce.

### **Analisi Statica (CFF Explorer)**

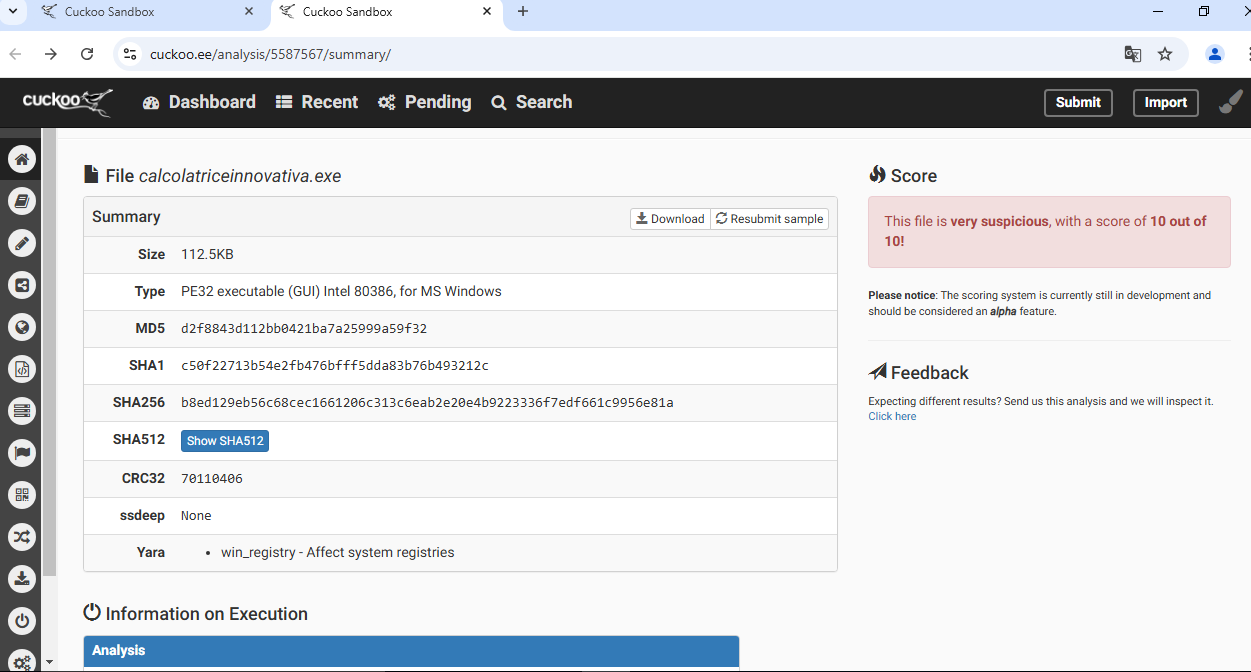
L'analisi statica ha permesso di esaminare la struttura interna del file eseguibile, rivelando:



* **Struttura tipica PE:** Il file presenta una struttura tipica dei file eseguibili Windows (PE), con sezioni distinte per il codice, i dati e le risorse.
* **Import di librerie:** Il malware importa diverse librerie di sistema, suggerendo un'ampia gamma di funzionalità, tra cui la manipolazione del sistema operativo, l'interazione con l'utente e la comunicazione di rete.
* **Stringhe sospette:** L'analisi delle stringhe ha rivelato la presenza di nomi di file, URL e frammenti di codice che indicano le potenziali azioni del malware.
* **Tecniche di offuscamento:** L'utilizzo di un packer suggerisce che gli autori del malware hanno cercato di nascondere il vero scopo del codice e di renderne più difficile l'analisi.

### **Analisi Dinamica (Cuckoo Sandbox)**

L'analisi dinamica ha permesso di osservare il comportamento del malware in un ambiente controllato:



* **Rilevamento multiplo:** Il malware è stato rilevato da numerosi motori antivirus e da regole Yara, confermandone la natura maliziosa.
* **Comportamenti sospetti:** Sono stati identificati comportamenti tipici dei malware, come l'allocazione di memoria eseguibile e la modifica del registro di sistema.
* **Influenza sul sistema:** Il malware è in grado di influenzare il comportamento del sistema operativo, potenzialmente causando danni o consentendo l'esecuzione di altri attacchi.

### **Riepilogo delle Minacce**

In base alle informazioni raccolte, possiamo ipotizzare che il malware "calcolatriceinnovativa.exe" sia in grado di:

* **Diffondersi:** Il malware potrebbe auto-replicarsi o diffondersi attraverso reti infette.
* **Rubare dati:** Potrebbe rubare informazioni sensibili dall'host infetto, come credenziali di accesso, informazioni personali o dati aziendali.
* **Creare backdoor:** Potrebbe creare una backdoor per consentire agli attaccanti di accedere al sistema in remoto e eseguire ulteriori attacchi.
* **Danneggiare il sistema:** Potrebbe danneggiare i file di sistema, corrompere i dati o rendere il sistema inutilizzabile.
* **Attaccare altri sistemi:** Potrebbe essere utilizzato come punto d'appoggio per attaccare altri sistemi all'interno della rete.

### **Conclusioni**

L'analisi approfondita del malware "calcolatriceinnovativa.exe" ha evidenziato un elevato livello di sofisticazione e pericolosità. Le informazioni raccolte sono fondamentali per comprendere le minacce associate a questo tipo di malware e per sviluppare le appropriate contromisure.

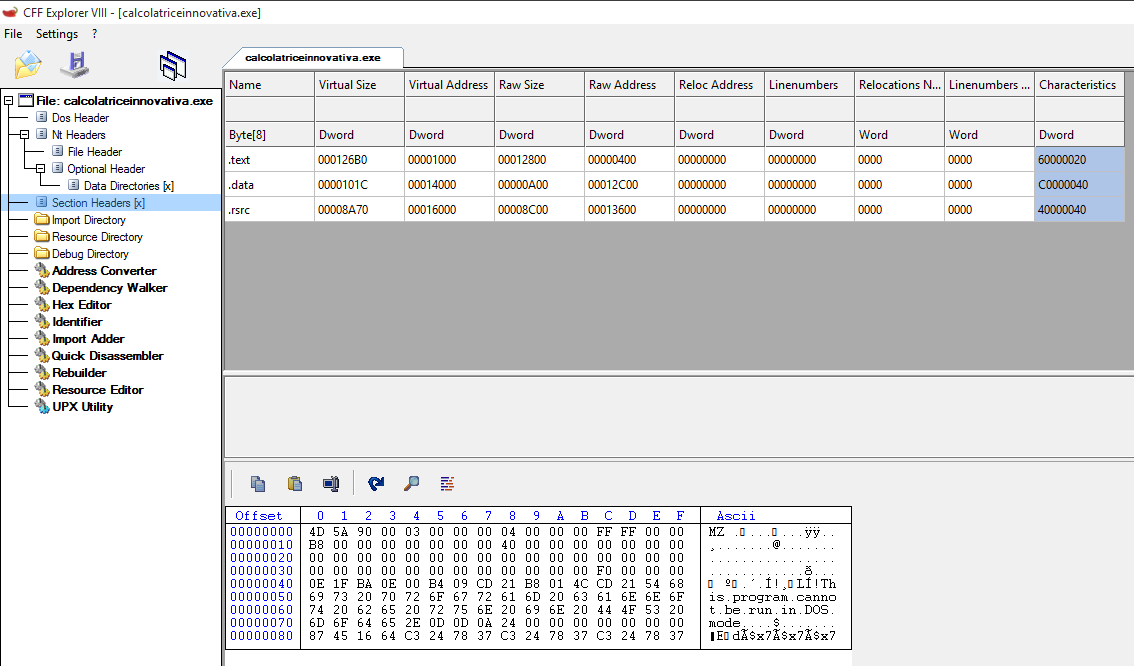
**Raccomandazioni:**

* **Aggiornare regolarmente i sistemi:** Mantenere aggiornati i sistemi operativi, le applicazioni e i software antivirus è fondamentale per proteggersi da nuove minacce.
* **Evitare di aprire file o link sospetti:** Fare attenzione quando si aprono file o si cliccano su link provenienti da fonti sconosciute.
* **Utilizzare software di sicurezza affidabile:** Installare e mantenere aggiornato un software antivirus di buona qualità può aiutare a prevenire le infezioni.
* **Effettuare regolarmente backup dei dati:** Effettuare backup regolari dei dati importanti può aiutare a recuperare le informazioni in caso di infezione.

**Ulteriori Analisi:**

Per un'analisi più approfondita, si consiglia di:

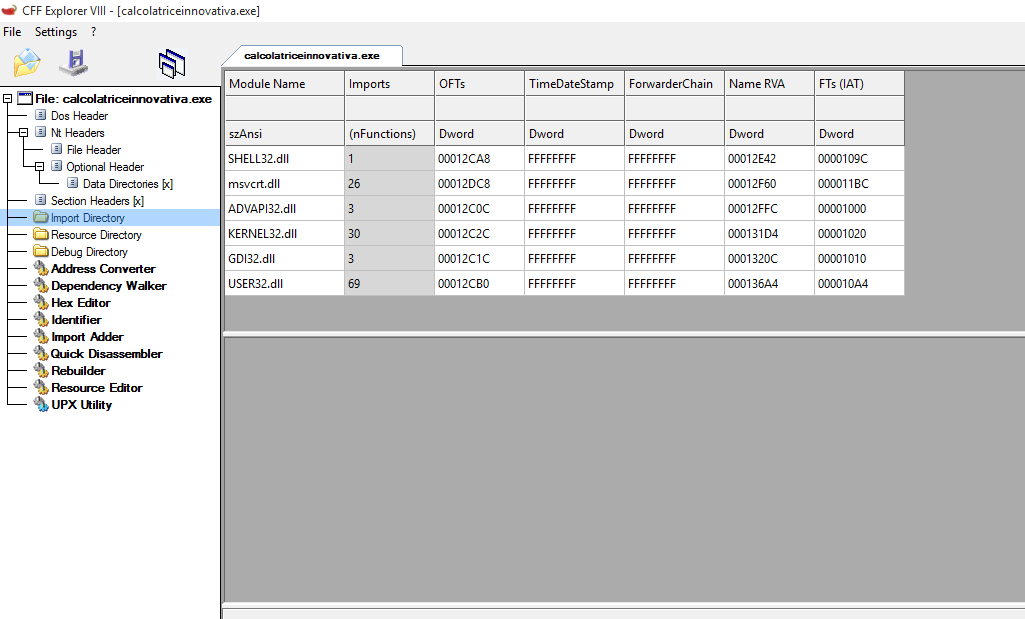
* **Decompilare il codice:** Eseguire un'analisi approfondita del codice decompilato per identificare le funzioni specifiche del malware.
* **Simulare attacchi mirati:** Simulare diversi scenari di attacco per valutare l'impatto del malware su un sistema e identificare le possibili conseguenze.
* **Confrontare con altri malware:** Confrontare il malware con altre famiglie di malware note per identificare eventuali somiglianze e differenze.

**Cosa ci mostra questo screenshot?**

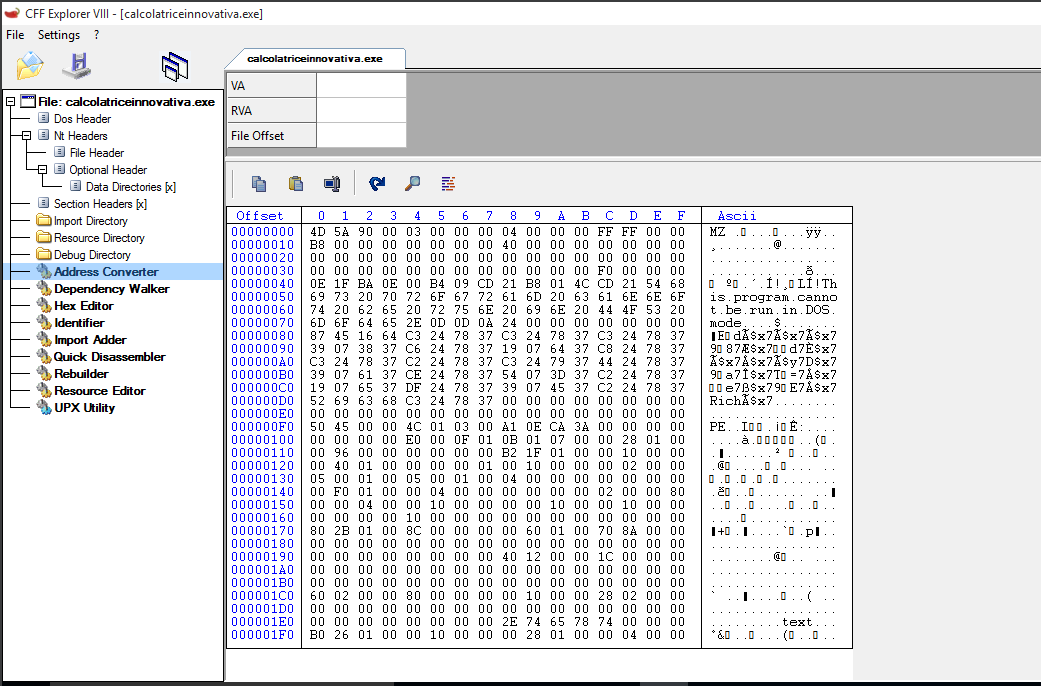
* **Sezioni del file:**
  + **.text:** Questa sezione contiene il codice eseguibile del programma. È la parte più importante per capire cosa fa il malware.
  + **.data:** Questa sezione contiene i dati inizializzati, come le variabili globali e le stringhe.
  + **.rsrc:** Questa sezione contiene le risorse del programma, come icone, messaggi di errore, e altri dati che possono essere utilizzati dall'applicazione.
* **Dimensioni delle sezioni:** Le dimensioni delle sezioni ci danno un'idea della complessità del malware. Una sezione .text grande indica che il malware potrebbe avere molte funzionalità.
* **Dump esadecimale:** La parte inferiore dello screenshot mostra il contenuto effettivo di alcune sezioni in formato esadecimale. Questo ci permette di cercare manualmente pattern o stringhe significative.

**Cosa possiamo dedurre da queste informazioni?**

* **Complessità:** Il malware sembra avere una struttura abbastanza complessa, con diverse sezioni e un codice eseguibile di dimensioni significative.
* **Funzionalità:** La presenza di una sezione .rsrc suggerisce che il malware potrebbe avere un'interfaccia utente o visualizzare dei messaggi.
* **Potenziali indizi:** Il dump esadecimale potrebbe contenere stringhe che ci aiutano a capire lo scopo del malware.

**Cosa possiamo dedurre da queste informazioni?**

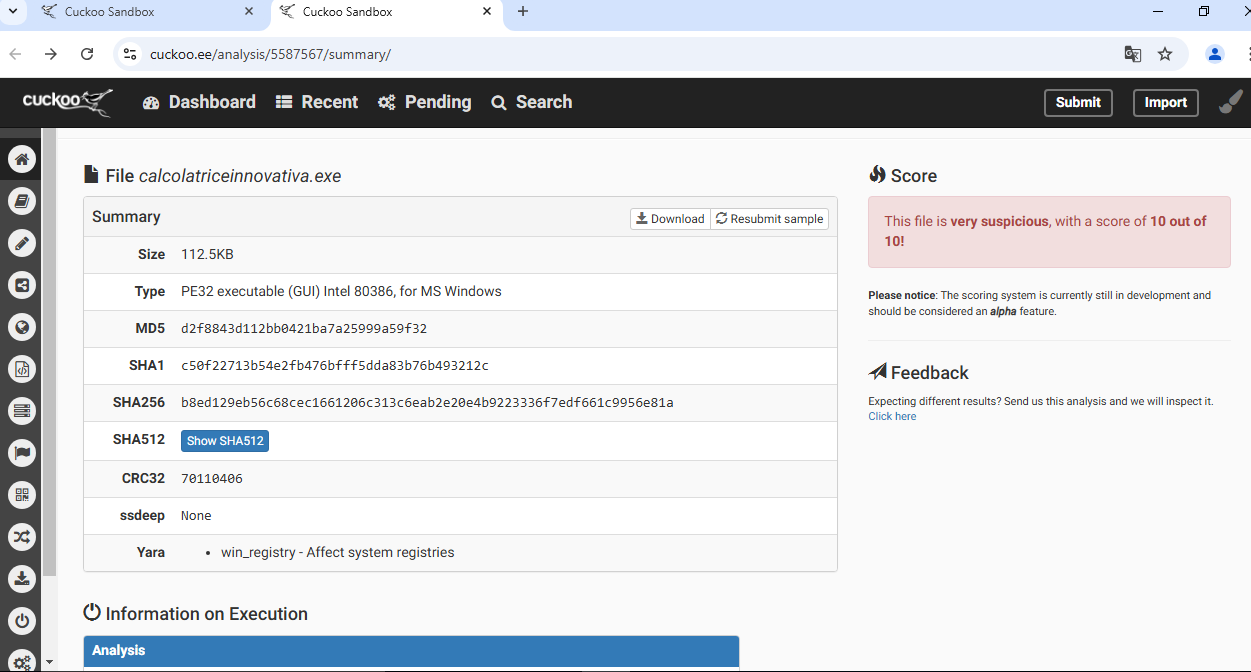
* **Funzionalità del malware:** Analizzando le funzioni importate da queste librerie, possiamo ottenere un'idea più precisa delle azioni che il malware potrebbe eseguire. Ad esempio, se il malware importa funzioni dalla libreria USER32.dll, potrebbe essere in grado di creare finestre, visualizzare messaggi o catturare input da tastiera.
* **Possibili comportamenti:** Le librerie importate possono suggerire il tipo di attività che il malware potrebbe svolgere. Ad esempio, l'importazione di funzioni dalla libreria KERNEL32.dll indica che il malware potrebbe interagire con il sistema operativo a basso livello.
* **Punti di attacco:** Le librerie importate possono rappresentare dei potenziali punti di attacco per il malware. Ad esempio, se il malware sfrutta una vulnerabilità in una di queste librerie, potrebbe essere in grado di eseguire codice arbitrario sul sistema.

**Cosa ci mostra questo screenshot?**

* **Dump esadecimale:** La parte principale dello screenshot mostra il contenuto di alcune sezioni del file in formato esadecimale, affiancato dalla corrispondente rappresentazione ASCII (caratteri leggibili).
* **Stringhe:** Sono evidenti diverse stringhe di testo all'interno del dump esadecimale. Queste stringhe possono fornire indizi importanti sul funzionamento del malware.

**Cosa possiamo dedurre da queste informazioni?**

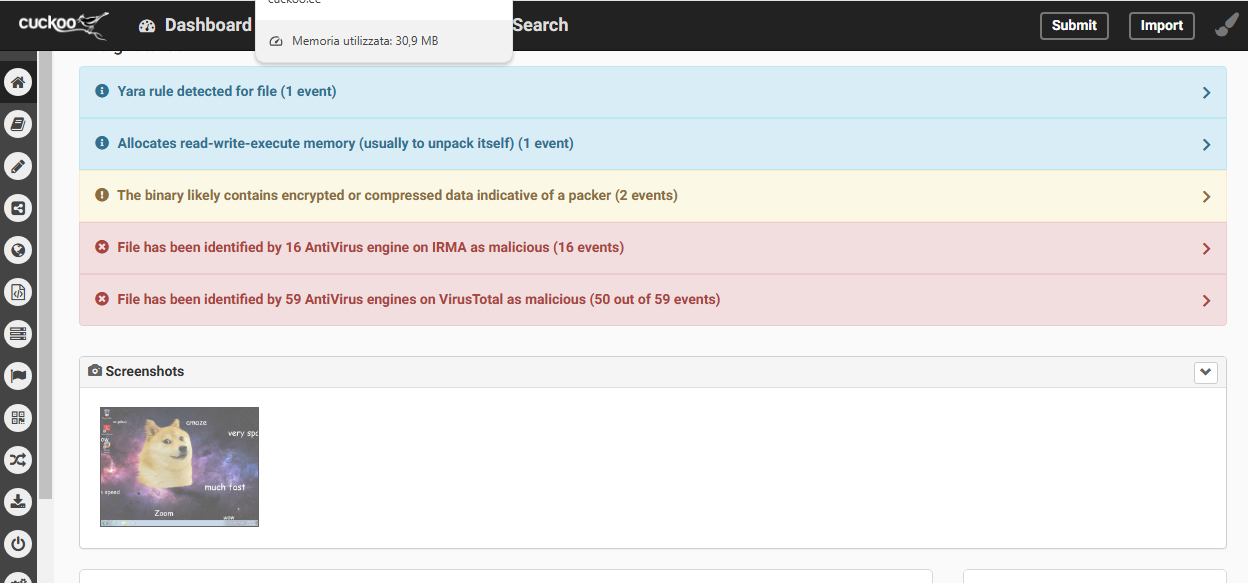
* **Stringhe significative:** Le stringhe identificate potrebbero essere nomi di file, URL, messaggi di errore, o frammenti di codice che rivelano le funzionalità del malware.
* **Tecniche di offuscamento:** La presenza di stringhe criptate o codificate suggerisce che il malware potrebbe utilizzare tecniche di offuscamento per nascondere il suo vero scopo.
* **Potenziali comportamenti:** Analizzando le stringhe, possiamo formulare ipotesi sul comportamento del malware, ad esempio se è in grado di connettersi a un server remoto, se modifica il registro di sistema, o se esegue altre azioni dannose.

**Cosa ci dice questo screenshot?**

* **Valutazione:** Il file è stato classificato come "molto sospetto" con un punteggio di 10 su 10. Questo indica che il malware presenta un alto livello di pericolosità.
* **Informazioni di base:** Il report fornisce informazioni di base sul file, come la dimensione, il tipo (eseguibile PE32), e gli hash (MD5, SHA1, SHA256, SHA512, CRC32).
* **Yara:** Il malware è stato rilevato da una regola Yara che indica che potrebbe influenzare il registro di sistema.

### **Cosa possiamo dedurre da queste informazioni?**

* **Alta pericolosità:** Il punteggio elevato e la regola Yara indicano che il malware è molto probabilmente dannoso.
* **Potenziali azioni:** Il fatto che il malware possa influenzare il registro di sistema suggerisce che potrebbe modificare le impostazioni del sistema, installare altri malware o persistere nel sistema anche dopo un riavvio.
* **Necessità di ulteriori analisi:** La mancanza di informazioni dettagliate sull'esecuzione del malware indica che sono necessarie ulteriori analisi per comprendere appieno il suo comportamento.



### **Cosa ci mostra questo screenshot?**

* **Rilevamenti multipli:** Il malware è stato rilevato da diverse regole Yara e da numerosi motori antivirus sia su VirusTotal che su IRMA. Questo conferma la sua natura maliziosa.
* **Comportamenti sospetti:** Il malware presenta comportamenti tipici dei malware, come l'allocazione di memoria eseguibile (spesso utilizzata per decomprimere o decriptare il payload) e l'utilizzo di tecniche di offuscamento (come l'utilizzo di un packer).
* **Confronto con altri malware:** Il fatto che sia stato rilevato da numerosi motori antivirus suggerisce che potrebbe essere una variante di un malware già noto o appartenere a una famiglia di malware particolarmente diffusa.

### **Cosa possiamo dedurre da queste informazioni?**

* **Alta pericolosità:** La combinazione di rilevamenti multipli e comportamenti sospetti conferma l'alta pericolosità del malware.
* **Tecniche di offuscamento:** L'utilizzo di un packer indica che gli autori del malware hanno cercato di nascondere il vero scopo del codice e di rendere più difficile l'analisi.
* **Necessità di un'analisi approfondita:** Sono necessarie ulteriori analisi per comprendere appieno le funzionalità del malware e identificare le sue potenziali minacce.