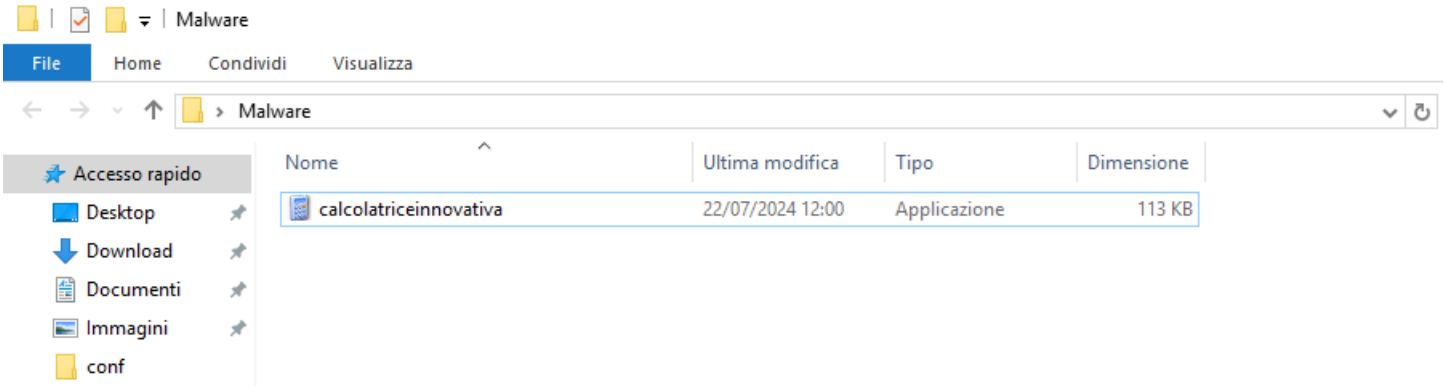
S9L2 Analisi Malware

Introduzione:

Il compito di oggi era svolgere un'analisi sia **statica** ma anche **dinamica**, del **malware** presente all'interno della macchina exploitabile Windows 10. Ovvero **calcolatriceinnovativa**:



1) Che cos'è l'analisi statica?

L'analisi statica è una tecnica di analisi del malware che consiste nell'esaminare il codice di un programma senza eseguirlo.

Punti a favore sono:

Sicurezza, Completezza, Velocità, Individuazione di vulnerabilità;

Punti a sfavore invece sono:

Limitazioni nell'interpretazione, Offuscamento del codice, Tempo e risorse, Conoscenza tecnica, Falsi positivi;

2) Che cos'è l'analisi dinamica?

A differenza dell'analisi statica che esamina il codice senza eseguirlo, l'analisi dinamica coinvolge l'esecuzione controllata del malware in un ambiente **isolato e sicuro**.

Punti a favore:

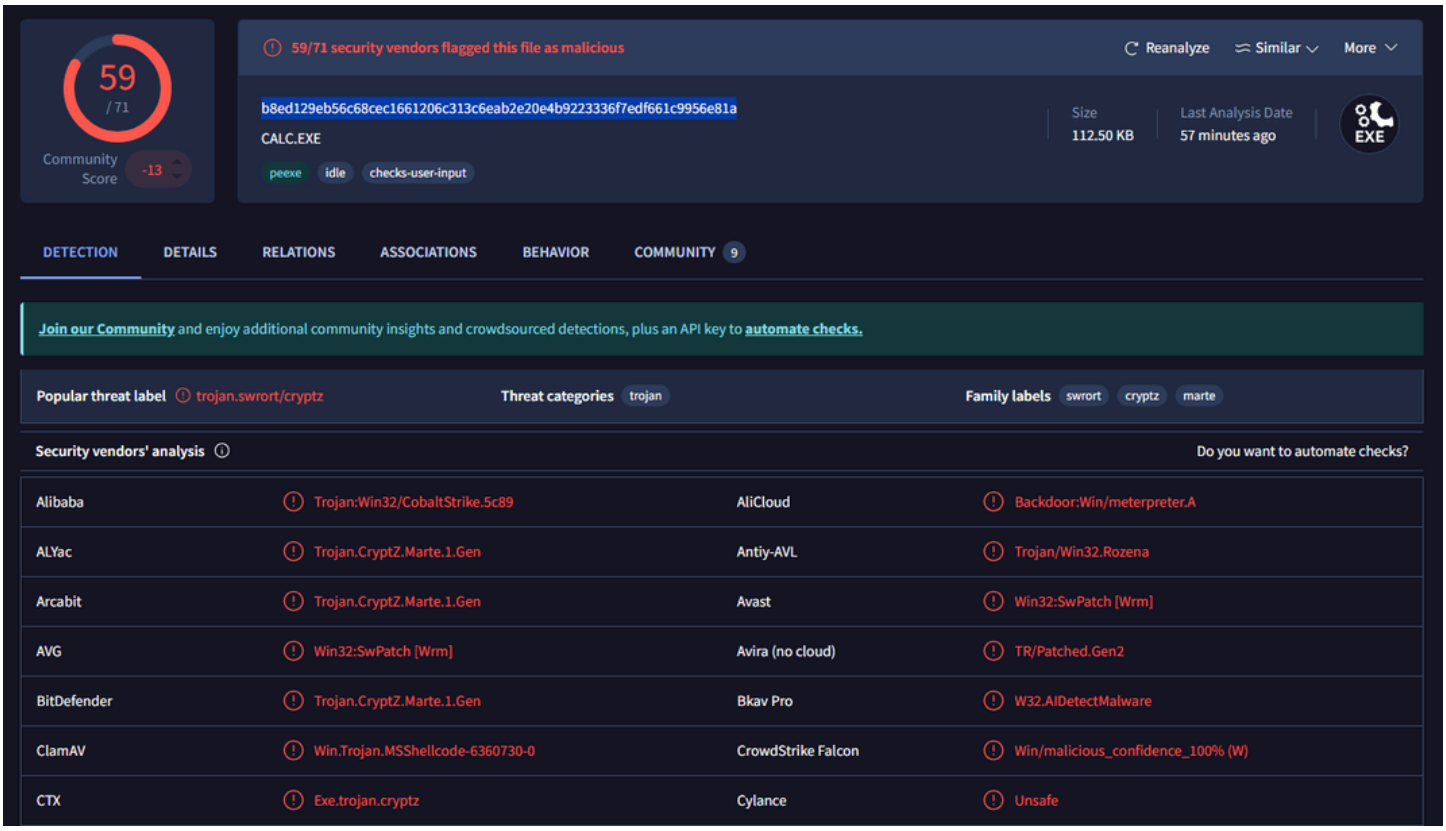
Osservazione diretta del comportamento, rilevamento di tecniche evasive, raccolta di indicatori di compromissione;

Punti a sfavore:

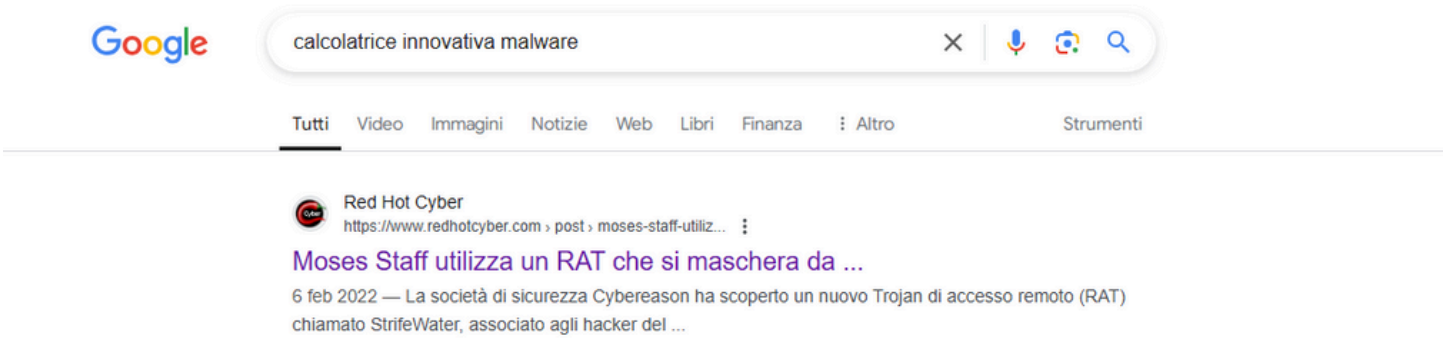
Necessità di un ambiente controllato, possibile mancato rilevamento.

Pratica:

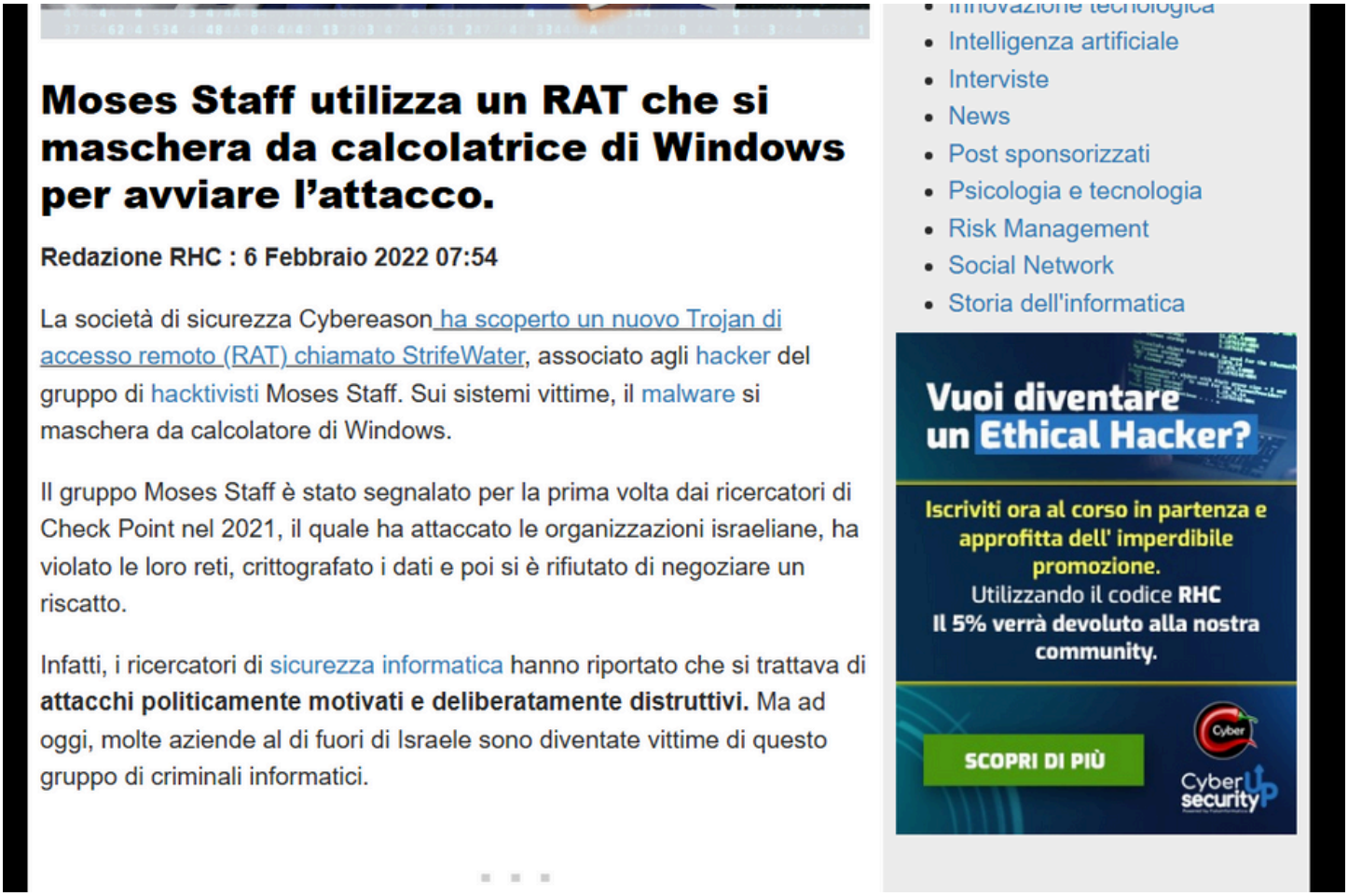
Prima di tutto ho fatto analizzare al software **VirusTotal** (analizza file, URL, domini e indirizzi IP sospetti per rilevare malware e altri tipi di minacce) l'applicazione per determinare se fosse o meno un **malware**, e la risposta è **chiaramente positiva**:



Successivamente tramite un **motore di ricerca** ho cercato il **malware** per vedere se ci fossero notizie a riguardo e se potessi trovare informazioni importanti riguardo quest'ultimo:



Cliccando sul primo risultato si apre una pagina che parla di questo malware in particolare:



Moses Staff utilizza un RAT che si maschera da calcolatrice di Windows per avviare l'attacco.

Redazione RHC : 6 Febbraio 2022 07:54

La società di sicurezza Cybereason ha scoperto un nuovo Trojan di accesso remoto (RAT) chiamato StrifeWater, associato agli hacker del gruppo di hacktivisti Moses Staff. Sui sistemi vittime, il malware si maschera da calcolatore di Windows.

Il gruppo Moses Staff è stato segnalato per la prima volta dai ricercatori di Check Point nel 2021, il quale ha attaccato le organizzazioni israeliane, ha violato le loro reti, crittografato i dati e poi si è rifiutato di negoziare un riscatto.

Infatti, i ricercatori di sicurezza informatica hanno riportato che si trattava di **attacchi politicamente motivati e deliberatamente distruttivi.** Ma ad oggi, molte aziende al di fuori di Israele sono diventate vittime di questo gruppo di criminali informatici.

Che successivamente mi rimanda a questo link:

Dove troviamo informazioni importantissime riguardo il malware:

Nuovo Remote Access Trojan (RAT): Un RAT recentemente non documentato chiamato StrifeWater è stato valutato come parte dell'arsenale utilizzato dal gruppo APT iraniano Moses Staff. Si ritiene che il RAT venga impiegato specificamente nella fase iniziale dell'infezione e successivamente sostituito con altri strumenti.

Varie funzionalità: Il RAT StrifeWater offre diverse capacità, tra cui: elencare i file di sistema, eseguire comandi di sistema, acquisire schermate, creare persistenza e scaricare aggiornamenti e moduli ausiliari.

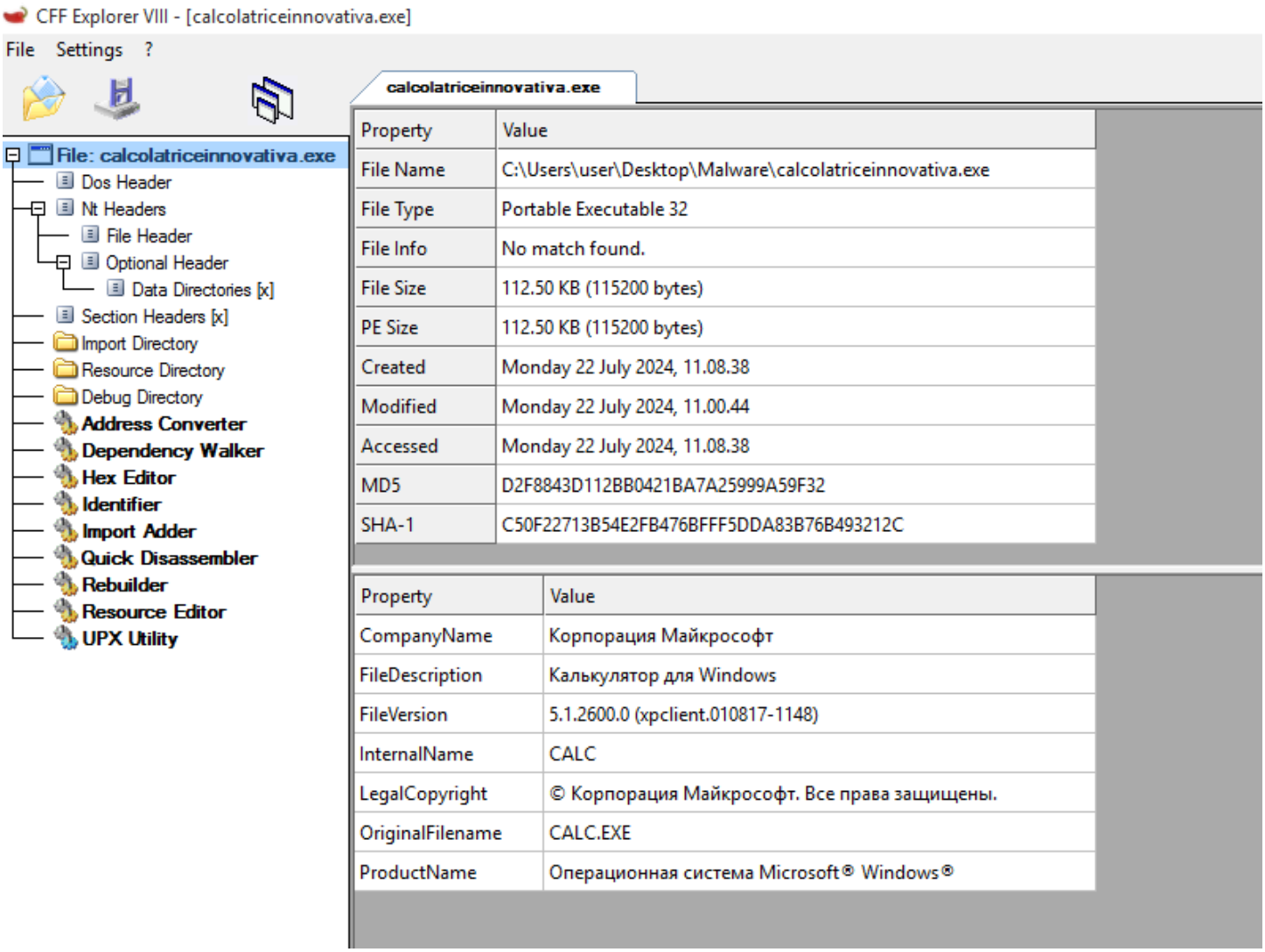
Sotto il radar: Il RAT StrifeWater sembra essere rimosso dall'ambiente infetto prima del dispiegamento del ransomware. Questa potrebbe essere la ragione per cui il RAT non è stato rilevato in precedenza.

Ransomware sponsorizzato dallo stato: Moses Staff impiega il ransomware post-esfiltrazione non per ottenere guadagni finanziari, ma per interrompere le operazioni, oscurare l'attività di spionaggio e infliggere danni ai sistemi per avanzare gli obiettivi geopolitici dell'Iran.

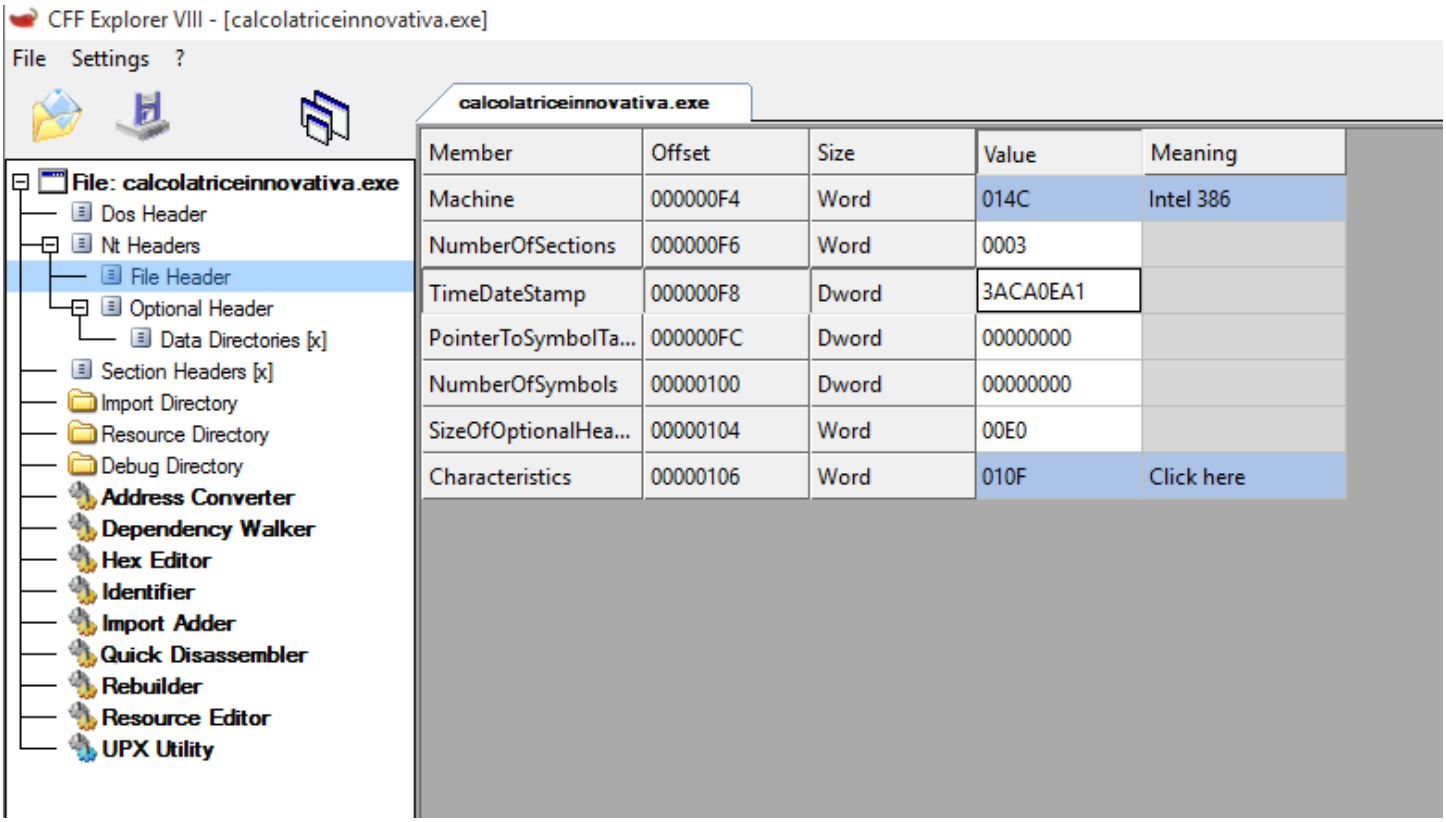
Vittime in tutto il mondo: La lista delle vittime di Moses Staff include numerosi paesi e regioni, tra cui: Israele, Italia, India, Germania, Cile, Turchia, Emirati Arabi Uniti e Stati Uniti.

CFF Explorer:

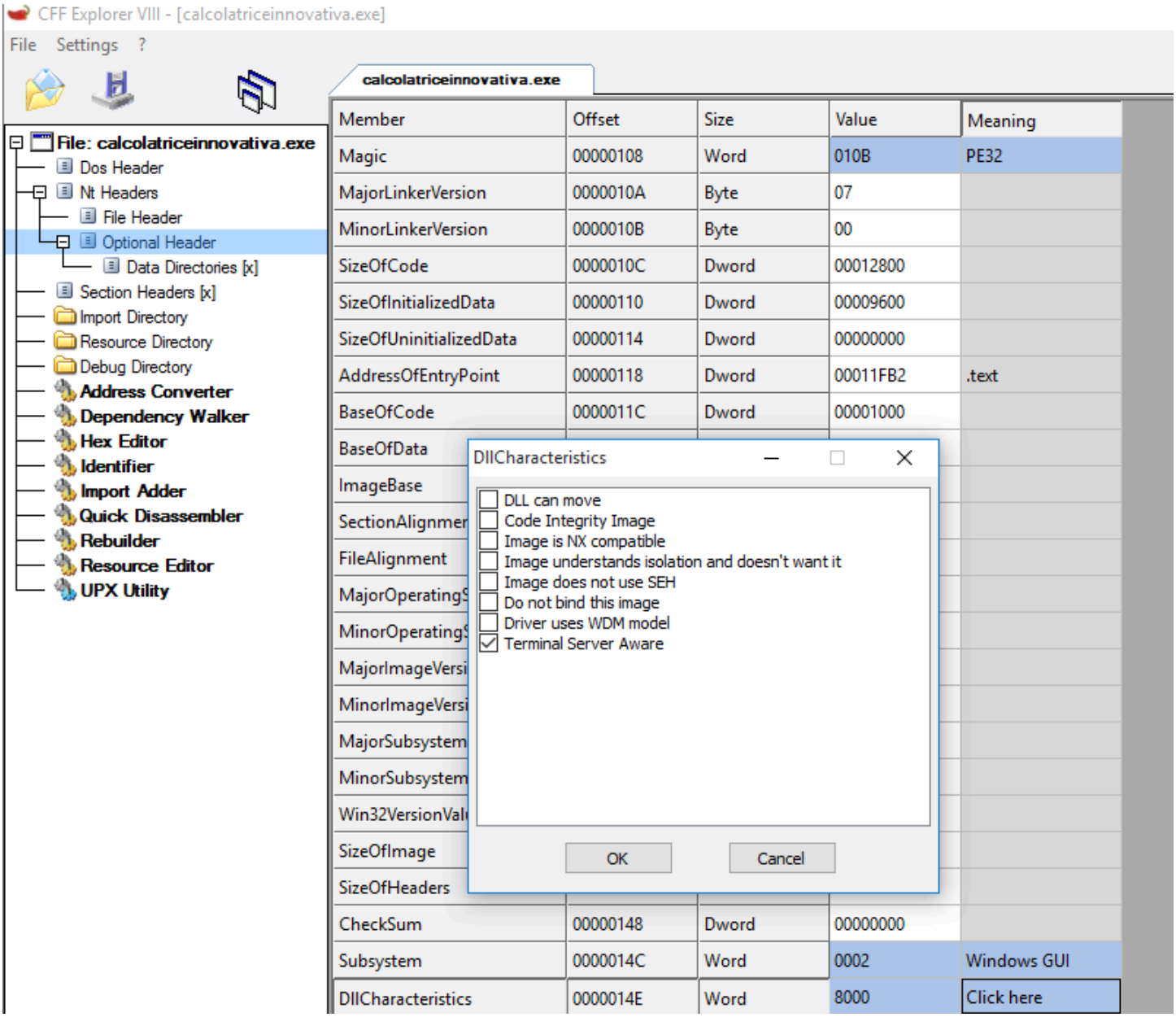
Successivamente con **CFF Explorer** uno strumento avanzato che permette di analizzare i file **PE** (Portable Executable, .exe, .dll), ho ispezionato il file:



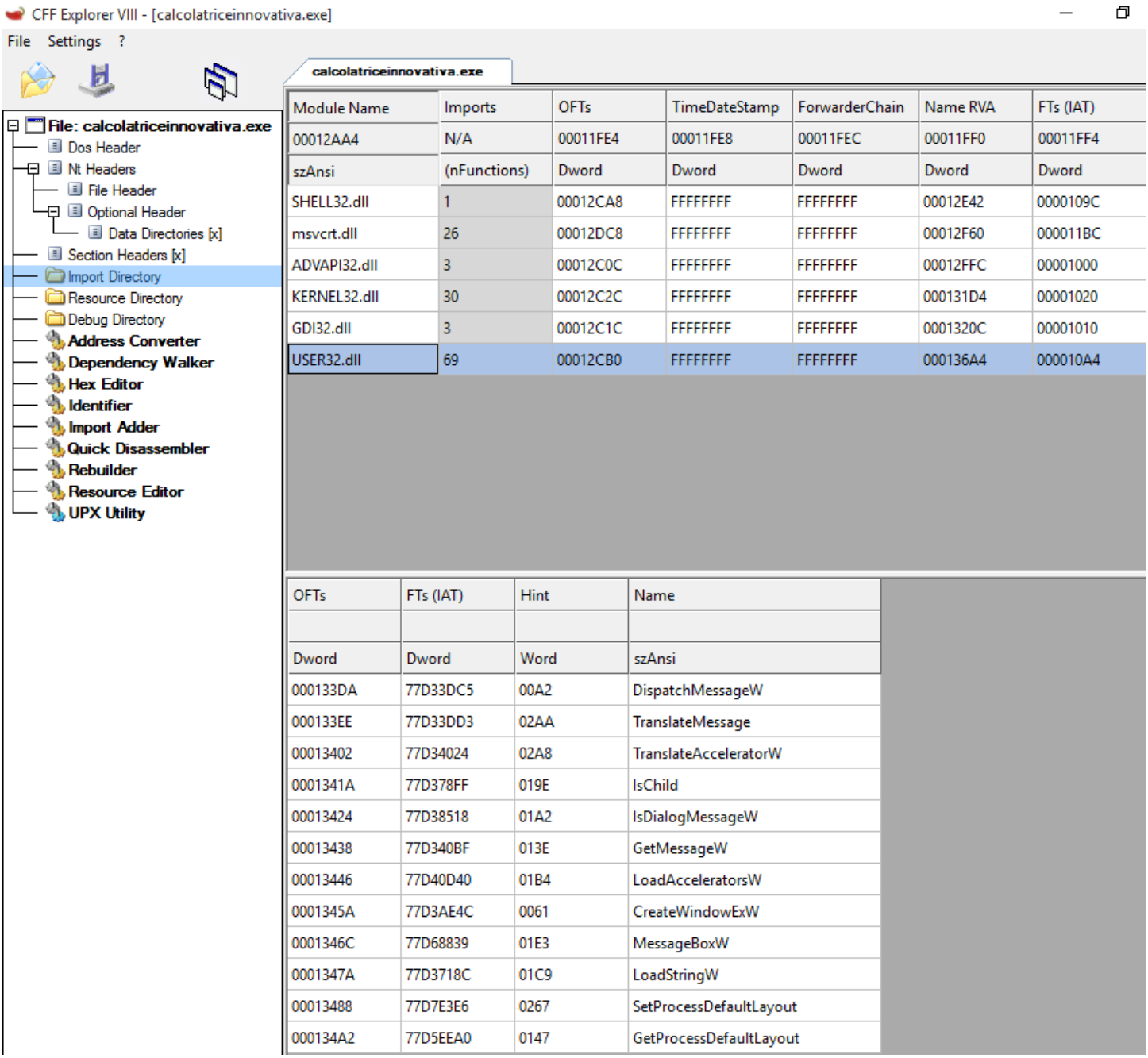
Controllando il **TimeDateStamp** non risulta nulla di strano, dato che la data risulta essere **19 aprile 2001, 11:47:13 (UTC)**:



La presenza di questo flag in un file non progettato per ambienti Terminal Server potrebbe destare sospetti. Potrebbe essere un tentativo di **eludere controlli** in sessioni remote.



In **USER32.dll** fornisce funzioni per l'interazione con l'interfaccia utente (messaggi, finestre, dialoghi). In un contesto sospetto potrebbe essere utilizzata per keylogging o per imitare finestre legittime.



Dall'elenco delle funzioni associate a questa libreria possiamo fare alcune considerazioni:

MessageBoxW: Potrebbe essere usata dal malware per visualizzare messaggi all'utente (es. richieste di riscatto nei ransomware).

CreateWindowExW: Utilizzata per creare finestre. Potenzialmente usata per imitare interfacce utente legittime.

DispatchMessageW, **TranslateMessage**: Usate per gestire eventi nell'interfaccia utente. Anche queste sono normali, ma se combinate con altre azioni sospette (es. keylogging), potrebbero essere rilevanti.

SetProcessDefaultLayout: È piuttosto insolita e potrebbe indicare manipolazioni più specifiche, anche se da sola non è immediatamente sospetta.

GetMessageW: Permette di ricevere messaggi dalla coda. In combinazione con funzioni che monitorano eventi, potrebbe essere usata per intercettare input dell'utente.