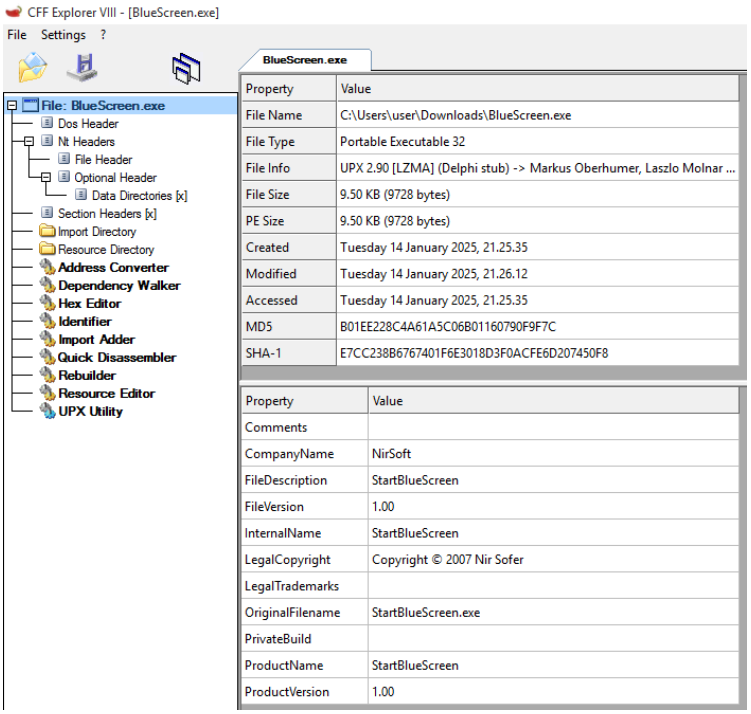
Esercitazione S9-L2 - Analisi file BlueScreen.exe (Trojan).

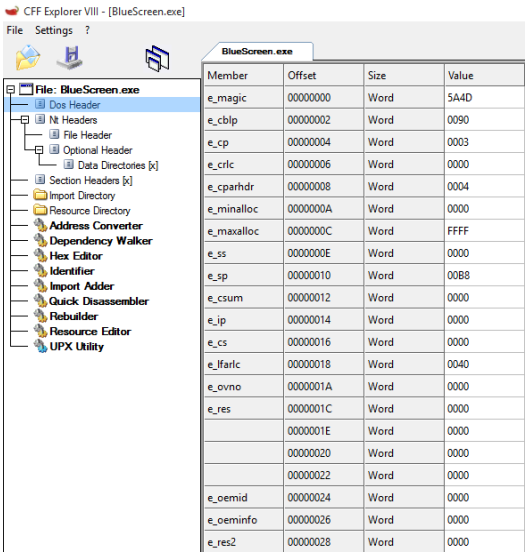
- **Analisi statica**

Il primo passo è stato quello di effettuare un'analisi statica del file sospetto. Per fare ciò, il file è stato scaricato sulla macchina Windows 10 ed analizzato tramite **CFF Explorer**.



La prima pagina ci fornisce già delle informazioni interessanti:

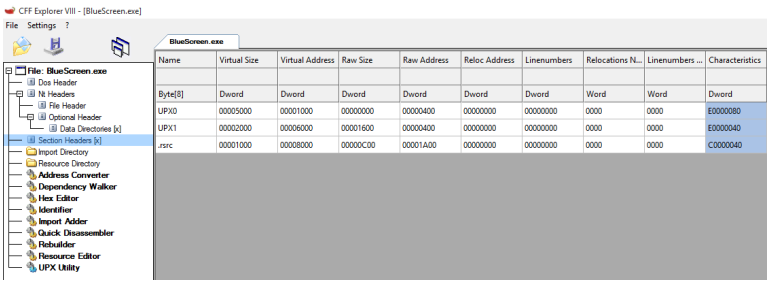
1. **File Type**: Portable Executable 32 ci dice che si tratta di un file eseguibile.
2. **File Info**: UPX 2.90.
   La dicitura **UPX 2.90** in un file esaminato con **CFF Explorer**, si riferisce al fatto che l'eseguibile è stato compresso o offuscato utilizzando il packer UPX. Si tratta di un packer open source ampiamente utilizzato per ridurre la dimensione dei file eseguibili. È legittimo e usato da sviluppatori per minimizzare la dimensione delle applicazioni distribuite.Tuttavia, **gli autori di malware spesso utilizzano UPX** per rendere più difficile l'analisi manuale o automatica, nascondendo il codice all'interno del file compresso.
3. Possiamo individuare 2 hash: **MD5** e **SHA-1**



Passiamo poi ad analizzare la sezione **Dos Header**:

1. **e_magic: 5A4D**
   Si tratta del codice MZ in ASCII che è una firma che indica che si tratta di un eseguibile DOS.
2. **e_cblp: 0090**
   Byte utilizzati nella pagina finale del file.
3. **e_cp: 0003**
   Numero di pagine nel file (512 byte per pagina).
4. **e_crlc: 0000**
   Voci nel file di rilocazione.
5. **e_cparhdr: 0004**
   Numero di paragrafi dell'header (16 byte per paragrafo).
6. **e_minalloc: 0000**
   Quantità minima di memoria aggiuntiva richiesta del programma.
7. **e_maxalloc: FFFF**
   Quantità massima di memoria aggiuntiva richiesta del programma. Si può notare che la forbice tra minima e massima è molto ampia.
8. **e_ss: 0000**
   Segmento del rgistro stack.
9. **e-sp: 00B8**
   Puntatore stack iniziale.

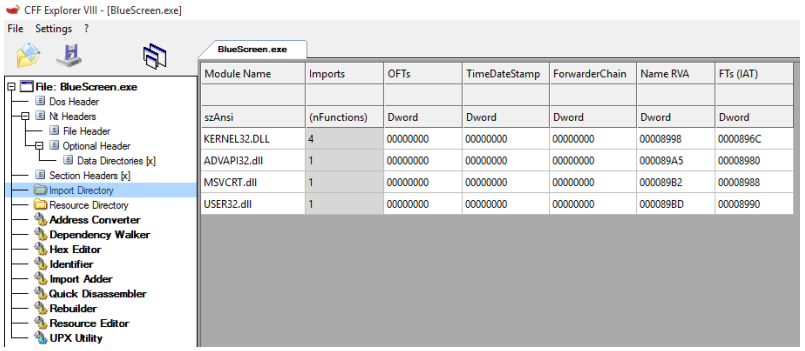
Tutti i restanti valori sono impostati su **0000**, impostazione standard.



Nella sezione **Section Header** di **CFF Explorer** troviamo sezioni denominate **UPX0**, **UPX1**. Significa che il file eseguibile è stato compresso o offuscato utilizzando il packer UPX:

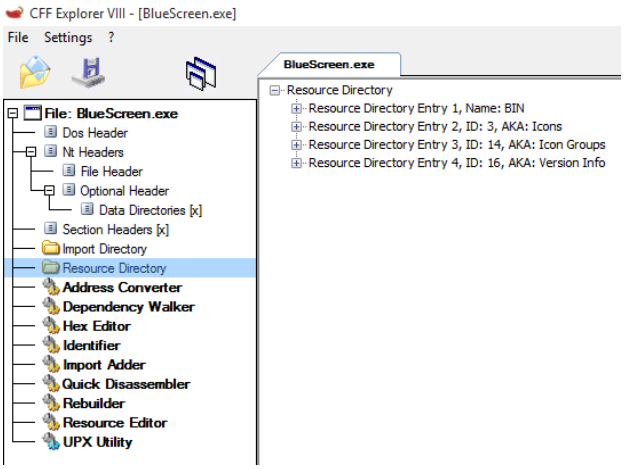
1. **UPX0**
   Questa sezione contiene il codice eseguibile compresso. Durante l'esecuzione, questa parte viene decompressa in memoria per eseguire il programma originale.
2. **UPX1**
   Questa sezione tipicamente contiene dati che vengono decompressi e utilizzati dal programma. Può includere codice aggiuntivo o risorse.

La presenza di queste due sezioni ci fornisce un'informazione molto importante in quanto, anche se legittimi, sono elementi tipici dei malware.



Nella sezione **import Directory** troviamo:

1. **KERNEL32.DLL**: 4 funzioni
   Si tratta di funzioni base del sistema Windows tra cui la gestione dei file e dei processi.
2. **ADVAPI32.dll**: 1 funzione
   Funzioni avanzate per la gestione delle applicazioni, come la gestione di servizi Windows e di siucrezza.
3. **MSVCRT.dll**: 1 funzione
   Libreria di sistema con funzionalità chiave come gestione della memoria e dei dispositivi I/O.
4. **USER32.dll**: 1 funzione
   Per la gestione dell'interfaccia utente.



Nella sezione **Resource directory** individuiamo delle icone tipicamente utilizzate da programmi che intendono interfacciarsi con l'utente.
Inoltre individuiamo del file **BIN**.
.bin è un'estensione che indica contenuto binario grezzo. Questo significa che i dati non sono immediatamente leggibili o decodificabili senza strumenti specifici.
Gli sviluppatori o autori di malware possono utilizzare file binari per:

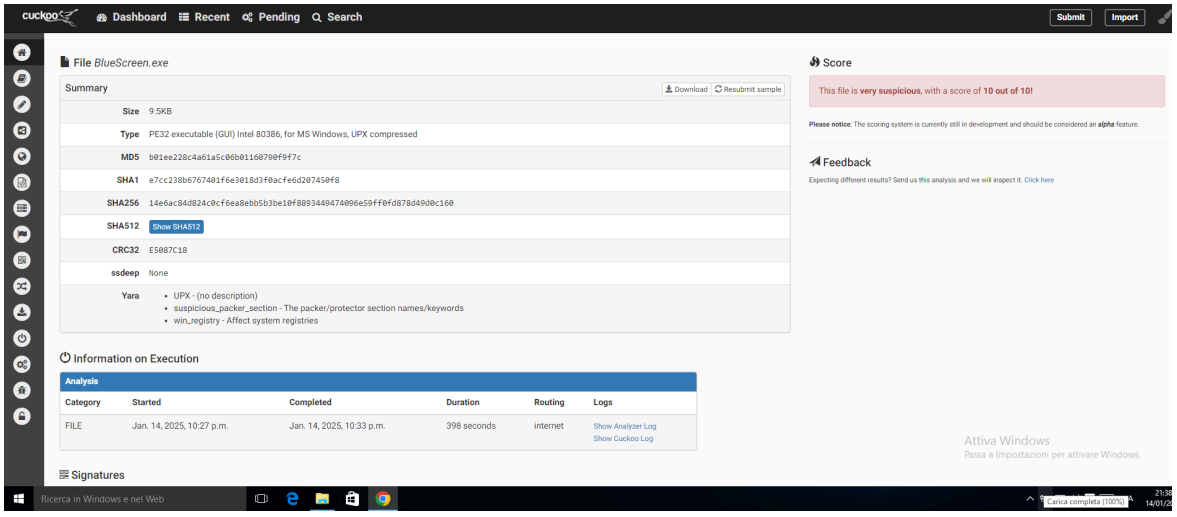
1. Incorporare payload aggiuntivi (come file eseguibili o librerie DLL) che verranno estratti e utilizzati in runtime.
2. Nascondere dati sensibili o codificati per evitare la semplice analisi.

Conclusioni analisi statica

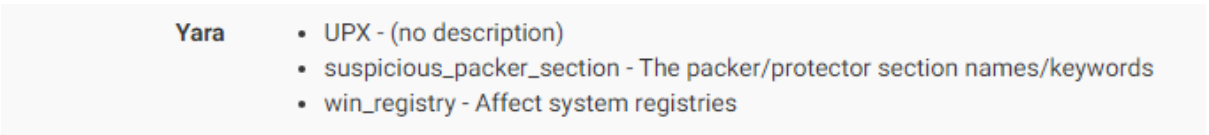
Da quanto visto attraverso la nostra analisi, possiamo giungere alla conclusione che ci troviamo davanti ad un file potenzialmente dannoso.
Probabilmente si tratta di un programma malevolo "travestito" da programma innocuo in grado di interfacciarsi con l'utente, Questo è chiaro dalla presenza di icone e dal fatto che esso sia un eseguibile.
La sua natura malevola viene tradita invece dai vari meccanismi di offuscamento presenti e dal largo utilizzo di funzioni di sistema.

- **Analisi dinamica**

L'analisi dinamica del file è stata esclusivamente condotta con l'utilizzo del servizio **Cuckoo**, il quale permette di eseguire il file in un ambiente controllato, tenendo d'occhio le azioni eseguite dal file con l'utilizzo di **Yara rules**.



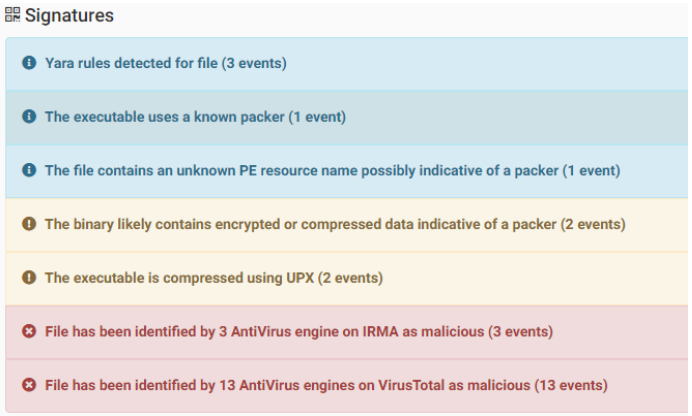
Dall'analisi emerge che il file viene ritenuto malevolo con un punteggio di **10/10**.
La pagina principale ci fornisce alcune informazioni sul file come il fatto che si tratti di un **Portable Executable 32**, oltre ai vari hash nei diversi formati (da MD5 a SHA512).
Sicuramente la sezione più importante è quella relativa alle YARA rules:



1. **UPX**
   UPX (Ultimate Packer for Executables) è uno dei packer più comuni utilizzati per comprimere o offuscare eseguibili.
   La presenza di questa regola significa che l'eseguibile analizzato è stato probabilmente compresso con UPX. I packer vengono spesso utilizzati da sviluppatori legittimi, ma anche da autori di malware per nascondere codice malevolo o renderne più difficile l'analisi.

2. **suspicious_packer_section**
   Questa regola viene attivata quando i nomi delle sezioni di un eseguibile contengono termini associati a packer o protector sospetti.
   Sezioni con nomi come **.text** o **.data** sono normali, mentre nomi come **.UPX0** o **.aspack**, o nomi insoliti (ad esempio xyz123) potrebbero indicare l'uso di strumenti di offuscamento o compressione usati per nascondere comportamenti malevoli.

3. **win_registry**
   Questa regola viene attivata quando il malware tenta di interagire con il **Registro di sistema** di Windows, una pratica comune per modificare le configurazioni di sistema o ottenere persistenza.



Inoltre **Cuckoo** ci indica che il file è stato riconosciuto come malevolo da un grande numero di Antivirus grazie all'utilizzo di servizi come **VirusTotal**.