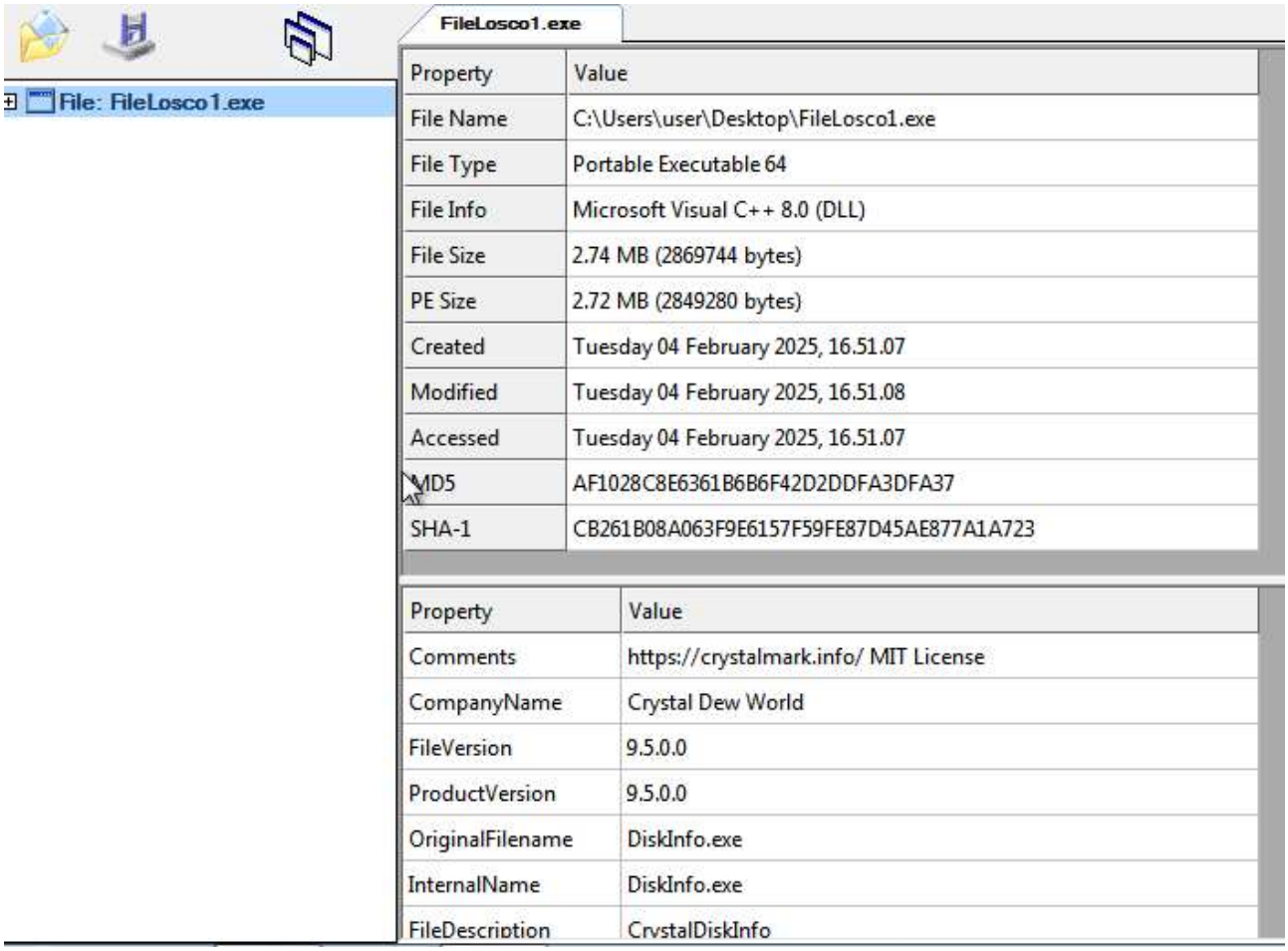
Per analizzare il malware ho usato CFF:



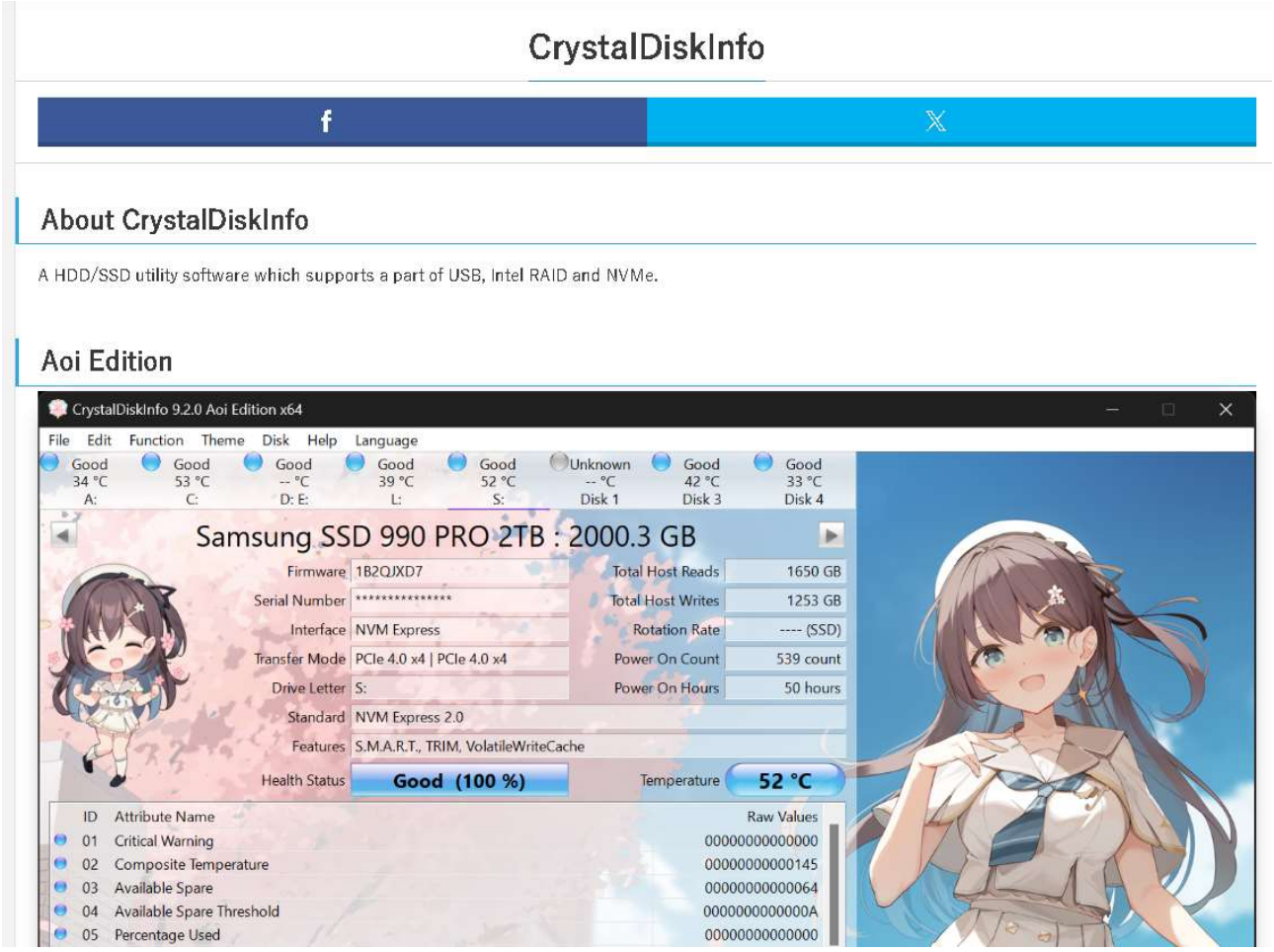
File Type: "Portable Executable 64" indica che si tratta di un file eseguibile per sistemi operativi Windows a 64 bit

File Info: La presenza di "Microsoft Visual C++ 8.0 (DLL)" suggerisce che il file è stato compilato con Visual Studio (versione 2005). Questo può fornire indizi sulla sua età o sul toolkit usato per svilupparlo.

File Size e PE Size: Le dimensioni del file e della struttura Portable Executable (PE) sono vicine, il che è normale per un programma legittimo, ma nei malware questa proporzione può essere alterata.

Ha due hash, MD5 e SHA-1

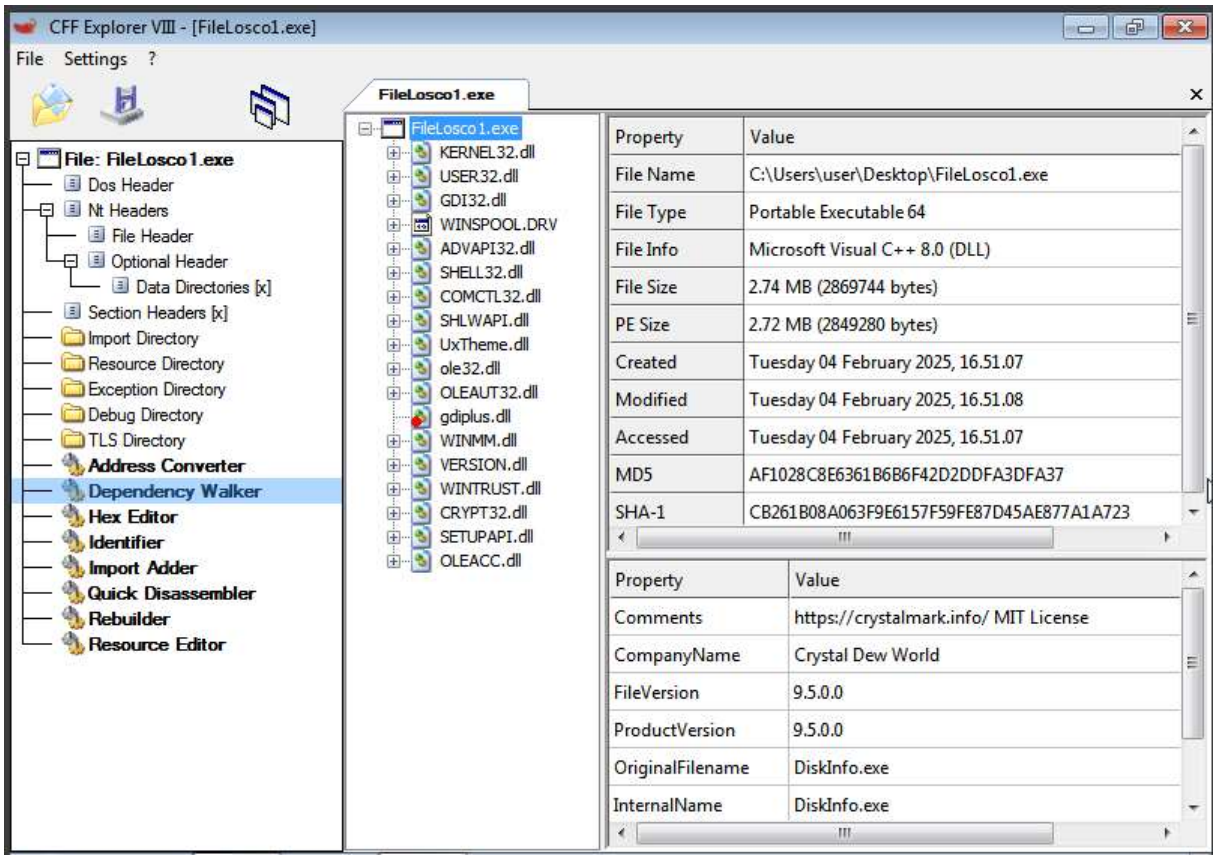
Nella sezione “Original” file name c’è critto “DiskInfo.exe” e su “Company name” c’è scirtto “Crystal Dew Wolrd” e cercando online ho trovato una pagina che nomina questo software con annesse foto



E sembra essere un software per avere un pannello personalizzato per poter visualizzare le prestazioni del dispositivo.

Magari un malintenzionato ha installato un malware dentro questo software così da poter infettare ignaramente chiunque lo installi.

Sono andato a visualizzare le dipendenze:



KERNEL32.dll

Fornisce funzionalità di base di sistema operativo, come la gestione della memoria, dei file e dei processi.

Al suo interno sono presenti:

ntdll.dll è una libreria che offre funzionalità a basso livello per il kernel di Windows. I malware spesso usano questa libreria per eseguire API non documentate, bypassare le protezioni di sicurezza o eseguire codice a basso livello.

KERNEL32.dll é una libreria di base che gestisce operazioni fondamentali come processi, file, memoria e comunicazioni. La maggior parte dei malware utilizza questa DLL.

ADVAPI32.dll libreria che contiene API per la gestione della sicurezza e dell'accesso al registro di sistema. I malware la usano per manipolare permessi o creare persistenza.

USER32.dll libreria che gestisce l'interazione dell'interfaccia utente, come finestre, pulsanti e input da tastiera/mouse.

ADVAPI32.dll

Contiene funzioni di gestione della sicurezza e del registro di sistema di Windows. La sua presenza è comune, ma è anche usata dai malware per manipolare i permessi o registrare chiavi.

CRYPT32.dll

Implementa funzioni di crittografia e gestione di certificati. Se usata in modo insolito, potrebbe indicare attività di cifratura o comunicazioni protette malevole.

OLEAUT32.dll e OLEACC.dll

Usate per la gestione di automazione e oggetti OLE. Potrebbero essere coinvolte se il malware tenta di comunicare con altre applicazioni.