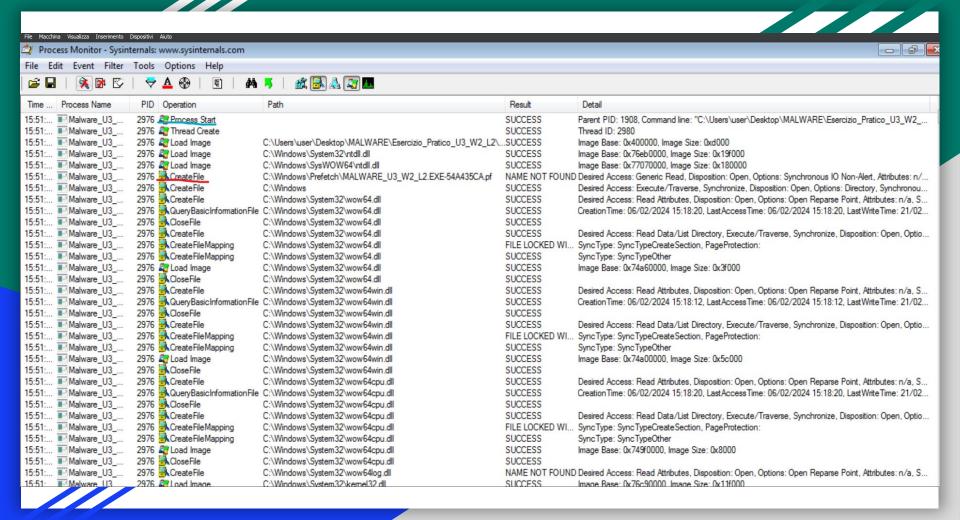
## S10/L2 Epicode Cybersecurity

Analisi dinamica basica

Nell'esercizio di oggi ci viene richiesto di effettuare un'analisi dinamica basica su un malware che ci è stato fornito ed identificare il tipo e le azioni che compie sul file system e sui processi.



Possiamo vedere come, avviando il malware, esso crei delle librerie '.dll', le legga e poi le chiuda.

Purtroppo, a differenza dell'esecuzione indicata nell'esercizio, questo è stato svolto su Windows 7 e il file che dovrebbe essere creato nella cartella non è presente.

Come possiamo vedere, il file utilizza 'svchost.exe.', un'applicazione di Windows spesso usata per iniettare virus.