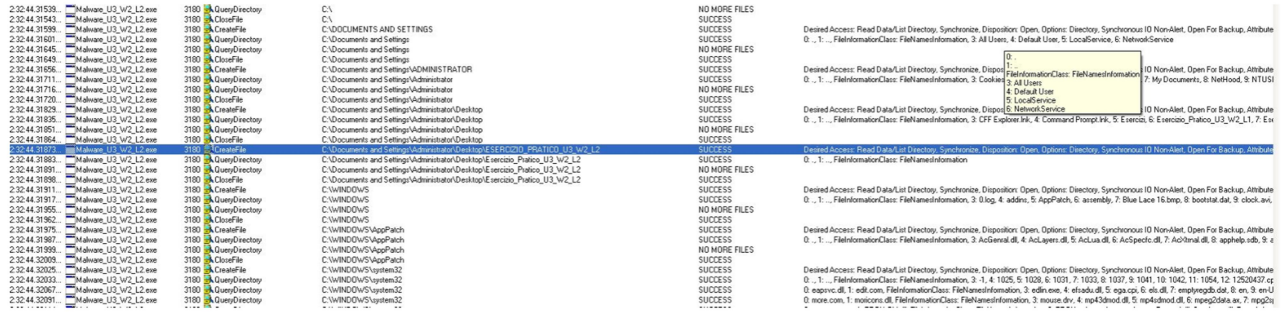
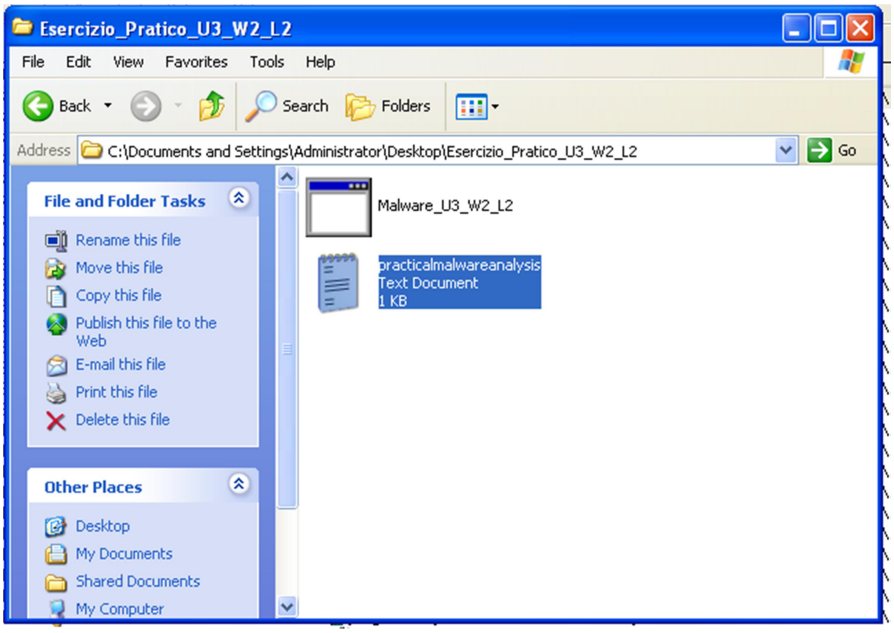
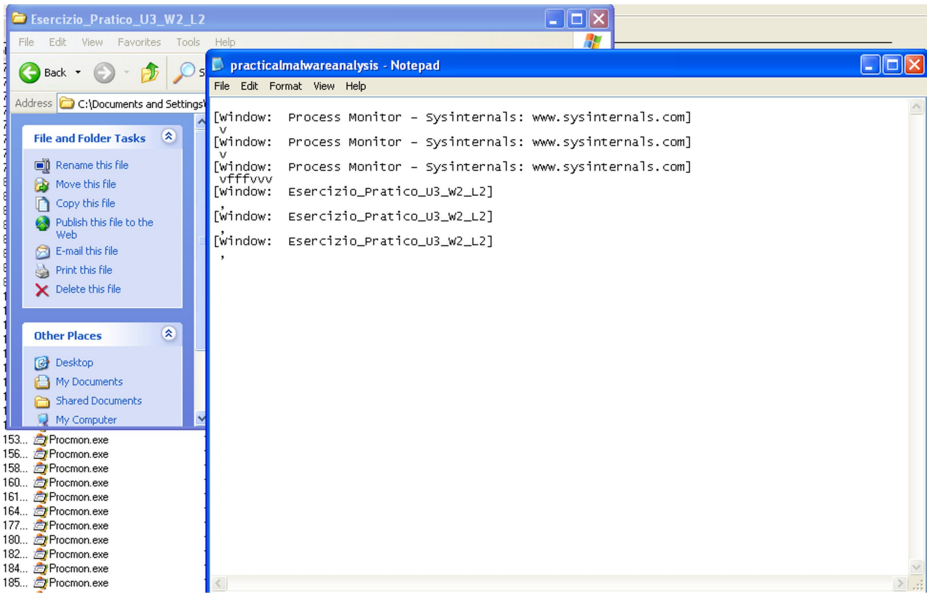


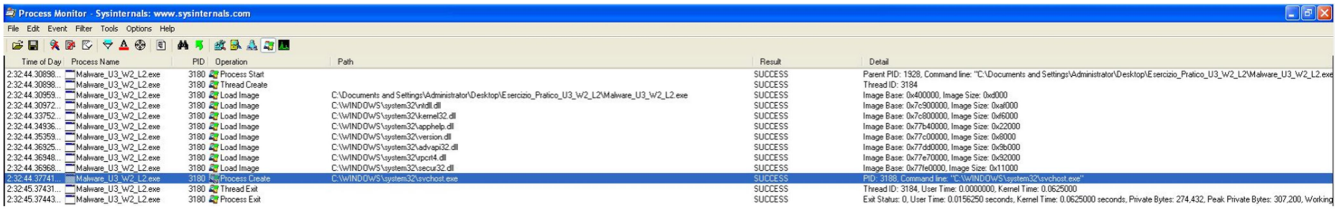
Proviamo a filtrare il report di Procmon per visualizzare esclusivamente le attività correlate al processo denominato "Malware_U3_W2_L2.exe". Dando un'occhiata al report, notiamo alcune operazioni che catturano l'attenzione nella colonna "operation", come "Create File", "Read File" e "Close File", insieme ai rispettivi percorsi dei file coinvolti.

Da questa riga vediamo che è stato creato un file .txt nella cartella del malware





Esaminiamo il contenuto del file per osservare che contiene una registrazione di alcuni caratteri digitati sulla tastiera durante l'esecuzione del malware. Questo è un comportamento tipico dei keylogger.



Nel report, notiamo l'utilizzo di alcune funzioni intriganti come "Load Image", impiegata per caricare il malware e le relative librerie (.dll) necessarie per l'esecuzione. Successivamente, osserviamo l'attività di "Process Create", che sembra essere finalizzata alla creazione di un processo denominato "svchost.exe", comunemente associato ai processi legittimi di Windows. Questo suggerisce un comportamento tipico dei malware, che cercano di mascherare la loro presenza sotto il nome di processi validi al fine di evitare la rilevazione da parte di software antivirus o anti-malware.