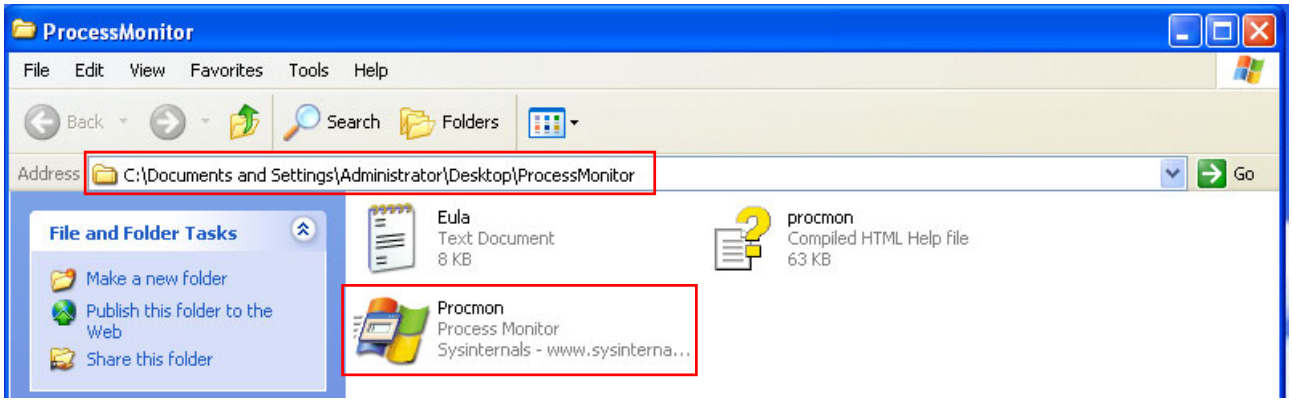
ANALISI DINAMICA BASICA

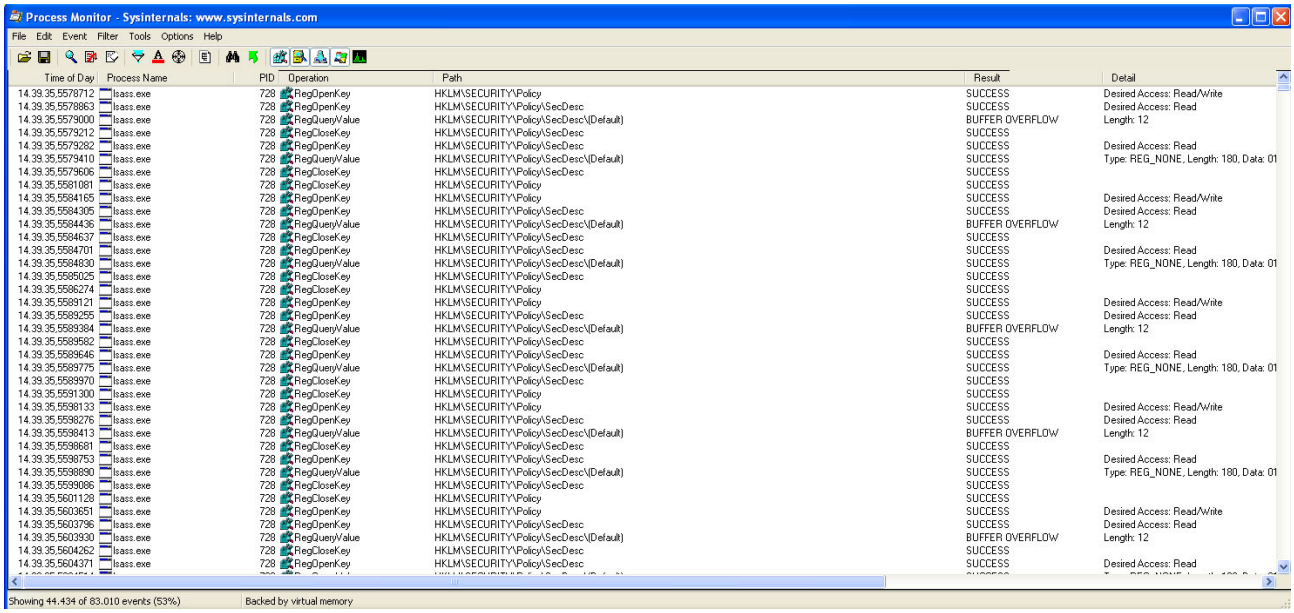
L'esercitazione di oggi consiste nella **ANALISI DINAMICA BASICA** del file eseguibile "**MALWARE_U3_W2_L2**"

FASE 1

Nella prima fase andiamo ad aprire il nostro Tool, già presente sulla nostra macchina "**Process Monitor**" (Procmon)

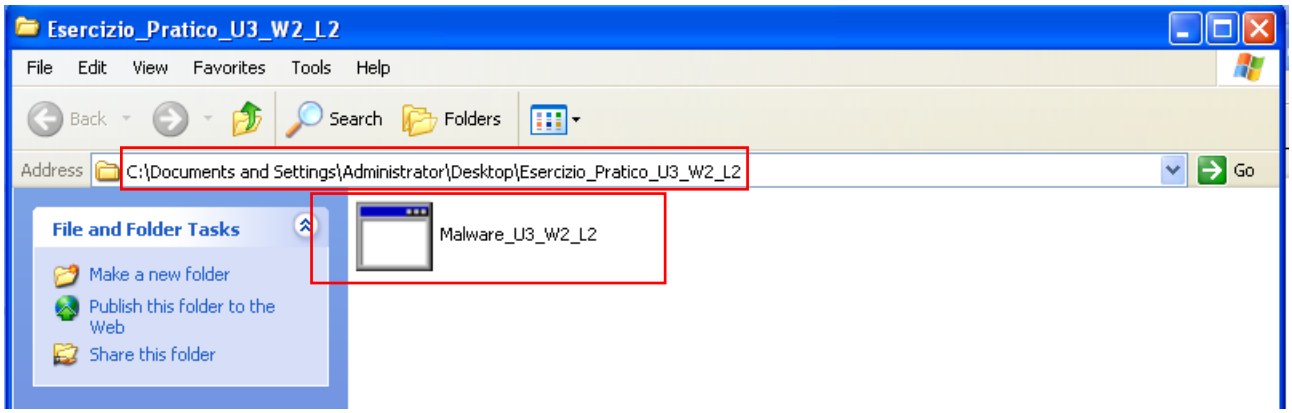


La schermata che ci si presenta inizialmente è una lista di processi attivi sulla nostra macchina

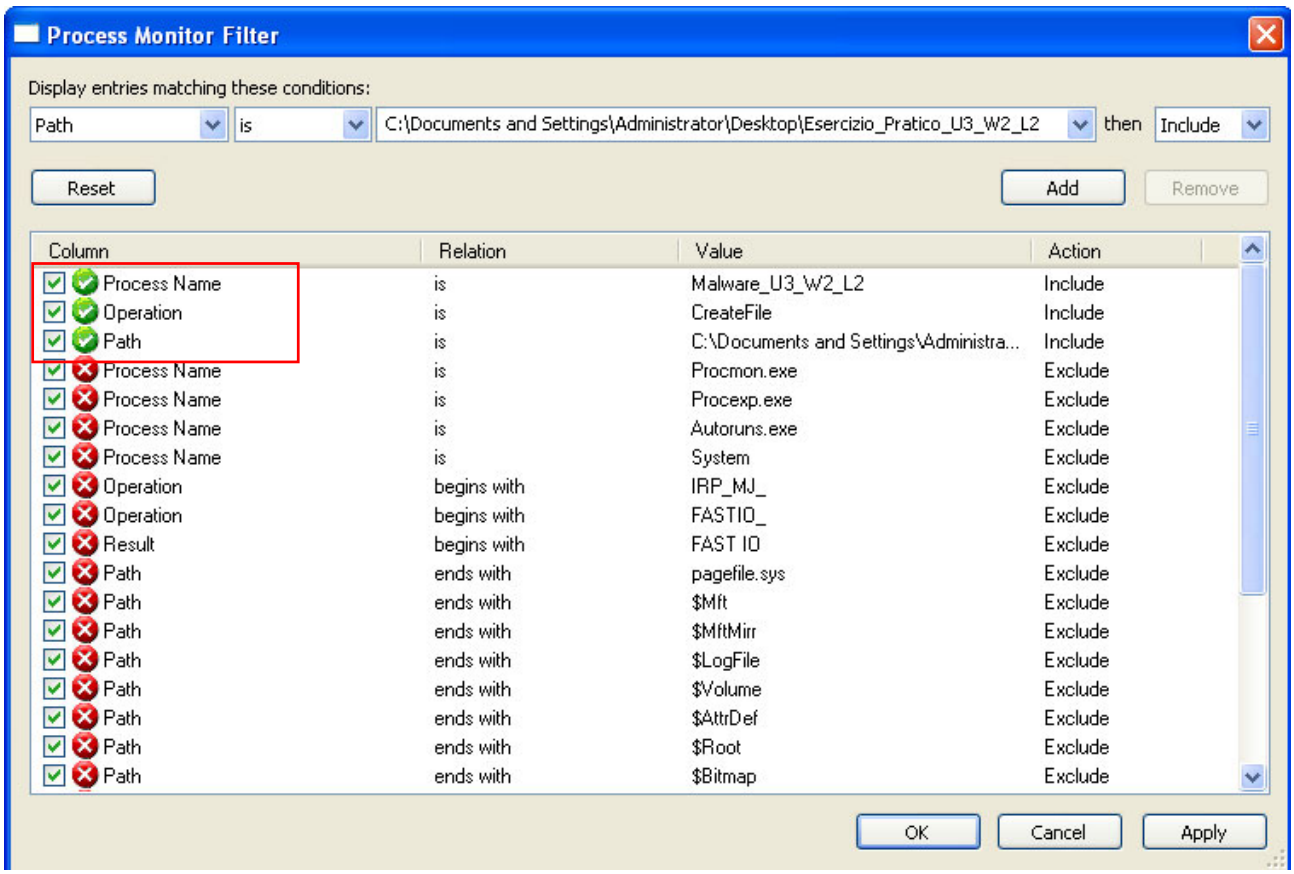


FASE 2

Nella seconda fase andiamo ad aprire l'eseguibile contenente il codice malevolo



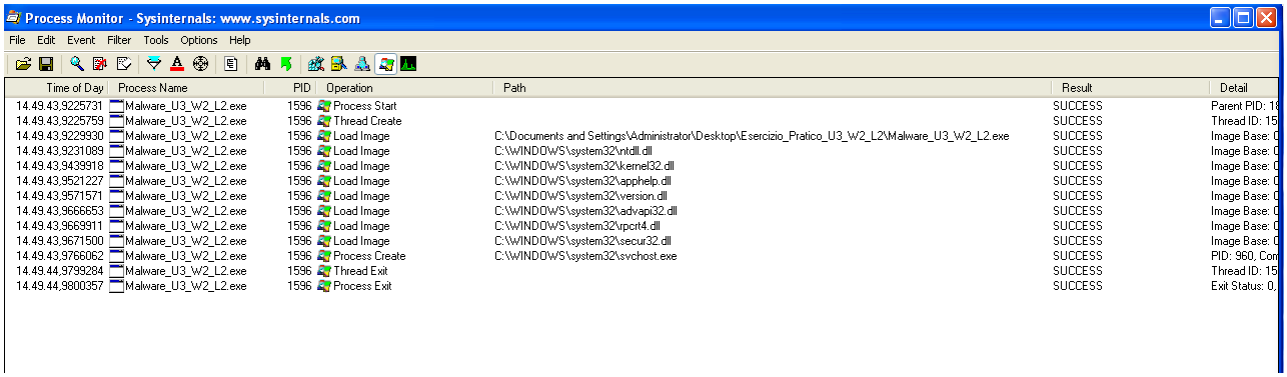
Una volta lasciato agire indisturbato il nostro eseguibile, andremo a creare dei filtri di "ricerca" su Procom.

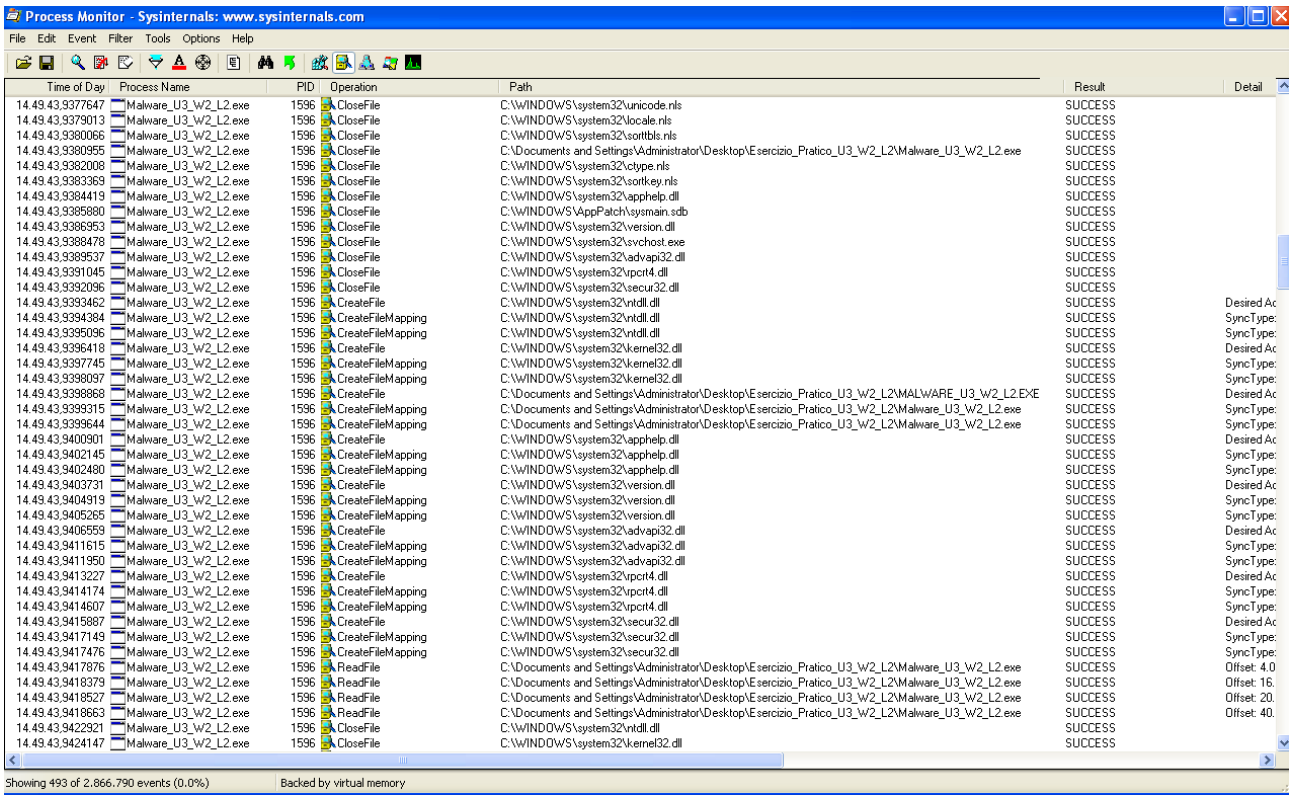


In questo caso creeremo dei filtri per Nome / Creation file / Path

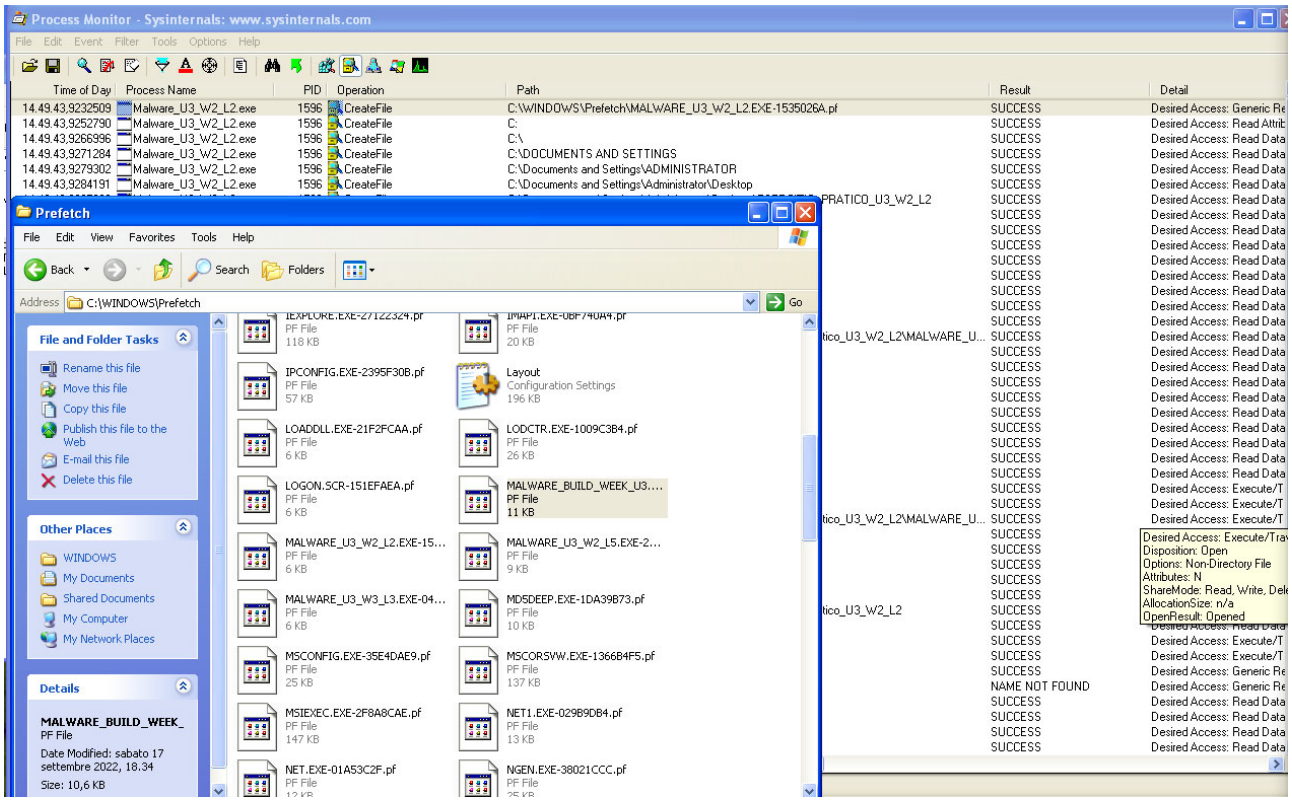
FASE 3

Una volta applicati i filtri ci spostiamo nelle task “File System” e “Thread Activity”





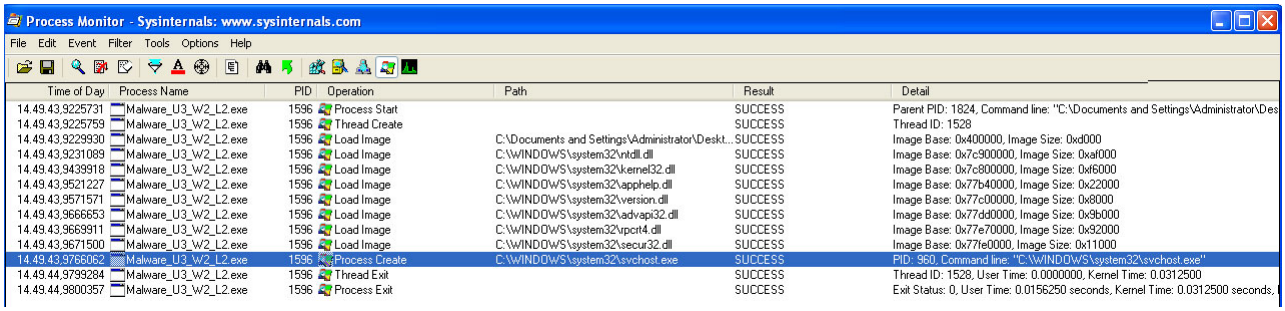
Con la Creazione del filtro create file, possiamo notare la creazione di un file con estensione .pf

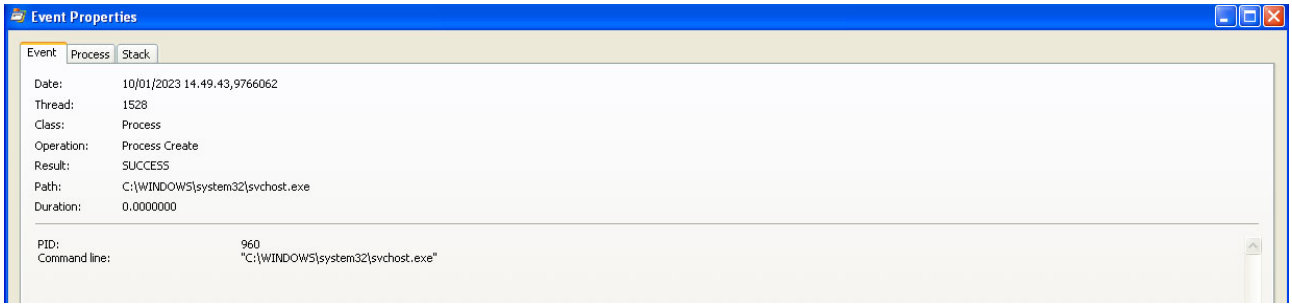


Il **prefetch** è una tecnica usata nei microprocessori per accelerare l'esecuzione dei programmi riducendo gli stati di attesa […].

"https://it.wikipedia.org/wiki/Prefetch"

Il nostro file eseguibile oltre alla creazione del file .pf ha creato anche un processo svchost.exe. Questo processo nativo di windows è stato alterato





I processi svchost.exe sono solitamente sicuri, ma gli hacker e i criminali informatici possono creare malware svchost per imitare i file svchost.exe legittimi. I file svchost.exe legittimi vengono talvolta segnalati dagli scanner antivirus poiché hanno accesso ad aree sensibili del computer. Normalmente, la cartella system32 contiene i file svchost.exe.
"https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8-feflb38AhUGS_EDHawICkEQFnoECB0QAw&url=https%3A%2F%2Fwww.avast.com%2Fc-what-is-svchost-file&usg=AOvVaw1-36XNW_kI81afbrldYmBE"

PROFILAZIONE

In base ai dati possiamo immaginare che il nostro eseguibile sia in verità un Trojan. File malevolo che si nasconde sotto il nome di un altro processo, in questo caso **svchost.exe**.

Per avere un ulteriore conferma possiamo ricavare la firma del nostro file e confrontarla sul database online
"https://www.virustotal.com/gui/file/ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce" con uno score negativo di **59/72**