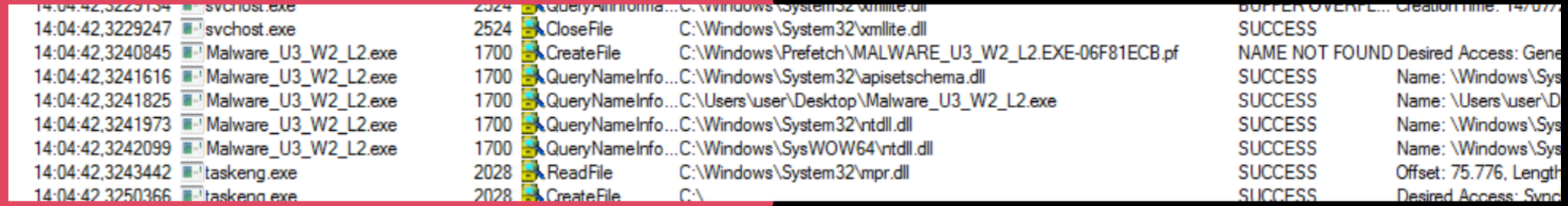
MALWARE ANALYSIS

IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SUL FILE SYSTEM UTILIZZANDO PROCESS MONITOR

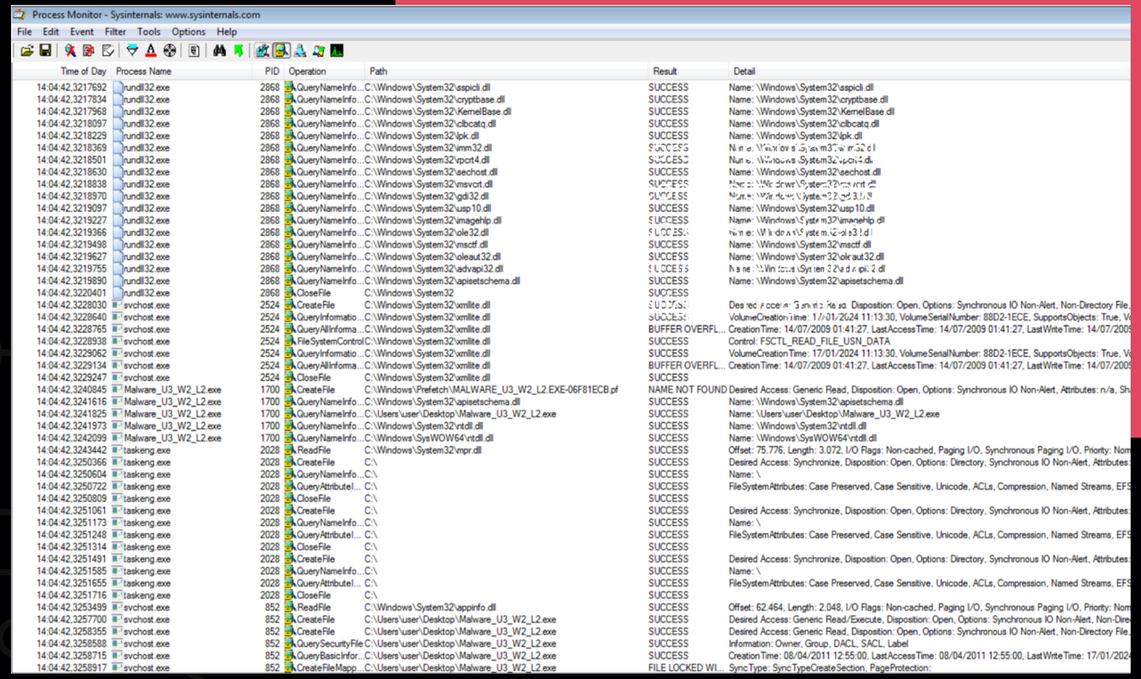
Process Monitor è uno strumento avanzato per monitorare l'attività del sistema, inclusi i cambiamenti nel file system e il comportamento dei processi.

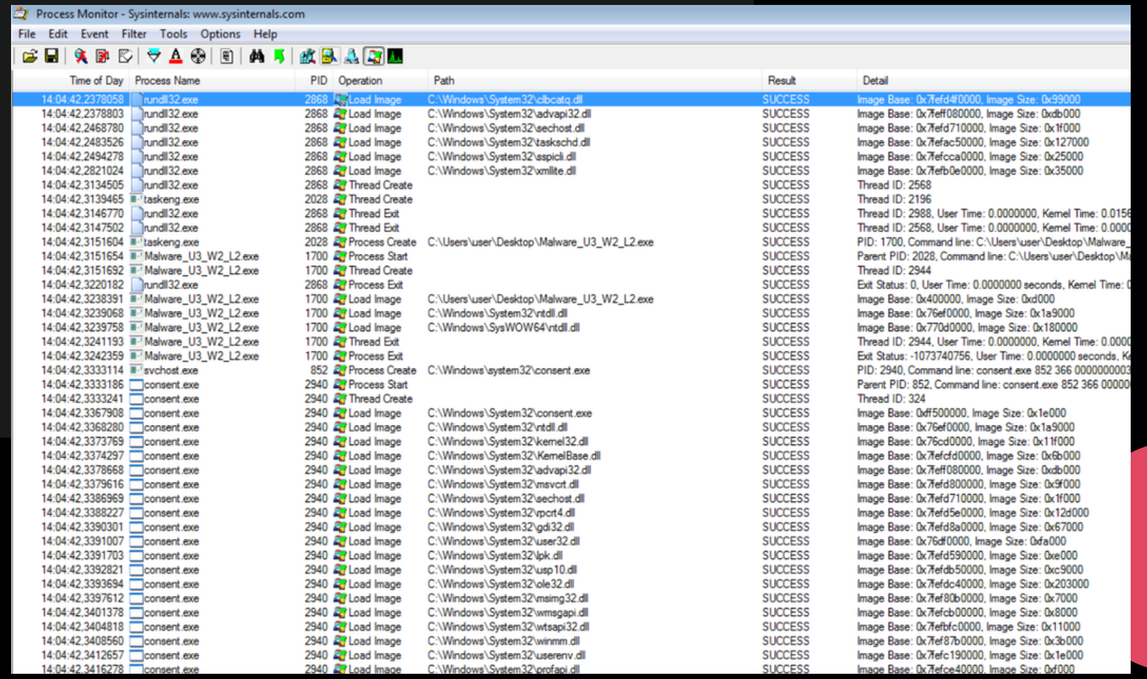
In questa circostanza, abbiamo eseguito un virus all'interno di una macchina virtuale e abbiamo impedito al virus di uscire da quest'ultima. Dopo l'avvio, abbiamo utilizzato Process Monitor per verificare l'attività del virus e lo abbiamo identificato con successo.

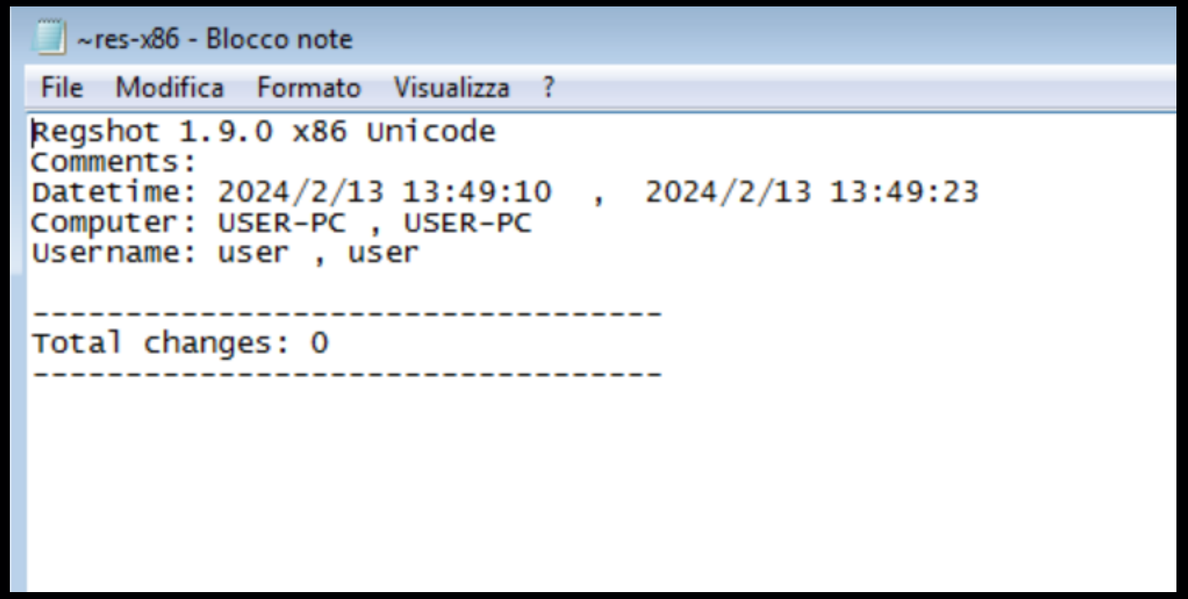


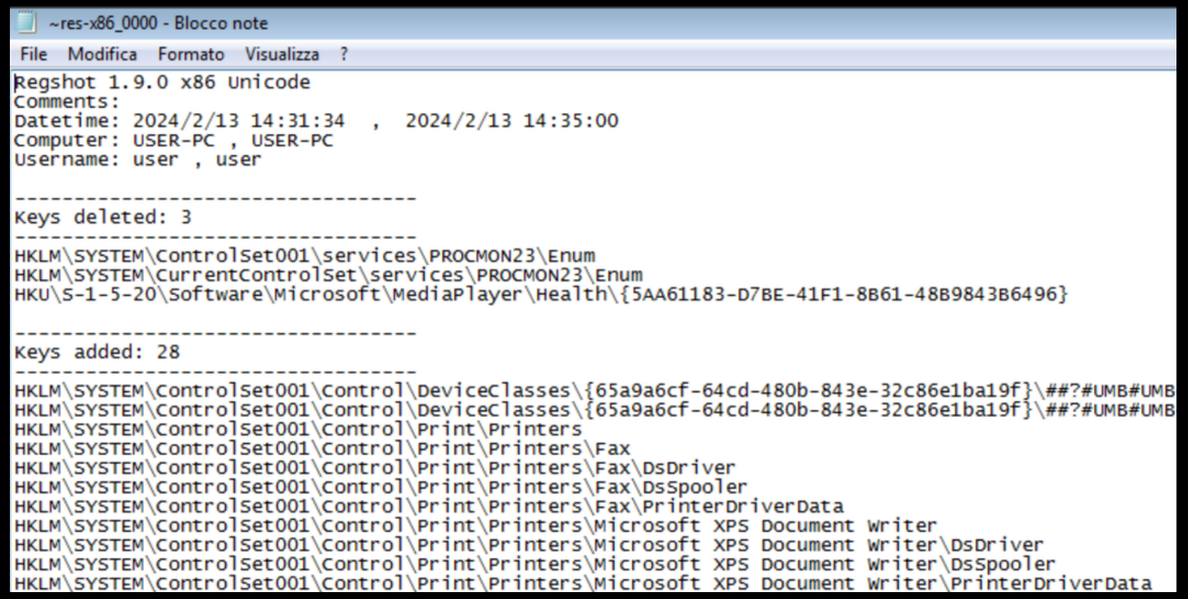
14:04:42,3229247	svchost.exe	2524	CloseFile	C:\Windows\System32\xmllite.dll	SUCCESS	
14:04:42,3240845	Malware_U3_W2_L2.exe	1700	CreateFile	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-06F81ECB.pf	NAME NOT FOUND	Desired Access: Gene
14:04:42,3241616	Malware_U3_W2_L2.exe	1700	QueryNameInfo...	C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\Sys
14:04:42,3241825	Malware_U3_W2_L2.exe	1700	QueryNameInfo...	C:\Users\user\Desktop\Malware_U3_W2_L2.exe	SUCCESS	Name: \Users\user\D
14:04:42,3241973	Malware_U3_W2_L2.exe	1700	QueryNameInfo...	C:\Windows\System32\ntdll.dll	SUCCESS	Name: \Windows\Sys
14:04:42,3242099	Malware_U3_W2_L2.exe	1700	QueryNameInfo...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Name: \Windows\Sys
14:04:42,3243442	taskeng.exe	2028	ReadFile	C:\Windows\System32\mpr.dll	SUCCESS	Offset: 75.776, Length
14:04:42,3250366	taskeng.exe	2028	CreateFile	C:\	SUCCESS	Desired Access: Sync

IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SU PROCESSI E THREAD UTILIZZANDO PROCESS MONITOR





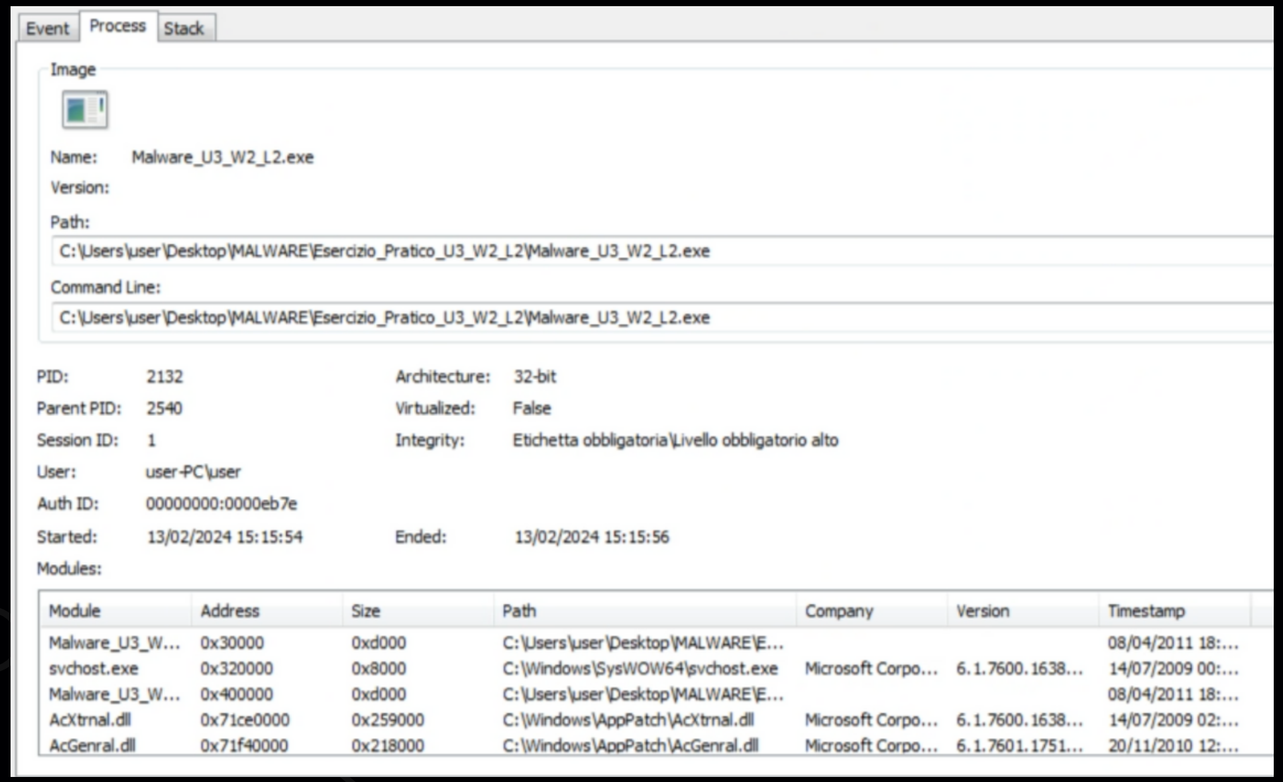




MODIFICHE DEL REGISTRO DOPO IL MALWARE

Per determinare eventuali modifiche apportate dal virus, abbiamo impiegato RegShot, un'applicazione che ci ha richiesto di eseguire un "PrimoShot" del sistema in uno stato privo del virus, seguito da un "SecondoShot" con il virus attivo. Durante questa procedura, abbiamo identificato variazioni nel registro di sistema. Il malware ha influenzato chiavi e valori di rilevanza fondamentale, minando la stabilità e la sicurezza del sistema.

PROVARE A PROFILARE IL MALWARE IN BASE ALLA CORRELAZIONE TRA «OPERATION» E PATH.



Sechost.dll

Sechost.dll è una libreria di collegamento dinamico (DLL) di sistema in ambienti Windows. Questa DLL è associata ai servizi di hosting della sicurezza del sistema operativo. La sua presenza è fondamentale per il corretto funzionamento del sistema e per garantire la sicurezza delle operazioni.

kernel32.dll

La kernel32.dll è una delle librerie di collegamento dinamico (DLL) essenziali nei sistemi operativi Windows. Questa DLL svolge un ruolo cruciale nel kernel del sistema operativo e offre una vasta gamma di funzioni di base per le applicazioni e il sistema stesso.