**Traccia:**

Configurare la macchina virtuale per l’analisi dinamica (il malware sarà effettivamente eseguito). Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L2» presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:

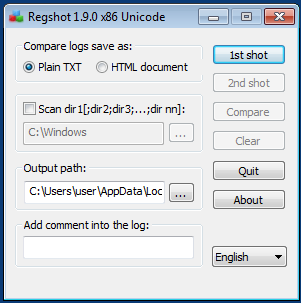
• Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon);

• Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor;

• Modifiche del registro dopo il malware (le differenze);

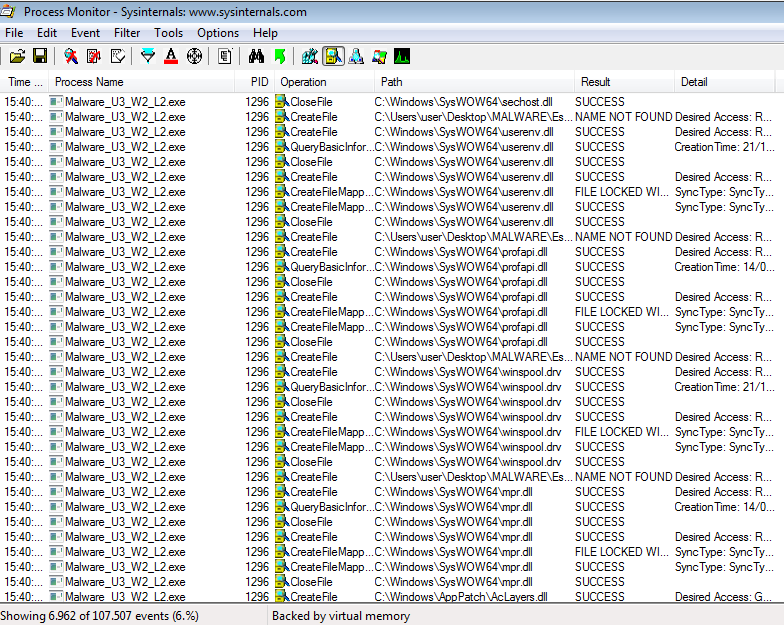
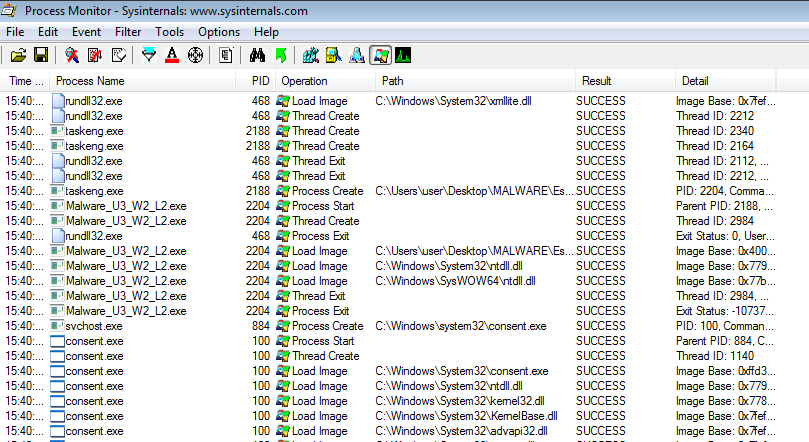
• Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Prima di eseguire il malware sulla nostra macchina virtuale, facciamo una prima scansione su **Regshot,** strumento open-source che viene utilizzato per confrontare lo stato del Registro di sistema di Windows prima e dopo l'installazione di un'applicazione, una modifica di configurazione o altre attività che possono influenzare il Registro di sistema:



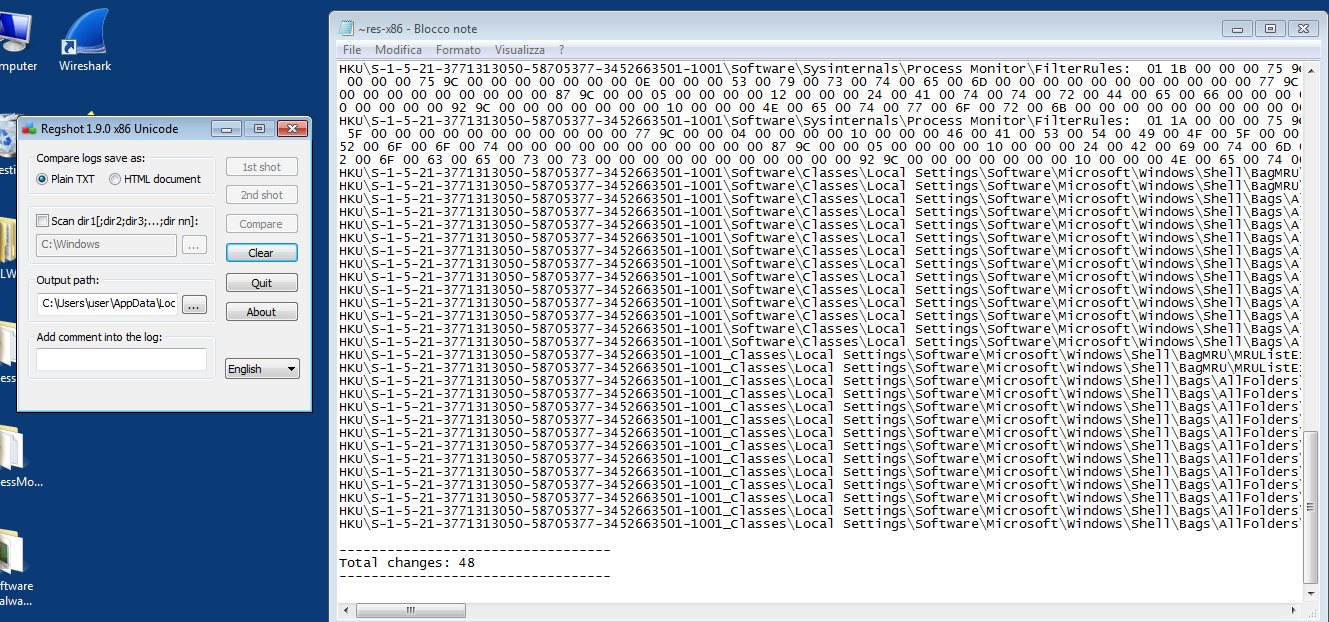
In seguito possiamo eseguire il nostro malware e iniziare la scansione con **Process Monitor (procmon).**

Process Monitor è uno strumento di *monitoraggio avanzato* sviluppato per il sistema operativo Windows. Consente agli utenti di monitorare e registrare l'attività del sistema in *tempo reale*, inclusi i processi in esecuzione, le operazioni del file system, le attività di rete e le modifiche al Registro di sistema. Esso fornisce una vasta gamma di informazioni dettagliate sulle attività del sistema, consentendo agli utenti di diagnosticare problemi, analizzare il comportamento delle applicazioni e risolvere eventuali problematiche di sistema:

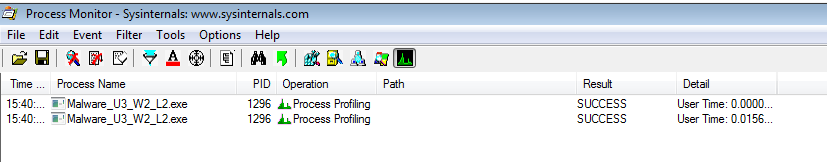
 

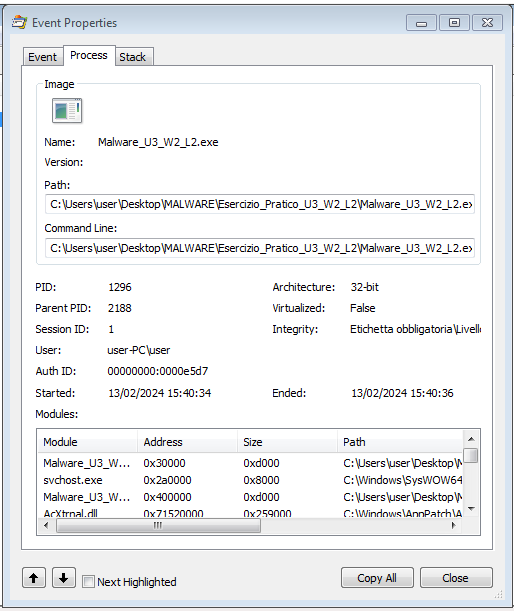
Come possiamo vedere dagli screenshot, una volta avviato il malware e filtrato attraverso gli appositi pulsanti in alto  (rispettivamente: *Registry, File System, Network, Process and Thread* e *Profiling*) possiamo identificare le azioni del malware per la sezione file system e process e thread, come richiesto dall’esercizio nei primi due punti. Riapriamo Regshot e facciamo una seconda scansione, a malware eseguito, e confrontiamo (attraverso l’apposito pulsante) entrambe le scansioni (prima e dopo) così da rispondere al terzo quesito dell’esercizio.

Come possiamo vedere, a seguito della comparazione, Regshot ha riscontrato ben *48 cambiamenti* apportati dal malware sul registro di sistema di Windows:



Effettuiamo una correlazione tra *Operation e Path*, come da richiesta numero quattro dell’esercizio:





Dai dati raccolti potrebbe trattarsi di un Trojan, un malware dalla subdola caratteristica di nascondersi e sembrare legittimo per poi effettuare azioni dannose.

Sembra che, in particolare, il malware in analisi abbia attaccato il file system e questo può causare una serie di problemi e danni al sistema operativo e ai dati dell'utente; potrebbe corrompere o danneggiare i file presenti nel sistema, rendendoli inaccessibili o non utilizzabili, eliminare o cancellare file critici o importanti, causando la perdita permanente di dati, creare nuovi file dannosi sul sistema e potrebbe ottenere accesso non autorizzato ai file dell'utente o ai dati sensibili presenti sul sistema.