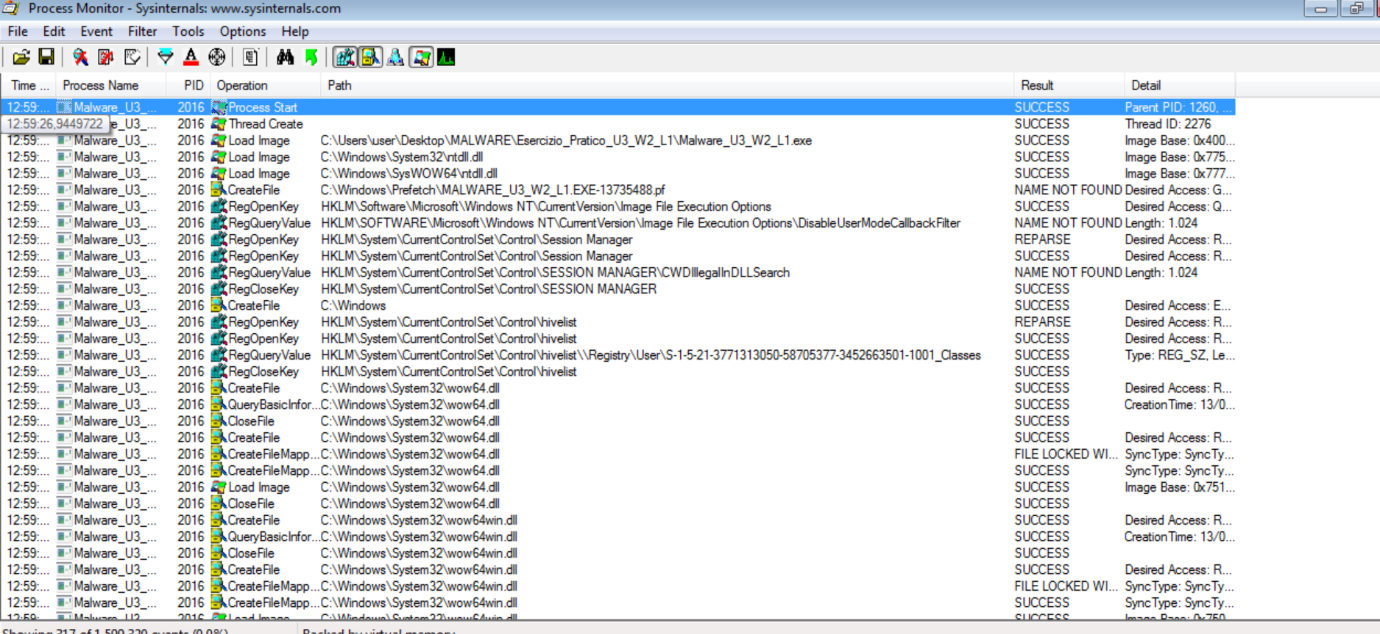
**Malware analysis**

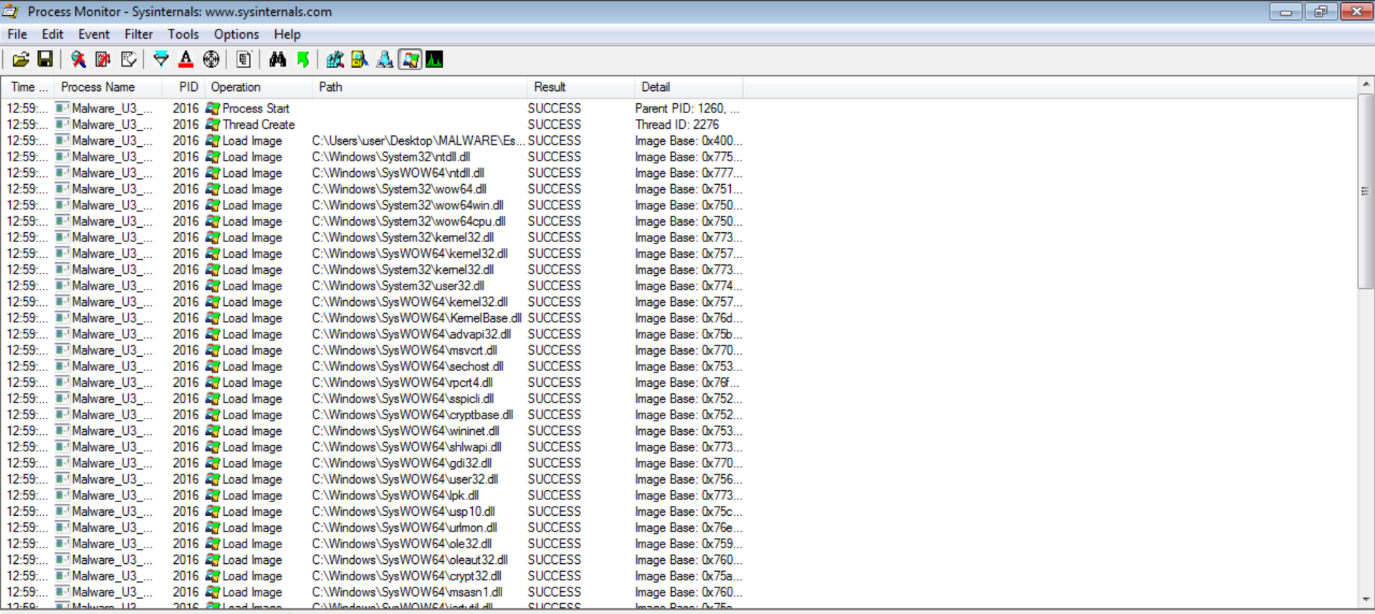
Traccia: Configurare la macchina virtuale per l’analisi dinamica (il malwaresarà effettivamente eseguito). Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L2» presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti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

1. Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon)
2. Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor
3. Modifiche del registro dopo il malware (le differenze)
4. Provare a profilare il malware in base alla correlazione tra «operation» e Path.

1)

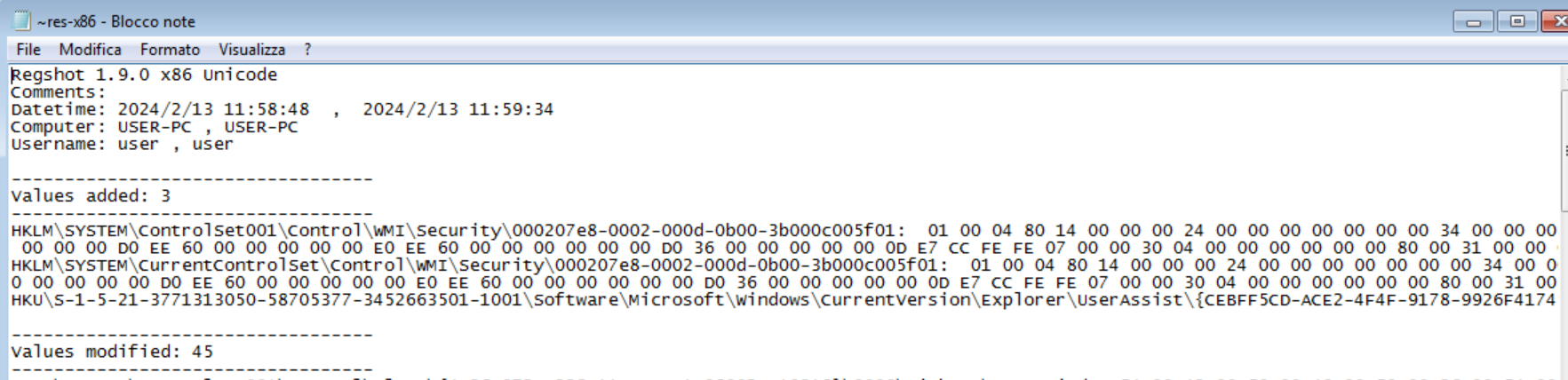
**Azioni sul File System**

1. **CreateFile**: Il malware crea file sul sistema. Questo può essere un indicatore che il malware sta tentando di scrivere i propri file sul disco, che potrebbero essere payload dannosi, moduli di aggiornamento, o file di log per tracciare l'esecuzione.
2. **CreateFileMapping**: Il malware sta mappando file esistenti o nuovi file nella memoria, che potrebbe essere utilizzato per modificare i file o eseguire codice all'interno dello spazio di memoria di un altro processo.
3. **QueryBasicInformationFile**: Questa azione indica che il malware sta ottenendo informazioni sui file, come le dimensioni, le date di creazione, ultima modifica e ultimo accesso. Questo può essere utilizzato per identificare file specifici da modificare o sostituire.
4. **RegSetInfoKey**: Sebbene sia un'operazione di registro, può essere correlata al file system se il malware sta cambiando i permessi su determinate chiavi di registro che influenzano il comportamento del file system.

2)

**Azioni su Processi e Thread**

1. **Process Start**: L'immagine mostra che il malware ha avviato un processo. Questo potrebbe essere un segno che il malware sta eseguendo altri componenti dannosi.
2. **Thread Create**: Il malware potrebbe creare nuovi thread all'interno del suo processo o in altri processi. I thread possono essere usati per eseguire codice simultaneamente, per compiere azioni in parallelo, o per iniettare codice in altri processi.
3. **Load Image**: Il caricamento di immagini (DLL) è un'azione che può influenzare sia il file system sia i processi/thread. Il malware potrebbe iniettare DLL malevoli in altri processi per eseguire codice dannoso.

3)

Dallo screenshot di un report di Regshot possiamo vedere che ci sono state tre nuove chiavi aggiunte e quarantacinque valori modificati.

4)

Dall'immagine vediamo diverse operazioni di un processo chiamato "Malware\_U3\_2016", il processo esegue diverse operazioni tipiche di un programma in esecuzione su Windows, ma ci sono alcune attività che possono essere indicative di comportamenti malevoli:

1. **RegQueryValue**: Questa operazione legge i valori delle chiavi di registro. Il malware spesso legge o modifica le chiavi di registro per configurare la propria persistenza o per modificare le impostazioni del sistema per favorire la propria esecuzione o comunicazione.
2. **Load Image**: Il caricamento di DLL (Dynamic Link Libraries) è normale, ma il malware spesso carica DLL malevole o sfrutta DLL per iniettare codice dannoso o per evadere il rilevamento.
3. **CreateFile** e **CreateFileMapping**: Queste operazioni possono essere utilizzate per creare nuovi file o per mappare file esistenti nella memoria, il che è comune in attività legittime, ma può essere anche utilizzato da malware per distribuire o eseguire codice dannoso.
4. **RegOpenKey** e **RegCloseKey**: L'apertura e la chiusura di chiavi di registro possono essere parte della configurazione del malware o tentativi di modificare le impostazioni del sistema per garantire la persistenza o alterare la sicurezza del sistema.
5. **RegSetInfoKey**: Il malware potrebbe utilizzare questa operazione per modificare i permessi o altre impostazioni delle chiavi di registro per nascondere la propria presenza o proteggere i propri componenti dalla rimozione.

Dall'analisi delle operazioni e dei percorsi, si potrebbe dedurre che questo malware sta tentando di:

* Ottenere la persistenza modificando il registro di sistema.
* Caricare o modificare DLL per eseguire o iniettare codice dannoso.
* Creare o modificare file, potenzialmente per diffondere componenti dannosi o manipolare processi esistenti.