Epicode
CS-0124
Pratica S10/L2

Francesco Ficetti

1. Traccia

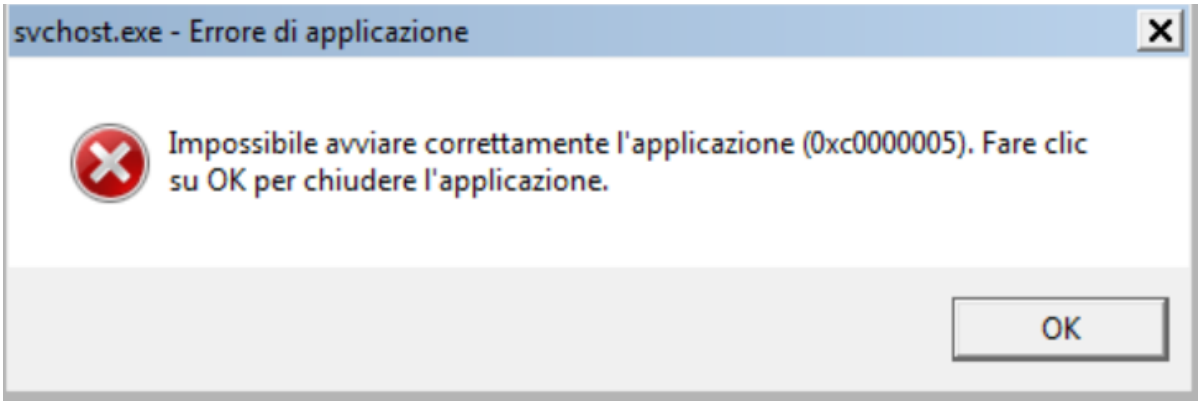
Con riferimento al malware allegato a questo esercizio rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor.
- Identificare eventuali azioni del malware sui processi ed i threads utilizzando ProcessMonitor.
- Modifiche del registro dopo il malware.
- Provare a profilare il malware in base alla correlazione tra Operation e Path.

2. Svolgimento

2.1 Esecuzione del malware su Windows 7

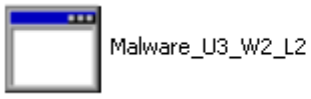
L'esecuzione del malware su Windows 7 restituisce il seguente errore.

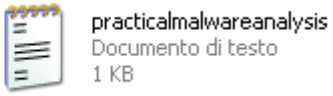


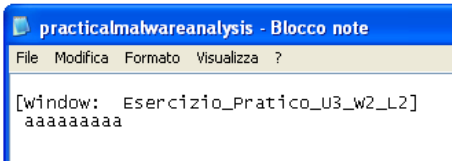
L'esercizio è quindi proseguito su Windows XP.

2.2 Esecuzione del malware su Windows XP

Per prima cosa si deve avviare *procmon*, in modo da iniziare la cattura dei processi. Successivamente è possibile avviare il malware.
Esso non impatta le prestazioni della macchina, se un utente lo dovesse eseguire involontariamente non ne noterebbe la presenza.
Non appena si preme un qualsiasi tasto, viene creato un file, nella stessa cartella del malware, chiamato "praticamalwareanalysis". Al suo interno si trova la "cronologia" di tutti i tasti premuti dall'esecuzione del malware.

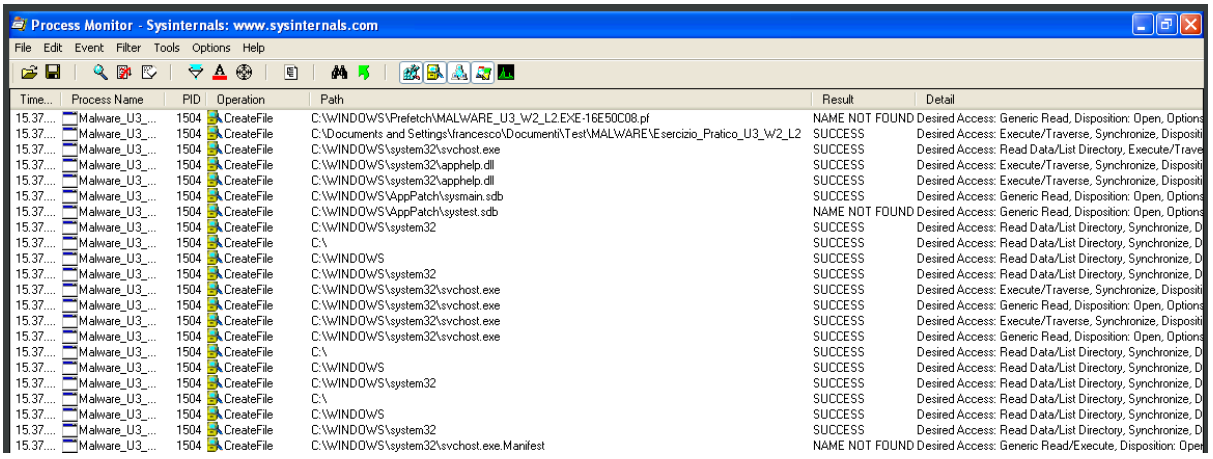






2.2.1 Azioni del malware su file system

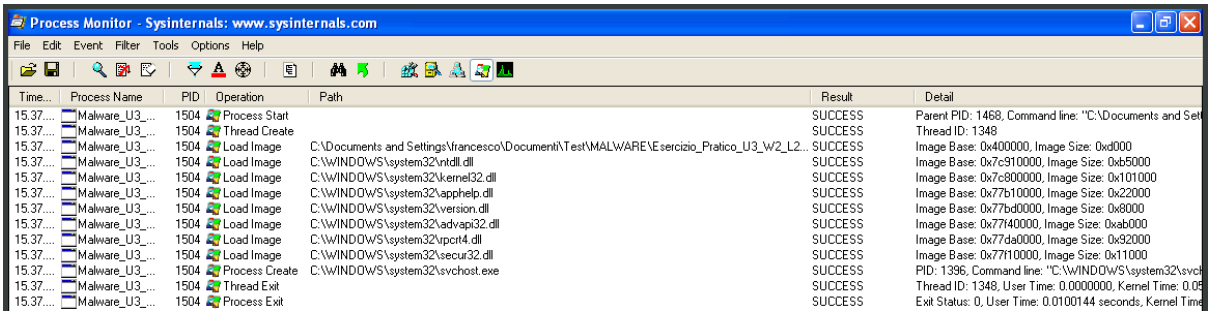
Su *procmon* è possibile filtrare la cattura dei processi. In questo caso sono stati applicati due filtri, il primo per vedere solo i processi riguardanti il malware eseguito, il secondo per vedere quelli che eseguivano un'operazione di creazione di un file. Il risultato è il seguente.



Come si può vedere, ci sono molte chiamate alla funzione CreateFile, tra le quali proprio quella che crea il file contenente i tasti premuti.

2.2.2 Azioni del malware su processi e threads

Per quanto riguarda questa parte di analisi, l'unico filtro applicato è quello per vedere solo i processi del malware eseguito.



Da questa cattura, si può vedere che viene richiamato il processo *svchost.exe*, processo di Windows che in questo caso serve al malware per camuffarsi agli occhi dell' antivirus.

2.2.3 Modifiche sul registro

Con il tool *regshot*, si può eseguire un'istantanea dei registri del sistema operativo prima di avviare il malware, ed una dopo averlo avviato. Successivamente è possibile effettuare una comparazione tra le due.
In questo caso, ci sono stati diversi cambiamenti.

3. Conclusioni

Tutti i comportamenti analizzati sono congrui con il comportamento di un keylogger.