Cybersecurity Specialist

Cyber Security & Ethical Hacking

ANALISI DINAMICA BASICA

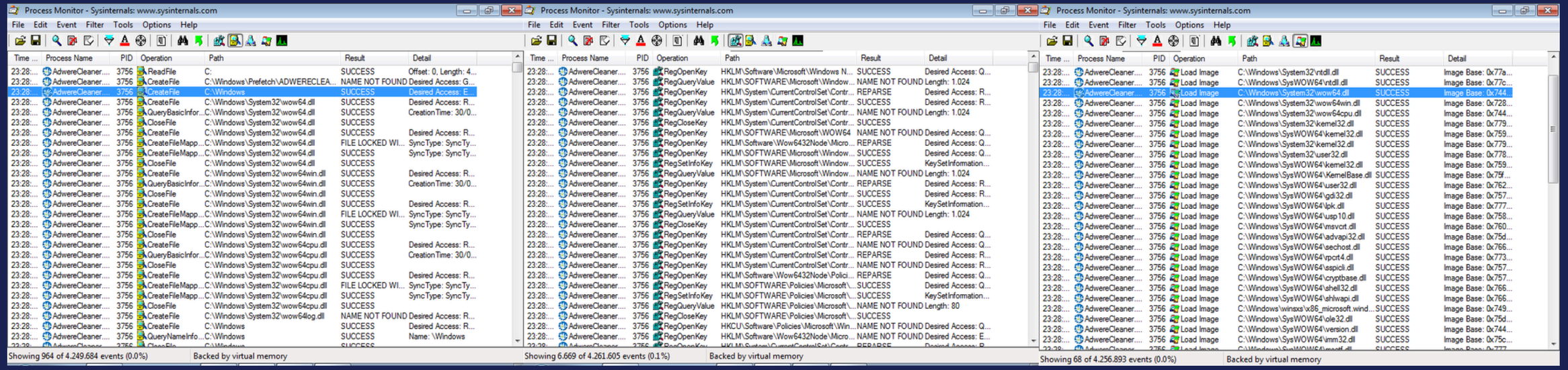
Alejandro Cristino
S10-L2

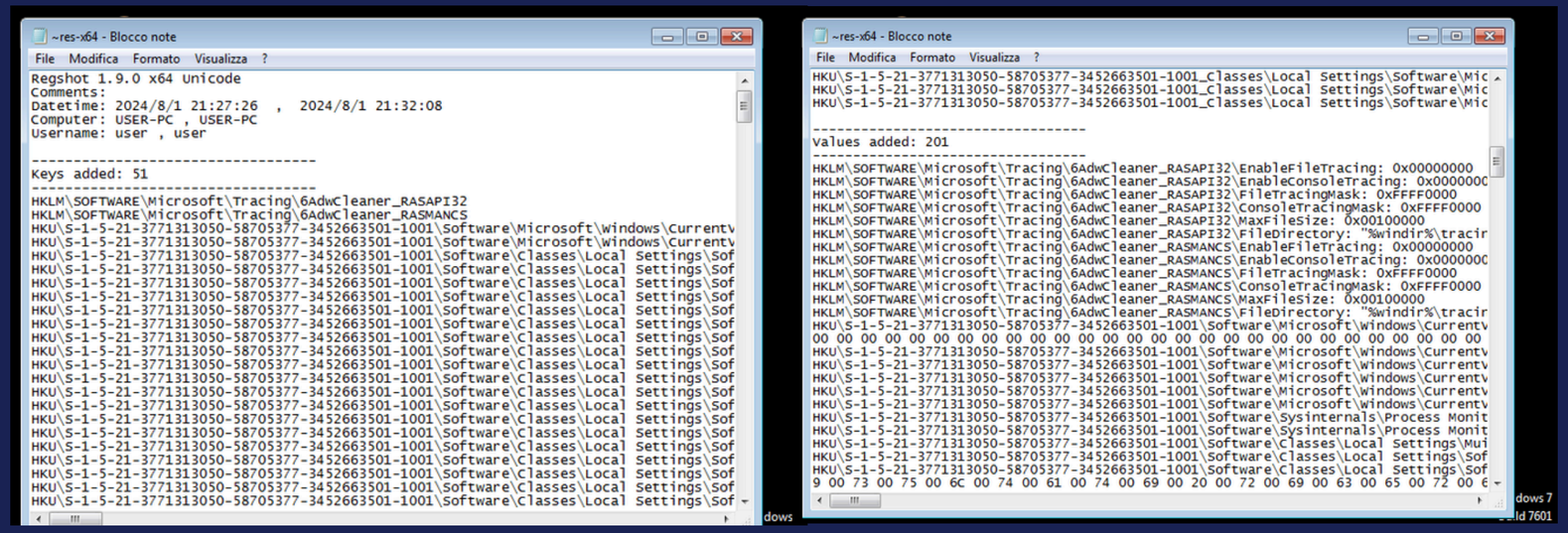
TRACCIA

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 Process Monitor (procmon)
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Modifiche del registro dopo il malware (le differenze)
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

ANALISI DI BASE DINAMICA





CONCLUSIONI

Dopo l’analisi possiamo concludere che si tratta di un malware che si spaccia per un fake AdwCleaner. in realta, il file può provocare danni come il furto di dati o l’installazione di ulteriori malware.
Tramite procmon possiamo osservare operazioni come la creazione di file o modifiche al registro di sistema.
Proseguendo con l’analisi possiamo notare threads creati dal malware, il che ci fa pensare che sta tentando di eseguire il download di altri malware.
Regshot ci indica una sezione che elenca le chiavi di registro aggiunte, modificate o cancellate durante il monitoraggio. Queste chiavi sembrano indicare tracce lasciate da un programma che potrebbe essere una versione fraudolenta di AdwCleaner, con varie chiavi di registro nei percorsi relativi a Microsoft Tracing e impostazioni locali dell’utente.