GIORNO 4

Traccia:

Preparate l’ambiente ed i tool per l’esecuzione del Malware(suggerimento: avviate principalmente Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware, facendo doppio click sull’icona dell’eseguibile

Cosa notate all’interno della cartella dove è situato l’eseguibile del Malware? Spiegate cosa è avvenuto, unendo le evidenze che avete raccolto finora per rispondere alla domanda Analizzate ora i risultati di Process Monitor (consiglio: utilizzate il filtro come in figura sotto per estrarre solo le modifiche apportate al sistema da parte del Malware). Fate click su «ADD» poi su «Apply» come abbiamo visto nella lezione teorica.

Filtrate includendo solamente l’attività sul registro di Windows .

-Quale chiave di registro viene creata?

-Quale valore viene associato alla chiave di registro creata?

Passate ora alla visualizzazione dell’attività sul File System.

-Quale chiamata di sistema ha modificato il contenuto della cartella dove è presente l’eseguibile del Malware?

Unite tutte le informazioni raccolte fin qui sia dall’analisi statica che dall’analisi dinamica per delineare il funzionamento del Malware.

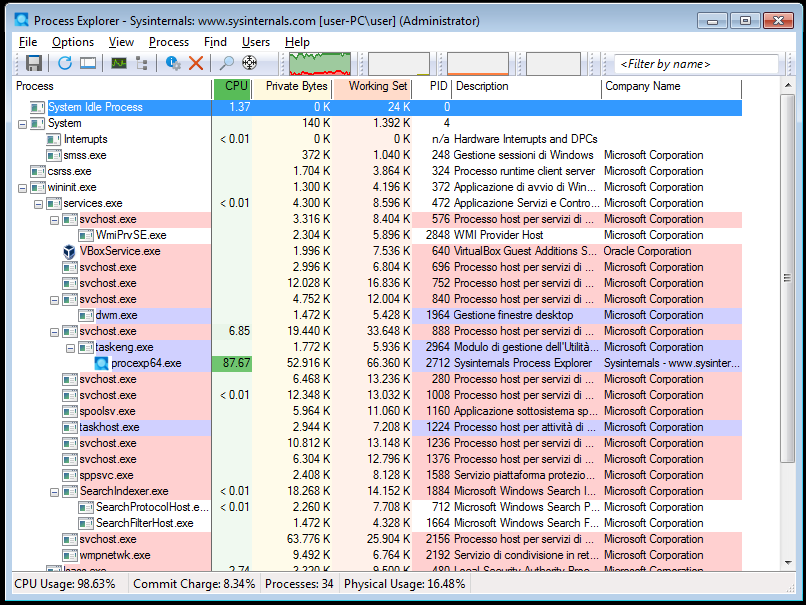
Glossario:

-Process Explorer: Tool che permette di osservare tutti i processi in esecuzione su un sistema.

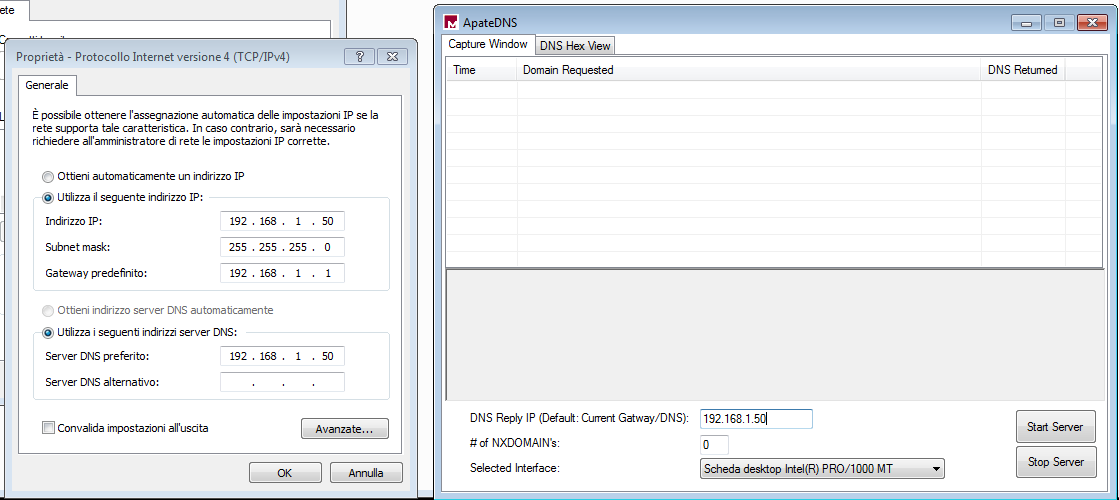
-ProcMon (Process Monitor): Tool avanzato di windows che permette di monitorare i thread attivi, le attività di rete, l’accesso ai file e le chiamate di sistema effettuate da un OS.

-Regshot: Tool che permette di confrontare lo stato delle chiavi di registro di un sistema con le loro istantanee prima e dopo l’esecuzione di un malware.

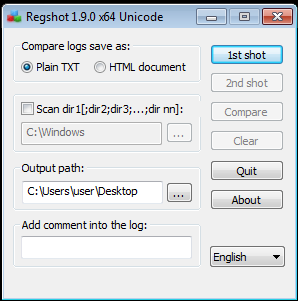
-Apate DNS: Tool che funge da server DNS utilizzato per intercettare tutte le richieste generate da un malware verso i domini Internet.



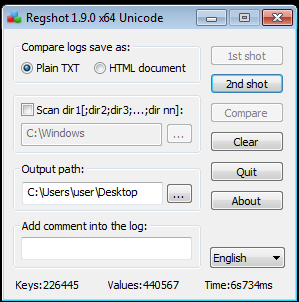
apertura process explorer



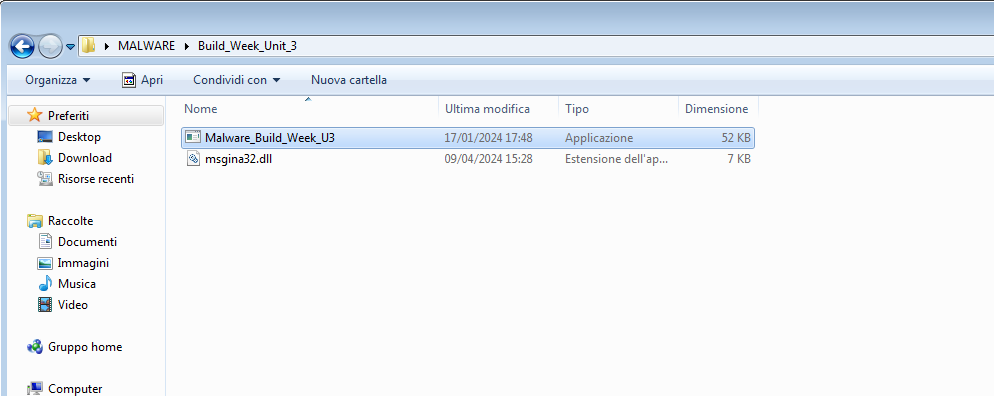
modifica dns per apate dns



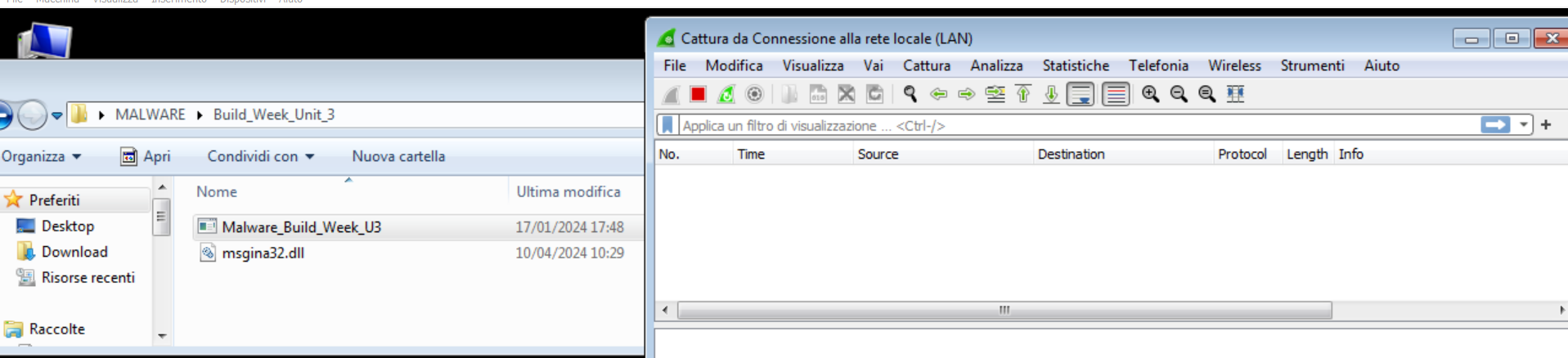
prima istantanea regshot



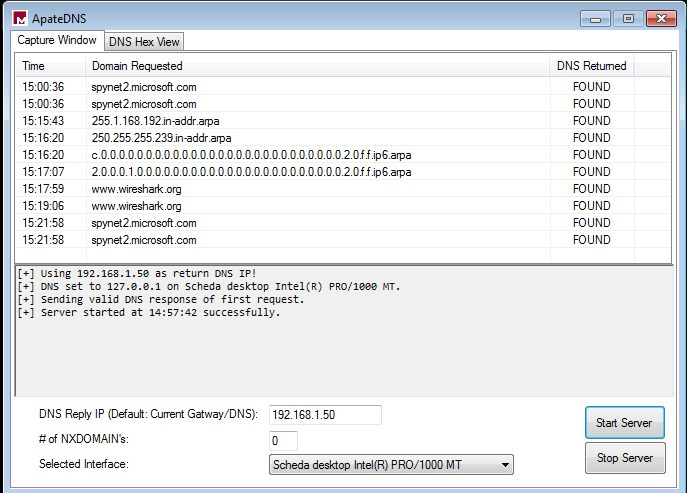
seconda istantanea regshot



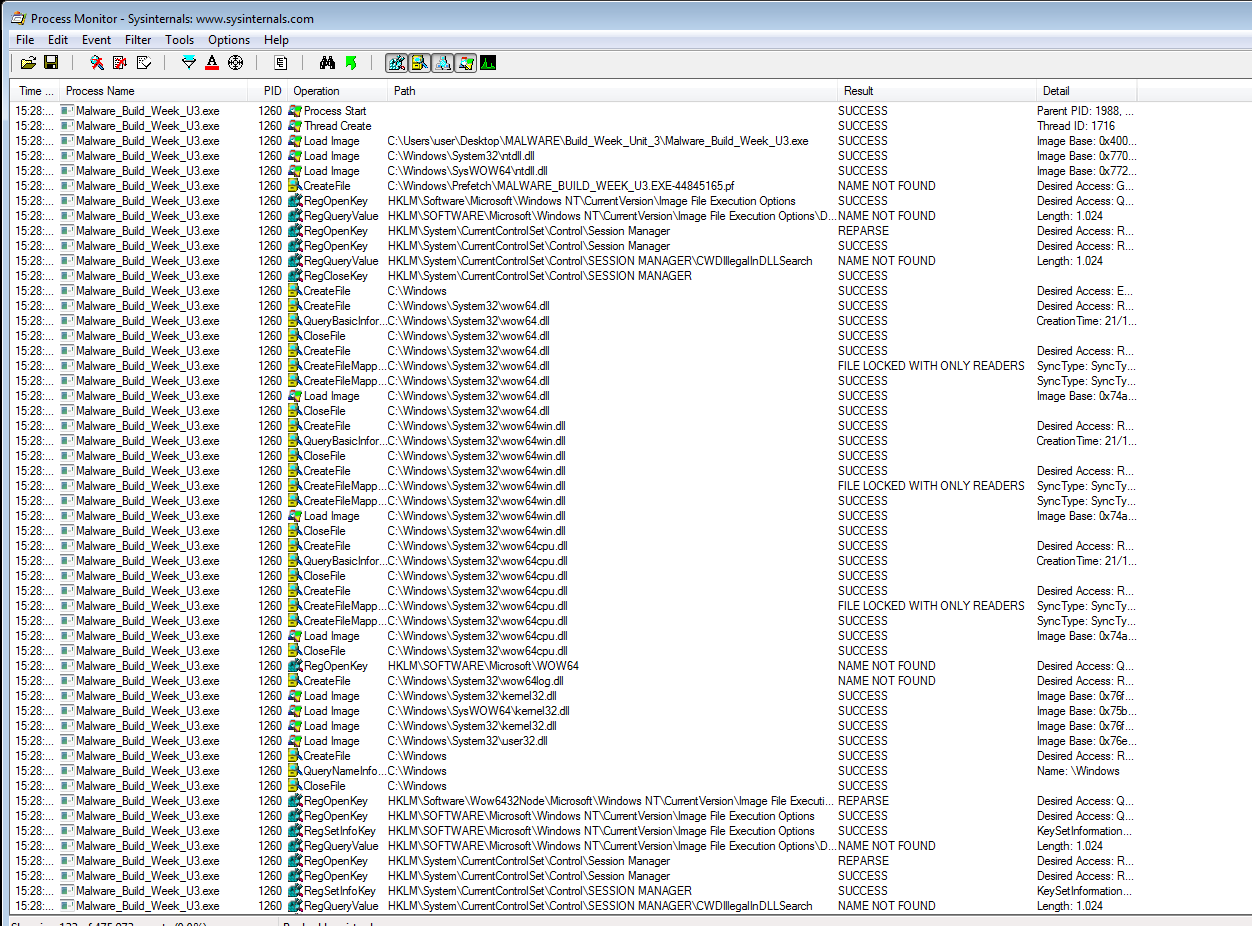
modifica cartella malware



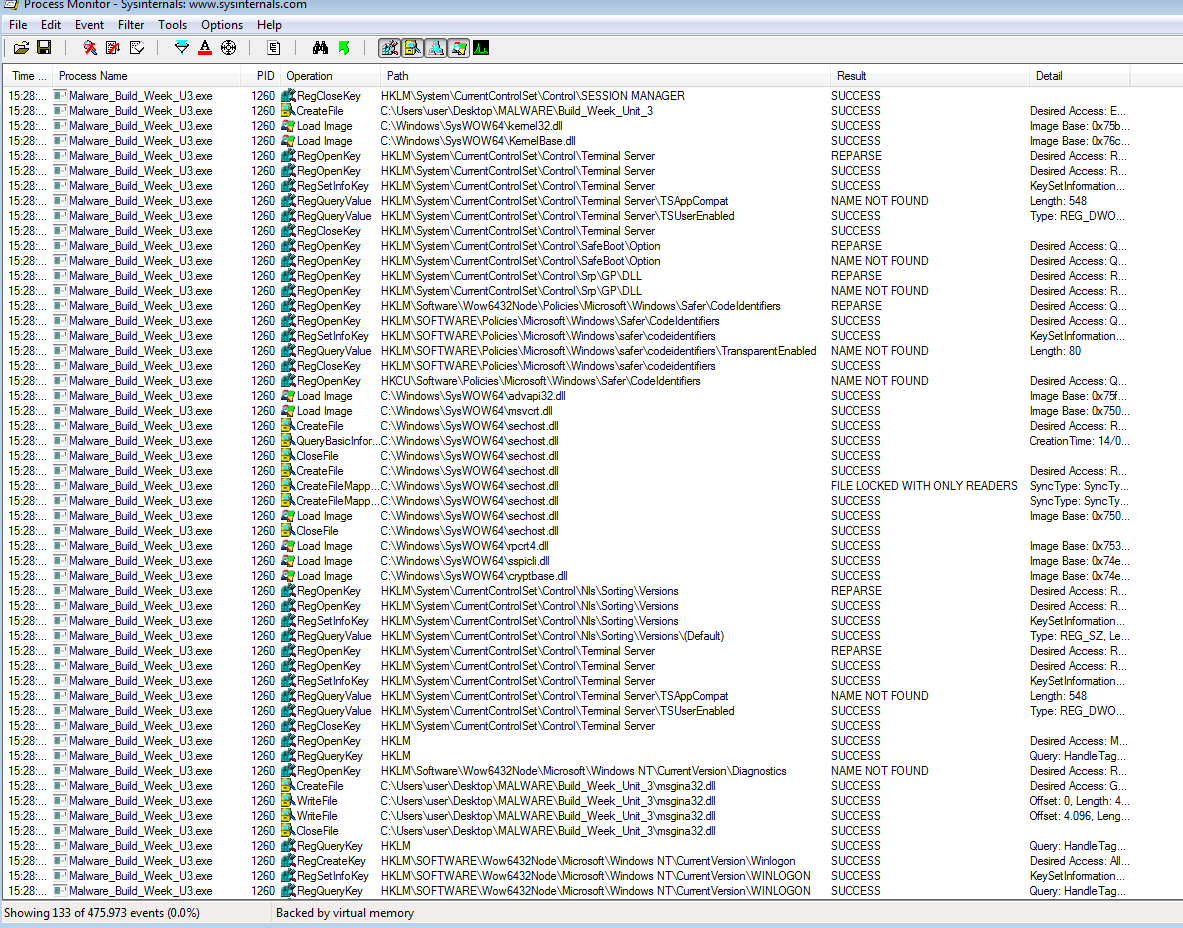
wireshark



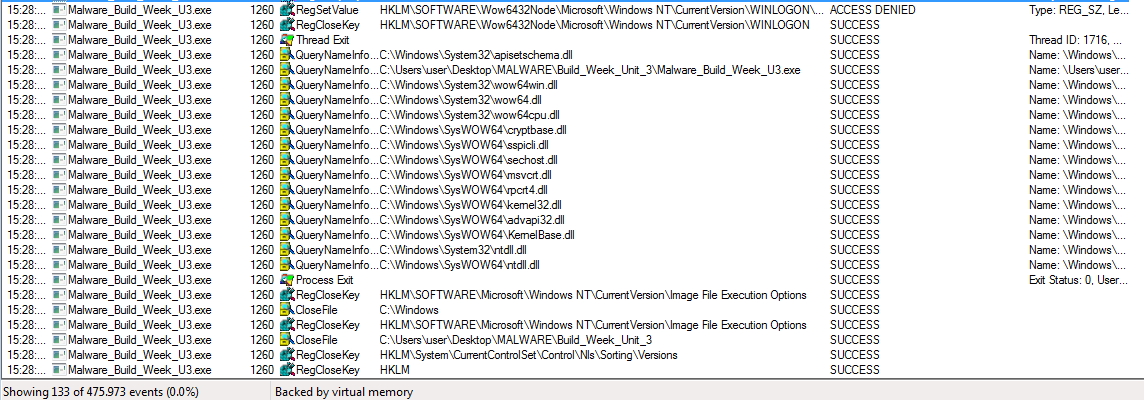
apate dns



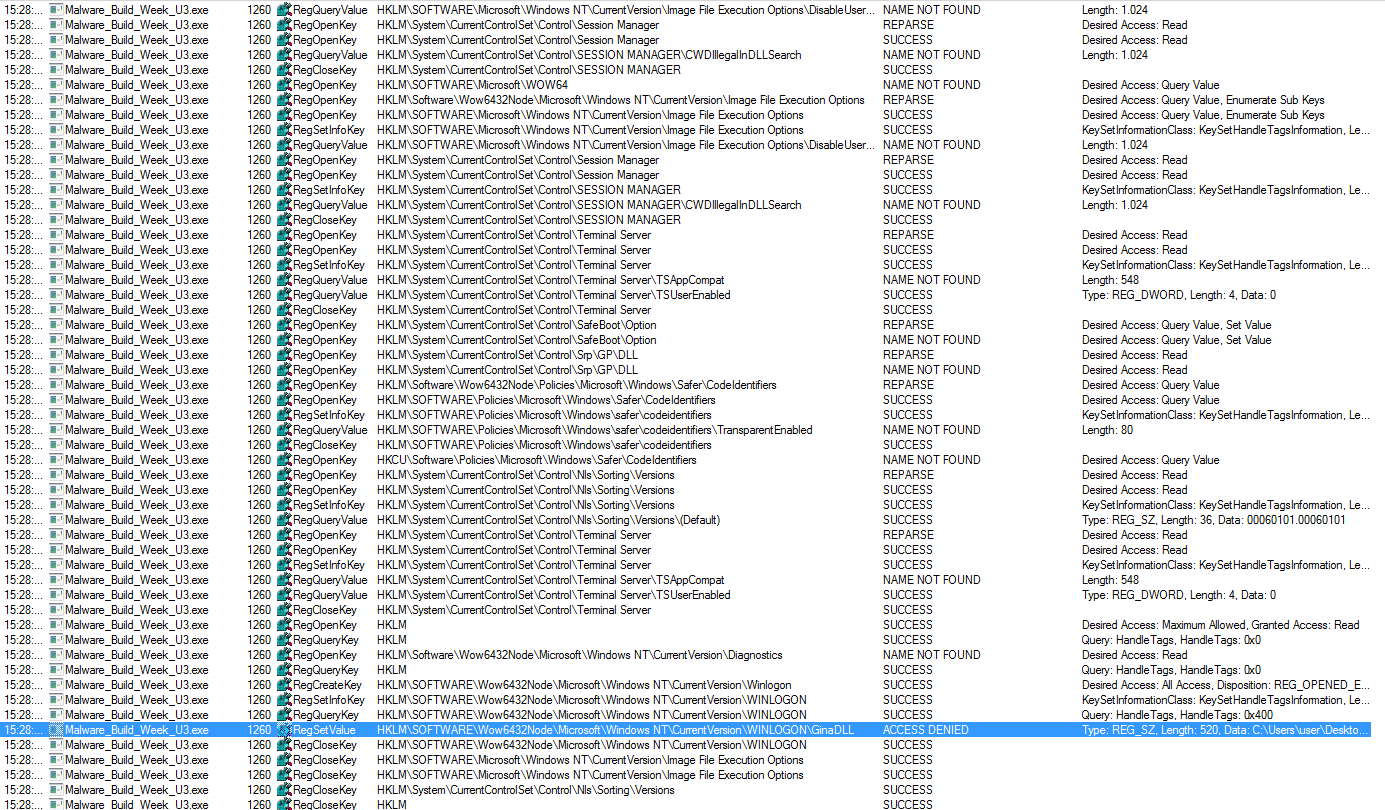
modifiche malware sul sistema 1



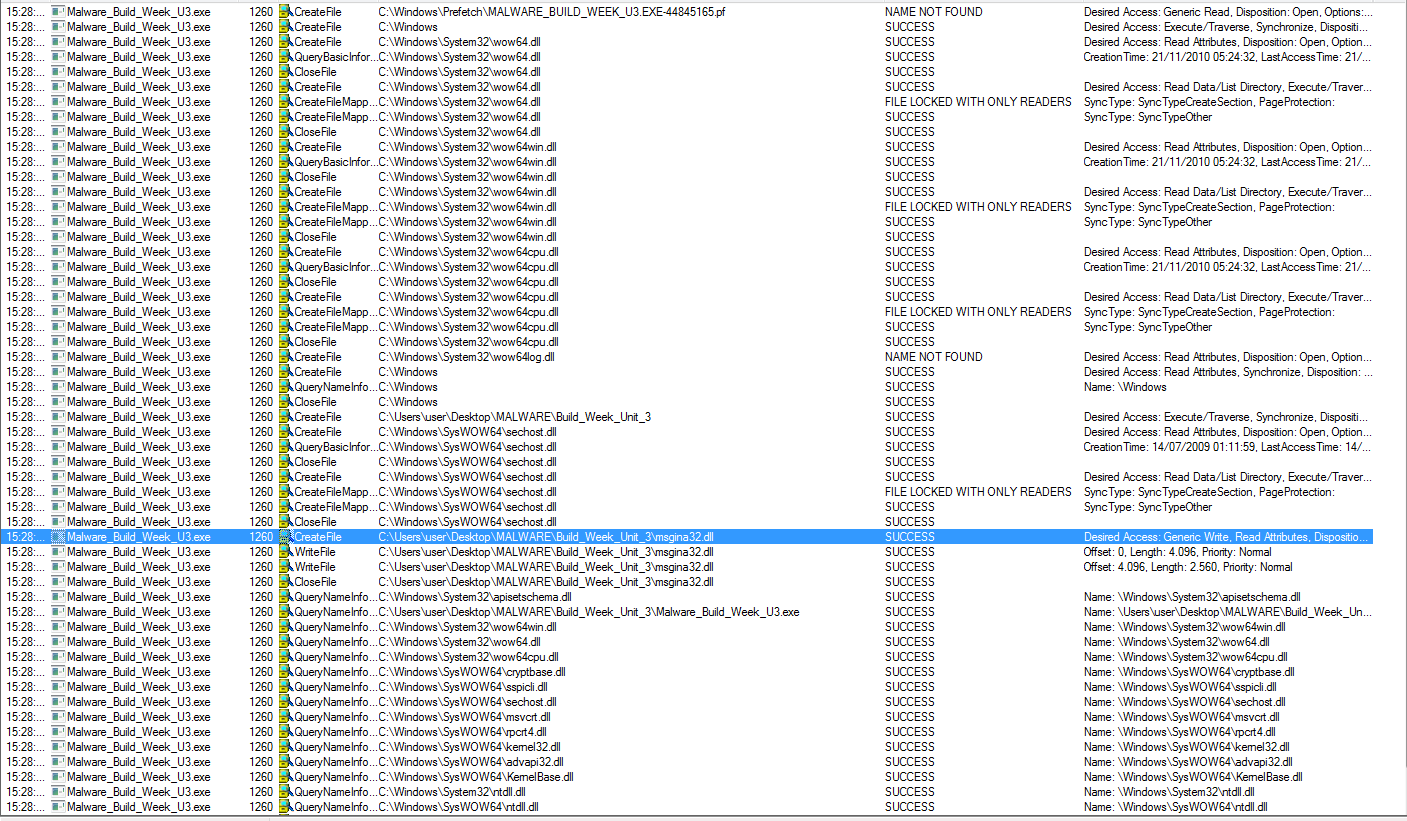
modifiche malware sul sistema 2



modifiche malware sul sistema 3



modifiche malware sul registro



modifiche malware sul file system