BWII:

TRACCIA 4

TRACCIA

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

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 ?

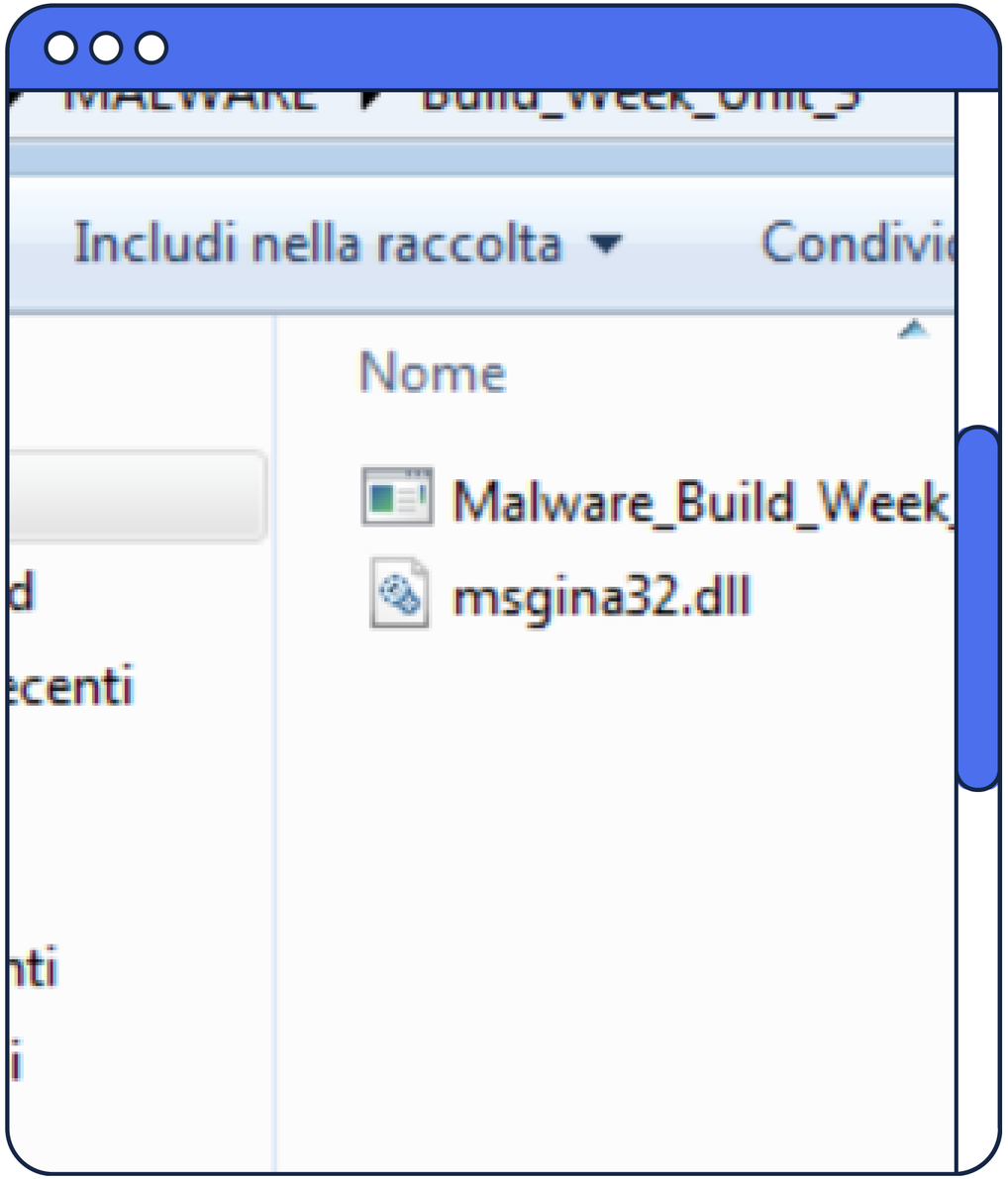
Unite tutte le informazioni raccolte fin qui sia dall’analisi statica che dall’analisi dinamica per delineare il funzionamento del Malware .

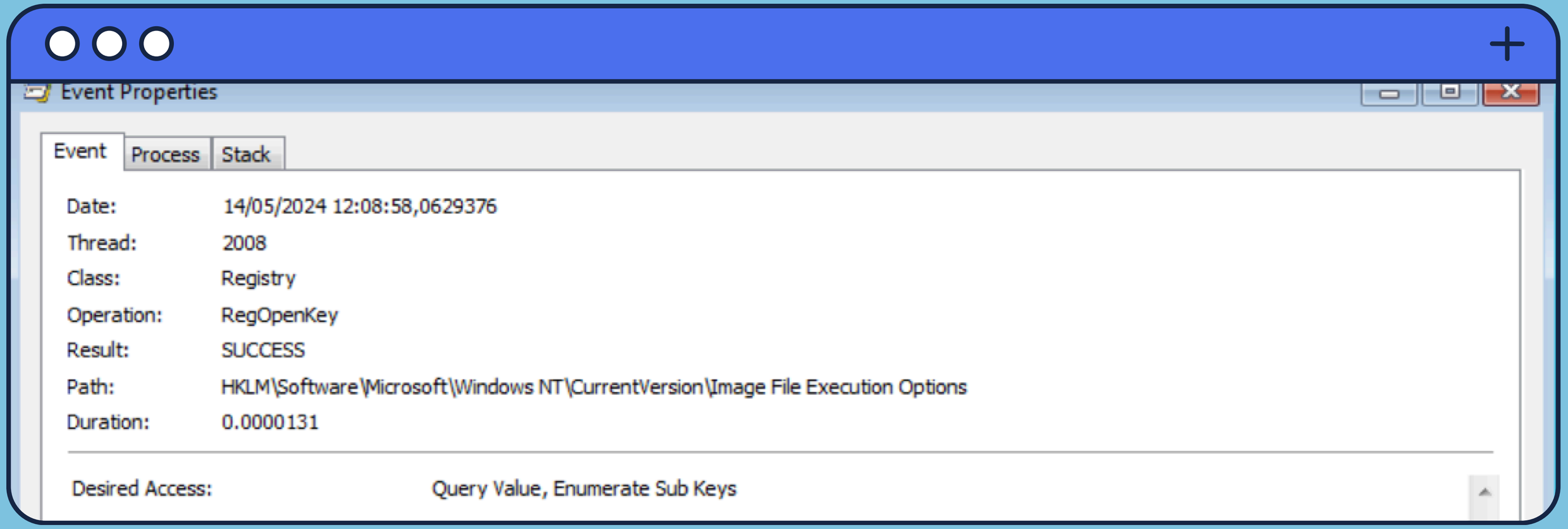
msgina32.dll

msgina.dll è un file di libreria a collegamento dinamico legittimo(DLL) e cruciale del sistema operativo Windows.
Fa parte del sottosistema di identificazione e autenticazione grafica (GINA) di Windows e svolge un ruolo fondamentale nel processo di accesso, come per esempio:

- Visualizzazione schermata di accesso
- Gestione credenziali utente
- Autenticazione utente

Nella cartella dove è presente il Malware una volta avviato lo stesso, viene creata un estensione chiamata “msgina32.dll un chiaro segnale di un attività malevola.
È molto probable che il malware abbia creato delle chiavi di registro per per memorizzare le proprie impostazioni e configurazioni e all'avvio del sistema crei l'estensione msgina.dll dannosa.





Avviato ProcessMonitor, filtrato il processo a noi interessato(Malware_Build_Week_U3), cerchiamo tra le “Operation” la funzione “RegOpenKey”, apriamo la finestra di eventi della funzione e ne deduciamo la chiave creata e il valore associato ad essa:

- La chiave di regitro creata è HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

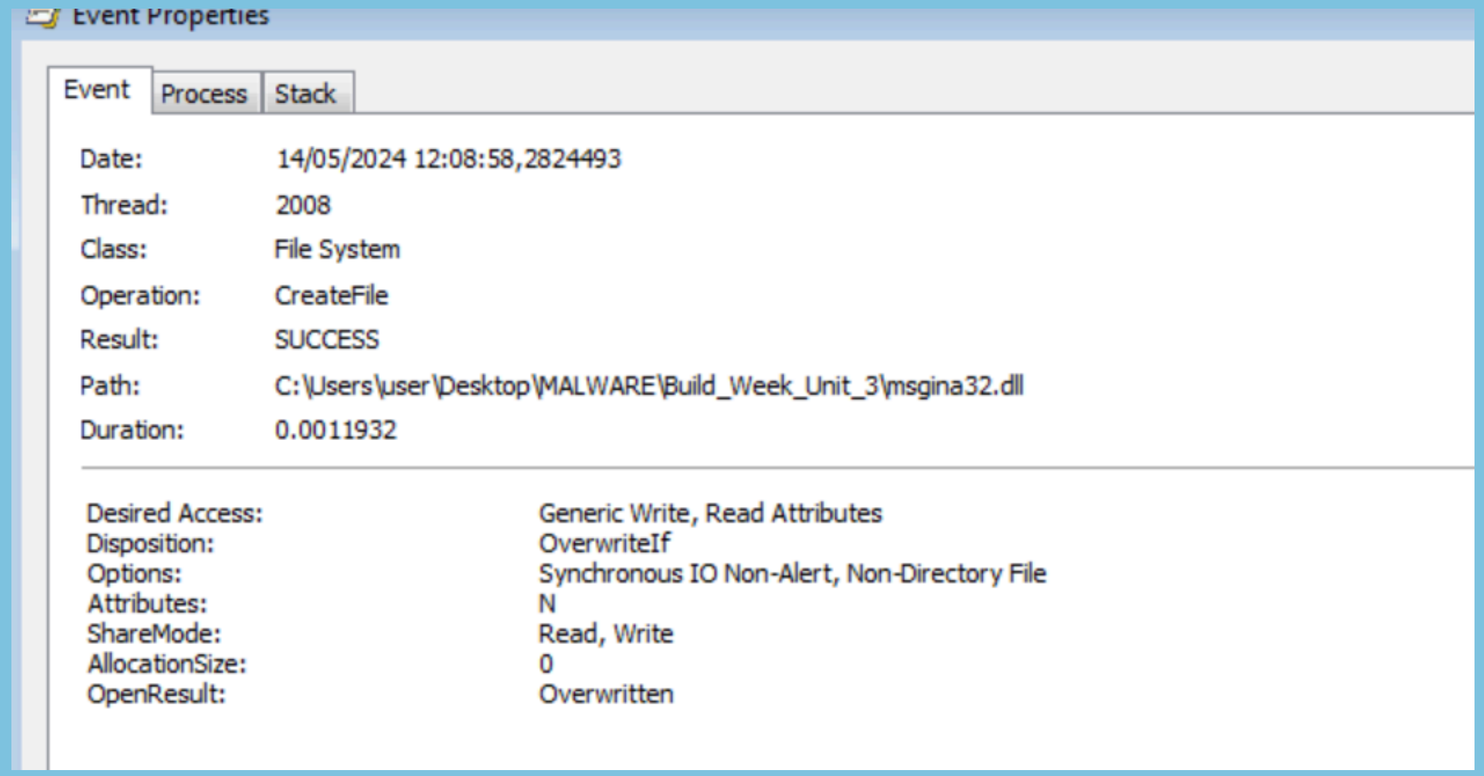
Da un analisi con Regshot siamo riusciti ad individuare che (come segue nelle slide successive):

- sono state aggiunte 2 keys nel registro HKEY_USER, aggiunti 25 valori all’interno della stessa e modificati 16 valori nel registro HKEY_LOCALMACHINE

```
---------------------------------
Keys added: 2
---------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\96\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\96\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
```

```
---------------------------------
Values modified: 16
---------------------------------
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastTime:  98 E2 2E 03 29 A1 DA 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastTime:  4E F6 44 31 A4 A6 DA 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\TransientValue:  49 2E BB 0F B0 4B 12 40
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\TransientValue:  9A D5 5A 72 F2 FC 13 40
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastCrimDataTime:  11 C4 3D 38 5A A0 DA 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastCrimDataTime:  86 DD 38 31 A4 A6 DA 01
```

```
Values added: 25
---------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shel
```



Come evidenziato in figura apriamo la finestra degli eventi per la funzione “CreateFile” vedendo il path, la funzione crea l’estensione “msgina.dll” all’interno della cartella \Malware\Build_Week_Unit_3\

CONCLUSIONI:

In conclusione dall’analisi statica e dinamica del Malware possiamo dedurre che:

- Analisi Statica: Da una prima analisi con CFF Explorer siamo riusciti a individuare quali librerie implementa il Malware(ADVAPI32.DLL e KERNEL32.DLL) e a vederne le funzioni e funzionalità che implementano, deducendo, che con ADVAPI32 instaura una persistenza all’interno del sistema Windows con le funzioni RegOpenKeyExA e RegCreateKeyExA come abbiamo visto in precedenza, mentre per la libreria KERNEL32, abbiamo ipotizzato che con funzioni tipo FindResouce, LoadResource e LockResource situate nella sezione .rsrc il Malware potrebbe essere un Dropper.
- Analisi Dinamica: Da una seconda analisi, grazie all’utilizzo di tool come ProcessMonitor una volta avviato il malware in un ambiente atto all’esecuzione, abbiamo potuto monitorare i processi dell’eseguibile visualizzando le attività dei registri e del file system come visto nelle slide precedenti, individuando la creazioni di chiavi di registro e la creazione dell’estensione msgina.dll all’interno della cartella Malware. Comprovando le nostre tesi iniziali.

GRAZIE PER L’ATTENZIONE