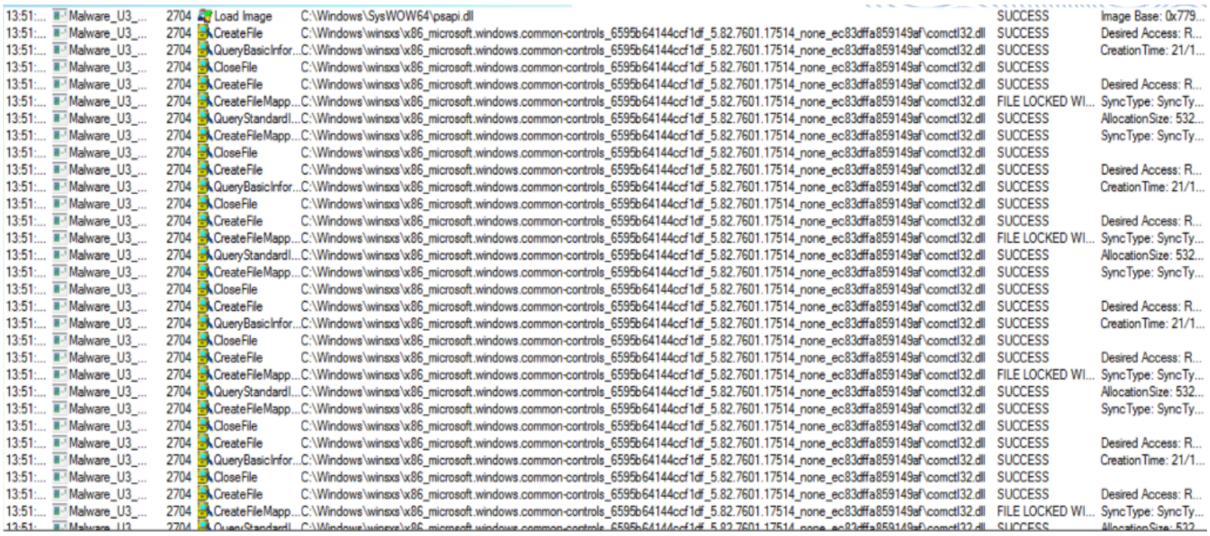
S10/L2

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:

- 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.

Per prima cosa configuriamo la macchina virtuale per l’analisi dinamica togliendo il flag su “abilita scheda di rete”e impostandola poi su rete interna. Inoltre deve essere disabilitata anche l’opzione di “abilita controller usb” per evitare che il malware si propaghi anche sulla macchina fisica. Creiamo poi un’istantanea della macchina virtuale nel suo stato iniziale, prima di iniziare tutte le analisi, in modo tale da ripristinarlo qualora ce ne fosse bisogno.

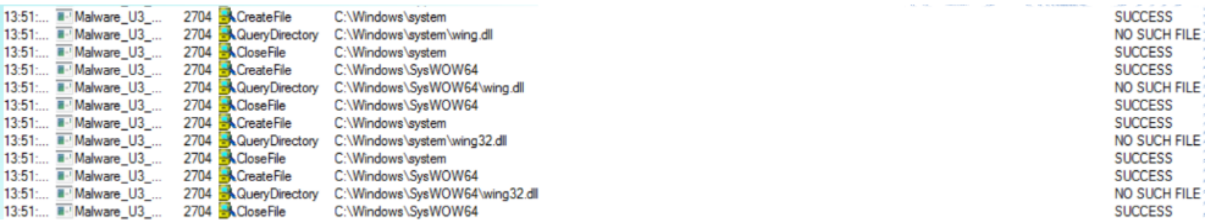
1.Eseguiamo il nostro malware, e andiamo ad analizzarlo tramite il tool “process monitor”, il quale ci permette, tra le altre cose, di  monitorare i processi ed i thread attivi sul sistema operativo.



```
13:51:... Malware_U3_...  2704 Load Image          C:\Windows\SysWOW64\psapi.dll                                                                                                SUCCESS            Image Base: 0x779...
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 QueryBasicInfor...  C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            CreationTime: 21/1...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  FILE LOCKED WI...  SyncType: SyncTy...
13:51:... Malware_U3_...  2704 QueryStandardI...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            AllocationSize: 532...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            SyncType: SyncTy...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 QueryBasicInfor...  C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            CreationTime: 21/1...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  FILE LOCKED WI...  SyncType: SyncTy...
13:51:... Malware_U3_...  2704 QueryStandardI...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            AllocationSize: 532...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            SyncType: SyncTy...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 QueryBasicInfor...  C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            CreationTime: 21/1...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  FILE LOCKED WI...  SyncType: SyncTy...
13:51:... Malware_U3_...  2704 QueryStandardI...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            AllocationSize: 532...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            SyncType: SyncTy...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 QueryBasicInfor...  C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            CreationTime: 21/1...
13:51:... Malware_U3_...  2704 CloseFile           C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS
13:51:... Malware_U3_...  2704 CreateFile          C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  SUCCESS            Desired Access: R...
13:51:... Malware_U3_...  2704 CreateFileMapp...   C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll  FILE LOCKED WI...  SyncType: SyncTy...
```

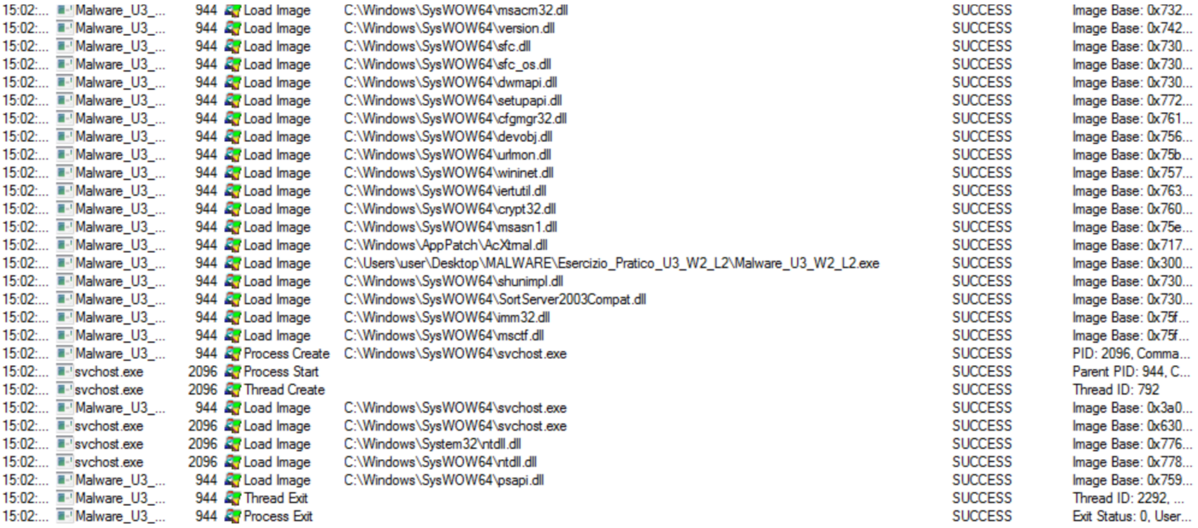
Andiamo a verificare le eventuali azioni del malware sul file system:

Notiamo subito la voce “create file”, ciò indica che il malware è riuscito a creare un nuovo file nel sistema, può dunque creare file per scopi dannosi come la persistenza, la diffusione (copiarsi su altri sistemi o dispositivi) o per archiviare dati sensibili rubati.



```
13:51:...  Malware_U3_...  2704  CreateFile      C:\Windows\system                    SUCCESS
13:51:...  Malware_U3_...  2704  QueryDirectory  C:\Windows\system\wing.dll           NO SUCH FILE
13:51:...  Malware_U3_...  2704  CloseFile       C:\Windows\system                    SUCCESS
13:51:...  Malware_U3_...  2704  CreateFile      C:\Windows\SysWOW64                  SUCCESS
13:51:...  Malware_U3_...  2704  QueryDirectory  C:\Windows\SysWOW64\wing.dll         NO SUCH FILE
13:51:...  Malware_U3_...  2704  CloseFile       C:\Windows\SysWOW64                  SUCCESS
13:51:...  Malware_U3_...  2704  CreateFile      C:\Windows\system                    SUCCESS
13:51:...  Malware_U3_...  2704  QueryDirectory  C:\Windows\system\wing32.dll         NO SUCH FILE
13:51:...  Malware_U3_...  2704  CloseFile       C:\Windows\system                    SUCCESS
13:51:...  Malware_U3_...  2704  CreateFile      C:\Windows\SysWOW64                  SUCCESS
13:51:...  Malware_U3_...  2704  QueryDirectory  C:\Windows\SysWOW64\wing32.dll       NO SUCH FILE
13:51:...  Malware_U3_...  2704  CloseFile       C:\Windows\SysWOW64                  SUCCESS
```

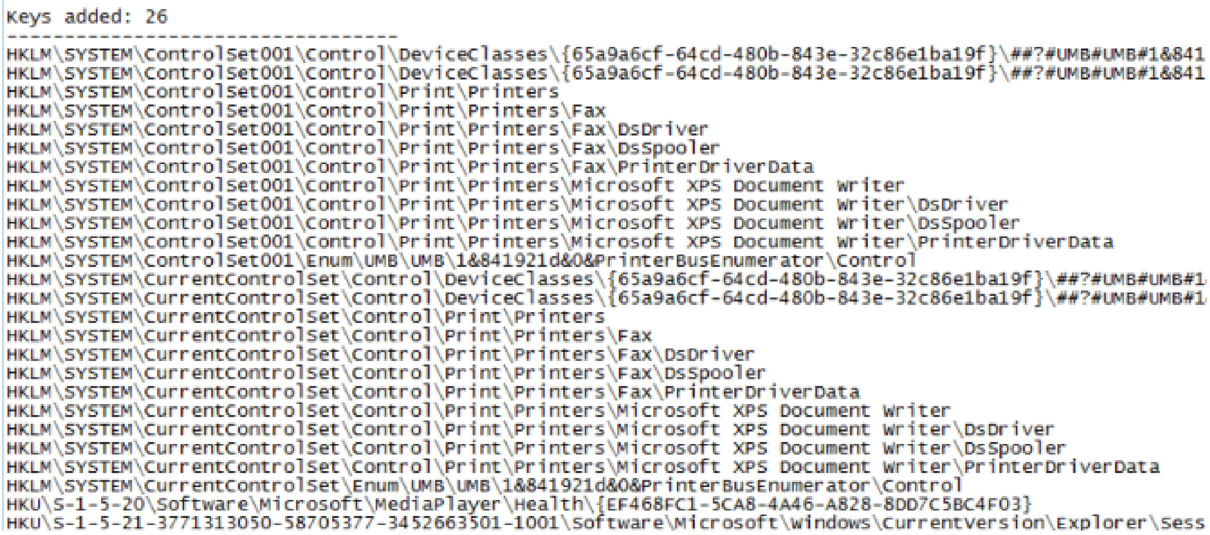
2.Vediamo ora le eventuali azioni su processi e thread:



```
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\msacm32.dll              SUCCESS  Image Base: 0x732...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\version.dll              SUCCESS  Image Base: 0x742...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\sfc.dll                  SUCCESS  Image Base: 0x730...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\sfc_os.dll               SUCCESS  Image Base: 0x730...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\dwmapi.dll               SUCCESS  Image Base: 0x730...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\setupapi.dll             SUCCESS  Image Base: 0x772...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\cfgmgr32.dll             SUCCESS  Image Base: 0x761...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\devobj.dll               SUCCESS  Image Base: 0x756...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\urlmon.dll               SUCCESS  Image Base: 0x75b...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\wininet.dll              SUCCESS  Image Base: 0x757...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\iertutil.dll             SUCCESS  Image Base: 0x763...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\crypt32.dll              SUCCESS  Image Base: 0x760...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\msasn1.dll               SUCCESS  Image Base: 0x75e...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\AppPatch\AcXtmal.dll              SUCCESS  Image Base: 0x717...
15:02:...  Malware_U3_...   944  Load Image      C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe  SUCCESS  Image Base: 0x300...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\shunimpl.dll             SUCCESS  Image Base: 0x730...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\SortServer2003Compat.dll SUCCESS  Image Base: 0x730...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\imm32.dll                SUCCESS  Image Base: 0x75f...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\msctf.dll                SUCCESS  Image Base: 0x75f...
15:02:...  Malware_U3_...   944  Process Create  C:\Windows\SysWOW64\svchost.exe              SUCCESS  PID: 2096, Comma...
15:02:...  svchost.exe     2096  Process Start                                                SUCCESS  Parent PID: 944, C...
15:02:...  svchost.exe     2096  Thread Create                                                SUCCESS  Thread ID: 792
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\svchost.exe              SUCCESS  Image Base: 0x3a0...
15:02:...  svchost.exe     2096  Load Image      C:\Windows\SysWOW64\svchost.exe              SUCCESS  Image Base: 0x630...
15:02:...  svchost.exe     2096  Load Image      C:\Windows\System32\ntdll.dll                SUCCESS  Image Base: 0x776...
15:02:...  svchost.exe     2096  Load Image      C:\Windows\SysWOW64\ntdll.dll                SUCCESS  Image Base: 0x778...
15:02:...  Malware_U3_...   944  Load Image      C:\Windows\SysWOW64\psapi.dll                SUCCESS  Image Base: 0x759...
15:02:...  Malware_U3_...   944  Thread Exit                                                  SUCCESS  Thread ID: 2292, ...
15:02:...  Malware_U3_...   944  Process Exit                                                 SUCCESS  Exit Status: 0, User...
```

Qui possiamo vedere eventuali processi creati dal malware, il quale può propagarsi sul sistema e renderlo non identificabile. Le funzioni sfruttate dai malware più comuni sono "Load Image" che indica il caricamento di un'immagine nel sistema per eseguire le sue funzionalità dannose. Ad esempio, potrebbe caricare una DLL malevola per compromettere il funzionamento del sistema o eseguire codice dannoso; e per l'esecuzione in memoria e attività sui processi e thread come Create Process e Create Thread che appunto servono per creare nuovi processi o thread all'interno di processi. Questi eventi associati a un malware, potrebbero indicare che il malware sta avviando nuovi processi o thread per eseguire le sue attività dannose, come ad esempio il furto di informazioni, l'esecuzione di codice dannoso o la persistenza nel sistema.

3.Per verificare le modifiche di registro dopo il malware, utilizziamo il tool "Regshot" attraverso due istantanee per poter controllare se il malware abbia modificato eventuali chiavi di registro. Le chiavi di registro sono le variabili di configurazione dei sistemi Windows e i valori delle chiavi rappresentano tutto ciò che viene caricato all'avvio del sistema. È molto frequente trovare malware che modificano le impostazioni dei sistemi operativi, e che quindi apportano dei cambiamenti ai valori delle chiavi di registro del sistema operativo.



```
Keys added: 26
----------------------------------
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841
HKLM\SYSTEM\ControlSet001\Control\Print\Printers
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax\DsDriver
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax\DsSpooler
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax\PrinterDriverData
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\DsDriver
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\DsSpooler
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\PrinterDriverData
HKLM\SYSTEM\ControlSet001\Enum\UMB\UMB\1&841921d&0&PrinterBusEnumerator\Control
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\DsDriver
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\DsSpooler
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\PrinterDriverData
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\DsDriver
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\DsSpooler
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\PrinterDriverData
HKLM\SYSTEM\CurrentControlSet\Enum\UMB\UMB\1&841921d&0&PrinterBusEnumerator\Control
HKU\S-1-5-20\Software\Microsoft\MediaPlayer\Health\{EF468FC1-5CA8-4A46-A828-8DD7C5BC4F03}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Sess
```

HKLM\system\controlset001\control\print\printers\fax → Questo percorso del registro indica una stampante fax. Potrebbe essere stato aggiunto dal malware se il malware ha installato o configurato una stampante fax virtuale per inviare o ricevere fax in modo fraudolento.

HKLM\system\currentcontrolset\control\print\printers\microsoft xps document writer: Questo percorso del registro indica una stampante virtuale Microsoft XPS Document Writer. Questa stampante viene di solito installata insieme al sistema operativo Windows e non è insolito trovarla nel registro. Tuttavia, la presenza o le modifiche a questa voce potrebbero essere un indicatore di attività anomale, come il tentativo del malware di interagire con la stampa o di modificare le impostazioni della stampante. Il servizio di spooler di stampa è responsabile della gestione dei lavori di stampa, inclusa la coda dei documenti da stampare e il loro invio alla stampante. La presenza di questa voce nel registro di sistema potrebbe indicare che il malware ha effettuato modifiche o ha interagito con il servizio di stampa del sistema operativo. Questo potrebbe essere un comportamento sospetto, poiché il malware potrebbe cercare di interrompere o manipolare il servizio di stampa per nascondere le proprie attività o per compromettere il normale funzionamento del sistema.

4.Profilare un malware in base alla correlazione tra le operazioni e i percorsi dei file utilizzando Process Monitor può essere un metodo efficace per comprendere il comportamento del malware e identificare eventuali attività sospette o dannose. Una volta avviato process monitor, utilizziamo i filtri per concentrarci sulle attività correlate al malware, vediamo le eventuali operazioni (come per esempio la creazione del file) ed esaminiamo poi il percorso dei file coinvolti nelle operazioni del malware. Questi percorsi possono fornire indicazioni su dove il malware si trova nel sistema e su quali risorse sta cercando di accedere o compromettere. Vediamo dunque che il malware sta operando nel file system, dobbiamo dunque cercare correlazioni tra le operazioni eseguite dal malware e i percorsi dei file coinvolti. Ad esempio, potremmo notare che il malware crea o modifica file eseguibili solo in una determinata directory.