Compito 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 sui 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.

Esercizio

Innanzitutto cerchiamo di capire a cosa servono gli eventi catturati con la nostra analisi dinamica.

Registri: gli eventi catturati permettono di controllare se il malware ha 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. Spesso capita di incontrare malware che modificano le chiavi di registro al fine di essere avviati automaticamente appena avviato il sistema.

File System: gli eventi di questa categoria permettono di monitorare e controllare tutte le interazioni tra il malware il file system come ad esempio: la creazione di un nuovo file, l'eliminazione di un file, la modifica di un file e così via. Generalmente queste attività sono supportate da «operation» quali Create File, Read File, Close File e così via.

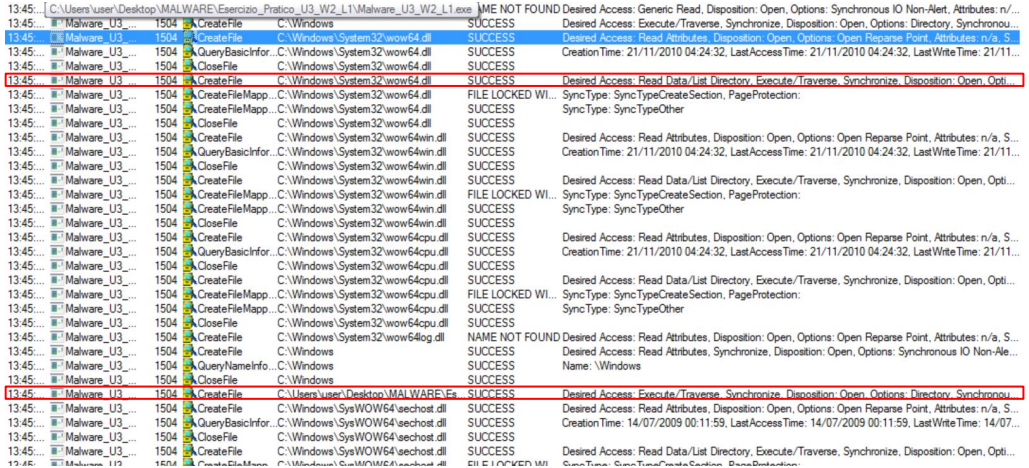
Esercizio

Processi: gli eventi di questa categoria aiutano ad identificare eventuali processi addizionali creati dal malware per propagarsi sul sistema o per rendere se stesso non identificabile. Alcuni malware infatti, tendono a creare nuovi processi con nomi piuttosto comuni oppure apparentemente innocui in modo tale da non destare sospetto sui sistemi vittima. Le funzioni sfruttate dai malware più comuni sono «LoadImage» per caricare eseguibili e librerie per esecuzione in memoria e attività sui processi e Thread Come Create Process, Create Thread Che appunto servono per creare nuovi processi o thread all'interno di processi.

Rete: le attività di questa categoria sono particolarmente importanti per monitorare il traffico generato dal malware verso internet e verso la rete interna. La maggior parte dei malware presenta attività di rete abbastanza marcate, che vanno dall'invio di file verso web server remoti, alla connessione verso domini infetti, fino alla creazione di backdoor.

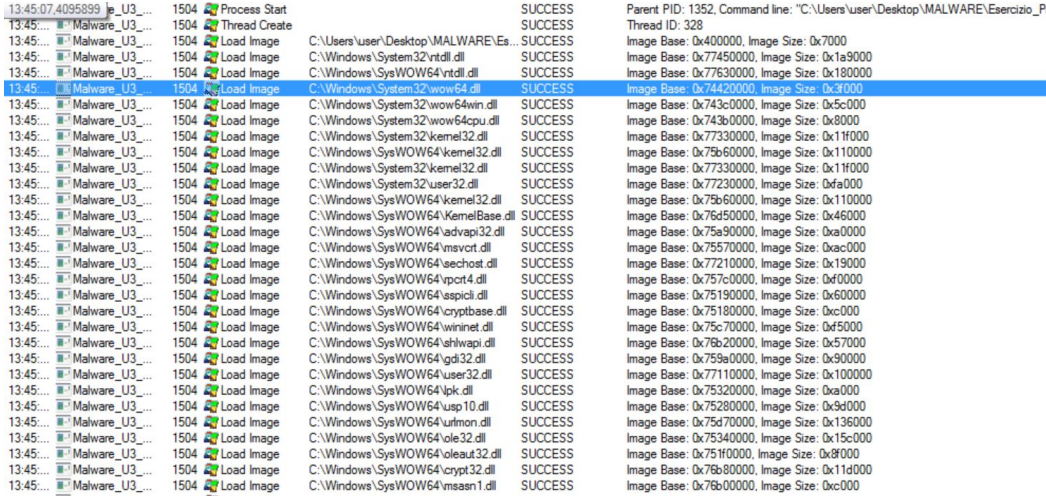
Esercizio

Il primo punto ci chiede di analizzare il file system. Ho utilizzato un filtro per cercare il malware più facilmente. Possiamo notare, in particolare, che cerca di creare dei file nella cartella system32 di Windows, ma anche nella sua stessa cartella originale.



Esercizio

Il secondo punto mi chiede di analizzare i processi e i thread. Come possiamo notare, questo malware sta creando un thread nella seconda riga e successivamente esegue uno spam di load image per caricare varie librerie.



13:45:07.4095899	e_U3_...	1504	Process Start	SUCCESS	Parent PID: 1352, Command line: "C:\Users\user\Desktop\MALWARE\Esercizio_P
13:45:...	Malware_U3_...	1504	Thread Create	SUCCESS	Thread ID: 328
13:45:...	Malware_U3_...	1504	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400000, Image Size: 0x7000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77450000, Image Size: 0x1a9000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77630000, Image Size: 0x180000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74420000, Image Size: 0x3f000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x743c0000, Image Size: 0x5c000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x743b0000, Image Size: 0x8000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77330000, Image Size: 0x11f000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75b60000, Image Size: 0x110000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77330000, Image Size: 0x11f000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77230000, Image Size: 0xfa000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75b60000, Image Size: 0x110000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x76d50000, Image Size: 0x46000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x75a90000, Image Size: 0xa0000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x75570000, Image Size: 0xac000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x77210000, Image Size: 0x19000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x757c0000, Image Size: 0xf0000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x75190000, Image Size: 0x60000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x75180000, Image Size: 0xc000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x75c70000, Image Size: 0xf5000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x76b20000, Image Size: 0x57000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x759a0000, Image Size: 0x90000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x77110000, Image Size: 0x100000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\lpk.dll	SUCCESS	Image Base: 0x75320000, Image Size: 0xa000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\usp10.dll	SUCCESS	Image Base: 0x75280000, Image Size: 0x9d000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Image Base: 0x75d70000, Image Size: 0x136000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x75340000, Image Size: 0x15c000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x751f0000, Image Size: 0x8f000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x76b80000, Image Size: 0x11d000
13:45:...	Malware_U3_...	1504	Load Image	C:\Windows\SysWOW64\msasn1.dll	SUCCESS	Image Base: 0x76b00000, Image Size: 0xc000

Esercizio

Infine, notiamo che dopo aver caricato le librerie, il malware ha creato ulteriori thread per poi terminarli.

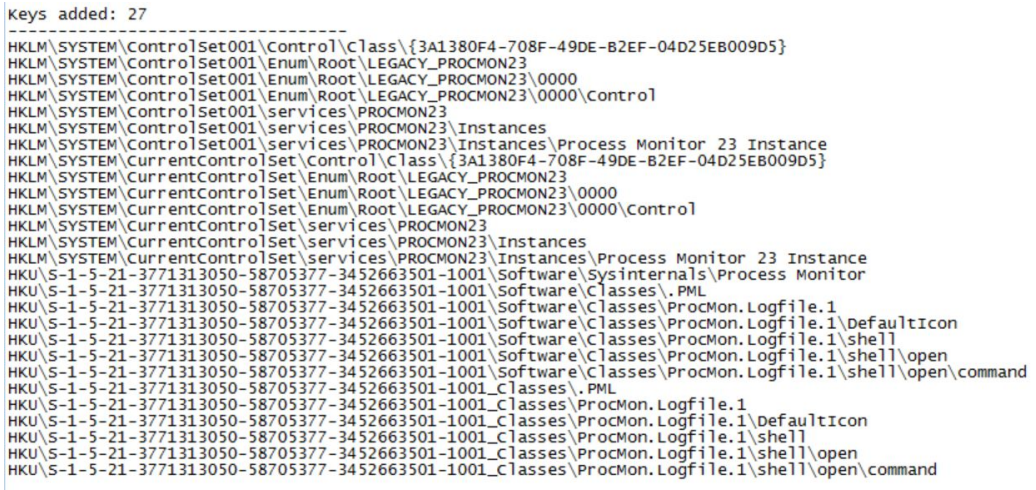
Esercizio

Per quanto riguarda il terzo punto, è importante notare che i nomi delle categorie delle chiavi di registro sono spesso abbreviati come segue:

- **HKEY_CURRENT_USER** diventa **HCU:** include le impostazioni e preferenze di sistema dell'utente che è attualmente connesso alla macchina.
- **HKEY_LOCAL_MACHINE** diventa **HKLM:** include le impostazioni comuni per tutti gli utenti del sistema indipendentemente dalle loro preferenze.
- **HKEY_USERS** diventa **HKU:** raggruppa le impostazioni di tutti gli utenti connessi al sistema.

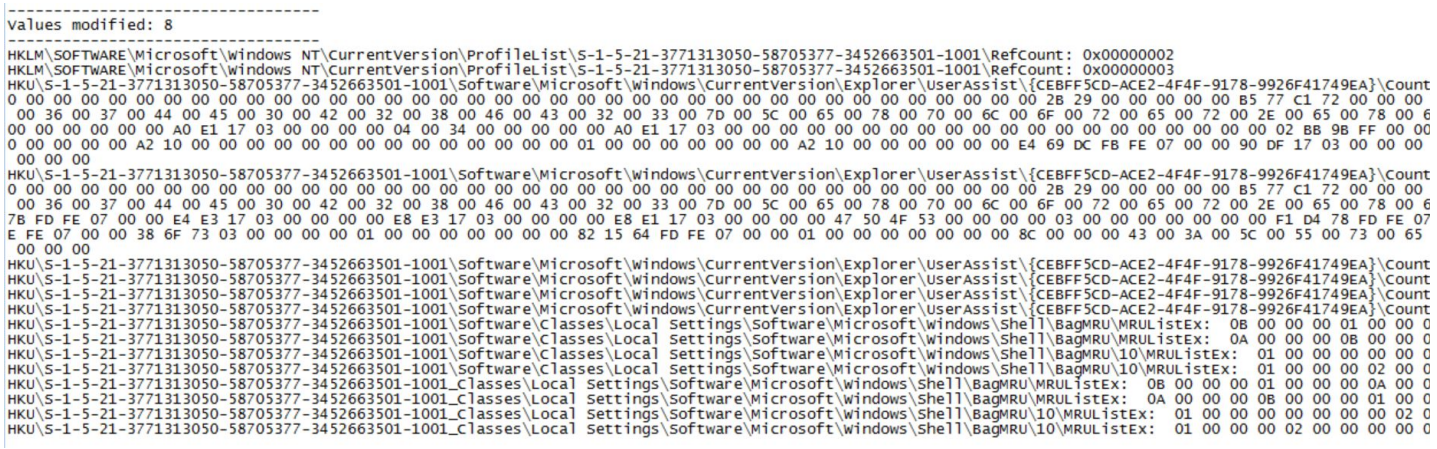
Esercizio

Nel registro, possiamo notare che in questa foto sono state aggiunte 27 chiavi a destra. Tuttavia, la maggior parte di esse appartiene a ProcMon (il software di prima) e non al malware, quindi possiamo proseguire.



Esercizio

Qui, sono stati modificati 8 valori, con alterazioni su file sospetti come ProifileList e diverse shell, oltre ad alcuni userAssist. Pertanto, se devo dare un profilo a questo malware, direi che si tratta di un Trojan o Spyware, poiché sembra raccogliere informazioni da un computer senza il consenso dell'utente. Inoltre, con le modifiche alle shell, potrebbe registrare tasti, monitorare attività online o raccogliere altre informazioni personali. (Voglio precisare che ho utilizzato il malware L1 dato che L2 mi dava un errore).



```
----------------------------------
Values modified: 8
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3771313050-58705377-3452663501-1001\RefCount: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3771313050-58705377-3452663501-1001\RefCount: 0x00000003
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2B 29 00 00 00 00 00 B5 77 C1 72 00 00 00
 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 65 00 78 00 6
00 00 00 00 00 00 A0 E1 17 03 00 00 00 00 04 00 34 00 00 00 00 00 A0 E1 17 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 BB 9B FF 00 00
0 00 00 00 00 A2 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 A2 10 00 00 00 00 00 00 E4 69 DC FB FE 07 00 00 90 DF 17 03 00 00 00
 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2B 29 00 00 00 00 00 B5 77 C1 72 00 00 00
 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 65 00 78 00 6
7B FD FE 07 00 00 E4 E3 17 03 00 00 00 00 E8 E3 17 03 00 00 00 00 E8 E1 17 03 00 00 00 00 47 50 4F 53 00 00 00 00 03 00 00 00 00 00 00 00 F1 D4 78 FD FE 07
E FE 07 00 00 38 6F 73 03 00 00 00 00 01 00 00 00 00 00 00 00 82 15 64 FD FE 07 00 00 01 00 00 00 00 00 00 00 8C 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65
 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0B 00 00 00 01 00 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0A 00 00 00 0B 00 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\MRUListEx:  01 00 00 00 00 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\MRUListEx:  01 00 00 00 02 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0B 00 00 00 01 00 00 00 0A 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0A 00 00 00 0B 00 00 00 01 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\MRUListEx:  01 00 00 00 00 00 00 00 02 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\MRUListEx:  01 00 00 00 02 00 00 00 00 0
```