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.

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.

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.

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.

1345 ■ Mahvare U3 1504 Acceptable Control of College	13:45:				ratico_U3_W2_L1\Malware_U3_W2_L1.ex	XE ME NOT FOUND	D Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/
3.45							Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronou
3.45 Mahvare U3 1504 More Part 1504 Mor							Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S
13.45 Malware U3 1504 A Create File C. Windows System 32 wow64 dil File C. C. Windows System 32 wow64 dil SUCCES Sync Type: Sync Type Other Sync Type: Sync Type Other Sync Type: Sync Type	13:45:	Malware_U3					Creation Time: 21/11/2010 04:24:32, LastAccess Time: 21/11/2010 04:24:32, LastWrite Time: 21/11
3.45. Malware U3							
3.45 Makware U3 1504 A.CoseFie C.Windows System32 wow64 dtl SUCCES SyncType: SyncTypeOther Syn	13:45:	■ Malware U3			C:\Windows\System32\wow64.dll		Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Opti
3.45 Mahvare U3 1504 A.CoseFile C. Windows System32 wow64-dil SUCCES Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Read Attributes, Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success Success Read Attributes, Disposition: Open, Options: Open Repairse Point, Attributes: n/o Success							SyncType: SyncTypeCreateSection, PageProtection:
3.45. Mahvare, U.3. 1504 A.Cueyeffelic C.Windows System32/wow64win dl SUCCESS Desired Access Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: m/s 21, 1420 10 424.32, Last Access Time: 21/11/2010 04.24.32, Last Acc	13:45:	Malware_U3					SyncType: SyncTypeOther
3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl S.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl S.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl S.Cosefie C.Windows System32 wow64win dl 3.45 Mahware U3 504 A.Cosefie C.Windows System32 wow64win dl S.Cosefie C.Windows System32 wow64win dl S.Cosefie C.Windows System32 wow64win dl A.Cosefie C.Windows System32 wow64win dl S.Cosefie	13:45:	Malware_U3			C:\Windows\System32\wow64.dll		
3.45. Mahvare_U3_ 1504 ACreateFiel C-Windows System 32 wow64vin_dl SUCCES 3.45. Mahvare_U3_ 1504 ACreateFiel C-Windows System 32 wow64vin_dl 3.45. Mahvare_U3_ 1504 ACreateFiel C-Windows System							Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S
3.45. Makware, U.3. 1504 A.CreateFile C.Windows (System32/wow64win dl 13.45. Makware, U.3. 1504 A.CreateFile C.Windows (System32/wow64cpu dl A.CreateFile C.Windows (System32/wow64cpu dl 13.45. Makware, U.3. 1504 A.CreateFile C.Windows (System32/wow64cpu dl A.CreateFile C.Windows (System32/wow64cpu dl 13.45. Makware, U.3. 1504 A.CreateFile C.Windows (System32/wow64cpu dl 13							Creation Time: 21/11/2010 04:24:32, LastAccess Time: 21/11/2010 04:24:32, LastWrite Time: 21/11
3.45 Mahvare U.3 1504 A.CreateFielkapp. C.Windows System 32 wow64win dl					C:\Windows\System32\wow64win.dll		
3.45. Malware U.3 1504 Acceste File Mapp. C. Windows System 32 wow64our dl SUCCES 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl SUCCES 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl SUCCES 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl SUCCES 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl SUCCES 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.3 1504 Acceste File C. Windows System 32 wow64our dl 3.45. Malware U.							Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Opti
3.45 Makware U3							SyncType: SyncTypeCreateSection, PageProtection:
13.45. Malware, U3. 1504 Acceste File C.Windows (System32)wow64cpu.dl SUCCESS	13:45:	Malware_U3			C:\Windows\System32\wow64win.dll		SyncType: SyncTypeOther
13.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File Mapp. C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File Mapp. C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File Mapp. C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File Mapp. C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System 32 work-facpu dl 3.45. ■ Malware, U.3. 1504 ACaser File C. Windows System Sys							
3.45. Malware_U3_ 1504 CaseFile C.\Windows\System32\wow64cpu_dl SUCCES 3.45. Malware_U3_ 1504 CaseFile C.\Windows\System32\wow64cpu_dl SUCCES 3.45. Malware_U3_ 1504 CaseFile C.\Windows\System32\wow64cpu_dl SUCCES SUCCES 3.45. Malware_U3_ 1504 CaseFile MappC.\Windows\System32\wow64cpu_dl SUCCES 3.45. Malware_U3_ 1504 CaseFile C.\Windows\System32\wow64cpu_dl							
13.45. ■ Malware, U.3. 1504							Creation Time: 21/11/2010 04:24:32, LastAccess Time: 21/11/2010 04:24:32, LastWrite Time: 21/11
3.45							
13.45. ■ Malware U3. 1504 CreateFile Mapp. C.Windows (System32/wow64cpu dl sUCCESS SyncType; Sy							
3.45 ■ Malware_U3_ 1504							
3.45.	13:45:	Malware_U3					SyncType: SyncTypeOther
13.45 ■ Malware_U3_ 1504							
13.45. ■ Malware, U.3. 1504 Access: Read Attributes, Disposition: Open, Options: Directory, Synchronize, Disposition: Open, Open, Options: Directory, Synchronize, Disposition: Open, Open, Open, Options: Directory, Synchronize, Disposition: Open,							
3.45. ■ Malware_U3 1504 CoseFile C:\Windows SUCCESS Success							
13.45. ■ Malvare, U3. 1504 ACreateFile C.\Linear\user\Desirco\MalkUARE\User\S SUCCESS Desired Access: Resorter/Traverse, Sunchronize, Disposition: Open Options: Directory, Synchronize, Disposition: Open Option							Name: \Windows
13.45 Malware_U3 1504 CreateFile C:\Windows\SysWOW64'sechost.dll SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a Creation Time: 14/07/2009 00:11:59, LastAccess Time: 14/07/2009 00:11:59, LastAcce							THE STATE OF THE S
13.45 ■ Malware_U3 1504 ■ QueryBasicInforC.\Windows\SysWOW64sechost.dll SUCCESS 1505 ■ QueryBasicInfor 1505 ■ QueryBasicInfor 1505 ■ QueryBasicInfor 1505 ■ Que							
13.45 Malware_U3 1504 Access C.\Windows\SysWOW64\sechost.dll SUCCESS 13.45 Malware_U3 1504 Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open. Open. Op							
13:45 Im Malware U3 1504 AcreateFile C:\Windows\Sys\WOW64\sechost.dll SUCCESS Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Op							CreationTime: 14/07/2009 00:11:59, LastAccessTime: 14/07/2009 00:11:59, LastWriteTime: 14/07
The second secon	12-45-	Mahuam 112	1504	Create EleMann	C:\Mindows\CvaMOMEA\eachost dll	EILE I UUNEU MI	CompTime: CompTimeCompteCaption DanaDoptection

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 R Process Start		SUCCESS	Parent PID: 1352, Command line: "C:\Users\user\Desktop\MALWARE\Esercizio_F
13:45: I Malware_U3	1504 R Thread Create		SUCCESS	Thread ID: 328
13:45: Malware_U3	1504 R Load Image	C:\Users\user\Desktop\MALWARE\Es.	SUCCESS	Image Base: 0x400000, Image Size: 0x7000
13:45: Malware_U3	1504 R Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77450000, Image Size: 0x1a9000
13:45: Malware_U3	1504 R 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\kemel32.dll	SUCCESS	Image Base: 0x77330000, Image Size: 0x11f000
13:45: Malware_U3	1504 🥞 Load Image	C:\Windows\SysWOW64\kemel32.dll	SUCCESS	Image Base: 0x75b60000, Image Size: 0x110000
13:45: Malware_U3	1504 R Load Image	C:\Windows\System32\kemel32.dll	SUCCESS	Image Base: 0x77330000, Image Size: 0x11f000
13:45: Malware_U3	1504 R Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77230000, Image Size: 0xfa000
13:45: Malware_U3	1504 🧗 Load Image	C:\Windows\SysWOW64\kemel32.dll	SUCCESS	Image Base: 0x75b60000, Image Size: 0x110000
13:45: Malware_U3	1504 🎎 Load Image	C:\Windows\SysWOW64\KemelBase.dl		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

SUCCESS

SUCCESS

Image Base: 0x751f0000, Image Size: 0x8f000

Image Base: 0x76b00000, Image Size: 0xc000

Image Base: 0x76b80000, Image Size: 0x11d000

C:\Windows\SysWOW64\oleaut32.dll

C:\Windows\SysWOW64\crypt32.dll

C:\Windows\SysWOW64\msasn1.dll

13:45:... Malware_U3_... 1504 2 Load Image

13:45:... Malware_U3_... 1504 2 Load Image

13:45:... Malware U3 ... 1504 & Load Image

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

45: Maiware_U3	1004 🙀 Inread Create
45:07,6732623 e_U3	1504 R Thread Create
45: Malware_U3	1504 Thread Create
45: Malware_U3	1504 Thread Create
45: Malware_U3	1504 R Thread Create
45: Malware_U3	1504 R Thread Create
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 R Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 A Thread Exit
45: Malware_U3	1504 Thread Exit
45: Malware_U3	1504 Thread Exit
AE: Mahuam 112	1504 Throad Euit

SUCCESS	Inread ID: 1824
SUCCESS	Thread ID: 1660
SUCCESS	Thread ID: 1860
SUCCESS	Thread ID: 2980
SUCCESS	Thread ID: 2312
SUCCESS	Thread ID: 1976
SUCCESS	Thread ID: 1640, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 2948, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 2984, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 3056, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 2924, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 2332, User Time: 0.0000000, Kernel T
SUCCESS	Thread ID: 536, User Time: 0.0000000, Kernel Tin
SUCCESS	Thread ID: 2568, User Time: 0.0000000, Kernel T
SUCCESS	Thread ID: 552, User Time: 0.0000000, Kernel Tin
SUCCESS	Thread ID: 2084, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 532, User Time: 0.0000000, Kernel Tin
SUCCESS	Thread ID: 952, User Time: 0.0000000, Kernel Tin
SUCCESS	Thread ID: 3004, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 1316, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 2140, User Time: 0.0000000, Kernel Ti
SUCCESS	Thread ID: 1824, User Time: 0.0000000, Kernel T
CITCCECC	Thread In: 1000 Hear Time: 0 0000000 Kemel Ti

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.

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.

```
Kevs added: 27
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\ControlSet001\services\PROCMON23
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances\Process Monitor 23 Instance
HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances\Process Monitor 23 Instance
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Sysinternals\Process Monitor
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\.PML
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\ProcMon.Logfile.1
HKU\5-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\ProcMon.Logfile.1\Defaulticon
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\ProcMon.Logfile.1\shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\ProcMon.Logfile.1\shell\open
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\ProcMon.Logfile.1\shell\open\command
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_classes\.PML
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_classes\ProcMon.Logfile.1
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\ProcMon.Logfile.1\DefaultIcon
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\ProcMon.Logfile.1\shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\ProcMon.Logfile.1\shell\open
HKU\5-1-5-21-3771313050-58705377-3452663501-1001_classes\ProcMon.Logfile.1\shell\open\command
```

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 HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 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 HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 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 78 FD FE 07 00 00 E4 E3 17 03 00 00 00 00 E8 E3 17 03 00 00 00 00 E8 E3 17 03 00 00 00 08 E1 17 03 00 00 00 04 7 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 00 082 15 64 FD FE 07 00 00 01 00 00 00 00 00 8C 00 00 043 00 3A 00 5C 00 55 00 73 00 65 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\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\COUNT\|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\MRULISTEX: 0B 00 00 00 10 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\NRULISTEX: 0D 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\10\MRULISTEX: 0D 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\NRULISTEX: 0D 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\MRULISTEX: 0D 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\MRULISTEX: 0D 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\MRULISTEX: 0D 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Microsoft\windows\Shell\BagMRU\MRULISTEX: 0D 00 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Wicrosoft\windows\Shell\BagMRU\NRULISTEX: 0D 00 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Wicrosoft\windows\Shell\BagMRU\NRULISTEX: 0D 00 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Wicrosoft\windows\Shell\BagMRU\NRULISTEX: 0D 00 00 00 00 \|
| HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settlings\Software\Wicrosoft\Win 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 00