

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 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.

Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\Prefetch\MALWARE_U3_...	NAME NOT FOUND	Desired Access: G...
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 21/1...
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
14:37:...	Malware_U3_...	1588	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/1...
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
14:37:...	Malware_U3_...	1588	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/1...
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
14:37:...	Malware_U3_...	1588	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
14:37:...	Malware_U3_...	1588	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
14:37:...	Malware_U3_...	1588	CloseFile	C:\Windows	SUCCESS	
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\SysWOW64	SUCCESS	Desired Access: E...
14:37:...	Malware_U3_...	1588	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...

Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
14:37:...	Malware_U3_...	1588	Process Start		SUCCESS	Parent PID: 520, C...
14:37:...	Malware_U3_...	1588	Thread Create		SUCCESS	Thread ID: 1168
14:37:...	Malware_U3_...	1588	Load Image	C:\Users\Admin\Desktop\MALWARE\...	SUCCESS	Image Base: 0x400...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x773...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74f...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x74f...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x750...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x771...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x751...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x771...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x772...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x751...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x76c...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x757...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x771...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x766...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\vpct4.dll	SUCCESS	Image Base: 0x76f...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x751...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x751...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x76e...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x76d...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x76a...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x76b...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\pk.dll	SUCCESS	Image Base: 0x759...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\usp10.dll	SUCCESS	Image Base: 0x770...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Image Base: 0x756...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x768...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x759...
14:37:...	Malware_U3_...	1588	Load Image	C:\Windows\SysWOW64\gspc22.dll	SUCCESS	Image Base: 0x767...
Showing 45 of 115.166 events (0.0%)				Backed by virtual memory		

Modifiche del registro dopo il malware(le differenze)

Possiamo notare che il malware aggiunge/interagisce con la chiave di registro HKU (che raggruppa le impostazioni di tutti gli utenti connessi al sistema) e HKLM (include le impostazioni comuni per tutti gli utenti del sistema indipendentemente dalle loro preferenze)

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 13:25:32 , 2024/2/13 13:40:55
Computer: ADMIN-PC , ADMIN-PC
Username: Admin , Admin

-----
Keys added: 72
-----
HKLM\SYSTEM\ControlSet001\services\Malservice
HKLM\SYSTEM\CurrentControlSet\services\Malservice
HKU\S-1-5-21-750839862-2335752535-148538984-1000\software\Micro
HKU\S-1-5-21-750839862-2335752535-148538984-1000\software\Micro
HKU\S-1-5-21-750839862-2335752535-148538984-1000\software\Micro
HKU\S-1-5-21-750839862-2335752535-148538984-1000\software\Micro
HKU\S-1-5-21-750839862-2335752535-148538984-1000\software\Micro
```



```

HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100
HKU\S-1-5-21-750839862-2335752535-148538984-100

```

```

-----
Total changes: 393
-----

```

Provare a profilare il malware in base alla correlazione tra «operation» e Path

In base all'analisi dinamica che abbiamo svolto possiamo intuire che il malware andrà a interagire con la directory system32 di windows la quale contiene elementi eseguibili essenziali per il corretto funzionamento del sistema operativo stesso. Il malware agisce ad esempio sulla libreria *wow64.dll*, che permette esecuzione di applicazioni a 32bit su sistemi a 64bit, con la operation "create file".

```

15:47:00 Malware_U... 156 CreateFile C:\Windows\System32\wow64.dll SUCCESS Desired Access: Read Attributes, Dispo...

```

Un'altra libreria che va ad intaccare ad esempio è quella *userenv.dll* che fornisce funzionalità per la gestione dell'ambiente e delle variabili dell'utente. In particolare, è coinvolta nella gestione dei profili utente e nell'elaborazione delle politiche di gruppo.

```

15:47:00 Malware_U3... 156 C:\Users\Admin\Desktop\MALWARE\MALWARE\Esercizio_Prati... NAME NOT FOUND Desired A
15:47:00 Malware_U12 156 C:\Windows\System32\userenv.dll SUCCESS Desired A

```