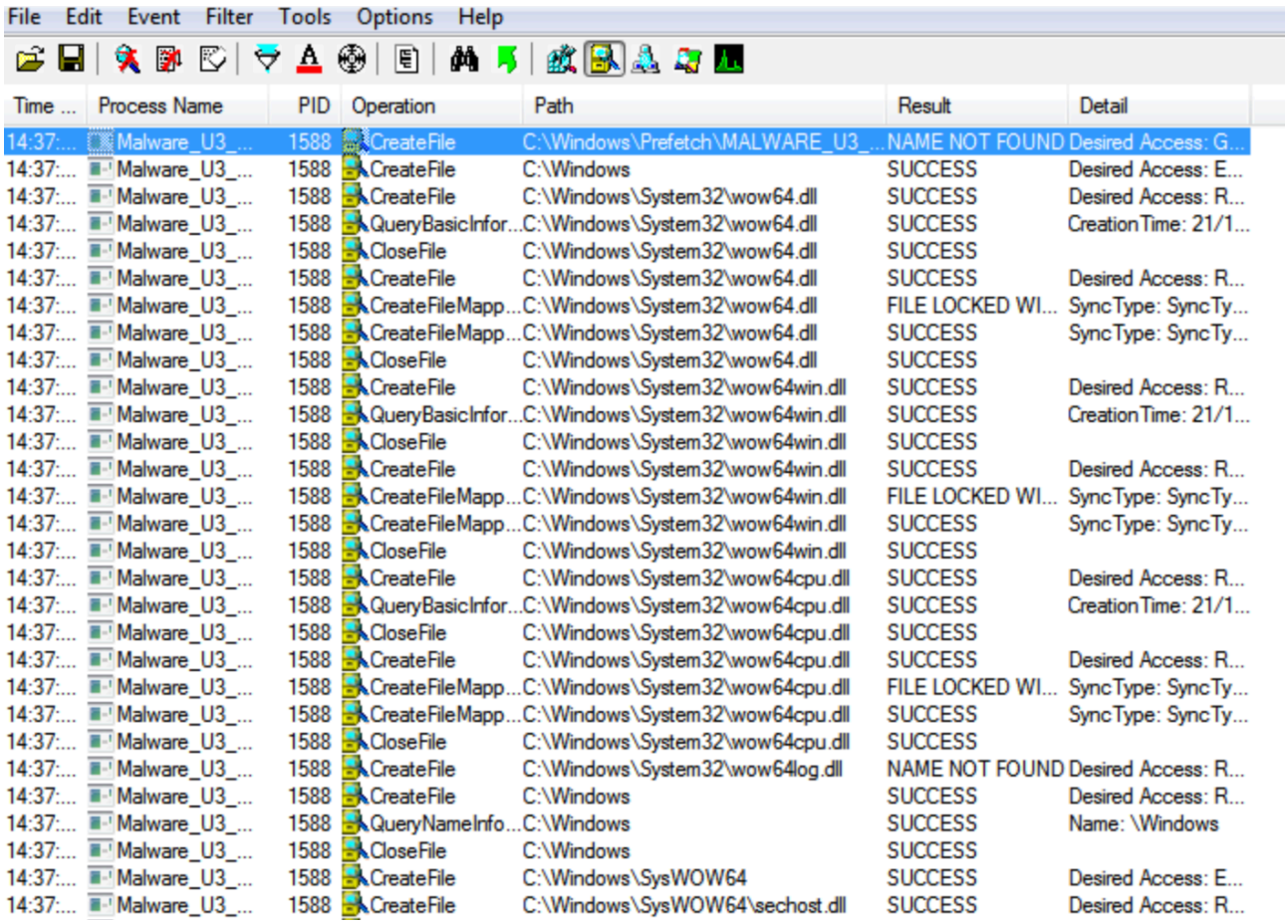
Traccia:

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:

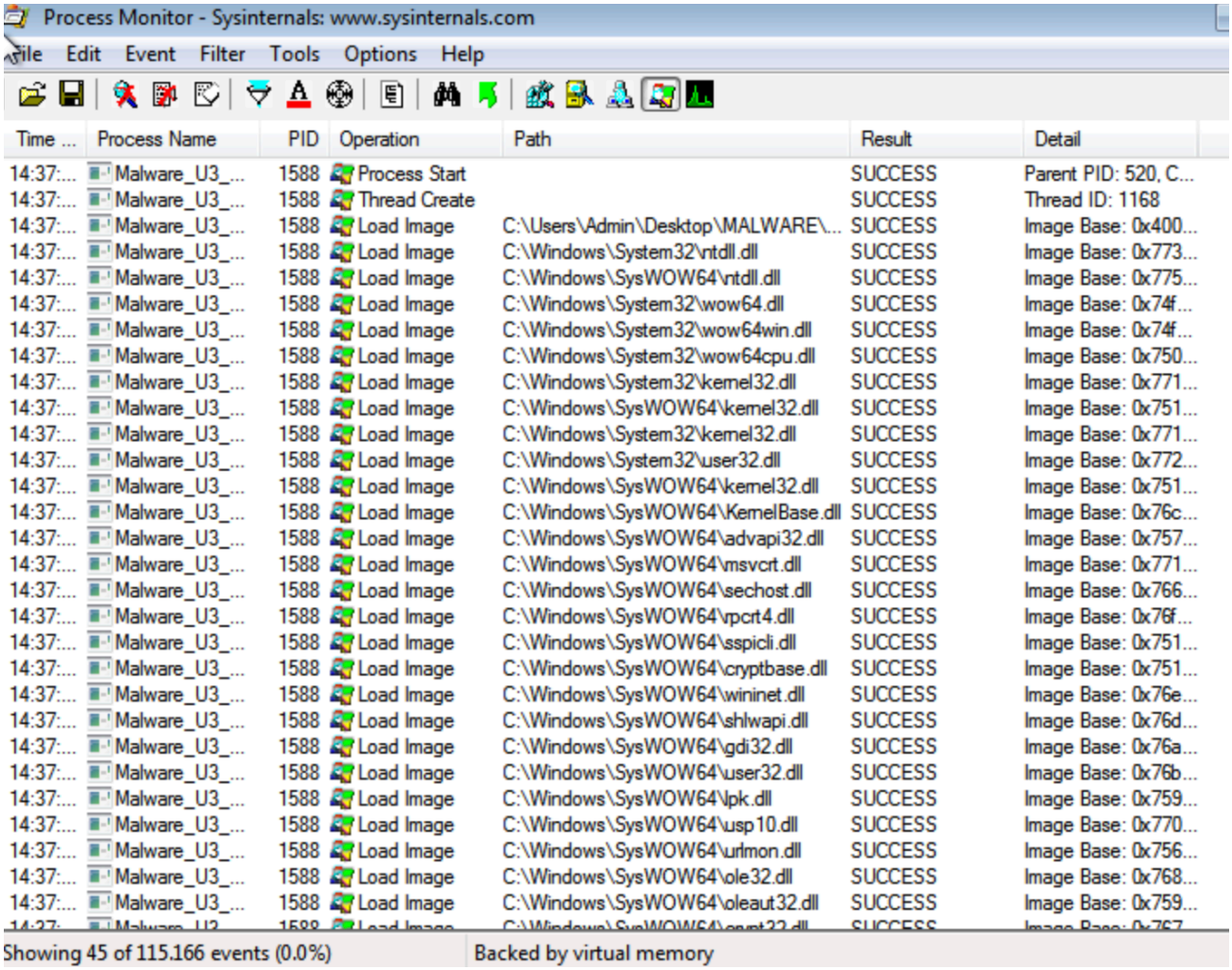
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Modifiche del registro dopo il malware(le differenze)
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

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



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-1-5-21-750839862-2335752535-148538984-100
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
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:...  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:...  Malware_U3_...  156  C:\Users\Admin\Desktop\MALWARE\MALWARE\Esercizio_Prati...  NAME NOT FOUND  Desired A
15:47:...  Malware_U3...   156  C:\Windows\SysWOW64\userenv.dll  SUCCESS  Desired A
```