PRATICA S10/L2

Analisi dinamica basica

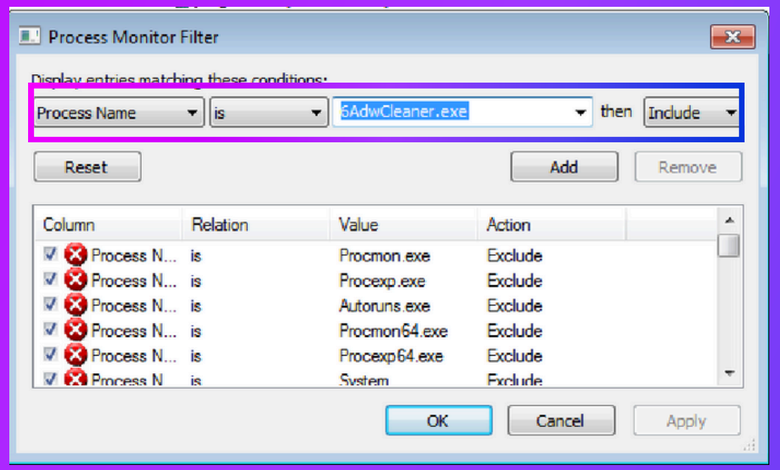
GIULIA FIACCHI

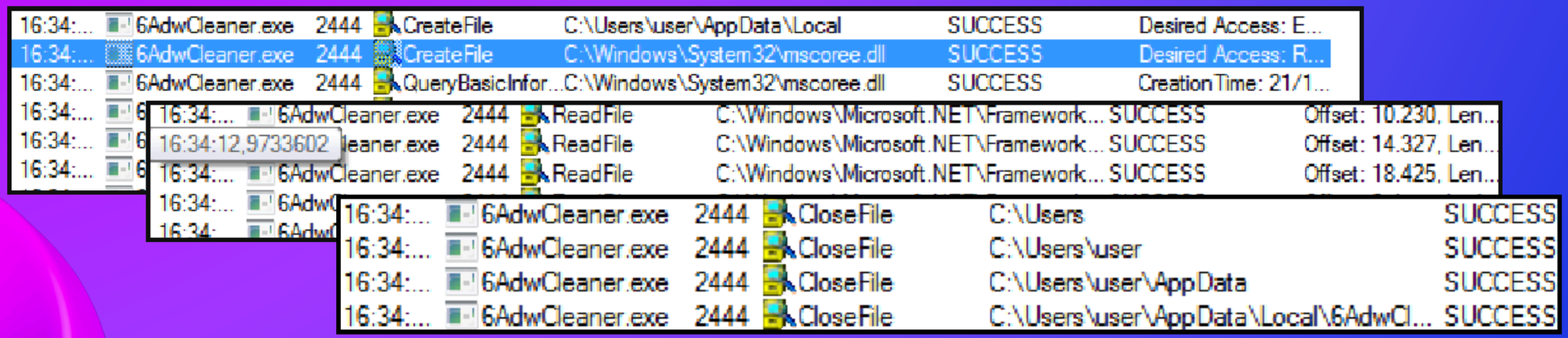
Traccia

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.

Dopo aver reso l'ambiente della macchina sicuro, andando a dis2.attivare le porte USB- impostando la rete su INTERNA - controllato le cartelle condivise, e per ultimo ma non meno importante creato un'istantanea della macchina, poi è stato aperto il tool "**PROCMON"** e avviamo il malware**.**
Poi inseriamo il filtro, guardare immagine. E notiamo che indica che è stato creato un file dalla dicitura **"Create file"** con varie dicitura in cui importava delle librerie come: mscoree.dll - kernel32.dll - kernelbase.dll . Poi anche vari "**read file"** e "**close file".** Tutte indicate con risultato: SUCCESS.





Per il rilevamento dei processi e dei thread è stato utilizzato il software “**Process Explorer**”,

```
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:34:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:35:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:35:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:35:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:35:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:35:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:35:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:36:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:36:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:36:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
16:36:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:37:...  6AdwCleaner.exe  2444  Thread Exit    SUCCESS
16:37:...  6AdwCleaner.exe  2444  Thread Create  SUCCESS
```

svchost.exe		6.444 K	17.540 K	824	Processo host per servizi di ...	Microsoft Corporation
dwm.exe		1.504 K	5.960 K	1976	Gestione finestre desktop	Microsoft Corporation
svchost.exe	8.70	27.636 K	45.068 K	856	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	8.596 K	18.000 K	212	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	27.612 K	30.760 K	896	Processo host per servizi di ...	Microsoft Corporation
spoolsv.exe		6.148 K	11.572 K	1188	Applicazione sottosistema sp...	Microsoft Corporation
taskhost.exe		7.924 K	9.416 K	1220	Processo host per attività di ...	Microsoft Corporation
svchost.exe		11.848 K	14.588 K	1252	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		6.408 K	41.608 K	1388	Processo host per servizi di ...	Microsoft Corporation
sppsvc.exe		7.748 K	13.884 K	1640	Servizio piattaforma protezio...	Microsoft Corporation
SearchIndexer.exe		21.792 K	18.996 K	1912	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		65.076 K	30.196 K	2528	Processo host per servizi di ...	Microsoft Corporation
wmpnetwk.exe	< 0.01	11.576 K	7.552 K	2424	Servizio di condivisione in ret...	Microsoft Corporation
svchost.exe		4.808 K	12.136 K	3872	Processo host per servizi di ...	Microsoft Corporation
lsass.exe		4.216 K	11.824 K	460	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2.296 K	4.392 K	468		
csrss.exe	1.45	2.032 K	6.488 K	364		
winlogon.exe		2.636 K	6.828 K	392		
explorer.exe	< 0.01	44.060 K	61.756 K	2000	Esplora risorse	Microsoft Corporation
VBoxTray.exe	< 0.01	2.104 K	7.916 K	872	VirtualBox Guest Additions Tr...	Oracle Corporation
Procmon.exe		3.640 K	10.412 K	3000	Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	< 0.01	39.716 K	44.324 K	3596		
procexp.exe		4.092 K	8.908 K	2404	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	8.70	19.868 K	37.260 K	2560	Sysinternals Process Explorer	Sysinternals - www.sysinter...
MpCmdRun.exe	< 0.01	3.364 K	7.736 K	1416		
6AdwCleaner.exe	< 0.01	34.000 K	31.648 K	2636	AdwareBooC	