

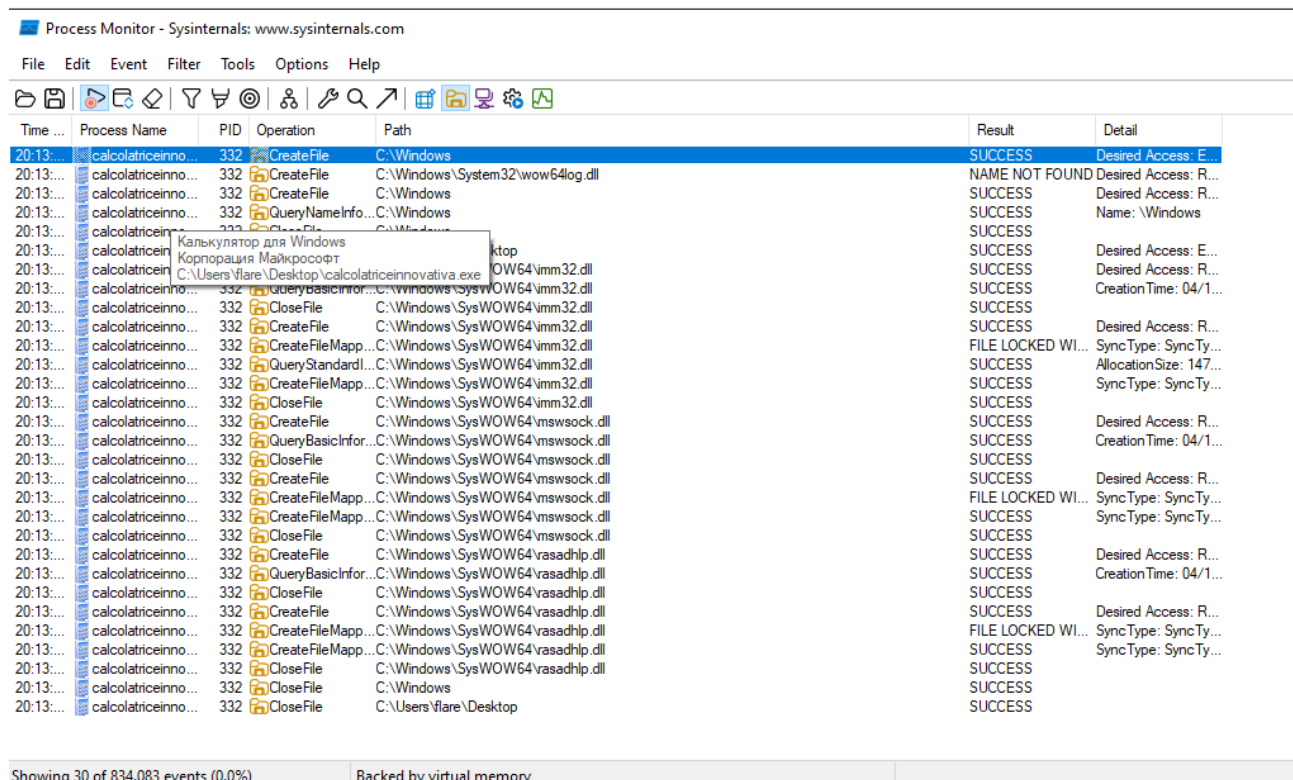
M6 - Consegna week 22 day 1 - Daniele Rufo

Analisi dinamica di base con Procmon

Dopo essermi assicurato che la mia sandbox (in questo caso una FlareVM montata su base windows10) fosse configurata correttamente, quindi isolata completamente dal sistema host e senza alcun accesso a internet, ho eseguito prima il Procmon e poi l'eseguibile `calcolatriceinnovativa.exe` per studiarne il comportamento.

In particolare l'esercizio richiedeva:

1 - Azioni sul file system



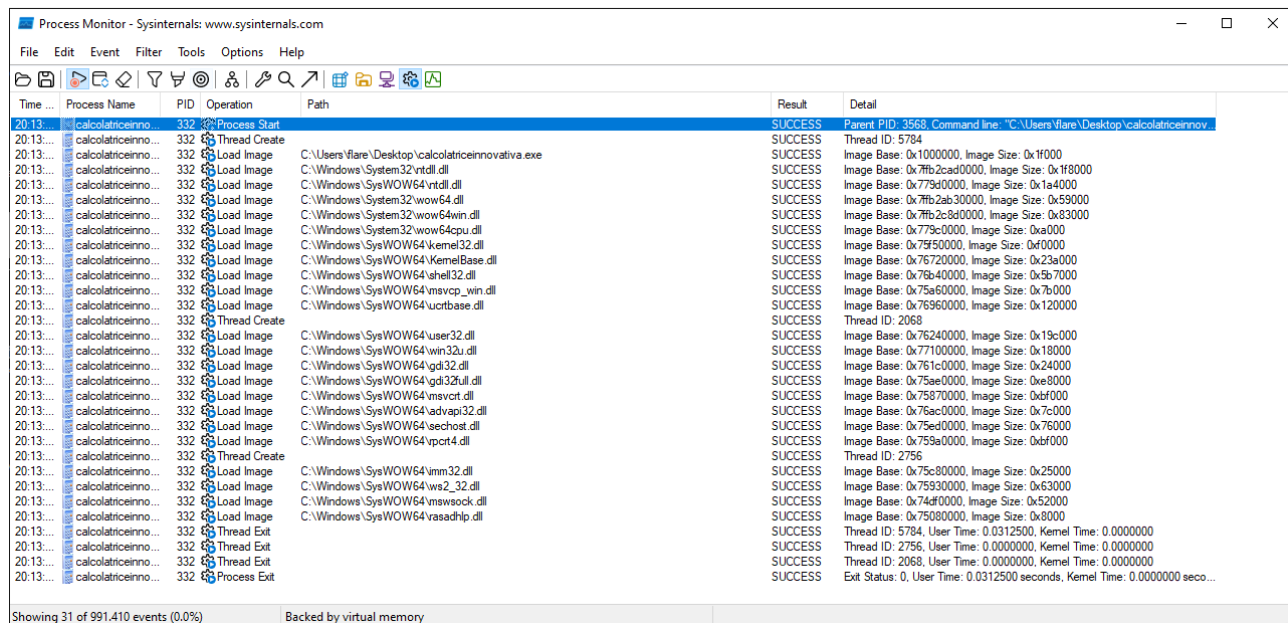
Time ...	Process Name	PID	Operation	Path	Result	Detail
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows	SUCCESS	
20:13:...	calcolatriceinnova...	332	QueryBasicInfo...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: E...
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	CreateFileMapping...	C:\Windows\System32\wow64\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
20:13:...	calcolatriceinnova...	332	QueryStandardI...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	AllocationSize: 147...
20:13:...	calcolatriceinnova...	332	CreateFileMapping...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	QueryBasicInfo...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	CreationTime: 04/1...
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	CreateFileMapping...	C:\Windows\System32\wow64\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
20:13:...	calcolatriceinnova...	332	CreateFileMapping...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	QueryBasicInfo...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	CreationTime: 04/1...
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	
20:13:...	calcolatriceinnova...	332	CreateFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	Desired Access: R...
20:13:...	calcolatriceinnova...	332	CreateFileMapping...	C:\Windows\System32\wow64\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
20:13:...	calcolatriceinnova...	332	CreateFileMapping...	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows\System32\wow64\wow64cpu.dll	SUCCESS	
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Windows	SUCCESS	
20:13:...	calcolatriceinnova...	332	CloseFile	C:\Users\flare\Desktop	SUCCESS	

Showing 30 of 834,083 events (0.0%) Backed by virtual memory

Ecco le operazioni inerenti al file system catturate con Procmon che il malware compie:

- tenta di aprire o creare file nelle cartelle di sistema “system32” e “SysWOW64”
- interroga il sistema sulle cartelle e file presenti in “C:\Windows” tramite *QueryNameInfo*
- sembra che usi diversi moduli DLL (dynamic link libraries) per interagire con il sistema. Ho notato che il malware lavora anche con il modulo per gestire le winsock, cioè le API fornite da Microsoft per interagire con la rete, e questo fa pensare a possibili attività e manipolazioni legate all'utilizzo delle connessioni di rete
- esegue “FileMapping”, che è una tecnica usata per modificare file senza doverli aprire direttamente su disco. In questo modo, il malware può iniettare codice nel file senza destare sospetti immediati.

2 - Azioni su processi e thread



Time ...	Process Name	PID	Operation	Path	Result	Detail
20:13:...	calcolatriceinnov...	332	Process Start		SUCCESS	Parent PID: 3568, Command line: "C:\Users\flare\Desktop\calcolatriceinnov...
20:13:...	calcolatriceinnov...	332	Thread Create		SUCCESS	Thread ID: 5784
20:13:...	calcolatriceinnov...	332	Load Image	C:\Users\flare\Desktop\calcolatriceinnovativa.exe	SUCCESS	Image Base: 0x1000000, Image Size: 0x1f000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77b2cad0000, Image Size: 0x1f8000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779d00000, Image Size: 0x1a4000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x77b2ab30000, Image Size: 0x59000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x77b2c8d0000, Image Size: 0x83000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x779c00000, Image Size: 0xa000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x79f500000, Image Size: 0xf0000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\kernelbase.dll	SUCCESS	Image Base: 0x767200000, Image Size: 0x23a000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x7b8400000, Image Size: 0x5b7000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x75a600000, Image Size: 0x7b000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x769600000, Image Size: 0x120000
20:13:...	calcolatriceinnov...	332	Thread Create		SUCCESS	Thread ID: 2068
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x762400000, Image Size: 0x19c000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\win32u.dll	SUCCESS	Image Base: 0x771000000, Image Size: 0x18000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x761c00000, Image Size: 0x24000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x75ae00000, Image Size: 0xe8000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x758700000, Image Size: 0xbf000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x76ac00000, Image Size: 0x7c000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x75ed00000, Image Size: 0x76000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\pcre.dll	SUCCESS	Image Base: 0x759a00000, Image Size: 0xbf000
20:13:...	calcolatriceinnov...	332	Thread Create		SUCCESS	Thread ID: 2756
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x75c800000, Image Size: 0x25000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x759300000, Image Size: 0x63000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x74df00000, Image Size: 0x52000
20:13:...	calcolatriceinnov...	332	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x750800000, Image Size: 0x8000
20:13:...	calcolatriceinnov...	332	Thread Exit		SUCCESS	Thread ID: 5784, User Time: 0.0312500, Kernel Time: 0.0000000
20:13:...	calcolatriceinnov...	332	Thread Exit		SUCCESS	Thread ID: 2756, User Time: 0.0000000, Kernel Time: 0.0000000
20:13:...	calcolatriceinnov...	332	Thread Exit		SUCCESS	Thread ID: 2068, User Time: 0.0000000, Kernel Time: 0.0000000
20:13:...	calcolatriceinnov...	332	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0312500 seconds, Kernel Time: 0.0000000 seco...

Showing 31 of 991,410 events (0.0%) Backed by virtual memory

Paasiamo ora alle operazioni inerenti ai processi ed ai thread catturate con Procmon che il malware compie:

- “LoadImage” fa riferimento al caricamento di librerie DLL, confermata anche dall’analisi precedente.
- Crea più thread, in questo caso ne vedo 3, per distribuire il carico di lavoro ed eseguire processi paralleli
- Chiusura di tutti i thread creati abbastanza celere. Probabilmente ci fa pensare che voglia fare meno rumore possibile per passare inosservato

Conclusione

In definitiva questa analisi ci ha permesso di confermare delle evidenze rilevate durante la fase di analisi statica. Inoltre ora abbiamo un’idea più chiara di cosa potrebbe fare il malware:

- ➔ iniettare codice malevolo undetected grazie al “FileMapping”
- ➔ manipolare le connessioni di rete o il traffico grazie all’utilizzo delle API winsock. L’analisi malware dal punto di vista networking è ancora priva di info, ciò può suggerire che le azioni compiute ora servono per attacchi futuri e non usano le funzionalità di rete del malware in questo momento. Vengono solamente predisposte
- ➔ modifiche al sistema operativo (probabilmente relative a configurazioni) nelle cartelle “System32” e “SysWOW64”
- ➔ stabilire una persistenza tramite le chiavi di registro di Windows