

MALWARE ANALYSIS I DINAMICA BASICA

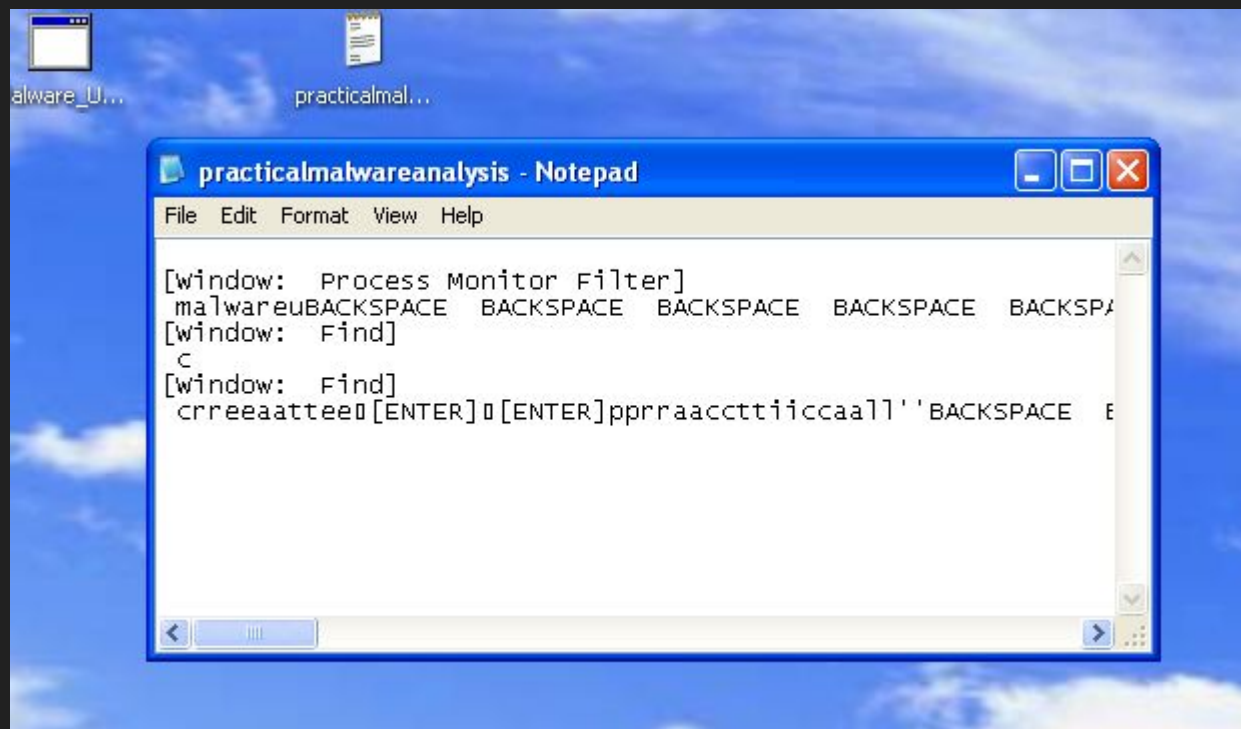
S10 - L2

| | | | | | | |
|------------------|----------------------|------|----------------|--|---------------|--|
| 2.32.44.31539... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\ | NO MORE FILES | |
| 2.32.44.31543... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\ | SUCCESS | |
| 2.32.44.31599... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\DOCUMENTS AND SETTINGS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31601... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService |
| 2.32.44.31645... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings | NO MORE FILES | |
| 2.32.44.31649... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\Documents and Settings | SUCCESS | |
| 2.32.44.31656... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\Documents and Settings\Administrator | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31711... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31716... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator | NO MORE FILES | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31720... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\Documents and Settings\Administrator | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31829... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\Documents and Settings\Administrator\Desktop | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31835... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31851... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop | NO MORE FILES | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31864... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\Documents and Settings\Administrator\Desktop | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31873... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31883... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31891... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | NO MORE FILES | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31898... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31911... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\WINDOWS | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31917... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31955... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS | NO MORE FILES | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31962... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\WINDOWS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31975... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\WINDOWS\AppPatch | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.31987... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS\AppPatch | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.31999... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS\AppPatch | NO MORE FILES | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.32009... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\WINDOWS\AppPatch | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.32025... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\WINDOWS\System32 | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.32033... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS\System32 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute |
| 2.32.44.32067... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS\System32 | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |
| 2.32.44.32091... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\WINDOWS\System32 | SUCCESS | 0. ...; 1. ...; FileInformationClass: FileNamesInformation, 3: Cookie, 4: All Users, 5: LocalService, 6: NetworkService |

| | | | | | |
|------------------|----------------------|------|----------------|--|---------|
| 2.32.44.31864... | Malware_U3_W2_L2.exe | 3180 | CloseFile | C:\Documents and Settings\Administrator\Desktop | SUCCESS |
| 2.32.44.31873... | Malware_U3_W2_L2.exe | 3180 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS |
| 2.32.44.31883... | Malware_U3_W2_L2.exe | 3180 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS |

Come possiamo vedere all'interno di procmod, dopo aver eseguito il file "Malware_U3_W2_L2", questo malware ha fatto parecchie cose alla nostra VM. Uno di questi è creare un file .txt nella directory in cui si trova il programma.

Infatti, possiamo vedere un nuovo file nella stessa directory del programma (Desktop). Aprendo il nuovo file denominato "practicalmalwareanalysis" possiamo vedere che sembra essere un file con il contenuto di un keylogger, che verrà sicuramente inviato a un utente malintenzionato.



Malware Analysis | Analisi dinamica basica

S10 - L2

| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|------------------|----------------------|------|----------------|--|---------|--|
| 10:22:02.5709... | Malware_U3_W2_L2.exe | 3500 | Process Start | | SUCCESS | Parent PID: 388, Command line: "C:\Documents and Settings\Admini... |
| 10:22:02.5709... | Malware_U3_W2_L2.exe | 3500 | Thread Create | | SUCCESS | Thread ID: 3504 |
| 10:22:02.5716... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\Documents and Settings\Administrator\Desktop\Malware_U3_W2_L2.exe | SUCCESS | Image Base: 0x400000, Image Size: 0xd000 |
| 10:22:02.5718... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\ntdll.dll | SUCCESS | Image Base: 0x7c900000, Image Size: 0xaf000 |
| 10:22:02.5718... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\kernel32.dll | SUCCESS | Image Base: 0x7c800000, Image Size: 0xf6000 |
| 10:22:02.6000... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Image Base: 0x77b40000, Image Size: 0x22000 |
| 10:22:02.6050... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\version.dll | SUCCESS | Image Base: 0x77c00000, Image Size: 0x8000 |
| 10:22:02.6106... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\advapi32.dll | SUCCESS | Image Base: 0x77dd0000, Image Size: 0x9b000 |
| 10:22:02.6109... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\iprt4.dll | SUCCESS | Image Base: 0x77e70000, Image Size: 0x92000 |
| 10:22:02.6113... | Malware_U3_W2_L2.exe | 3500 | Load Image | C:\WINDOWS\system32\securl32.dll | SUCCESS | Image Base: 0x77fe0000, Image Size: 0x11000 |
| 10:22:02.6165... | Malware_U3_W2_L2.exe | 3500 | Process Create | C:\WINDOWS\system32\svchost.exe | SUCCESS | PID: 3508, Command line: "C:\WINDOWS\system32\svchost.exe" |
| 10:22:03.6077... | Malware_U3_W2_L2.exe | 3500 | Thread Exit | | SUCCESS | Thread ID: 3504, User Time: 0.0000000, Kernel Time: 0.0312500 |
| 10:22:03.6092... | Malware_U3_W2_L2.exe | 3500 | Process Exit | | SUCCESS | Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0312500 |

Andando nella parte superiore dell'interfaccia utente di Procmon, possiamo filtrare per "thread e processi". Una volta filtrato, troviamo azioni interessanti, come Load Image che serve per "caricare" l'esecuzione del malware e la libreria necessaria (.dll), e possiamo vedere "Process Create" che serve per creare un processo, in questo caso un processo chiamato svchost.exe, un processo Windows integrale. Questo ci dice che il malware sta cercando di nascondersi, prendendo il nome di un processo legittimo invece che di uno evidentemente allarmante.

Sembra che quando il programma viene avviato, richiama alle librerie necessarie di maniera runtime, poi crea un servizio con nome falso, un servizio che potrebbe essere il keylogger visto previamente. Questo keylogger sicuramente andrà inviato ad un utente malintenzionato.