MALWARE ANALYSIS I DINAMICA BASICA

S10 - L2

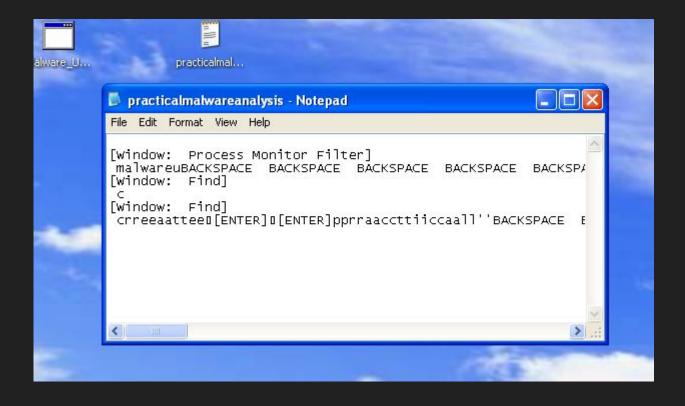
Malware Analysis | Analisi dinamica basica \$10 - L2

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 Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe 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	0: .
2:32:44.31656	Malware_U3_W2_L2.exe	3180 ScreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Dispos
2:32:44.31711	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	D: ., 1: FileInformationClass: FileNamesInformation, 3: Cookies 3: All Users 7: My Documents, 8: NetHood, 9: NTUS
2:32:44.31716	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	4 Default User
2:32:44.31720	Malware_U3_W2_L2.exe	3180 CloseFile	C:\Documents and Settings\Administrator	SUCCESS	5: LocalService
2:32:44.31829	Malware_U3_W2_L2.exe	3180 CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Dispos 6: NetworkService ID Non-Alert, Open For Backup, Attribute
2:32:44.31835	Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	 "1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer.Ink, 4: Command Prompt Ink, 5: Esercizi, 6: Esercizio_Pratico_U3_W2_L1, 7: Es
2:32:44.31851	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
2:32:44.31864	Malware_U3_W2_L2.exe	3180 CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
	Malware_U3_W2_L2 exe	3180 CreateFile	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
2:32:44.31883	Malware_U3_W2_L2.exe	3180 QueryOirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0:, 1:, FileInformationClass: FileNamesInformation
2:32:44.31891	Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
2:32:44.31898	Malware_U3_W2_L2.exe	3180 CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31911	Malware_U3_W2_L2.exe	3180 🖳 CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31917	Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16.bmp, 8: bootstat.dat, 9: clock.avi,
2:32:44.31955	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\WINDOWS	NO MORE FILES	
2:32:44.31962	Malware_U3_W2_L2.exe	3180 CloseFile	C:\WINDOWS	SUCCESS	
2:32:44.31975	Malware_U3_W2_L2.exe	3180 CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.31987	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua.dll, 6: AcSpectc.dll, 7: AcVanal dll, 8: apphelp.sdb, 9: a
2:32:44.31999	Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe	3180 A QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
2:32:44.32009	Malware_U3_W2_L2.exe	3180 A CloseFile	C:\WINDOWS\AppPatch	SUCCESS	
2:32:44.32025	Malware_U3_W2_L2.exe	3180 CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attribute
2:32:44.32033	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\WINDOWS\system32	SUCCESS	 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 12520437.cj
2:32:44.32067	Malware_U3_W2_L2.exe	3180 QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: eapsvc.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edin.exe, 4: efsadu.dll, 5: ega.cpi, 6: els.dll, 7: emptyregdb.dat, 8: en, 9: en-L
2:32:44.32091	Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe	3180 A QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: more.com, 1: moricons.dll, FileInformationClass: FileNamesInformation, 3: mouse.drv, 4: mp43dmod.dll, 5: mp4sdmod.dll, 6: mpeg2data.ax, 7: mpg2s

		at a second or a s	
2:32:44.31864 Malware_U3_W2_L2.exe		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 RueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2.22 H 21001 - H 1 112 M 2 12	2100 G O D I	ere a reministration in the state of the second	NO HODE CILCO

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 "practicalmalwarea nalysis" 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 \$10 - L2

	A4 🦻 🎎 🗟 🚉 💹			
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\Admi
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
10:22:02:5918 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\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
10:22:02.6113 Malware_U3_W2_L2.exe	3500 🥰 Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
10:22:02.6165 Malware_U3_W2_L2.exe	3500 Rrocess 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: 0.0312

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 manera runtime, poi crea un servizio con nome falso, un servizio che potrebbe essere il keylogger visto previamente. Questo keylogger sicuramente andrá inviato ad un utente malintenzionato.